CONSILIUL NAŢIONAL DE SOLUŢIONARE A CONTESTAŢIILOR
C. N. S. C.
Str. Stavropoleos nr. 6, sector 3, Bucureşti, cod poştal 030084, România
Tel: +4 021.310.46.41 Fax: +4 021.890.07.45 şi +4 021.310.46.42 www.cnsc.ro

În conformitate cu prevederile art. 266 alin. (2) din OUG nr. 34/2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, aprobată prin Legea nr. 337/2006,cu modificările şi completările ulterioare, Consiliul adoptă următoarea

DECIZIE
Nr. ..../.../..., ...
Data: ....

Prin contestaţia nr. T/.../..., înregistrată la Consiliul Naţional de Soluţionare a Contestaţiilor sub nr. .../..., depusă de către ..., cu sediul în ..., având număr de înregistrare la Oficiul Registrului Comerţului ... şi Cod Unic de Înregistrare ..., formulată împotriva adresei nr. 13760/16.03.2015 reprezentând comunicarea rezultatului procedurii de atribuire, emisă de către ..., în calitate de autoritate contractantă, cu sediul în ..., în cadrul procedurii de „licitaţie deschisă”, pentru atribuirea contractului de achiziţie publică de servicii, având ca obiect „Servicii de arhivare fizică şi servicii de arhivare electronică a documentelor elaborate/gestionate în cadrul ...”, s-a solicitat:
- anularea raportului procedurii de atribuire, a adresei nr. 13760/16.03.2015 privind comunicarea rezultatului procedurii de atribuire, precum şi a tuturor actelor subsecvente acestora,
- obligarea autorităţii contractante la continuarea procedurii în vederea atribuirii contractului prin reevaluarea ofertei depuse de ..., a ofertei depuse de asocierea formată din ....

Prin contestaţia nr. T/.../..., înregistrată la Consiliul Naţional de Soluţionare a Contestaţiilor sub nr. .../..., depusă de către ..., cu sediul în ..., având număr de înregistrare la Oficiul Registrului Comerţului ... şi Cod Unic de Înregistrare ..., formulată împotriva raportului procedurii de atribuire, emis de către ..., în calitate de autoritate contractantă, cu sediul în ..., în cadrul procedurii de atribuire antemenţionată, s-a solicitat:
- anularea tuturor actelor emise de către autoritatea contractantă, acte prin care s-a stabilit ca fiind câştigătoare oferta depusă de Asocierea formată din ..., pentru motive de netemeinicie şi nelegalitate, incluzând raportul procedurii de atribuire şi toate actele subsecvente acestuia, inclusiv toate adresele de comunicare a rezultatului procedurii,
- obligarea autorităţii contractante la reluarea procedurii de atribuire, prin reevaluarea ofertelor şi stabilirea ofertei câştigătoare cu respectarea prevederilor legale în materia achiziţiilor publice,

- în subsidiar, în măsura în care nu pot fi dispuse măsuri de remediere, obligarea autorităţii contractante la anularea procedurii de atribuire.

Prin adresa nr. .../..., înregistrată la Consiliu sub nr..../..., ce reprezintă „cerere de intervenţie" formulată de ... cu sediul în ..., reprezentată convenţional de ... având sediul în ..., având număr de înregistrare la Oficiul Registrului Comerţului ... şi Cod Unic de Înregistrare ..., lider al Asocierii ..., în calitate de câştigătoare a procedurii de „licitaţie deschisă" organizată de ... în vederea atribuirii contractului de achiziţie publică de servicii, având ca obiect „Servicii de arhivare fizică şi servicii de arhivare electronică a documentelor elaborate/gestionate în cadrul ..." în care solicită respingerea ca nefondată a contestaţiei, cu consecinţa menţinerii rezultatului procedurii prin care oferta ... a fost declarată câştigătoare.

Prin adresa nr. .../..., înregistrată la Consiliu sub nr.../..., ce reprezintă „cerere de intervenţie" formulată de ... cu sediul în ..., reprezentată convenţional de ... având sediul în ..., având număr de înregistrare la Oficiul Registrului Comerţului ... şi Cod Unic de Înregistrare ..., lider al Asocierii ..., în calitate de câştigătoare a procedurii de „licitaţie deschisă" organizată de ... în vederea atribuirii contractului de achiziţie publică de servicii, având ca obiect „Servicii de arhivare fizică şi servicii de arhivare electronică a documentelor elaborate/gestionate în cadrul ..." în care solicită respingerea ca tardiv formulată şi ca fiind lipsită de interes contestaţia, în principal, iar în subsidiar, ca nefondată, cu consecinţa menţinerii rezultatului procedurii prin care oferta ... a fost declarată câştigătoare, iar oferta ... neconformă în temeiul art. 36 alin. (2) lit. a) din HG nr. 925/2006.

În baza legii şi a documentelor depuse de părţi,
CONSILIUL NAŢIONAL DE SOLUŢIONARE A CONTESTAŢIILOR

DECIDE:

În temeiul art. 278 alin. (2) şi (4) din OUG nr. 34/2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, cu modificările şi completările ulterioare, admite în parte contestaţia nr. T/.../... formulată de ..., în contradictoriu cu ... şi dispune reevaluarea ofertei asocierii ...

În temeiul art. 278 alin. (5) din OUG nr. 34/2006, respinge ca nefondată contestaţia în partea dedicată reevaluării ofertei proprii.

În temeiul art. 65 alin. (1) şi art. 67 din Codul de procedură civilă, admite cererea de intervenţie accesorie nr. .../..., înregistrată la Consiliu sub nr..../..., formulată de ... în calitate de lider al asocierii ..., în partea privitoare la neconformitatea ofertei contestatoarei. În temeiul art. 278 alin. (5) din ordonanţa de urgenţă menţionată, respinge ca nefondată cererea respectivă în partea referitoare la solicitarea contestatoarei de reevaluare a ofertei sale.

În temeiul art. 278 alin. (5) din OUG nr. 34/2006, respinge ca

tardiv introdusă contestaţia nr. T/1179/20.04.2015, înregistrată la Consiliul Naţional de Soluţionare a Contestaţiilor sub nr. 6190/20.04.2015, depusă de către ....

În temeiul art. 65 alin. (1) şi art. 67 din Codul de procedură civilă, admite cererea de intervenţie nr. .../..., înregistrată la Consiliu sub nr. .../..., formulată de către ... în calitate de lider al asocierii ....

În temeiul art. 65 alin. (1) şi art. 67 din Codul de procedură civilă, va admite cererea de intervenţie accesorie formulată de ... în calitate de lider al asocierii ..., în partea privitoare la neconformitatea ofertei contestatoarei. În temeiul art. 278 alin. (5) din ordonanţa de urgenţă menţionată, va respinge ca nefondată cererea respectivă în partea referitoare la reevaluarea ofertei sale.

Prezenta decizie este obligatorie pentru părţi, în conformitate cu dispoziţiile art. 280 alin. (1) şi (3) din Ordonanţa de urgenţă a Guvernului nr. 34/2006.

Împotriva prezentei decizii se poate formula plângere în termen de 10 zile de la comunicare.

Măsurile dispuse vor fi aduse la îndeplinire într-un termen de maximum 15 zile de la comunicarea prezentei.

MOTIVARE

În luarea deciziei s-au avut în vedere următoarele:

Prin contestaţia nr. T/.../..., înregistrată la Consiliul Naţional de Soluţionare a Contestaţiilor sub nr. .../..., ..., în calitate de operator economic participant la procedura de licitaţie deschisă indicată mai sus, organizată de ..., critică rezultatul procedurii de atribuire prin care oferta sa a fost respinsă ca neconformă, câştigătoare fiind oferta depusă de asocierea ...

În fapt, contestatoarea menţionează că potrivit anunţului de participare şi fişei de date, scopul proiectului îl constituie crearea unui sistem de arhivă electronică care să gestioneze documentele aparţinând Ministerului, convertite de pe suport hârtie în varianta electronică, prin serviciile solicitate în prezentul proiect. Contractul nu este împărţit în loturi. Valoarea estimată a contractului, fără TVA, este de 28.830.000 RON, iar durata contractului este de 12 luni de la data atribuirii acestuia/emiterii ordinelor de începere a serviciilor.

De asemenea, este menţionat faptul că prezenta procedură a fost deja marcată de un număr semnificativ de nereguli, atât anterior depunerii ofertelor, cât şi ulterior acestei date. Acest aspect este cu atât mai grav cu cât prezentul proiect este finanţat prin fonduri europene nerambursabile în cadrul Programului Operaţional Asistenţă Tehnică. Astfel, tocmai ministerul responsabil de aceste fonduri europene şi anume ..., în calitatea sa de autoritate contractantă în acest proiect, pune în mod serios sub semnul întrebării corectitudinea utilizării fondurilor europene.

Astfel, până la data depunerii ofertelor, au fost înregistrate 9 contestaţii în cadrul acestei proceduri, cele mai multe dintre acestea vizând aspecte de îngrădire a concurenţei. Printre contestatoare s-a

numărat şi ..., contestaţia sa asupra documentaţiei de atribuire şi asupra răspunsurilor la întrebările de clarificăre vizând cerinţele de securitate ale sistemului informatic.

Astfel, contestatoarea susţine că a atras atenţia la rândul său în aceste contestaţii că respectivele cerinţe sunt limitative şi îngrădesc concurenţa, prin faptul că singura soluţie care putea răspunde acestor cerinţe nu poate fi decât cea furnizată de operatorul economic .... Restricţionarea competiţiei prin favorizarea acestui operator economic a fost de altfel reţinută chiar de către Consiliu, care prin Decizia nr. .../.../..., ..., ..., ..., ..., .../... a dispus eliminarea cerinţelor restrictive ale documentaţiei de atribuire. În urma acestei decizii, caietul de sarcini a fost amendat prin Modificarea nr. 8, emisă în data de 17.06.2014. Deşi Consiliul a recomandat renunţarea la capitolul legat de securitatea sistemului, iar ... a reformulat cele mai multe din aceste cerinţe, totuşi esenţa restrictivă a acestora a fost păstrată, astfel că doar două oferte au fost depuse în cadrul procedurii, respectiv:

- Asocierea formată din ...;
- ....

De asemenea, ulterior deschiderii ofertelor, la data de 23.02.2015, urmare a unei noi contestaţii depuse de ..., Consiliul a emis Decizia nr. .../.../.../..., prin care a reţinut că cerinţa de prezentare a sesiunii demonstrative inclusă în caietul de sarcini aferent acestei proceduri este clauză nescrisă în înţelesul dispoziţiilor art. 33 alin. (3) din OUG nr. 34/2006; excesivă faţă de regula instituită prin pct. IV.4.1) "Modul de prezentare a propunerii tehnice" al fişei de date conform cărora "Ofertantul trebuie să justifice acoperirea cerinţelor prin prezentarea de: capturi de ecrane şi descriere funcţională explicită pe fluxuri de lucru"); solicitarea autorităţii contractante de repetare a respectivei sesiuni motivată doar prin invocarea faptului că, în cazul înlocuirii unui membru ai comisiei de evaluare, „toţi membrii cu drept de vot ai comisiei să poată participă la toate etapele necesare evaluării ofertelor", considerent contrar dispoziţiilor art. 72 alin. (4) teza a II-a din HG nr. 925/2006; expertul tehnic cooptat participant la sesiunea demonstrativă a rămas neschimbat, precum şi faptul că la dosar nu se regăseşte niciun act de natura "raportului de specialitate cu privire la aspectele tehnice", prin care să se revendice vreo eventuală necesitate de reluare a sesiunii demonstrative.

Aşa fiind, Consiliul a constatat că cererea ... de anulare a adreselor autorităţii contractante nr. .../DAPITA 2486/02.02.2015, nr. .../DAPITA 2753/04.02.2015 şi nr. .../DAPITA 3203/10.02.2015, precum şi a actelor subsecvente acestora este întemeiată. Consiliul a stabilit că, în eventualitatea în care comisia de evaluare nu este pe deplin edificată asupra conformităţii ofertelor cu cerinţele şi specificaţiile caietului de sarcini, aceasta are la dispoziţie procedura reglementată de art. 78 din HG nr. 925/2006, respectiv, de stabilire a clarificărilor şi completărilor formale sau de confirmare necesare pentru evaluarea fiecărei oferte, pe care le va formula clar, precis şi prin care se va defini în mod explicit şi suficient de detaliat în ce constau solicitările comisiei de evaluare, în

strictă corelare cu conţinutul precizărilor şi regulilor documentaţiei de atribuire.

Faţă de cele constatate, Consiliul a dispus anularea adreselor atacate ale autorităţii contractante, pe care a obligat-o să continue şi să finalizeze procedura de atribuire cu respectarea dispoziţiilor legale în materie în vigoare şi cu aplicarea regulilor documentaţiei de atribuire.

Decizia Consiliului fiind obligatorie, potrivit dispoziţiilor art. 280 alin. (3) din OUG nr. 34/2006, autoritatea contractantă a procedat la transmiterea către ... a unui set de întrebări de clarificare, cu adresa nr. .../DAPITA/4498/03.03.2015, la care aceasta din urmă susţine că a răspuns prin adresa înregistrată cu nr. .../DAPITA/4598/06.03.2015. Contestatoarea precizează că mai primise anterior în cadrul procesului de evaluare un set de întrebări de clarificare, şi anume cu adresa nr. .../DAPITA/3597/14.10.2014, la care a răspuns prin adresa înregistrată cu nr. .../DAPITA /3696/20.10.2014.

În urma primirii răspunsurilor la solicitările de clarificare, prin dresa nr. 13760/16.03.2015 privind Comunicarea rezultatului procedurii de atribuire, (denumită în continuare şi „Comunicarea rezultatului procedurii"), autoritatea contractantă a considerat ca oferta ... nu respectă cerinţele minime ale caietului de sarcini şi a procedat la respingerea acesteia ca „neconformă" în temeiul art. 36 alin. (2) lit. a) din H.G. nr.925/2006.

De asemenea, prin aceeaşi comunicare a rezultatului procedurii, contestatoarea susţine că a fost informată că oferta Asocierii ... a fost declarată câştigătoare.

În ceea ce priveşte respingerea ofertei sale ca fiind nelegală, contestatoarea menţionează următoarele:

Motivul 1: autoritatea contractantă consideră că oferta ... nu îndeplineşte cerinţa enunţată la cap. 3.3.7 din caietul de sarcini, respectiv: „Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificate din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional".

Această cerinţă a fost introdusă în caietul de sarcini prin Modificarea nr. 8, emisă în data de 17.06.2014 în urma Deciziei Consiliului nr. ..../..../..., ..., ..., ..., ..., .../....

Contestatoarea afirmă că potrivit autorităţii contractante, nerespectarea cerinţei menţionate rezultă atât din oferta tehnică depusă ..., dar şi din răspunsurile de clarificare oferite de aceasta. Toate argumentele autorităţii în opinia contestatoarei fiind false, acestea nereprezentând altceva decât o interpretare distorsionată, vădit răuvoitoare, atât a conţinutului ofertei, cât şi a clarificărilor depuse.

Astfel, contestatoarea precizează că potrivit autorităţii contractante, din informaţiile prezentate prin oferta tehnică (pag. 292, 312 şi 319-321) s-au constatat următoarele:

- Soluţia PKI Safe Layer reprezintă o soluţie de management a certificatelor digitale şi nu implementează funcţionalităţile de semnare, criptare/decriptare, ştergere sigură a fişierelor;
- În cadrul paragrafelor care descriu soluţiile de semnare (pag. 312), criptare/decriptare, ştergere sigură a fişierelor (pag. 319-321) care se instalează pe staţiile de lucru, este prezentată soluţia DigiSigner, pentru care nu reiese din ofertă că este certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional.

Se mai arată că prin solicitarea de clarificări nr. ..../DAPITA/3597/14.10.2014 , întrebarea nr. 23, s-a cerut identificarea cu exactitate a soluţiei care implementează funcţionalităţile menţionate. La aceasta, ... ar fi răspuns prin adresa nr. .../DAPITA/3696/20.10.2014, făcând trimitere la componenta de tip server a soluţiei, care implementează funcţionalităţile de management a certificatelor digitale (emitere, revocare, emitere CRL, validare), şi precizând, totodată, că există o componentă client – DigiSigner. Autoritatea susţine, în mod complet eronat, că soluţia care se instalează pe staţiile de lucru pentru a implementa funcţionalităţile solicitate (semnare, criptare/decriptare, ştergere sigură) este, de fapt, soluţia DigiSigner, iar nu SafeLayer PKI. Autoritatea notează că pentru soluţia DigiSigner, nu există menţiuni în ofertă privind certificarea acesteia din punct de vedere al securităţii informatice, conform cerinţelor caietului de sarcini şi menţionează că a solicitat prin adresa nr. .../DAPITA/4498/03.03.2015 clarificarea acestui aspect.

La aceasta, se arată în continuare, ... a răspuns prin adresa nr. .../DAPITA/4598/06.03.2015, precizând că platforma SafeLayer este certificată şi, împreună cu componenta client DigiSigner, asigură funcţionalităţile de semnare, criptare/decriptare, ştergere, sigură cerute prin caietul de sarcini. Cu toate acestea, autoritatea se declară nemulţumită de clarificarea oferită, apreciind în continuare că nu se prezintă niciun document care să ateste certificarea cerută pentru DigiSigner şi că răspunsurile la solicitările de clarificare ar modifica oferta depusă, prin menţionarea produsului DigiSigner şi indicarea faptului că referirea la acesta s-ar regăsi la pag. 292 din ofertă.

Având în vedere cele precizate anterior, contestatoarea menţionează că temeiurile de respingere invocate de autoritate nu au niciun suport în prevederile caietului de sarcini şi ignoră cu rea-credinţă argumentele expuse. La pag. 292 din oferta tehnică ... a prezentat în mod nechivoc modul în care soluţia ofertată răspunde cerinţelor caietului de sarcini.

Aşa cum se observă din extrasul de mai sus, în ofertă contestatoarea susţine că a indicat cu claritate că înţelege să probeze îndeplinirea cerinţei prin soluţia SafeLayer PKI, care prin tehnologia TrustedX implementează funcţionalităţile solicitate prin caietul de sarcini (semnare, criptare/decriptare, ştergere sigură a fişierelor) şi deţine certificarea din punct de vedere al securităţii informatice emisă de către un organism abilitat la nivel internaţional, respectiv certificarea Common

Criteria EAL 4+, care răspunde întrutotul cerinţei menţionate. Această certificare menţionată în extrasul de la pag. 292 din oferta tehnică este listată public la adresa: http://www.commoncriteriaportal.org., unde de altfel sunt listate toate certificările obţinute de SafeLayer PKI.

În răspunsul la întrebarea 23 din solicitarea de clarificare nr. .../DAPITA/3597/14.10.2014, a confirmat că înţelege să îndeplinească cerinţa caietului de sarcini prin soluţia SafeLayer PKI şi a explicat că DigiSigner este doar o aplicaţie, o componentă utilizată la nivel de client, adică al staţiilor de lucru/PC-urilor, pentru a apela funcţionalităţile disponibile la nivelul soluţiei SafeLayer PKI.

Ulterior, în cadrul răspunsurilor la clarificări cu nr. .../DAPITA/4598/06.03.2015, s-a precizat în mod clar faptul că tehnologia pe care se bazează SafeLayer PKI este integrată la nivelul librăriilor criptografice accesate cu componenta DigiSigner, aceasta din urmă acţionând ca o interfaţă pentru soluția SafeLayer PKI propusă. Or, soluţia SafeLayer PKI este certificată ISO/IEC 15408 EAL4+ din punct de vedere al securităţii informatice, fapt menţionat la pag. 292 din oferta tehnică, fiind evident în aceste condiţii că nu este necesar să se demonstreze certificarea şi pentru componenta/aplicaţia DigiSigner. În acelaşi timp, contrar susţinerilor autorităţii, componenta DigiSigner nu este nou introdusă în ofertă, ci se regăseşte menţionată la pag. 312 şi 319-321, aşa cum, de altfel, chiar autoritatea contractantă recunoaşte în comunicarea rezultatului procedurii, răspunsurile ... din 14.10.2014, respectiv 06.03.2015 având rolul de a clarifica asupra paginii unde se regăseşte certificarea solicitată cu privire la soluţia SafeLayer PKI (cea prin care se demonstrează îndeplinirea cerinţei caietului de sarcini) şi asupra modului în care soluţia SafeLayer PKI acţionează ca o interfaţă pentru componenta DigiSigner.

Astfel, în setul de răspunsuri de clarificare din 06.03.2015 contestatoarea susţine că a explicat diferenţa dintre o soluţie certificată şi o aplicaţie/componentă care asigură interfaţa cu aceasta (sau, în limbaj tehnic, „o apelează”) folosind standarde de comunicaţii Web Service. De asemenea, a explicat cum o aplicaţie/componentă, şi anume un browser web, poate apela o soluţie certificată:

“De exemplu, o soluţie software care deţine o certificare din punct de vedere al securităţii informatice, poate fi apelată/integrată/interfaţată sau interogată de orice aplicaţie prin standarde de comunicaţie Web Service, aceasta fiind şi situaţia browserelor web (Mozilla Firefox, Google Chrome, Internet Explorer, etc) prin care se apelează funcţii ale unei soluţii certificate”.

În condiţiile în care soluţia este certificată Common Criteria EAL 4+, necesităţile de securitate informatică ale autorităţii contractante sunt pe deplin asigurate, fără a fi necesară o certificare de securitate similară pentru browserul web prin care este accesată. De asemenea, accesarea prin browser nu atrage retragerea sau pierderea certificării respective pentru soluţia în sine. Aşadar, soluţia este diferită de aplicaţia (componenta) care permite accesul la aceasta.

Referitor la afirmaţiile de la lit. a)-d) expuse în motivarea pct. 1 din comunicarea rezultatului procedurii (adresa autorităţii contractante nr. .../DAPITA/13760/16.03.2015), contestatoarea afirmă că acestea nu pot justifica respingerea ofertei:

Afirmaţia a): „Produsul Digisigner nu este prezent în locul menţionat" – Aşa cum însăşi autoritatea contractantă recunoaşte prin adresa din 16.03.2015, componenta DigiSigner se regăseşte în oferta tehnică, fiind menţionată la pag. 312, 319-321. Contestatoarea susţine că a trimis la pag. 292 doar pentru a indica locul unde se face vorbire de certificarea soluţiei SafeLayer PKI. În orice caz, autoritatea nu avea dreptul de a declara oferta neconformă pentru motivul că un anume produs „nu se regăseşte în locul menţionat". Autoritatea avea obligaţia de a examina oferta în ansamblul său şi de a depune diligenţa necesară pentru a se edifica asupra modului în care diferitele părţi ale ofertei tehnice se corelează între ele – având în acest sens la dispoziţie o serie de experţi tehnici.

Afirmaţia b): „TrustedX nu face parte din platforma KeyOne" în opinia contestatoarei, afirmaţia este irelevantă şi nu poate justifica respingerea ofertei. Atât serverul TrustedX, cât şi platforma SafeLayer KeyOne PKI Platform sunt elemente ale arhitecturii soluţiei SafeLayer PKI ofertate, ambele prezentate la pag. 287 din oferta tehnică. TrustedX este un server de alocare şi gestionare de roluri utilizatori (în limbaj tehnic, de „federare" de roluri) care poate fi integrat cu o serie largă de servicii şi aplicaţii client sau furnizori de identitate. Produsul poate fi folosit împreună cu platforma SafeLayer KeyOne PKI Platform, precum şi cu alte platforme furnizate de SafeLayer. La contractarea platformei SafeLayer KeyOne PKI Platform, producătorul recomandă integrarea cu serverul TrustedX, exact aşa cum a fost ofertat şi descris în oferta tehnică. Serverul TrustedX şi platforma SafeLayer KeyOne PKI Platform sunt prezentate la pag. 287 din ofertă, ca elemente ale arhitecturii soluţiei SafeLayer PKI.

De asemenea, aceste elemente apar şi la pag. 37 din ofertă, unde este indicat locul lor în arhitectura soluţiei.

Afirmaţia c): „TrustedX nu are nicio legătură cu funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură", în opinia contestatoarei afirmaţia este falsă, iar captura de ecran prezentată de autoritatea contractantă nu este menită decât să inducă în eroare în mod grosolan. Captura în cauză nu are cum să ilustreze funcţionalităţile enunţate, pentru că ea prezintă funcţionalitatea de autentificare a TrustedX, oferită prin intermediul platformei TrustedX Authentication Platform, însă ... nu s-a referit la această funcţionalitate şi nu a invocat capabilităţile acestei platforme. Funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură oferite de TrustedX pot fi dovedite prin accesarea site-ului web al producătorului, secţiunea „TrustedX Electronic Signature".

Mai mult decât atât, în aceeaşi pagină web, dar de altfel şi în oferta tehnică la pag. 290 este prezentată tehnologia TrustedX în cadrul unei arhitecturi posibile şi este specificat faptul că funcţionalităţile TrustedX pot fi accesate (utilizate) fie prin interfaţă web (ca web service), fie în

interfaţă cu diverse aplicaţii (cum este aplicaţia Digisigner), fie prin combinaţia dintre aceste două metode.

Referitor la afirmaţia d): „În continuare, nu prezentaţi niciun document care să ateste certificarea produsului DigiSigner, colaborarea acestuia cu platforma SafeLayer nefiind suficientă în acest sens”, contestatoarea susţine că DigiSigner este doar o componentă, o aplicaţie care accesează funcţionalităţile asigurate de soluţia SafeLayer PKI prin tehnologia TrustedX, certificările acesteia în domeniul securităţii informatice emise de o entitate abilitată la nivel internaţional fiind disponibile public la adresa https://www.commoncriteriaportal.org, aşa cum s-a indicat în oferta tehnică la pag. 292. Pentru acest motiv, nu este necesară prezentarea unei certificări şi pentru DigiSigner, certificarea care răspunde integral cerinţelor caietului de sarcini fiind cea emisă pentru soluţia SafeLayer PKI.

În concluzie, prin răspunsurile la solicitările de clarificare, contestatoarea apreciază că nu a modificat oferta depusă, toate elementele la care a făcut referire în clarificări fiind deja prezentate în oferta tehnică. Autoritatea contractantă ignoră specificarea clară în ofertă a faptului că soluţia ofertată se bazează pe funcţionalităţile tehnologiei TrustedX, parte integrantă a soluţiei SafeLayer PKI propuse, care este certificată ISO/IEC 15408 EAL4+ din punct de vedere al securităţii informatice, certificare prezentată în pag. 292 a ofertei tehnice, şi care este integrată la nivelul librăriilor criptografice utilizate cu DigiSigner, tehnologia TrustedX fiind cea care permite executarea operațiunilor de semnare, criptare/decriptare, ştergere sigură solicitate de autoritatea contractantă.

Motivul 2: autoritatea contractantă susţine că nu este îndeplinită următoarea cerinţă a caietului de sarcini: „În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele: (...)”.

Autoritatea se bazează pe următoarele „argumente”:

- În oferta ... (pag. 305) nu s-ar regăsi versiunea de produs ofertată pentru această aplicaţie;
- Linkul http://www.safelayer.com/en/solutions/mobile-pki redirecţionează către o altă pagină, respectiv http:// www.safelayer.com/en/solutions/mobile-identification, care, susţine autoritatea, ar prezenta doar „conceptul de utilizare”, nu şi aplicaţia ofertată;
- În oferta ... nu se regăseşte modalitatea de îndeplinire a cerinţei de „generare a cheilor criptografice direct pe terminalul mobil”;
- Adresa nr. .../DAPITA/4598/06.03.2015, conţinând răspunsul ... la întrebarea nr. 24 din solicitarea de clarificări nr. .../DAPITA/4498/03.03.2015, unde a indicat o aplicaţie denumită „Mobile PKI”, care în opinia autorităţii contractante „nu există”.

Referitor la constatările autorităţii contractante cu privire la acest punct, contestatoarea precizează că acestea sunt în întregime false, având în vedere următoarele:

- ... a confirmat autorităţii în scris, atât prin adresa nr. .../DAPITA/4598/06.03.2015, cât şi prin adresa anterioară de clarificări, nr. .../DAPITA/3696/20.10.2014, că produsul oferit nu este comercializat cu un model de versionare, acesta fiind motivul pentru care în ofertă nu se regăseşte versiunea de produs ofertată.

- Aplicaţia de generare a cheilor criptografice direct pe terminalul mobil, care este menţionată în ofertă, poartă denumirea completă de „Safelayer Mobile ID", aşa cum de altfel s-a explicat în adresa nr. .../DAPITA 4598/06.03.2015, la care se face referire şi sub denumirile de „Mobile ID" sau „Mobile PKI", având în vedere capabilităţile oferite, aspect susţinut prin declaraţia producătorului Safelayer, ataşată ca Anexa nr. 1 la adresa mai sus menţionată. În mod evident, fiecare producător are libertatea de a-şi denumi sau supranumi propriul produs după cum consideră de cuviinţă (evident, în limitele legale), iar Safelayer a decis să se refere la aplicaţia de generare a cheilor criptografice pentru terminale mobile sub denumirea "Mobile PKI", fapt atestat şi de declaraţia de producător pusă la dispoziţia autorităţii.

Autoritatea a refuzat, însă, în mod nejustificat să ia în considerare atât declaraţia de la producător, cât şi răspunsurile ... din 06.03.2015, care lămuresc corespondenţa Mobile PKI cu oferta sa tehnică.

- Autoritatea contractantă susţine în mod eronat că pagina http://www.safelayer.com/en/solutions/mobile-identification prezintă doar „conceptul de utilizare".

- Declaraţia producătorului Safelayer atestă şi faptul că respectivele chei criptografice sunt generate direct pe terminalul mobil sau pe un smart card ataşat.

- În acelaşi sens este de altfel şi concluzia de la punctul 3 al sesiunii demonstrative din 13.11.2014, consemnată în procesul verbal nr. 4198/13.11.2014 din care este reprodus mai jos un extras:

3. Aplicaţia pentru generarea cheilor şi a cererilor de certificare este prezentă în Google Play/App store sau în alt store de aplicaţii?

Răspuns ofertant: Da, ofertantul a demonstrat că aplicaţia ofertată pentru generarea cheilor şi a cererilor de certificare este prezentă în APP store. Pentru Android a fost prezentată versiunea de autentificare din browser.

- Contestatoarea afirmă că este de notorietate faptul că Google Play şi App Store sunt cataloagele oficiale pentru a descărca aplicaţii pentru sistemele de operare Google Android, respectiv Apple iOS, folosite pe dispozitivele mobile de tip smartphone. Astfel, deşi prin procesul verbal din 13.11.2014 autoritatea contractantă a confirmat că a luat act de demonstrarea acestor funcţionalităţi, în mod inexplicabil, prin comunicarea rezultatului procedurii din 16.03.2015 autoritatea susţine cu vădită rea-intenţie exact contrariul.

În contextul celor precizate anterior, contestatoarea apreciază constatarea neîndeplinirii acestei cerinţe ca fiind vădit lipsită de

fundament, iar soluţia respingerii ofertei sale pe acest considerent este nelegală şi abuzivă.

Motivul 3: Autoritatea susţine că nu sunt îndeplinite cerinţele din caietul de sarcini privind accesul unui utilizator de pe PC în sistem. Autoritatea consideră că:

- Nici informaţiile prezentate în oferta ... la pag. 308-311 şi nici clarificările furnizate prin adresa nr. .../DAPITA/4598/06.03.2015 conţinând răspunsul la întrebarea nr. 24 din solicitarea de clarificări nr. .../DAPITA/4498/03.03.2015, nu demonstrează îndeplinirea cerinţelor menţionate, deoarece s-a invocat componenta KeyOne XRA a soluţiei SafeLayer PKI. Or, aceasta este componenta de „Registration Authority" („RA") a soluţiei enunţate, care în viziunea autorităţii nu face dovada îndeplinirii cerinţelor referitoare la accesul unui utilizator de pe PC în sistem, deoarece componenta în cauză ar avea numai funcţionalităţi de înregistrare a utilizatorilor în sistem, însă nu şi funcţionalităţi în ceea ce priveşte accesul utilizatorilor la sistem.

- În opinia autorităţii, ... nu a detaliat capabilităţile sistemului informatic ofertat de a asigura accesul utilizatorilor, considerând că s-a făcut referire doar la emiterea certificatelor digitale de către furnizorul Digisign fără a prezenta, însă, integrarea dintre acesta şi componenta KeyOne XRA şi modalitatea de utilizare a certificatelor de către modulul de autentificare şi autorizare a utilizatorilor.

- În plus, autoritatea contractantă consideră că prin adresa nr. .../DAPITA/4598/06.03.2015 s-a modificat totodată oferta, deoarece s-a făcut referire la soluţia de autentificare şi autorizare a utilizatorilor TrustedX, care nu a fost menţionată nici în oferta scrisă şi nici în adresa anterioară de clarificări, nr. .../DAPITA/3696/20.10.2014.

Referitor la argumentele autorităţii contractante cu privire la acest punct, contestatoarea arăta că acestea sunt în întregime eronate din punct de vedere tehnic şi invocate cu rea-credinţă, în scopul respingerii în mod abuziv a ofertei sale.

Astfel, contestatoarea învederează următoarele:

- Cerinţa exprimată în documentaţia de atribuire priveşte accesul la sistem. Orice proces de control al accesului are două componente principale: autentificarea şi autorizarea.
    - Autentificarea reprezintă procesul prin care unui utilizator i se acordă un set unic de credenţiale (identificatori) care au rolul de a-l identifica în mod unic;
    - Autorizarea este procesul prin care utilizatorului i se acorda accesul la resurse în funcţie de drepturile de acces setate de administratorii sistemului.
- Componenta de autentificare a sistemului informatic ofertat este realizată prin intermediul KeyOne XRA, componenta prezentată în cadrul ofertei tehnice, aşa cum recunoaşte chiar autoritatea contractantă, iar componenta de autorizare (control acces) este realizată prin integrarea TrustedX în cadrul sistemului ofertat, precum şi prin integrarea cu alte sisteme de control acces cum ar fi LDAP, Radius etc., menţionate în contextul prezentării platformei TrustedX în oferta tehnică. În descrierea

produsului este stipulat expres „digital certificate management for a wide range of user platforms and devices”, respectiv capacitatea de integrare cu o serie largă de tehnologii şi echipamente, inclusiv pentru autentificarea utilizatorilor, funcţia principală a certificatelor digitale.

Contestatoarea precizează în acest sens că TrustedX este un sistem de autentificare versatil, ce permite integrarea flexibilă şi adaptivă cu o serie largă de aplicaţii de autentificare, inclusiv dezvoltate intern de client, conform descrierii produsului, din care: „TrustedX se comportă ca un agent între aplicaţiile utilizatorului şi serviciile de furnizare a identităţii. Aplicaţiile folosesc protocoalele OAuth 2.0 şi SAML 2.0 pentru a invoca TrustedX, fiind suportate servicii de furnizare a identităţii LDAP/AD, RADIUS sau PKI” (în cazul de faţă KeyOne PKI). Pentru a integra autentificarea, TrustedX are la dispoziţie câteva strategii: (i) standard, strategie care foloseşte interfaţa de autentificare nativă a TrustedX; (ii) interfaţa grafică delegată, ce permite o experienţă de utilizare armonioasă, integrată cu aplicaţiile, externalizată în alte servicii de furnizare a identităţii, completate cu funcţiile de autentificare adaptată şi SSO din TrustedX.

- Autoritatea contractantă susţine, în mod fals, că ... nu a detaliat capabilităţile sistemului informatic ofertat de a asigura accesul utilizatorilor. Toate elementele necesare în privinţa explicitării modului de acces al utilizatorilor sunt prezente în oferta tehnică, fiind descrise toate secvenţele acestui proces, însoţite de scheme şi arhitecturi explicative, precum şi în adresa nr. .../DAPITA/4598/06.03.2015.

- Corelarea KeyOne XRA cu alte elemente prezente în oferta tehnică, între care şi TrustedX, la care s-a făcut referire în adresa nr. .../DAPITA/4598/06.03.2015, nu a servit altui scop decât de a răspunde întrebărilor autorităţii contractante, în vederea clarificării modului de înţelegere a soluţiei ofertate. Componenta TrustedX este prezentă atât în schema de licenţiere, cât şi în arhitectura PKI propusă pentru acest proiect în oferta tehnică depusă, motiv pentru care susţinerea autorităţii că s-ar fi operat o modificare de ofertă este nefondată.

- Toate elementele prezentate în ofertă şi în clarificările transmise au fost ignorate în mod grosolan de autoritatea contractantă. Aşa cum ea însăşi indică în adresa de comunicare a rezultatului procedurii nr. .../DAPITA/13760/16.03.2015, autoritatea a luat act de faptul că autoritatea de certificare sub care sunt emise certificatele digitale este Root CA a Digisign.

În Anexa nr. 3 la adresa nr. .../DAPITA/4598/06.03.2015, în susţinerea celor expuse în oferta tehnică, contestatoarea susţine că a prezentat declaraţia producătorilor Safelayer şi Digisign, care au explicitat cu claritate schimbul de informaţii şi modul de integrare cu privire la certificatele digitale între produsele software ofertate Autoritatea contractantă a solicitat această clarificare suplimentară a modului de integrare între o autoritate de certificare şi o autoritate de înregistrare, în ciuda faptului că acest lucru nu a fost solicitat nici în documentaţia de licitaţie, nici în cadrul sesiunii demonstrative, precum şi în ciuda faptului ca această integrare nu se poate face decât prin mijloace standard,

uzitate în cadrul oricăror infrastructuri cu chei publice (PKI).

În concluzie, ignorarea atât a elementelor ofertei, cât şi a răspunsului de clarificare mai sus menţionat, care nu face altceva decât să indice elementele din ofertă care se corelează, dovedeşte reaua-credinţă a autorităţii contractante. Mai mult, având în vedere că nu se introduc elemente sau componente noi, ci se indică doar componente deja prezentate în oferta tehnică, inclusiv în descrierile din broşurile anexate acesteia, concluzia autorităţii contractante în sensul că s-a fi procedat la o modificare a ofertei este nelegală şi abuzivă.

Motivul 4: Autoritatea contractantă consideră că nu s-a probat îndeplinirea cerinţei ca aplicaţia de generare a cheilor criptografice direct pe terminalul mobil să realizeze „înscrierea certificatului digital atât pe dispozitivul mobil, cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta”.

Autoritatea contractantă apreciază în acest sens că:

- Din informaţiile prezentate la pag. 307 din oferta tehnică nu reiese modalitatea de îndeplinire a cerinţei.

- Prin adresa nr. .../DAPITA/3696/20.10.2014, de răspuns la solicitarea de clarificări nr. .../DAPITA/3597/14.10.2014, la întrebarea nr. 27, ... a făcut referire la componenta SafeLayer KeyOne PKI, care este componenta de tip server ce implementează funcţionalităţile de management ale certificatelor digitale (emitere, revocare, emitere CRL, validare), neexplicând modalitatea în care certificatele sunt înscrise pe terminalul mobil sau pe dispozitivul criptografic conectat la terminalul mobil şi modul în care este îndeplinită cerinţa.

Referitor la acest motiv, contestatoarea apreciază că autoritatea contractantă a ignorat atât răspunsurile sale din adresa de clarificare nr. .../DAPITA/4598/06.03.2015, cât şi propriile sale concluzii trase în urma sesiunii demonstrative susţinute.

- Astfel, în primul rând, din declaraţia de la producătorul Safelayer (Anexa nr. 2 la adresa nr. .../DAPITA/4598/06.03.2015) reiese clar şi fără echivoc că aplicaţia care implementează partea de înscriere certificate pentru echipamente mobile este “Mobile PKI” (aceeaşi cu „Safelayer Mobile ID”, susţinut de declaraţia Safelayer – Anexa nr. 1 la adresa nr. .../DAPITA/4598/06.03.2015). Conform declaraţiei de la producător, soluţia propusă permite înscrierea cheilor criptografice direct pe terminalul mobil şi pe dispozitive criptografice de tip smartcard, conectat la terminalul mobil.

- În al doilea rând, autoritatea contractantă a confirmat în urma sesiunii demonstrative din 13.11.2014 faptul că această cerinţă este îndeplinită, fapt consemnat în procesul verbal nr. 4198/13.11.2014 din care a reprodus mai jos extrasul relevant:

5. Demonstraţia include utilizarea certificatelor digitale pe terminalele mobile stocate pe dispozitivul criptografic propriu, conectat la terminalul mobil?

Răspuns ofertant: Da, a fost făcută o demonstraţie în cadrul sesiunii de prezentare a autentificării cu dispozitivul criptografic conectat la terminalul mobil Andriod.

6. Demonstraţia include utilizarea certificatelor digitale pe terminalele mobile stocate pe terminalul mobil?

Având în vedere cele antemenţionate, contestatoarea apreciază că argumentele autorităţii contractante cu privire la neîndeplinirea acestei cerinţe apar ca vădit neântemeiate.

Motivul 5: Probabil, pentru a adăuga în mod artificial un motiv în plus de respingere a ofertei ca neconformă, autoritatea reia la acest punct, în mod identic, argumentele de la Motivul 3, considerând că nu sunt îndeplinite cerinţele din caietul de sarcini privind accesul unui utilizator de pe PC în sistem.

Astfel, contestatoarea reiterează explicaţiile pe care le-a furnizat cu privire la Motivul 3, respectiv faptul că din punct de vedere al accesului, componenta de autentificare a sistemului informatic ofertat este realizată prin intermediul KeyOne XRA, componenta prezentată în cadrul ofertei tehnice (după cum recunoaşte chiar autoritatea contractantă), iar componenta de autorizare este realizată prin integrarea TrustedX în cadrul sistemului ofertat, precum şi prin integrarea cu alte sisteme de control acces cum ar fi LDAP, Radius etc., menţionate în contextul prezentării platformei TrustedX în oferta tehnică. În descrierea produsului este stipulat expres „digital certificate management for a wide range of user platforms and devices", respectiv capacitatea de integrare cu o serie largă de tehnologii şi echipamente, inclusiv pentru autentificarea utilizatorilor, funcţia principală a certificatelor digitale.

Motivul 6: Autoritatea contractantă consideră că nici prin ofertă şi nici prin cele două adrese de răspuns la solicitările de clarificare nu s-a demonstrat îndeplinirea cerinţei generale „Accesul unui utilizator la sistem se va putea realiza şi de pe propriul terminal mobil utilizând certificatul digital propriu" şi a celor din paragrafele subsecvente acesteia – deşi autoritatea nu indică, în mod concret, care sunt aceste cerinţe pretins neîndeplinite.

- În esenţă, argumentul autorităţii la acest punct este bazat pe faptul că informaţiile prezentate în ofertă la pag. 310 şi clarificările furnizate prin adresa nr. .../DAPITA/3696/20.10.2014, ca răspuns la întrebarea nr. 29 din solicitarea de clarificări nr. .../DAPITA/3597/14.10.2014, vizează componenta KeyOne XRA a soluţiei SafeLayer PKI. Or, aceasta fiind componenta de „Registration Authority" („RA") a soluţiei enunţate, autoritatea consideră că nu face dovada îndeplinirii cerinţelor privind accesul unui utilizatorilor sistem, întrucât ar avea numai funcţionalităţi de înregistrare a utilizatorilor, nu şi de acces al utilizatorilor la sistem.
- Mai departe, nici adresa nr. .../DAPITA/4598/06.03.2015 conţinând răspunsul la solicitarea de clarificări nr. .../DAPITA/4498/03.03.2015, nu ar demonstra, în opinia autorităţii, îndeplinirea cerinţelor menţionate. Autoritatea consideră că „Procesul de autentificare este, în mod indubitabil, definit ca începând prin furnizarea de orice tip de credenţiale deja existente de către requester către autoritatea de validare (server, etc.). Înregistrarea (în acest caz, înrolarea certificatelor) este cu totul alt proces".

În plus, autoritatea contractantă consideră că prin adresa nr. .../DAPITA/4598/06.03.2015, s-a modificat oferta, deoarece s-a făcut referire atât la aplicaţia Mobile ID, care nu apare în ofertă, cât şi la soluţia de autentificare şi autorizare a utilizatorilor TrustedX, care, de asemenea, nu a fost menţionată în ofertă.

Referitor la acest motiv, contestatoarea constată că autoritatea contractantă ignoră atât răspunsurile sale de clarificare, cât şi propriile concluzii obţinute în urma sesiunii demonstrative susţinute de ....

- Astfel, prin adresa nr. .../DAPITA/4598/06.03.2015, contestatoarea susţine că a furnizat următorul răspuns la întrebarea nr. 8: „Pentru conformitate în oferirea unui răspuns clar şi fără echivoc la solicitarea dumneavostră, autentificarea de pe terminalele mobile se realizează folosind certificatele digitale stocate fie pe dispozitivele mobile, fie pe dispozitive criptografice conectate direct la terminalul mobil, fie de pe smartcardurile conectate cu cititoare la aceste terminale mobile. Prin intermediul aplicaţiei Mobile ID (menţionată în răspunsul 4), care la rândul său apelează platforma TrustedX Adaptive Authentication integrată cu KeyOne XRA utilizatorilor li se verifică credenţialele şi li se permite accesul la aplicaţiile solicitate prin maparea acestor credenţiale pe drepturile şi rolurile asociate”.

- Prin „Mobile ID” se face referire la aplicaţia „Safelayer Mobile ID”, aceeaşi cu „Mobile PKI”, , fapt susţinut de declaraţia Safelayer prezentată ca Anexă nr. 1 la adresa nr. .../DAPITA/4598/06.03.2015. Aplicaţia de generare a cheilor criptografice direct pe terminalul mobil, care poartă denumirea completă de „Safelayer Mobile ID” şi la care se face referire şi sub denumirile de „Mobile ID” sau „Mobile PKI” este menţionată în ofertă, aşa încât nu se poate considera că prin adresa nr. .../DAPITA/4598/06.03.2015 s-a adăugat la ofertă acest produs.

- Corelarea KeyOne XRA cu alte elemente prezente în oferta tehnică, între care şi TrustedX, la care s-a făcut referire în adresa nr. .../DAPITA/4598/06.03.2015, nu a servit altui scop decât de a răspunde întrebărilor autorităţii contractante, în vederea clarificării modului de înţelegere a soluţiei ofertate. Componenta TrustedX este prezentă atât în schema de licenţiere, cât şi în arhitectura PKI propusă pentru acest proiect în oferta tehnica depusă, motiv pentru care susţinerea autorităţii că s-ar fi operat o modificare/completare de ofertă prin menţionarea acestei componente este nefondată.

- Odată lămurită împrejurarea că nu se află în ipoteza unei completări sau modificări de ofertă, contestatoarea învederează Consiliului că întreaga argumentaţie a autorităţii se bazează pe o confuzie fundamentală gravă între procesul de autentificare şi procesul de autorizare. Afirmaţia din comunicarea rezultatului procedurii în sensul că „Procesul de autentificare este, în mod indubitabil, definit ca începând prin furnizarea de (…) credenţiale deja existente” este o afirmaţie naivă, complet lipsită de fundament tehnic, probabil datorată unei traduceri nefericite. În orice caz, această „definire” a procesului de autentificare nu are suport în prevederile caietului de sarcini, care nu conţin niciun fel de precizări în sensul afirmaţiei mai sus citate. Aşa fiind, interpretând astfel

cerinţele documentaţiei, autoritatea nu face decât să adauge în mod nepermis la cerinţele caietului de sarcini în etapa de evaluare a ofertelor.

- În realitate, autentificarea are rolul de a valida identitatea unui utilizator, iar autorizarea are rolul de a-i acorda acestuia dreptul de acces la resurse, conform drepturilor sale de acces. În mod concret, procesul de autentificare este procesul de a asigna un set de credenţiale unui anumit utilizator, iar procesul de autorizare este procesul prin care se acordă dreptul acelui utilizator la anumite resurse. Aceste două componente, autentificarea si autorizarea, permit controlul accesului. În sprijinul celor menţionate, contestatoarea indică aceeaşi sursă citată de autoritatea contractantă, Wikipedia, la adresa: http://en.wikipedia.org/wiki/Authentication#Authorization.

- Faptul că s-a demonstrat îndeplinirea cerinţei conform căreia „Accesul unui utilizator la sistem se va putea realiza şi de pe propriul terminal mobil utilizând certificatul digital propriu" este cu prisosinţă confirmat de punctele 5 şi 6 din procesul verbal nr. 4198/13.11.2014 încheiat în urma sesiunii demonstrative din 13.11.2014, din care este reprodus mai jos extrasul relevant:

5. Demonstraţia include utilizarea certificatelor digitale pe terminalele mobile stocate pe dispozitivul criptografic propriu, conectat la terminalul mobil?

Răspuns ofertant: Da, a fost făcută o demonstraţie în cadrul sesiunii de prezentare a autentificării cu dispozitivul criptografic conectat la terminalul mobil Andriod.

6. Demonstraţia include utilizarea certificatelor digitale pe terminalele mobile stocate pe terminalul mobil?

Răspuns ofertant: Da a fost făcută o demonstraţie în cadrul sesiunii de prezentare.

Motivul 7: Autoritatea contractantă susţine că oferta ... nu demonstrează îndeplinirea cerinţei ca soluţia de securitate propusă „să permită contexte diferite de securitate în funcţie de sesiunea din sistem accesată de către utilizator. Soluţia trebuie să permită prin configurare conexiuni http (publice, care nu necesită autentificare) şi https (cu autentificare) în funcţie de aceste contexte".

Argumentele oferite de autoritatea contractantă în acest sens pot fi sintetizate astfel:

- Prin clarificările furnizate prin adresa nr. .../DAPITA /3696/20.10.2014, ca răspuns la întrebarea nr. 32 din solicitarea de clarificări nr. .../DAPITA/3597/14.10.2014 , s-a precizat că soluţia de securitate constă în soluţia SafeLayer propusă.

- Ulterior, prin solicitarea de clarificări nr. .../DAPITA/ 4498/03.03.2015, autoritatea contractantă a solicitat să se precizeze care sunt produsele software componente ale infrastructurii SafeLayer PKI, care împreună cu Microsoft Active Directory asigură „contexte diferite de securitate în funcţie de sesiunea din sistem accesată de către utilizator". La această solicitare, prin adresa nr. .../DAPITA /4598/06.03.2015, contestatoarea a precizat că aplicaţia TrustedX îndeplineşte cerinţa enunţată. Autoritatea contractantă se declară, însă, nemulţumită de acest

răspuns, apreciind că serverul TrustedX nu face parte din platforma SafeLayer KeyOne PKI Platform.

- În plus, autoritatea consideră că prin răspunsurile la cele două solicitări de clarificare, ... a modificat oferta.

- Atât serverul TrustedX, cât şi platforma SafeLayer KeyOne PKI Platform sunt elemente ale arhitecturii soluţiei SafeLayer PKI ofertate de ..., ambele prezentate la pag. 287 din oferta tehnică. TrustedX este un server de alocare şi gestionare de roluri utilizatori (în limbaj tehnic, de „federare" de roluri) care poate fi integrat cu o serie largă de servicii şi aplicaţii client sau furnizori de identitate. Produsul este distinct de Safelayer KeyOne PKI Platform, însă recomandarea producătorului este de a folosi produsul TrustedX ca parte integrantă din SafeLayer KeyOne PKI Platform sau pentru integrarea cu alte platforme furnizate de SafeLayer. Aşadar, la contractarea platformei SafeLayer KeyOne PKI Platform, producătorul recomandă integrarea cu serverul TrustedX. Aşa a fost, de astfel, întocmită şi oferta ..., care a prezentat cele două elemente sub forma unui singur produs integrat.

- Referitor la concluzia autorităţii contractante cu privire la neîndeplinirea cerinţei enunţate a caietului de sarcini, contestatoarea consideră că răspunsul nr. 9 oferit în setul de clarificări din 06.03.2015 indică în mod neechivoc cum platforma TrustedX interacţionează şi interoperează, printre altele, cu Microsoft Active Directory, precizând paginile din oferta tehnică la care sunt descrise aceste funcţionalităţi şi asigurând astfel conformitatea ofertei cu cerinţele din documentaţia de atribuire mai sus menţionate: „În vederea asigurării acestor funcţionalităţi, TrustedX este o componentă a infrastructurii SafeLayer PKI şi are rolul de a administra drepturile şi permisiunile utilizatorilor, împreună cu Microsoft Active Directory, aşa cum reiese clar atât din răspunsul la întrebarea nr. 32, adică pag. 286, 287, 288, 289, cât şi pag. 311 a ofertei tehnice".

- TrustedX este o componentă a arhitecturii PKI prezentate în oferta tehnică (a se vedea pag. 287), iar răspunsul la solicitarea de clarificări din partea autorităţii contractante nu a avut decât rolul de a corela elementele prezentate în ofertă, cu scopul de a detalia înţelegerea soluţiei ofertate, şi pe cale de consecinţă nu modifică oferta, aşa cum în mod nefundamentat concluzionează autoritatea contractantă.

Motivul 8: Autoritatea contractantă consideră că oferta ... nu îndeplineşte cerinţa din caietul de sarcini ca soluţia de securitate propusă „să permită autentificarea utilizatorilor exclusiv pe baza certificatului digital X.509 v3 personal. Certificatele digitale pot fi emise de multiple Autorităţi de certificare definite de încredere, iar modulul trebuie să fie configurabil să se integreze cu oricare dintre ele folosind interfeţe şi protocoale standard".

Argumentele pe care autoritatea la invocă în sprijinul acestei concluzii ar putea fi rezumate după cum urmează:

- Prin clarificările furnizate prin adresa nr. .../DAPITA/3696/20.10.2014, ca răspuns la întrebarea nr. 32 din solicitarea de clarificări nr. .../DAPITA/3597/14.10.2014, contestatoarea

susţine că a explicat faptul că soluţia de securitate constă în infrastructura de tip PKI, adică soluţia SafeLayer propusă, împreună cu Microsoft Active Directory.

- Autoritatea consideră că această lămurire este insuficientă, deoarece integrarea cu Microsoft Active Directory nu este dovedită de informaţiile din ofertă ori de pe site-urile producătorilor.

În opinia contestatoarei, autoritatea contractantă urmăreşte, probabil să creeze confuzie prin argumentele prezentate, însă în niciun caz nu reuşeşte să demonstreze vreun aspect de neconformitate legat de oferta sa. Este discutabil cum ipotetica lipsă a explicitării modului de integrare cu Microsoft Active Directory poate justifica presupusa neîndeplinire a cerinţei conform căreia „Certificatele digitale pot fi emise de multiple autorităţi de certificare definite de încredere, iar modulul trebuie să fie configurabil să se integreze cu oricare dintre ele folosind interfeţe şi protocoale standard”.

- Referitor la cerinţa potrivit căreia certificatele digitale pot să provină de la mai multe autorităţi de certificare, contestatoarea face precizarea că soluţia ofertată permite maparea mai multor autorităţi de certificare, această împrejurare fiind de altfel constatată chiar de către autoritatea contractantă, care în adresa de comunicare a rezultatului procedurii, la pag. 7, arată că: „Prin documentaţia de atribuire nu a fost solicitată implementarea unei infrastructuri PKI în cadrul sistemului, ci emiterea certificatelor digitale de către un furnizor de servicii de certificare. La paginile 285, 300, 302 şi 303, ofertantul precizează explicit furnizorul, Digisign, şi autoritatea sub care sunt emise certificatele digitale – Root CA a Digisign”.

- Cu alte cuvinte, aşa cum o arată şi citatul din adresa autorităţii, platforma de control acces TrustedX, prin intermediul KeyOne XRA, poate lucra cu Digisign, însă pentru identitate de raţiune, aceasta poate lucra şi cu orice altă autoritate de certificare. Nu există nicio constrângere ca pe lângă autoritatea de certificare Root CA a Digisign să fie mapată o altă autoritate agreată de către ... („definită de încredere”), fapt menţionat atât în oferta tehnică, dar şi în răspunsurile de clarificare cuprinse în adresa nr. .../DAPITA/4598/06.03.2015 , respectiv:

o Răspunsul la întrebarea nr. 7: „Pentru a invoca TrustedX, aplicaţiile folosesc protocoalele Oauth 2.0 sau SAML 2.0, iar ca servicii de furnizare a identităţii sunt suportate LDAP/Active Directory, RADIUS şi servicii PKI, în cazul nostru KeyOne XRA”;

o Răspunsul la întrebarea nr. 2: „Referitor la întrebarea dvs. nr. 2, în care solicitaţi specificarea rolului componentei ADSS OCSP Server, răspunsul nostru este precizat în Oferta tehnică la pag. 315 si 316. ADSS OCSP Server răspunde cerinţelor AC cu privire la funcţionalitatea Intelligent routing, astfel încât să poată fi validate certificate digitale emise de alte CA-uri decat cea din prezenta Soluţie de securitate, implementată în prezentul proiect, iar KeyOne VA este solutia de verificare a validităţii certificatelor digitale aferente acestui sistem”.

Contestatoarea precizează că integrarea cu LDAP se face prin intermediul TrustedX, ca parte integrantă din soluţia PKI oferită de

SafeLayer. Produsul TrustedX, care este un server de autorizare şi federare de roluri, este parte integrantă din soluţia PKI propusă de Safelayer, reunind mai multe modalităţi de verificare a identităţii, printre care soluţii PKI (Safelayer KeyOne PKI Platform sau altele), autentificare de tip RADIUS, sau autentificare de tip LDAP/Active Directory, după cum reiese din specificaţiile tehnice ale produsului.

De altfel, contestatoarea învederează că autoritatea contractantă nu i-a cerut niciodată clarificări, în mod specific, în legătură cu îndeplinirea cerinţei privind posibilitatea soluţiei de a asigura maparea mai multor autorităţi de certificare.

În aceste condiţii, pentru toate motivele arătate, se constată reaua-credinţă de care autoritatea a dat dovadă în evaluarea ofertei ..., precum şi neluarea în considerare a ofertei tehnice şi a răspunsurilor de clarificare prezentate, subliniind, în acelaşi timp, că pretinsul motiv de neconformitate care a stat la baza respingerii ofertei, apare ca vădit nefondat şi abuziv.

Motivul 9: La acest punct, autoritatea contractantă susţine că oferta ... nu îndeplineşte cerinţa caietului de sarcini privitoare la modul de realizare a criptării, respectiv: „Criptarea trebuie să poată fi realizată astfel: a. La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată”.

Autoritatea contractantă îşi bazează concluzia pe următoarele argumente:

- Autoritatea susţine că prin clarificările furnizate prin adresa nr. .../DAPITA/3696/20.10.2014, ca răspuns la întrebarea nr. 32 din solicitarea de clarificări nr. .../DAPITA/3597/14.10.2014, referitoare la cerinţa din caietul de sarcini privind „Asigurarea confidenţialităţii datelor”, cap. 3.3.7.3.2, ... ar fi arătat că „Aplicaţia DigiSigner propusă integrează în tehnologiile PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici si asimetrici. Astfel, produsul BitLocker suportă algoritmul criptografic simetric 3DES atât prin intermediul componentei client DigiSigner, care integrează algoritmul criptografic simetric 3DES, cât şi prin dispozitivele criptografice securizate SafeNet e-Token PRO (…)”.
- Autoritatea însă pretinde că a constatat următoarele:
  - o Dispozitivele securizate SafeNet e-Token PRO suportă algoritmul 3DES, dar realizează această criptare numai dacă aplicaţia care solicită criptarea implementează acest algoritm. Or, BitLocker nu implementează algoritmul 3DES, ci doar AES, conform documentaţiei producătorului;
  - o Deşi ... ar fi precizat că BitLocker implementează funcţionalitatea de blocare a accesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului de la staţia de lucru, aspect evidenţiat la pag. 320, paragraful 3 din oferta tehnică, autoritatea consideră că în locul indicat din ofertă se precizează numai că accesul la partiţia criptată, respectiv deblocarea acesteia, poate fi realizat prin utilizarea unui smartcard, fără a detalia cum anume se realizează

blocarea la deconectarea acestuia.

Având în vedere cele precizate anterior, contestatoarea apreciază că autoritatea contractantă săvârşeşte grave confuzii, probabil menite să inducă în eroare:

- În primul rând, contestatoarea menţionează că răspunsul la întrebarea nr. 2 din solicitarea de clarificări invocată de autoritate se referă la cap. 3.3.7.3.1, iar nu la cap. 3.3.7.3.2., fiind reprodusă mai jos întrebarea nr. 32: *„Având în vedere cerinţele din caietul de sarcini, cap. 3.3.7.3.1., respectiv cele referitoare la Modulul de autentificare şi autorizare, vă rugăm să precizaţi, indicând cu exactitate numărul de pagini, precum şi litera/paragraful, unde se regăseşte în ofertă tehnica şi în ce constă „soluţia de securitate", care, în conformitate cu răspunsul dumneavoastră din matricea de conformitate, împreună cu Microsoft Active Directory răspunde cerinţelor referitoare la Modul de autentificare şi autorizare".*

- În caietul de sarcini nu există o cerinţă privitoare la „Asigurarea confidenţialităţii datelor" având cuprinsul menţionat de autoritate, respectiv: *„Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici si asimetrici, astfel:*
  - *Criptarea asimetrică, utilizând certificatele X509v3 si algoritmul RSA,*
  - *Criptarea simetrică folosind algoritmii 3DES si AES".*

- În schimb, o cerinţă cu conţinutul enunţat se află în subcapitolul „Asigurarea confidenţialităţii documentelor". La acest punct, răspunsul ... la cerinţa menţionată este următorul: *„Aplicatia DigiSigner propusă integrează în tehnologiile PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici şi asimetrici, după cum urmează: Referinţe: Broşura_DigiSigner.pdf*

- Criptarea asimetrica se realizează utilizând certificatele X.509 v3 şi algoritmul RSA.

- Criptarea simetrică se realizează utilizând algoritmii 3DES şi AES."

Astfel, contestatoarea afirmă că răspunsul său este conform cerinţei caietului de sarcini, iar aplicaţia prin care se realizează funcţiile de criptare este Digisigner, aşa cum este menţionat. De remarcat în acest context că referirea la cerinţa suportului pentru algoritmul 3DES se află în capitolul dedicat „Asigurării confidenţialităţii documentelor", răspunsul său fiind conform cerinţei având în vedere că aplicaţia DigiSigner suportă toţi algoritmii criptografici solicitaţi.

- Produsul BitLocker, în schimb, realizează criptarea partiţiilor, care nu are nicio legătură cu cerinţa mai sus menţionată, care se referă la „Asigurarea confidenţialităţii documentelor". BitLocker răspunde la cerinţa referitoare la criptarea aplicaţiilor, pretins neîndeplinită, conform căreia „Criptarea trebuie să poată fi realizată astfel: a. La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată". De remarcat că în cuprinsul cerinţei menţionate nu se specifică nimic despre algoritmul criptografic 3DES. Prin urmare, caietul de sarcini nu impune ca BitLocker să

implementeze algoritmul 3DES.

În concluzie, produsul BitLocker răspunde la cerinţa pretins neîndeplinită, însă nu are nicio legătură cu tehnologia PKI şi nici cu cerinţa de asigurare a confidenţialităţii documentelor (aceasta din urmă fiind cea în care se specifică necesitatea criptării utilizând algoritmul 3DES).

- Mai departe, în ceea ce priveşte dovada funcţionalităţii de blocare a accesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului, contestatoarea precizează că aceasta a fost evidenţiată în cadrul sesiunii demonstrative din 13.11.2014, cu prilejul demonstraţiei pe care ... a făcut-o pe fişiere criptate şi pe partiţii criptate, despre care se face menţiune la punctul 8 din procesul verbal nr. 4198/13.11.2014 încheiat în urma respectivei SESIUNI DEMONSTRATIVE: *„8. Sunt prezentaţi algoritmii criptografici folosiţi pentru criptare fişiere şi critare partiţii? Răspuns ofertant: Da, ofertantul a făcut o demonstraţie pe fişiere criptate şi pe partiţii criptate”.*

- Abordarea cerinţei enunţate la pag. 320 paragraful 3 din oferta tehnică, dublată de demonstraţia practică susţinută, este întrutotul conformă Caietului de sarcini, în cadrul căruia nu s-a impus ofertanţilor un mod specific în care să detalieze sau să probeze modalitatea de îndeplinire a cerinţei în cauză.

Motivul 10. Autoritatea contractantă a reţinut în fapt trei motive de neconformitate, după cum urmează:

(a) Autoritatea a apreciat că „Nu se regăseşte în ofertă nicio precizare cu privire la integrarea dintre StarSign şi DigiSigner”.

- Analizând modul în care autoritatea a ajuns la concluzia de mai sus, contestatoarea afirmă că deşi a răspuns în mod conform, detaliat şi la obiect, prezentând modalităţile în care modulul StarSign şi aplicaţia DigiSigner sunt conforme cu toate cerinţele specificate în comunicarea rezultatului procedurii, referitoare la „Modulul 8 : Modulul de arhivare a documentelor”, subcapitolul „3.3.8.1 – Componenta de Comunicare cu Arhiva Electronica Legala”, atât în cadrul ofertei tehnice depuse, cât şi prin răspunsul la întrebarea cu nr. 43 din solicitarea de clarificări nr. .../DAPITA/3597/14.10.2014, autoritatea a ales, în mod total netransparent şi discreţionar, să nu ia în considerare în evaluarea acestui aspect răspunsul la întrebarea de clarificare nr. 10 din solicitarea de clarificări nr. .../DAPITA/4498/03.03.2015, clarificare solicitată exact cu privire la aspect invocat de autoritate în comunicarea rezultatului procedurii.

- În susţinerea afirmaţiilor sale, contestatoarea reproduce răspunsul său la întrebarea de clarificare nr. 10, care infirmă în totalitate evaluarea autorităţii şi clarifică, argumentând cu extrase din oferta tehnică depusă, modul în care modulul StarSign, inclus în SEAL Compliance Edition, foloseşte şi se integrează cu componenta DigiSigner SDK pusă la dispoziţie de aplicaţia client DigiSigner – SDK (Software Development Kit) solicitat şi ofertat conform cu cerinţele caietului de sarcini, atât pentru aplicarea de semnături digitale şi mărci temporale conform cerinţelor enunţate în oferta tehnică, cât şi pentru a permite integrarea în aplicaţiile

care vor utiliza documente semnate electronic:

„Întrebarea nr. 10.

10. Referitor la răspunsul dumneavoastră la întrebarea cu nr. 43 din solicitarea de clarificări MFE/DAPITA nr. 3600/14.10.2014: Aţi menţionat faptul că „modulul StarSign, inclus în SEAL, asigură aplicarea de semnături digitale şi mărci temporale prin intermediul componentei client DigiSigner". Vă rugăm să precizaţi, indicând cu exactitate numărul paginii, precum şi litera/paragraful unde acestea sunt menţionate în oferta dumneavoastră şi unde descrisă integrată modului StarSign cu componenta clent DigiSigner.

Răspuns:

„Referitor la solicitarea dumneavoastră vă comunicăm următoarele:

- Modulul StarSign, inclus în SEAL Compliance Edition, foloseşte componenta DigiSigner SDK pusă la dispoziţie de aplicaţia client DigiSigner - SDK solicitat si ofertat conform cu cerinţele caietului de sarcini, pentru aplicarea de semnături digitale şi mărci temporale, aşa cum rezultă din următoarele informaţii specificate în cadrul ofertei tehnice înaintate, la paginile şi paragrafele indicate în cele ce urmează:

o Pag. 36, în cadrul detalierii arhitecturii sistemului propus şi ofertat: Figura – Arhitectura logică, unde pe serverele ARH1(VM) si ARH2(VM) se vor instala componentele:

- Seal Compliance Edition – Enterprise Unlimited, care include şi modulul StarSign şi
- Digisigner DSK

O Pag. 37, în cadrul tabelului cu alocarea componentelor ce vor fi virtualizate pe maşini fizice, unde pe serverele ARH1 şi ARH2 se vor instala componentele sus menţionate, respectiv (extras din acest tabel):

Denumire nod	***Componenta ce va fi instalată***	***Noduri***	***Core/nod***	***RAM/nod***
ARH_01 *ARH_02*	*SEAL Compliance Edition - Enterprise Unlimited* *DigiSigner SDK*	*2 - Load Balancing*	*2*	*16*

o Pag. 40, în cadrul tabelului cu produsele care vor fi licenţiate pentru sistemul propus şi ofertat, unde se specifică livrarea şi licenţierea acestor componente, respectiv (extras din acest tabel):

Producator	***Denumire produs***	***Cantitate***
Star Storage	*SEAL Compliance Edition - Enterprise Unlimited*	*4*
DigiSign	*Pachet licente DigiSigner - 300 utilizatori*	*1*
DigiSign	*Pachet licențe DigiSigner SDK*	*1*

o Pag. 317-318, unde se specifică această componentă, Digisigner SDK, care va fi folosită de asemenea, prin integrarea cu modulul StarSign şi pentru funcţionalităţile de verificare a documentelor electronice, conform răspunsurilor tehnice detaliate la aceste pagini pentru capitolul „Verificarea documentelor" din cadrul ofertei tehnice înaintate, funcţionalităţi care au fost de altfel demonstrate şi în cadrul sesiunii demonstrative încheiate prin PV nr. 4198/13.11.2014., respectiv (extras din oferta tehnică):

• *Aplicaţia trebuie să fie oferită şi sub forma unui SDK care va permite verificarea semnăturilor documentelor*	***DA***	*Se va oferi un SDK ce va permite verificarea semnăturilor documentelor electronice. SDK-ul oferit va permite*

electronice. SDK-ul va permite realizarea următoarelor operaţiuni către aplicaţiile care îl apelează:		*realizarea următoarelor operaţiuni către aplicaţiile care îl apelează, după cum urmează:*
• *Extragerea informaţiilor privind semnătura electronică şi certificatul semnatarului;*	***DA***	*Se va asigura extragerea informaţiilor privind semnătura electronică şi certificatul semnatarului, astfel încât acestea să poată fi consultate de către utilizatori.*
• *Extragerea datelor în clar din documentul semnat.*	***DA***	*Se va asigura extragerea datelor în clar din documentul semnat şi încapsulat PKCS#7. Aceste date pot fi ulterior consultate de către utilizatori.*
• *Pentru SDK se va oferi documentaţia tehnică necesară pentru a permite integrarea în aplicaţiile care vor utiliza documente semnate electronic.*	***DA***	*Am luat la cunoştinţă. Se va livra documentaţia tehnică aferentă SDK-ului pentru a permite integrarea în aplicaţiile care vor utiliza documente semnate electronic.*

- În plus, StarSign, SEAL Compliance Edition şi DigiSigner sunt menţionate şi descrise în oferta tehnică înaintată la paginile 312-330, cât şi paginile 331-338, ca răspunsuri tehnice oferite la toate cerinţele respective, răspunsuri care cuprind toate detaliile solicitate de îndeplinire".

(b) Referitor tot la răspunsul la întrebarea de clarificare nr. 10 enunţat mai sus, autoritatea a apreciat că „răspunsul precizează că «cerinţa este îndeplinită de soluţia ofertată prin intermediul proiectării, dezvoltării, configurării şi implementării» ceea ce induce necesitatea unui proces de proiectare şi dezvoltare în vederea îndeplinirii cerinţei".

Contestatoarea apreciază că autoritatea a evaluat în mod eronat îndeplinirea cerinţei de către oferta sa, conform cerinţelor din fişa de date şi caietul de sarcini, şi a ignorat informaţii incluse în oferta tehnică înaintată astfel:

(i) Fişa de date cuprinde următoarele capitole, unde se precizează în mod neechivoc că se solicită inclusiv servicii informatice şi servicii conexe (i.e., de dezvoltare software pentru gestionarea documentelor):

o Cap. II.1.2 Tipul contractului şi locul de executare a lucrărilor, de livrare a produselor sau de prestare a serviciilor îl reprezintă: Servicii7 - Servicii informatice şi servicii conexe

o Cap. II.1.6 Clasificare CPV (vocabularul comun privind achiziţiile) menţionează următoarele servicii şi pachete software:

- *72252000-6 Servicii de arhivare computerizata (Rev.2);*
- *72212311-2 Servicii de dezvoltare de software pentru gestionarea documentelor (Rev.2);*
- *79995100-6 Servicii de arhivare (Rev.2);*
- *39132000-6 Sisteme de arhivare (Rev.2);*
- *48983000-2 Pachete software de dezvoltare (Rev.2);*

toate acestea fiind corespunzătoare unor faze de proiectare şi dezvoltare specifice implementării unui astfel de sistem informatic complex cum este cel solicitat.

o Cap. II.1.5 Descrierea succintă a contractului sau a achiziţiei/achiziţiilor:

Obiectivul general al contractului îl constituie implementarea unui sistem informatic integrat în vederea arhivării şi gestionării documentelor existente în cadrul Ministerului Fondurilor Europene.

Sistemul informatic integrat va cuprinde următoarele module:

- *Modulul 1: Servicii de prelucrare a fondului arhivistic;*
- *Modulul 2: Serviciu de inventariere a documentelor;*
- *Modulul 3: Suport tehnic pentru elaborarea Nomenclatorului arhivistic;*
- *Modulul 4: Servicii de digitizare a documentelor;*
- *Modulul 5: Portal;*
- *Modulul 6: Sistemul Informatic de Management al Documentelor;*
- *Modulul 7: Componenta de Securizare Acces si Documente (certificate digitale, validare in timp real, verificare semnaturi electronice);*
- *Modulul 8: Modulul de arhivare a documentelor;*

(ii) Prin caietul de sarcini aferent acestei proceduri se solicită:

- Aceleaşi tipuri de servicii conform cap. 1.2. Denumirea serviciilor, unde se precizează:
  - „Servicii de arhivare a documentelor" - cod CPV 79995100-6 (Servicii de arhivare);
  - „Servicii de arhivare electronică a documentelor" - cod CPV 92512000-3 (Servicii prestate de arhive);
  - „Sistem de dezvoltare software pentru gestionarea documentelor" - cod CPV 72212311-2;
- „Pachete software de dezvoltare" - cod CPV 48983000-2; Aceleaşi tipuri de servicii conform cap. 2.1. Obiectul contractului, unde se precizează: „În vederea realizării obiectivelor contractului se vor achiziţiona următoarele:
  - Servicii de prelucrare arhivistică, inventariere şi digitizare a documentelor;
  - Servicii de arhivare electronică;
  - Servicii de depozitare fizică a documentelor după prelucrarea arhivistică;
  - Soluţie de gestiune a documentelor şi a fluxurilor de lucru, cu serviciile de implementare aferente;
  - Servicii de dezvoltare portal, inclusiv licenţele aferente;
  - Servicii de certificare a semnăturii electronice, inclusiv dispozitive securizate de generare a semnăturii electronice;
  - Soluţie de securizare a staţiilor de lucru, inclusiv licenţele aferente."

(iii) În cadrul ofertei tehnice depuse:

- În Cap. C. Soluţia propusă, la pag. 30 - 40, se descriu in detaliu tehnologiile ofertate şi arhitectura soluţiei propuse, precizându-se în clar, la pag. 30: *„Soluţia propusă de consorţiul nostru va fi livrată ca*

un sistem la cheie cu toate componentele ofertate şi livrate conform cerinţelor specificate în caietul de sarcini, instalate pe echipamentele hardware şi infrastructura software puse la dispoziţie de autoritatea contractantă, configurate şi funcţionale conform cerinţelor specificate în caietul de sarcini".

- În Cap. D. Management de Proiect, la pag. 41 - 55, se descrie în detaliu metodologia utilizata de subscrisa pentru implementarea sistemului integrat solicitat şi propus, care cuprinde ca şi faze principale, pentru prestarea serviciilor care sunt solicitate în cadrul procedurii de achiziţie:
  - Cap. 2. Analiza (pag. 44-46 din oferta tehnică);
  - Cap. 3. Proiectare (pag. 46-48);
  - Cap. 4. Dezvoltare şi configurare (pag. 48);
  - Cap. 5. Testarea şi asigurarea calităţii (pag. 49);
  - Cap. 6. Teste operaţionale (pag. 49-51);
  - Cap. 7. Implementare (pag. 51-53);

- În cadrul ofertei tehnice înaintate, în Anexa 1 – Matricea de conformitate, în cap. 3 Servicii solicitate, pag. 80 - 351, sunt oferite răspunsurile conforme şi detaliate la serviciile solicitate de autoritatea contractantă.

(iv) Chiar în Răspuns la întrebarea nr. 2 din CLARIFICAREA nr. 17 transmisă în SEAP, autoritatea contractantă a confirmat că „Ofertantul va construi o soluţie tehnică conformă cu cerinţele din caietul de sarcini şi conform planului de implementare şi a metodologiei pe care o propune în oferta tehnică":

(c) Tot referitor la răspunsul la întrebarea de clarificare nr. 10 mai sus menţionat, autoritatea a apreciat că „Din conţinutul propunerii tehnice şi al răspunsurilor ofertantului la clarificările solicitate rezultă că nu este îndeplinită cerinţa minimă a caietului de sarcini, în sensul că soluţia propusă nu este una matură ci va rezulta în urma unor dezvoltări ulterioare semnării contractului".

Contestatoarea precizează că în documentaţia de atribuire nu există nicio cerinţă ca „soluţia propusă" să fie „matură", aşa cum menţionează autoritatea contractantă. Toate referirile la o soluţie „matură" au fost eliminate din caietul de sarcini prin Modificarea nr. 8, emisă în data de 17.06.2014 în urma Deciziei Consiliului nr. .../.../..., ..., ..., ..., ..., .../.... De altfel, aceste referiri erau în flagrantă contradicţie cu celelalte dispoziţii ale documentaţiei de atribuire, precum şi cu clarificările oferite de însăşi autoritatea contractantă, cum este de exemplu cea mai sus menţionată.

Produsele software ofertate în scopul îndeplinirii cerinţei minime solicitate, respectiv SEAL Compliance Edition, StarSign (inclusă în SEAL Compliance Edition), DigiSigner şi DigiSigner SDK sunt produse comerciale „mature", în sensul că au fost lansate şi se află pe piaţă de mult timp, fiind achiziţionate şi utilizate de un număr semnificativ de clienţi din mediul privat şi public.

III. Decizia autorităţii contractante privind declararea ofertei Asocierii ... ca fiind câştigătoare, este nelegală, având în vedere faptul că

această ofertă este inadmisibilă şi neconformă.

În acest sens, din examinarea documentaţiei de atribuire, luând în considerare Secţiunea 2, cap 3.3.8.3 – Componenta de depozitare fizică din caietul de sarcini, contestatoarea constată că autoritatea contractantă a impus un set de cerinţe tehnice obligatorii ce trebuiau respectate de ofertanţi cu privire la Centrul de arhivare fizică a documentelor. Conform secţiunii menţionate din caietul de sarcini, acesta trebuie să întrunească următoarele cerinţe minime:

- *"Va trebui ca aplicatia de gestiune a informatiilor electronice referitoare la arhiva fizica sa poata gestiona la nivel de cod de bare unic si dosarele din interiorul unei cutii, nu doar cutiile cu documente. Aplicatia va trebui sa poate gestiona inclusiv etichete cu coduri de bare RFID pasive";*
- *"Va trebui ca fluxul operational, inclusiv pe perioada transportului, sa fie monitorizat online".*

În acest moment niciunul dintre operatorii membri în Asocierea declarată câştigătoare nu îndeplineşte condiţia de gestionare a etichetelor cu coduri de bare RFID Pasive. Acest lucru este cel mai probabil o consecinţă a faptului că până în acest moment nu au existat proceduri de achiziţie care să impună acest mod de lucru, tagurile RFID nefiind solicitate şi nici recomandate spre utilizare de către Arhivele Naţionale.

Trebuie avut în vedere şi faptul că ... a preluat unele dintre fondurile arhivistice ce au fost găzduite în trecut de companii ce fac parte din Asocierea declarată câştigătoare şi nu a identificat pe niciuna dintre cutiile preluate etichete RFID pasive care să permită o gestiune a informaţiilor electronice pe baza acestora.

În aceste condiţii contestatoarea consideră că oferta Asocieri ... este neconformă, ea nerespectând cerinţele tehnice minime din caietul de sarcini al procedurii de atribuire.

De asemenea, autoritatea contractanta solicită ca ofertanţii să poată oferi un flux operaţional monitorizat online inclusiv pe perioada transportului. Şi în acest caz, companiile din Asocierea declarată câştigătoare nu oferă acest serviciu, aplicaţia pusă la dispoziţie pentru clienţi în vederea monitorizării permiţând vizualizarea anumitor evenimenite (de exemplu, intrare şi ieşire din depozit), fără însă a monitoriza online cutiile cu documente pe perioada transportului astfel încât să se poată observa uşor orice oprire neprogramată ce se poate transforma într-o posibilă breşă de securitate.

Prin adresa nr. 237/03.04.2015, ... formulează cerere de intervenţie în care menţionează că ulterior depunerii ofertelor şi desfăşurării activităţii de evaluarea a acestora, autoritatea contractantă a încunoştiinţat-o despre faptul că oferta sa a fost declarată admisibilă şi câştigătoare.

În conţinutul cererii sale de intervenţie, ... invocă excepţia lipsei de interes a ... în formularea de critici faţă de oferta declarată câştigătoare.

În acest sens, intervenienta invocă prevederile art. 255 alin. (1) din OUG nr. 34/2006 şi afirmă că interesul unui ofertant respins de a contesta ofertele admisibile nu îndeplineşte cerinţa ca interesul să fie născut şi actual. Astfel, în măsura în care se va respinge oferta ...,

autoarea contestaţiei nu mai poate justifica un interes legitim, născut, actual şi direct pentru criticarea ofertei declarate câştigătoare.

În cazul societăţii contestatoare, culpa pentru nedepunerea unei oferte în conformitate cu documentaţia de atribuire aparţine exclusiv acesteia, astfel că, din această perspectivă, este evident că nu poate pretinde un interes legitim pentru a critica oferta declarată câştigătoare.

În analizarea îndeplinirii condiţiei interesului unui ofertant respins în a critica oferta declarată câştigătoare, Curtea de Apel Cluj, prin Decizia civilă nr. 6243 din 16 iulie 2012, a reţinut următoarele:

„Câtă vreme contestatoarea nu mai avea calitatea de participant la procedura de achiziţie publică, urmare a validării deciziei de respingere a ofertei sale, este evident că nu are nici interesul în a contesta desfăşurarea ei, instanţele de judecată nefiind chemate să se pronunţe cu privire la chestiuni teoretice, ci să rezolve un conflict deja născut, în care interesul petentei derivă din prejudiciul real şi concret la care s-ar expune dacă nu ar promova, în acel moment, demersul judiciar.

Astfel fiind, la momentul pronunţării Consiliului, nu se mai justifică solicitarea de verificare a caracterului inacceptabil/neconform al ofertei intervenientei. Nu se poate reţine că interesul intimatei ar ţine de posibilitatea anulării procedurii şi necesitatea demarării alteia, petenta şi intervenienta relevând corect că el nu este nici actual şi nici legitim.

În consecinţă, intervenienta arată corect că dacă oferta unui participant la procedură a fost respinsă de către autoritatea contractantă şi dacă această măsură a fost confirmată, de asemenea, de către Consiliu, atunci acelaşi ofertant nu mai poate justifica interesul, în sens procesual civil, pentru a învesti acelaşi Consiliu cu o cerere având ca obiect critici privind neconformitatea ofertei declarate câştigătoare sau, cum este cazul de faţă, anularea raportului procedurii de atribuire”.

În condiţiile în care interesul contestatoarei în cadrul procedurii de atribuire a contractului de achiziţie publică este constituit de folosul practic al adjudecării contractului, folos care, în raport de dispoziţiile art. 200 din OUG nr. 34/2006 şi cele ale art. 37 din HG nr. 925/2006, este imposibil de realizat prin depunerea unei oferte neconforme, iar în situaţia în care procedura de atribuire este delimitată strict ca fiind constituită din totalitatea demersurilor procedurale întreprinse în intervalul determinat de momentul iniţierii procedurii prin publicarea anunţului/invitaţiei de participare şi momentul finalizării acesteia, definit de art. 93 alin. (1) din HG nr. 925/2006, nu se poate reţine un eventual interes al ... într-o eventuală reevaluare a ofertei declarate câştigătoare din moment contestatoarea nu va mai avea calitatea de ofertant în cadrul procedurii în condiţiile respingerii definitive a ofertei acesteia.

Întrucât interesul trebuie să fie personal şi direct, în sensul că folosul practic trebuie să o vizeze pe contestatoare, ceea ce nu este cazul în procedura analizată, prin faptul că oferta contestatoarei este neconformă, dar şi născut şi actual – existent în cadrul procedurii derulate, ci nu eventual, trebuie să se constate lipsa de interes a ... în formularea criticilor referitoare la oferta Asocierii ...

În acelaşi sens s-a pronunţat inclusiv Curtea de Apel Constanţa - Secţia a II-a civilă, de contencios administrativ şi fiscal, în cuprinsul Deciziei civile nr. 152/CA din 24 aprilie 2013 reţinând următoarele:

„Având în vedere netemeinicia contestaţiei ofertantei referitoare la declararea ofertei sale ca inacceptabilă, nu se mai impune analizarea celorlalte critici formulate de aceasta referitoare la decizia prin care a fost declarată oferta câştigătoare, la legalitatea raportului procedurii şi a tuturor actelor subsecvente, întrucât motivele invocate de contestatoare nu îi asigură participarea la procedura de atribuire în curs, neînlăturând caracterul inacceptabil al ofertei sale astfel că nu sunt îndeplinite în cauză condiţiile prevăzute de art. 255 alin. (2) lit. a) şi b) din ordonanţă."

Pe fond, intervenienta solicită respingerea contestaţiei ca nefondată, având în vedere următoarele:

a) Aspecte privind legala respingere a ofertei societăţii contestatoare:

- În fapt, raportat la conţinutul documentaţiei de atribuire, autoritatea contractantă şi-a propus achiziţia următoarelor: Servicii de prelucrare arhivistica, inventariere si digitizare a documentelor;
- Servicii de arhivare electronica;
- Servicii de depozitare fizica a documentelor după prelucrarea arhivistica;
- Soluţie de gestiune a documentelor si a fluxurilor de lucru, cu serviciile de implementare aferente;
- Servicii de dezvoltare portal, inclusiv licenţele aferente;
- Servicii de certificare a semnăturii electronice, inclusiv dispozitive securizate de generare a semnăturii electronice;
- Soluţie de securizare a staţiilor de lucru, inclusiv licenţele aferente.

Elementele de neconformitate din contestaţie se referă la componentele descrise în caietul de sarcini prin:

- Modulul 7 - Componenta de Securizare Acces şi Documente, prin care se detaliază cerinţele tehnice pentru achiziţionarea a:
  - 300 de certificate digitale simple, stocate pe token-uri criptografice si/sau in format software pe dispozitive mobile;
  - O soluţie de autentificare la sistemul informatic integrat, rezultat al întregului proiect, bazată pe certificatele digitale ale utilizatorilor;
  - O soluţie de validare a certificatelor digitale care să implementeze funcţionalităţile unui OCSP Responder;
  - Aplicaţii pentru semnătura electronică: creare şi validare de semnături la nivel de staţie de lucru şi validare de semnături la nivel de server;
  - Aplicaţii pentru asigurarea confidenţialităţii documentelor, prin criptarea datelor şi ştergerea sigură a acestora (prin suprascriere);

- Modulul 8 - Modulul de arhivare a documentelor, prin care se detaliază cerinţele tehnice pentru achiziţionarea:
  - Componentei de Comunicare cu Arhiva Electronică Legală
  - Componentei de Arhiva Electronică Legală
  - Componentei de Depozitare Fizică

Pentru Modulul 7, din parcurgerea titlurilor subcapitolelor aferente acestuia, aşa cum sunt prezentate în cadrul Modificării 8, publicată în SEAP în data de 17.06.2014, reies clar componentele solicitate de autoritatea contractantă:

3.3.7. Modulul 7: Componenta de Securizare Acces şi Documente

3.3.7.1. Principii de securitate 3.3.7.2. Certificate digitale 3.3.7.3. Utilizarea certificatelor digitale 3.3.7.3.1. Autentificarea la sistem 3.3.7.3.2. Semnătura electronica

Verificarea semnăturii

Verificarea certificatelor

Verificarea documentelor

Asigurarea confidenţialităţii documentelor

Intervenienta afirmă că din conţinutul contestaţiei sunt de reţinut elementele care denotă neînţelegerea de către ofertantul ... a cerinţelor documentaţiei de atribuire, arătând în mod clar că oferta acestuia este neconformă în ceea ce priveşte îndeplinirea cerinţelor Modulului 7 şi Modulului 8 din caietul de sarcini.

1. Nu este clar care este rolul unei soluţii PKI (SafeLayer KeyONE) în cadrul ofertei tehnice, din moment ce nu s-a solicitat o astfel de soluţie, iar din contestaţie reiese că certificatele digitale solicitate în cadrul procedurii sunt furnizate de către Autoritatea de Certificare DigiSign: ”La paginile 285, 300, 302 şi 303, ofertantul precizează explicit furnizorul, Digisign, şi Autoritatea sub care sunt emise certificatele digitale - Root CA a Digisign”.

Introducerea unei soluţii PKI distincte în ofertă presupune că:

1. Autoritatea contractantă urmează să gestioneze singură certificatele digitale simple solicitate,

2. Pentru a putea emite certificate digitale simple, conform cerinţelor din documentaţia de atribuire, autoritatea contractantă trebuie să se declare ca furnizor de servicii de certificare şi să îndeplinească cerinţele definite prin Legea nr. 455/2001 privind semnătura electronică.

Niciunul dintre aceste lucruri nu au fost solicitate prin documentaţia de atribuire, cerinţele privind certificatele digitale fiind foarte clare:

”Se vor emite 300 de certificate digitale simple. Ofertanţii trebuie să prezinte următoarele informaţii despre furnizorul acestora:

- *denumirea acestuia,*
- *daca furnizorul este acreditat sau nu in conformitate cu Legea 455/2001,*
- *informatii referitoare la certificatul radacina sub care sunt emise certificatele digitale simple”.*

Utilizarea la implementarea proiectului a altor certificate digitale decât cele emise de o soluţie PKI care nu este a furnizorului DigiSign, sub Root CA Digisign, așa cum este indicat în oferta tehnică contravine cerinţelor minime ale autorităţii contractante şi este neconformă.

II. Nu rezultă în mod explicit care este soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) şi care trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional, prezentată în cadrul ofertei ...:

a. În situaţia în care este DigiSigner, aceasta nu deţine certificări de securitate, aşa cum reiese din cadrul contestaţiei;

b. În situaţia în care este soluţia PKI SafeLayer este necesar a fi precizat că SafeLayer KeyONE, respectiv componentele CA, XRA, VA şi Mobile PKI ofertate, nu deţin funcţionalităţi privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură), întrucât aceste componente au rolul de a asigura managementul certificatelor digitale, respectiv de emitere, revocare şi validare a acestora;

c. În situaţia în care este TrustedX, niciunul dintre produsele din ”familia” produse TrustedX prezente pe site-ul producatorului SafeLayer nu deţine capabilităţi de criptare/decriptare şi ştergere sigură a informaţiilor de pe staţiile de lucru.

Astfel, fie este propus un produs ce nu îndeplineşte cerinţele privind certificarea din punct de vedere al securităţii, respectiv DigiSigner, fie este propusă o soluţie tehnică ce nu îndeplinşte functionalităţi privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură), respectiv SafeLayer KeyONE sau TrustedX.

Prin urmare, reiese în mod evident că oferta tehnică nu este conformă cu privire la cerinţa *„Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional”.*

III. Având în vedere faptul că cerinţa a fost de certificare a soluţiei care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru, admiţând faptul că există o componentă ”client” – DigiSigner şi o componentă ”server” – TrustedX, nu se poate invoca exclusiv certificarea componentei de tip server pentru a justifica certificarea întregii soluţii, în condiţiile în care pe staţiile de lucru se instalează componenta ”client”, care nu deţine nicio certificare; certificarea nu se realizează pe o singură componentă a soluţiei, ci pe întreg sistemul integrat conţinând atât componentele server cât şi componentele client sau specificând precis care sunt cerinţele pe care trebuie să le îndeplinească o componentă client.

De pe site-ul DigiSign, al producătorului DigiSigner, din manualul de utilizare al aplicaţiei DigiSigner disponibil on-line la adresa https://www.

digisign.ro/uploads/Manual-de-utilizare-DigiSigner.pdf precum şi instalând aplicaţia DigiSigner disponibilă pentru descărcare la adresa https://www.digisign.ro/uploads/DigiSigner.zip reies următoarele:

1. Aplicaţia DigiSigner se instalează ca aplicaţie independentă, pe staţiile de lucru şi nu necesită instalarea unei componente server TrustedX,
2. Aplicaţia DigiSigner nu oferă funcţionalităţi de ştergere sigură a fişierelor, aşa cum reiese din funcţionalităţile descrise şi captura de ecran prezentă în manualul de utilizare, manual actualizat la data 16.10.2014, şi din captura de ecran a aplicaţiei descărcată de pe site-ul producătorului.

Astfel, este neverosimil că există o integrare între DigiSigner şi TrustedX. Mai mult, aplicaţia DigiSigner nu implementează funcţionalităţi de ştergere sigură a informaţiilor şi nu răspunde cerinţelor:

"informaţiile în clar trebuie să poată fi distruse prin rescriere cu date aleatoare utilizând algoritmi standard, recunoscuţi internaţional, minim cei enumeraţi respectiv:

- *în 7 paşi, conform specificaţiilor standardului 5220.22-M al DoD*
- *in 35 de paşi, conform specificaţiilor metodei Peter Gutman".*

Prin urmare, reiese din nou, în mod evident că oferta tehnică nu este conformă cu privire la cerinţele:

o *„Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional".*

o *„informaţiile în clar trebuie să poată fi distruse prin rescriere cu date aleatoare utilizând algoritmi standard, recunoscuţi internaţional, minim cei enumeraţi respectiv:*

- în 7 paşi, conform specificaţiilor standardului 5220.22-M al DoD

- în 35 de paşi, conform specificaţiilor metodei Peter Gutman".

IV. ... susţine că aplicaţia SafeLayer Mobile ID „nu este comercializat cu un model de versionare".

Intervenienta afirmă că este prima oară când ia cunoştinţă de existenţa unui producător reputat de software care publică aplicaţii fără un model de versionare, în condiţiile în care acelaşi producător deţine produse certificate EAL 4+, certificare care se aplică în mod explicit pentru versiunea produsului în configuraţia evaluată şi în conjuncţie cu raportul de certificare/validare. Prin urmare, caracterul afirmaţiei că aplicaţia SafeLayer Mobile ID „nu este comercializat cu un model de versionare" este cel puţin îndoielnic atâta vreme cât, cel puţin în App Store această aplicaţie (SafeLayer Mobile ID) este prezentă, cu versiunea 1.3.1.

Utilizatorii care accesează App Store pot vedea informaţii privind versiunea actuală şi istoricul versiunilor anterioare ale SafeLayer Mobile

ID, de la versiunea 1.0.0 publicată în februarie 2014 până la cea curentă, publicată în decembrie 2014. În acest moment, pentru toate aplicaţiile care sunt încărcate în App Store şi Google Play se solicită numele aplicaţiei, versiunea şi producătorul.

Astfel, prin contestaţia înaintată, ... furnizează autorităţii contractante informaţii false cu privire la lipsa versiunilor pentru aplicaţia SafeLayer Mobile ID.

De asemenea, deoarece autoarea contestaţiei susţine atât în contestaţie, cât şi în răspunsurile la întrebările de clarificare că aplicaţia indicată nu are o versiune, este evident că nu este îndeplinită cerinţa „Toate funcţionalităţile referitoare la utilizarea certificatelor digitale trebuie să fie implementate de către aplicaţii disponibile comercial la momentul ofertării. Interfaţa aplicaţiilor va fi cel puţin în limba română. În acest sens se vor ataşa ofertei manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul,..".

V. În contestaţia înaintată ... susţine că aplicaţia SafeLayer Mobile ID, este publicată în App Store şi Google Play. Cu toate acestea, căutând SafeLayer Mobile ID în Google Play nu a fost identificată această aplicaţie şi nici o altă aplicaţie publicată de SafeLayer.

Astfel, intervenienta învederează că prin contestaţia înaintată ... furnizează autorităţii contractante informaţii false cu privire la disponibilitatea SafeLaye Mobile ID în Google Play.

VI. Deşi în contestaţia ... aplicaţia SafeLayer Mobile ID este prezentată ca aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care poate genera aceste chei atât software cât şi hardware "pe un dispozitiv criptografic de tip smartcard, conectat la terminalul mobil", în propoziţia imediat următoare celei evidenţiate în primul chenar din captura de ecran de la pagina 13 din contestaţie, reiese faptul că aplicaţia SafeLayer Mobile ID "furnizează protecţie împotriva furtului de identitate fără a utiliza produse de autentificare adiţionale (matrix card, OTP device sau smart card)".

Prin urmare este neverosimilă conformitatea acestei aplicaţii cu specificaţiile solicitate, respectiv capabilitatea de a se integra cu dispozitive criptografice de tip smartcard (pentru generare de chei criptografice şi înscriere de certificate digitale pe acestea).

VII. Prin afirmaţiile făcute în contestaţie, în opinia intervenientei este evident faptul că ... nu deţine noţiunile termenilor de autentificare şi autorizare a unui utilizator într-un sistem informatic, invocând în acest sens faptul că definiţia dată autentificării în cadrul contestaţiei este complet eronată în contextul unui sistem informatic.

Astfel, definiţia reprodusă „Autentificarea reprezintă procesul prin care unui utilizator i se acordă un set unic de credenţiale (identificatori) care au rolul de a-l identifica în mod unic.." reprezintă, de fapt, definiţia identificării.

Componenta KeyONE XRA ofertată nu reprezintă o componentă de autentificare a utilizatorilor, ci este interfaţa de Autoritate de Inregistrare (RA - Registration Authority), interfaţă prin care sunt înregistraţi utilizatorii pentru emiterea certificatelor digitale – elementele de

identificare, a soluţiei PKI SafeLayer KeyONE, rezultând prin urmare că ..., din nepricepere sau din rea-intenţie, încearcă să inducă în eroare autoritatea contractantă.

De altfel componenta KeyONE XRA nu a fost solicitată şi nu se cunoaşte rolul ei în cadrul ofertei tehnice din moment ce, pe de-o parte, credenţialele de acces solicitate (cele 300 de certificate digitale) sunt emise de către Autoritatea de Certificare DigiSign, care are componenta de înregistrare a utilizatorilor disponibilă la adresa: https://secure.digisign.ro/portal/edit_cerere.php?tip=pf&__new.

Pe de altă parte autentificarea unui utilizator la un sistem informatic presupune ca acesta să deţină deja un set de credenţiale (în cazul de faţă a certificatului digital), sens în care procesul de identificare şi emitere a credenţialelor are loc a priori procesului de autentificare şi nu este necesar ca pentru fiecare acțiune de autentificare să fie emis un nou set de credențiale, certificate digitale, utilizatorului. Practic, folosirea KeyONE XRA nu este necesară în procesul de autentificare a utilizatorilor.

Astfel, folosirea KeyONE XRA ca soluţie tehnică prin care se răspunde la cerinţele privind autentificarea utilizatorilor nu este corectă deoarece KeyONE XRA nu oferă funcţionalităţi de autentificare, fapt pentru care oferta tehnică a ... nu este conformă cu cerinţele minime din caietul de sarcini.

VIII. Specificaţiile prevăzute în capitolul Asigurarea confidenţialităţii documentelor trebuie tratate în integralitatea lor, în sensul că aplicaţiile ofertate pentru asigurarea funcţionalităţilor de criptare trebuie să implementeze aceste funcţionalităţi prin mecanismele de criptare prevăzute în documentaţie. Astfel, inclusiv aplicaţia care realizează criptare ”La nivel de sistem de operare, prin crearea unei partiţii criptate” trebuie să răspundă cerinţelor:

”Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici şi asimetrici, astfel:

- *Criptarea asimetrică, utilizând certificatele X509v3 şi algoritmul RSA*
- *Criptarea simetrică folosind algoritmii 3DES şi AES*

.....

Certificatele care vor fi utilizate în procesul de criptare trebuie să fie disponibile local, pe staţia de lucru pe care se realizează criptarea, sau prin publicarea într-un serviciu de directoare standard LDAPv3. Criptarea va trebui să poată fi realizată pentru mai mulţi utilizatori simultan, iar pentru utilizatorul care a iniţiat procesul de criptare, documentul trebuie sa poată fi criptat în mod automat.

Certificatele necesare decriptării pot fi stocate atât pe smart card compatibil cu standardul PKCS #11cât şi în format software conform cu standardul PKCS#12”.

Prin urmare, aplicaţia BitLocker propusă de ..., disponibilă pentru sistemele de operare Microsoft Windows (Vista, 7, ediţiile Pro şi Enterprise ale Windows 8 si 8.1, Server 2008 şi ulterioare) nu poate reprezenta o soluţie de criptare la nivel de operare prin crearea unei partiţii criptate care respectă cerinţele autorităţii contractante, întrucât

BitLocker utilizează ca algoritm de criptare simetrică doar unul dintre algoritmii solicitaţi, respectiv AES, în conformitate cu informaţiile prezente pe site-ul oficial al producătorului Microsoft.

Totodată, este neclar care sunt aplicaţiile ofertate pentru îndeplinirea funcţionalităţilor prezentate în cadrul acestui subcapitol, atâta vreme cât tot din cadrul contestaţiei reiese că aceste functionalităţi ar fi îndeplinite de către aplicaţia DigiSigner, iar soluţia TrustedX nu îndeplineşte cerinţele. Trebuie menţionat, însă că în acest context, DigiSigner implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura), dar nu respectă cerinţa de a deţine certificări de securitate.

Prin urmare, reiese în mod evident că oferta tehnică nu este conformă deoarece aplicaţia BitLocker nu utilizează algoritmul 3DES, iar aplicaţia DigiSigner nu deţine o certificare din punct de vedere al securităţii informatice emisă de către un organism abilitat la nivel naţional, european sau internaţional.

IX. Prezentarea extraselor din procesul verbal întocmit în urma sesiunii demonstrative invocat la pagina 27/36 din contestaţie demonstrează:

- Că nu a fost ofertată o aplicaţie client, instalată pe terminalele mobile cu sistem de operare Android, care să răspundă la cerinţa *„utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil”*, deoarece afirmaţia din contestaţie *„3. Aplicaţia pentru generarea cheilor şi a cererilor de certificate este prezentă în Google Play/App store sau în alt store de aplicatii?*

Răspuns ofertant: Da, ofertantul a demonstrat că aplicaţia ofertată pentru generarea cheilor şi a cererilor de certificate este prezenta în App store. Pentru Android a fost prezentată versiunea de autentificare din browser.” arată doar faptul că a fost realizată o autentificare, nu şi că a fost prezentată aplicaţia care să realizeze generare a cheilor criptografice direct pe terminalul mobil cu sistem de operare Android.

- Că nu a fost ofertată o aplicaţie client, instalată pe terminalele mobile cu sistem de operare Android, care *„Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta”* deoarece afirmaţia din contestaţie *”5. Demonstraţia include utilizarea certificatelor digitale pe terminalele mobile stocate pe dispozitivul criptografic propriu, conectat la terminalul mobil?*

Răspuns ofertant: Da, a fost făcută o demonstraţie în cadrul sesiunii de prezentare a autentificării cu dispozitiv criptografic conectat la terminalul Android” arată doar faptul că a fost realizată o autentificare, nu şi că a fost prezentată aplicaţia care să realizeze înscrierea certificatului digital pe terminalul mobil cu sistem de operare Android.

- Că nu este îndeplinită cerinţa de blocare a accesului la informaţiile aflate pe partiţia criptat la deconectarea smartcard-ului, deoarece afirmaţia *”8. Sunt prezentaţi algoritmii criptografici utilizaţi pentru criptarea fişiere şi criptarea partiţii?*

Răspuns ofertant: Da. Ofertantul a făcut o demonstraţie pe fişiere criptate şi pe partiţii criptate" dovedește, că au fost prezentaţi „algoritmii criptografici folosiţi pentru criptare fişiere şi criptare partiţii", nereiesind care au fost aplicaţiile utilizate în cadrul demonstraţiei şi nici că aplicaţia BitLocker permite blocarea accesului la partiţiile criptate.

Prin urmare, reiese în mod evident că oferta tehnică nu este conformă cu privire la cerinţele:

- "Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta".
- "utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil".
- "Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată", iar ... prezintă informaţii care conduc la inducerea în eroare a autorităţii contractante.

De asemenea, în ceea ce priveşte criticile aduse ofertei Asocierii ..., intervenienta învederează că dispoziţiile imperative ale art. 36 alin. (1) din H.G. nr. 925/2006, cu modificările şi completările ulterioare, reglementează în mod expres şi limitativ situaţiile în care o ofertă poate fi respinsă ca inacceptabilă de către comisia de evaluare a ofertelor.

Cum niciunul dintre motivele de inacceptabilitate nu au fost inserate în cuprinsul contestaţiei, simplele afirmaţii ale societăţii contestatoare nu pot fi avute în vedere pentru a se putea analiza incidenţa, în cauză, a prevederilor art. 36 alin. (1) din H.G. nr. 925/2006, aspect pentru care intervenienta solicită respingerea ca nefondată a acestei critici

Același aspect trebuie avut în vedere şi cu privire la criticile contestatoarei referitoare la propunerea tehnică depusă de Asociere, prin care consideră că oferta acesteia trebuia respinsă ca neconformă.

Astfel, făcând referire la conţinutul documentaţiei de atribuire, autoarea contestaţiei afirmă că „Din cunoştinţele noastre, în acest moment niciunul dintre operatorii membrii în Asocierea declarată câştigătoare nu îndeplineşte condiţia de gestionare a etichetelor cu coduri de bare RFID Pasive. Acest lucru este cel mai probabil o consecinţă a faptului că până în acest moment nu au existat proceduri de achiziţie care să impună acest mod de lucru, tagurile RFID nefiind solicitate şi nici recomandate spre utilizare de către Arhivele Naţionale".

Totodată, referindu-se la cerinţa din documentaţia de atribuire privind fluxul operaţional monitorizat online inclusiv de perioada transportului, ... afirmă că „Şi în acest caz, din cunoştinţele noastre, companiile din Asocierea declarată câştigătoare nu oferă acest serviciu, aplicaţia pusă la dispoziţie pentru clienţi în vederea monitorizării permiţând vizualizarea anumitor evenimente (de exemplu, intrare şi ieşire din depozit), fără însă a monitoriza online cutiile cu documente pe perioada transportului, astfel încât să se poată observa uşor orice oprire neprogramată ce se poate transforma într-o posibilă breşă de securitate".

Faţă de cele susţinute în cuprinsul contestaţiei, intervenienta invocă prevederile art. 270 alin. (1) lit. e) şi f) din O.U.G. nr. 34/2006, şi afirmă

că la soluţionarea contestaţiei deduse judecăţii, societatea contestatoare nu a înţeles să evidenţieze în cuprinsul contestaţiei motivele de fapt pentru care consideră că oferta ... trebuia respinsă ca neconformă, și nici mijloacele de probă avute în vedere pentru a face dovada că propunerea tehnică a ... nu îndeplinește cerinţele minime din caietul de sarcini, iar simpla menţiune „din cunoştinţele noastre” nu poate corespunde unei motivări în fapt corespunzătoare.

În susţinerea celor de mai sus, intervenienta învederează cele reţinute de Curtea de Apel Bucureşti – Secţia a VIII-a contencios administrativ şi fiscal în cuprinsul Deciziei civile nr. 3770 din 26 septembrie 2013: *„În al doilea rând, după cum corect arată şi Consiliul, art. 270 din ordonanţă nu lasă la aprecierea contestatoarei posibilitatea de a indica motivarea în fapt şi în drept a cererii adresate Consiliului ci, dimpotrivă, îi impune o astfel de obligaţie procesuală, sub sancţiunea respingerii cererii. Totodată, nu se poate deduce din dispoziţiile ordonanţei că s-ar recunoaşte în favoarea petentei ce se pretinde vătămată un drept de sesizare a Consiliului cu o simplă cerere în anularea actului administrativ al autorităţii contractante fără ca petentul să cunoască la acel moment motivele în fapt şi în drept care îi susţin temeinicia pretenţiei sale, astfel încât cauza acţiunii declanşate să o identifice eventual după studierea dosarului achiziţiei în cadrul procedurii administrativ-jurisdicţionale. A porni de la premisa menţionată ar avea drept consecinţă deturnarea drepturilor procesuale recunoscute de legiuitor prin dispoziţiile art. 255 şi următoarele din ordonanţă, scopul lor nemaifiind protejarea împotriva vătămărilor produse de actele autorităţilor contractante, ci ar deveni legat de promovarea speranţei operatorului economic de a descoperi vreun/orice motiv pe care să îl pretindă împotriva actului care îl nemulţumeşte”.*

Prin urmare, în lumina celor mai sus arătate, lipsa unei motivări în fapt concrete din partea contestatoarei, nu poate duce decât la respingerea ca nefondate a criticilor aduse propunerii tehnice întocmită de către asocierea declarată câştigătoare.

În ceea ce priveşte afirmaţiile contestatoarei potrivit cărora „Precizăm că ne rezervăm dreptul de a completa prezenta contestaţie cu motive şi argumente referitoare la oferta Asocierii ... care vor reieşi din analizarea documentelor aflate la dosarul achiziţiei publice, la care urmează să ni se acorde accesul în conformitate cu dispoziţiile legale”, intervenienta menţionează că aceste afirmaţii, sunt incompatibile cu dispoziţiile legale privind completarea contestaţiei cu noi motive, în afara termenului de contestare. În susţinerea acestei afirmaţii trebuie avută în vedere Decizia nr. 6087 din 03 iunie 2013 a Curţii de Apel Alba Iulia din cuprinsul căreia intervenienta evidenţiază următoarele: *„(…) persoana vătămată trebuie să sesizeze Consiliul în termenul menţionat anterior, iar contestaţia trebuie să cuprindă, printre altele, motivarea în fapt şi în drept. Numai în situaţia în care contestaţia nu este completă, Consiliul are obligaţia de a-i solicita contestatorului completări (art. 270 alin. (2)). Or, în speţă, nu ne aflăm într-o astfel de situaţie. Aşadar, completarea*

contestaţiei cu noi motive, în afara termenului de contestare, este incompatibilă cu dispoziţiile legale".

În acelaşi sens s-a pronunţat şi Curtea de Apel Bacău care, prin Decizia nr. 2732 din 13 decembrie 2012 a reţinut următoarele: *„Potrivit dispoziţiilor art. 270 alin. (1) lit. e) din ordonanţă, contestaţia se formulează în scris şi trebuie să conţină motivarea în fapt şi în drept. Atât timp cât petenta, prin contestaţie, nu a invocat şi acest motiv, el fiind prezentat pentru prima oară în concluziile scrise şi în completarea intervenită după studierea dosarului, în mod corect Consiliul nu l-a luat în considerare.*

Partea care se consideră vătămată are dreptul, cu respectarea prevederilor art. 256 ind. 2, art. 270 şi 271 din ordonanţă, de a se adresa Consiliului în vederea soluţionării contestaţiei pe cale administrativ-jurisdicţională. Pentru ca şi acest motiv să fi putut fi analizat de către Consiliu, el trebuia expus în termenul prevăzut de legiuitor la art. 256 ind. 2 pentru depunerea contestaţiei, completarea contestaţiei cu noi motive în afara termenului legal de contestare a actului vătămător fiind incompatibilă cu dispoziţiile normative în vigoare în materia achiziţiilor publice".

În Decizia civilă nr. 3370 din 26 septembrie 2013, având de analizat o situaţie similară celei deduse judecăţii, Curtea de Apel Bucureşti – Secţia a VIII-a contencios administrativ şi fiscal a reţinut următoare aspecte legate de posibilitatea completării contestaţiei după studierea dosarului la CNSC: „Faţă de toate cele arătate mai sus, Curtea apreciază că este legală şi temeinică soluţia Consiliului în sensul de a nu se da loc la o judecată în ceea ce priveşte motivele noi expuse prin concluziile/notele scrise depune de petentă la 26.07.2013 şi 02.08.2013. În acest sens, Curtea reţine că partea contestatoare este limitată în dreptul său de a acţiona în faţa Consiliului de respectarea unui termen de 10 zile din ziua următoare luării la cunoştinţă despre un act al autorităţii contractante considerat nelegal, astfel cum indică art. 256 ind. 2 alin. (1) lit. a) din ordonanţă.

Ab inition, Curtea arată că în mod corect a făcut referire Consiliul la Hotărârea Curţii Europene de la Luxemburg din 11 octombrie 2007, pronunţată în Cauza C-241/06, Lammerzahl GmgH/Freie Hansestadt Bremen, prin care, la paragraful 50, s-a statuat că <trebuie amintit faptul că Directiva 89/665 nu se opune unei reglementări naţionale care prevede că orice cale de atac împotriva unei decizii a autorităţii contractante trebuie formulată într-un termen prevăzut în acest scop şi că orice neregularitate a procedurii de atribuire invocată în sprijinul acestei căi de atac trebuie invocată în acelaşi termen, sub sancţiunea decăderii, astfel încât, după împlinirea acestui termen, nu mai este posibil să se conteste o astfel de decizie sau să se invoce o astfel de neregularitate, în măsura în care termenul respectiv este rezonabil (Hotărârea din 12 decembrie 2002, Universale-Bau şi alţii, C-470/99)>.

Pe cale de consecinţă, prevederea prin norma juridică internă a unui termen rezonabil în care partea interesată să fie obligată să conteste un

act al autorităţii contractante, sub sancţiunea decăderii, nu contravine dreptului Uniunii Europene.

În acest context, faţă de limitarea temporală instituită de art. 256 ind. 2 alin. (1) din ordonanţă, nu se poate recunoaşte în beneficiul petentei vreun drept de a sesiza Consiliul oricând, la propria sa apreciere subiectivă, cu privire la criticile în privinţa actului pretins vătămător emanat de la autoritatea contractantă".

De altfel, jurisprudenţa este unitară în acest sens, fiind inadmisibilă completarea contestaţiei cu motive noi ulterior termenului legal reglementat pentru depunerea acesteia.

Autoritatea contractantă a transmis documentele necesare soluţionării contestaţiei precum şi punctul său de vedere nr. 14599/03.04.2015, înregistrat la Consiliu cu nr. 4939 din 03.04.2015, în care menţionează că motivul respingerii ofertei îl reprezintă neconformitatea tehnică, incapacitatea ofertantului de a prezenta şi susţine o ofertă care să îndeplinească cerinţele documentaţiei de atribuire şi completarea ofertei cu informaţii suplimentare transmise prin răspunsurile la întrebările de clarificare. Prin răspunsurile la întrebările de clarificare ofertantul face inclusiv declaraţii eronate.

Din expunerea de motive pe care o supune atenţiei, autoritatea contractantă precizează că se desprind următoarele concluzii generale:

- Oferta depusă nu este conformă în raport cu cerinţele documentaţiei de atribuire,
- Faţă de oferta tehnică depusă iniţial, contestatoarea a adus prin răspunsurile la întrebările de clarificare o serie de completări ce sunt detaliate pe larg în expunerea de motive de mai jos ;
- Prin răspunsurile la întrebările de clarificare contestatoarea nu a clarificat aspectele solicitate de autoritatea contractantă,
- Contestatoarea face o serie de afirmaţii şi declaraţii neadevărate cu scopul de a induce în eroare autoritatea contractantă,
- Prin oferta depusă, contestatoarea dovedeşte necunoaşterea domeniului, amestecând produse cu tehnologii, concepte cu aplicaţii;
- Deşi autoritatea contractantă a formulat întrebările de clarificare concis şi clar, strict în raport cu prevederile documentaţiei de atribuire, ofertantul a evitat să răspundă la obiect sau, după caz, a prezentat prin răspunsurile sale elemente vădit neadevărate.
- Deşi intră în atribuţia ofertantului realizarea şi prezentarea unei oferte tehnice integrate prin care să explice cum înţelege să răspundă cerinţelor documentaţiei de atribuire acesta a înţeles să prezinte un amalgam de soluţii, produse şi concepte fără o arhitectură tehnică, sau să furnizeze, ca soluţii pentru nevoile expuse de caietul de sarcina, nume de pachete de aplicaţii, a căror utilitate urma să fie descoperită de autoritatea contractantă, incluzând aici tehnologii extrem de complexe şi funcţionalităţi care pot fi înţelese numai în urma unui studiu relativ îndelungat şi de specialitate (un exemplu ar fi certificarea interconectării între aplicaţii produse de furnizori diferiţi (Microsoft, SafeLayer, etc).

În ceea ce priveşte motivul I, prezentat ca „Aspecte relevante privind procedura publică organizată de MFE pentru atribuirea contractului de achiziţie publică furnizare „Servicii de arhivare fizică și servicii de arhivare electronică a documentelor elaborate/gestionate în cadrul Ministerului Fondurilor Europene”, autoritatea contractantă nu înţelege relevanţa expunerii acestor aspecte, atâta vreme cât procedura de atribuire a respectat întru totul cadrul legal de desfăşurare a achiziţiilor publice.

Astfel, autoritatea contractantă consideră că întreaga pledoarie prezentată în cadrul motivului I este nerelevantă din punct de vedere a motivelor de declarare a ofertei contestatarei ca necâștigătoare.

Prin Decizia nr. ..../.../...,...,...,...,.../ .... Consiliul a dispus eliminarea cerinţelor restrictive ale documentaţiei de atribuire. Autoritatea contractantă a pus în aplicare această decizie, prin revizuirea caietului de sarcini şi publicarea Modificării nr. 8, emisă în data 17.06.2014. După publicarea modificării, dacă orice operator economic interesat de prezenta procedură se simţea discriminat şi considera că cerinţele sunt în continuare restrictive avea posibilitatea să conteste din nou Modificare nr. 8.

Atacarea modului de derulare a procedurii de achiziţie este tardivă, iar aspectele expuse în motivul 1 nu au drept scop decât punerea într-o lumină negativă a demersului autorităţii contractante de a-şi eficientiza activitatea prin implementarea unui sistem informatic complet funcţional şi integrat în vederea arhivării şi gestionării documentelor existente în cadrul Ministerului Fondurilor Europene, urmare a unei proceduri de achiziţie publică derulate corect, legal şi transparent la care contestatoarea a depus ofertă, asumându-şi astfel documentaţia de atribuire, în integralitatea ei.

În urma evaluării ofertelor, Comisia de evaluare a declarat oferta depusă de către ... ca fiind necâștigătoare, ca urmare a constatării elementelor de neconformitate având în vedere prevederile art. 36 alin. (2) lit. a) din HG nr. 925/2006, cu modificările şi completările ulterioare. Aceste aspecte, însoţite de motivele de respingere a ofertei explicate pe larg, au fost comunicate ofertantului ... prin adresa nr. 13760/16.03.2015.

În ceea ce priveşte legalitatea respingerii ofertei ..., autoritatea contractantă explică în continuare argumentele care au stat la baza acestei decizii.

II. În ceea ce priveşte certificarea din punct de vedere al securităţii informatice a soluţiei care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura) (motivul 1 de neconformitate), cerinţa este prevăzută în cadrul capitolului 3.3.7.1. Principii de securitate, şi este enunţată astfel:

Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura) trebuie să fie certificată din punct de vedere al securităţii

informatice de către un organism abilitat la nivel naţional, european sau internaţional.

Cerinţelor pentru *funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura)* sunt detaliate în capitolul 3.3.7.3. *Utilizarea certificatelor digitale astfel:*

- Pentru semnătură electronică în capitolul 3.3.7.3.2. Semnătura electronică, cu precizarea *"Semnătura electronică se va aplica prin aplicaţii specializate, instalate pe staţiile de lucru ale utilizatorilor […]"*
- Pentru criptare/decriptare şi ştergere sigură în secţiunea *Criptarea documentelor*

Astfel, cerinţa privind certificarea "din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional" se referă în mod clar la aplicaţiile cu funcţionalităţile descrise în capitolul 3.3.7.3.2. Semnătura electronică şi în secţiunea Criptarea documentelor din capitolul 3.3.7.3. Utilizarea certificatelor digitale.

În oferta tehnică a contestatoarei, la pagina 292, în vederea demonstrării conformităţii cu cerinţa privind certificarea "din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional" ofertantul precizează următoarele:

„Soluţia SafeLayer PKI platform implementează funcţionalităţile tehnologiei TrustedX privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura). Această soluţie este certificată din punct de vedere al securităţii informatice de către un organism internaţional.

https://www.commoncriteriaportal.org/ccra/

http://www.safelayer.com/en/about-safelayer/press-releases/150-authentication-electronic-signature-and-encryption-functions-are-included-in-the-one-platform-with-the-maximum-security-guarantees".

Prin urmare, ofertantul indică, fără echivoc, că aplicaţiile Safelayer îndeplinesc cerinţa privind certificarea *"din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional",* fără a face nicio referire la aplicaţia DigiSigner sau la o posibilă integrare dintre acestea.

În matricea de conformitate, pentru demonstrarea îndeplinirii cerinţelor aplicaţiilor care realizează semnare, criptare/decriptare, ştergere sigură, la paginile 312-314 şi 319-321 este descrisă aplicaţia DigiSign.

Astfel, în matricea de conformitate ofertantul prezintă, în mod clar, că cerinţele funcţionale care ţin de semnare, criptare/decriptare, ştergere sigură sunt îndeplinite de aplicaţia DigiSigner, fără a face nicio referire la aplicaţiile Safelayer sau la o posibilă integrare dintre acestea. De asemenea, sunt anexate ofertei tehnice:

- Documentaţia aferentă aplicaţiei Digisigner la paginile 386-388. Documentul descrie exclusiv funcţionalităţile privind semnare, verificare a semnăturilor, criptare, decriptare şi ştergere sigură ale aplicaţiei

Digisigner fără să facă referire la produsele Safelayer şi o eventuală integrare şi nici la deţinerea unei certificări din punct de vedere al securităţii informatice eliberata de către un organism abilitat la nivel naţional, european sau internaţional.

- Documentaţia aferentă produselor Safelayer, unde nu se prezintă integrarea cu aplicaţia Digisigner şi nici modalitatea de îndeplinire a cerinţelor din capitolul 3.3.7.3.2. Semnătura electronică şi din secţiunea Criptarea documentelor din documentaţia de atribuire.
    - KeyOne Certification Authority: paginile 447 – 448
    - Mobile PKI Speaker – Date: paginile 449 – 469
    - KeyOne Registration Authority: paginile 470 – 471
    - TrustedX Adaptive Authentication: paginile 472-473
    - KeyOne Validation Authority: paginile 474 – 475
    - KeyOne Autoritate de Certificare: paginile 476 – 477
    - SOLUTII MOBILE PKI: paginile 478 – 501
    - Autoritatea de Inregistrare KeyOne: paginile 503 – 504
    - Autentificare Adaptiva TrustedX: paginile 505 – 506
    - Autoritatea de Validare KeyOne: paginile 507 – 508

Paginile din oferta tehnică care prezintă documentaţia produselor Safelayer se regăsesc în anexele acestui document.

Este evident faptul că, în oferta tehnică, ofertantul a propus o soluţie incompletă şi neconformă:

- Cerinţa privind certificarea de securitate este îndeplinită de aplicaţiile Safelayer pentru care nu se demonstrează îndeplinirea funcţionalităţilor privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura).
- Cerinţele privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura) sunt îndeplinite de aplicaţia Digisigner pentru care, însă, nu este demonstrată certificarea din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional.
- Oferta tehnică nu descrie eventuala integrare dintre produsele Safelayer şi Digisigner.

Astfel, analizând cele precizate de către contestatoare în oferta tehnică precum şi datele publice existente pe site-ul producătorului SafeLayer s-au constatat următoarele:

- soluţia PKI SafeLayer reprezintă o soluţie de management a certificatelor digitale (respectiv înregistrarea, emiterea, revocarea, publicarea, validarea certificatelor digitale). Aceasta soluţie NU se instalează pe staţiile de lucru şi nu implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura). De altfel soluţia PKI SafeLayer nu face altceva decât să realizeze managementul certificatelor digitale, pe toată perioada de viaţă a unui astfel de element de identificare, şi are componente (conform paginii oficiale http://www.safelayer.com/en/products/keyone-pki-platform, tab-ul Components.
- În cadrul paragrafelor din oferta tehnică ce descriu soluţiile de semnare (pag. 312), criptare/decriptare, ştergere sigură (pag 319-321)

care se instalează pe staţiile de lucru, este prezentată soluţia DigiSigner, pentru care nu reiese din oferta că este certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional. Prin urmare a fost adresată contestatoarei următoarea întrebare de clarificare, prin adresa nr.3600/14.10.2014:

„23. Având în vedere cerinţa: «Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional» precum şi informaţiile prezentate în oferta dvs. la paginile 292, 312, 319-321 s-au constatat următoarele:

- soluţia PKI SafeLayer reprezintă o soluţie de management a certificatelor digitale şi nu implementează funcţionalităţile de semnare, criptare/decriptare, ştergere sigură a fişierelor

- în cadrul paragrafelor care descriu soluţiile de semnare (pag. 312), criptare/decriptare, ştergere sigură (pag 319-321) care se instalează pe staţiile de lucru, este prezentată soluţia DigiSigner pentru care nu reiese din ofertă că este certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional, vă rugăm să specificaţi unde anume în propunerea tehnică, prin precizarea exactă a paragrafului şi paginii, se găseşte descrierea cu privire la îndeplinirea cerinţei”.

Faţă de această întrebare, contestatoarea a formulat următorul răspuns:

„Referitor la solicitarea dumneavoastră privind modul de îndeplinire a cerinţei:

Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificată din punct de vedere al securităţii informaţiei de către un organism abilitat la nivel naţional, european sau internaţional.

Precizăm că platforma PKI SafeLayer KeyOne este certificată ISO/IEC 15408 EAL4+iar acesta implementrază funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură prin intermediul tehnologiei TrustedX şi a componentei client – DigiSigner, aşa cum a fost prezentat în clar în ofertă la pagina 292, paragraful 2

Menţionăm că răspunsurile ofertantului la solicitarea de clarificare nu aduc modificări ofertei înainte ci doar clarifică aspectele solicitate”.

Analizând acest răspuns al contestatoarei se pot constata două aspecte:

a. Contestatoarea susţine că aspectele menţionate au fost prezentate în clar în ofertă la pagina 292, paragraful 2, afirmaţie evident falsă, întrucât în pagina respectivă nu apare menţiunea că funcţionalităţile solicitate ar fi implementate printr-o ”componentă client” şi nici eventualul nume al acestei componente client, adică ”DigiSigner”. Contestatoarea face o afirmaţie eronată, încercând să inducă în eroare autoritatea contractantă.

b. Contestatoarea introduce în cadrul răspunsului aferent certificării soluției care implementează aceste funcționalități o nouă ”componentă client” a platformei PKI SafeLayer KeyOne– DigiSigner. Nu este prezentata nicio referire la oferta tehnică prin care să se ateste integrarea ”componentei client” DigiSigner cu componenta server SafeLayer PKI, cu atât mai mult cu cat cele două aplicații sunt realizate de producători diferiți: SafeLayer si Digisign. Este de remarcat totodată ca în paginile în care este descrisa aplicația DigiSigner ca aplicație pentru semnare, criptare/decriptare, stergere sigura, adică 312-314 şi 319-321, precum și în documentația aplicație DigiSigner de la paginile 386-388 nu există nici-o referire la faptul că DigiSigner ar fi ”componenta client” a soluției PKI SafeLayer KeyOne. De asemenea, nici în documentația produselor Safelayer de la paginile 447-508, în care pagina 502 este pagină albă, nu se prezintă integrarea aplicațiilor Safelayer cu aplicația DigiSigner și nici nu se demonstrează îndeplinirea funcționalităților privind utilizarea certificatelor digitale pe statiile de lucru (semnare, criptare/decriptare, stergere sigura).

Prin răspunsul la o întrebare precisă, punctuală, a comisiei, contestatoarea:

- nu indică în cadrul propunerii tehnice paragraful şi pagina care să arate că aplicaţia DigiSigner, care îndeplineşte cerinţele descrise în capitolul 3.3.7.3.2. Semnătura electronică şi în secţiunea Criptarea documentelor, este certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional.
- aduce completări ofertei tehnice înaintată prezentând aplicaţia DigiSigner ca o componentă client a PKI SafeLayer KeyOne.

Urmare a ambiguităţii, comisia a adresat o nouă solicitare de clarificare, cu nr. .../DAPITA 4498/03.03.2015, prin răspunsul înregistrat cu nr. .../DAPITA 4598/06.03.2015, *„La pagina 292 se menţionează tehnologia TrustedX, nu şi produsul software Digisigner. În răspunsul dumneavoastră, aţi menţionat faptul că platforma PKI SafeLayer KeyOne este certificată ISO/IEC 15408 EAL4+, însă, în continuare, aţi mai menţionat şi produsul Digisigner, despre care nu aţi prezentat nicio informaţie referitoare la certificarea din punct de vedere al securităţii informatice. În acest caz, vă rugăm încă o dată să precizaţi unde anume în ofertă este prezentată o referinţă către certificarea produsului Digisigner.”*, la care contestatoarea a formulat următorul răspuns:

„3. Sistemul de securitate ofertat conform cerinţelor din documentaţia de atribuire, printre care este solicitat ca „Soluţia care implementează funcţionălităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional”. Astfel, în conformitate cu răspunsul la întrebarea nr. 23 din cadrul solicitării de clarificări nr. 3600/14.10.2014, DigiSigner interferează serviciul TrustedX, integrat la nivelul librăriilor criptografice utilizate, care execută operaţiunile solicitate de autoritatea contractantă prin tehnologia

TrustedX, ca subcomponentă a platformei SafeLayer, respectiv soluţia care implementează funcţionalităţile privind utilizarea certificatelor degitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) şi care este certificată ISO/IEC 15408 EAL4+ din punct de vedere al securităţii informatice, certificare prezentată la pag. 292 a ofertei tehnice.

De exemplu, o soluţie software care deţine o certificare din punct de vedere al securităţii informatice, poate fi apelată/integrată/interferată sau interogată de orice aplicaţie prin standarde de comunicare Web Service, acesta fiind şi situaţia browserelor web (Mozilla Firefox, Google Chrome, Internet Explorer etc) prin care se apelează funcţii ale unei soluţii certificate.

Din nou, la întrebarea precisă a comisiei *„vă rugăm încă o data să precizaţi unde anume în ofertă este prezentată o referinţă către certificarea produsului Digisigner”*, contestatoarea nu răspunde şi continuă să aducă alte completări ofertei tehnice înaintată.

Astfel, în opinia contestatoarei, dacă o aplicaţie 3rd party (DigiSigner) care se instalează pe staţii de lucru apelează funcționalităţi ale unei platforme certificate instalată pe un server (SafeLayer) prin intermediul unei platforme/tehnologii/produs/server (TrustedX) rezultă că întreaga soluţie deţine certificarea, afirmaţie, evident, eronată.

Ca argumentare a celor susţinute anterior, autoritatea contractantă prezintă spre exemplu, un extras din pagina publică a site-ului http://www.commoncriteriaportal.org/, site la care face referire inclusiv contestatoarea în oferta sa şi în care se pot distinge în mod evident categoriile de produse şi soluţii ce sunt certificate în raport cu standardul ISO 15408 (Criterii de evaluare pentru securitatea IT).

Se pot distinge, astfel, cu uşurinţă categoriile de produse ce fac obiectul certificării din care sunt menţionate cele mai importante:

- Protecţia Datelor - 62 de produse certificate
- Baze de Date – 29 de produse certificate
- Sisteme de management ale cheilor – 29 de produse certificate
- Alte sisteme si echipamente – 274 de produse certificate
- Produse pentru semnarea electronică – 83 de produse certificate.

În acest fel, urmărind logica contestatoarei prin care un produs care se integrează cu un alt produs certificat, înseamnă că este şi el certificat, înseamnă că orice produs/aplicaţie care se integrează de exemplu cu un sistem de operare certificat (cum ar fi Microsoft Windows Vista ce deţine CC EAL 1) este şi el certificat. Pe cale de consecinţă, un virus sau un program malware ce în mod evident rulează pe un sistem de operare va fi şi el certificat din punct de vedere al securităţii, aspect evident neadevărat. Se observă astfel confuzia gravă în care este contestatoarea precum şi lipsa dovezilor tehnice care să vină în justificarea argumentelor sale.

Din exemplul de mai sus, se poate distinge, în mod evident, că aceste certificări de securitate se acordă în funcţie de tipul produsului şi elementele de securitate pe care acesta le deţine, precum şi în raport cu o versiune precisă şi o configuraţie clară. Nicăieri, în cadrul site-ului de

mai sus nu este menţionat produsul Digisigner, cum nu este menţionat nici în oferta tehnică, la paragraful în care contestatoarea a prezentat îndeplinirea cerinţei.

Prin urmare, din oferta tehnică înaintată şi răspunsurile la cele două întrebări de clarificare, autoritatea contractantă a reţinut:

1. Cerinţa privind certificarea de securitate: pentru aplicaţiile Safelayer ofertate la acest capitol nu se demonstrează îndeplinirea funcţionalităţilor privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura).

2. Cerinţele privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura) sunt îndeplinite de aplicaţia Digisigner pentru care, însă, nu este demonstrată certificarea din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional.

3. Oferta tehnică nu descrie eventuala integrare dintre produsele Safelayer şi Digisigner

4. Răspunsurile la întrebările de clarificare aduc completări ofertei tehnice depusă iniţial.

Astfel, contestatoarea nu a demonstrat îndeplinirea cerinţei privind certificarea din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional a aplicaţiei Digisigner, ofertată pentru utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură şi din acest motiv oferta tehnică înaintată a fost considerată neconformă.

În cadrul contestaţiei înregistrată cu numărul 5098/27.03.2015 contestatoarea susţine, de asemenea, că DigiSigner ”este doar o aplicație, o componentă utilizată la nivel de client de staţiile de lucru pentru a apela funcționalitățile disponibile la nivelul soluţiei SafeLayer PKI”, fără să mai facă trimitere la platforma/tehnologia/produsul/ serverul TrustedX, ci la faptul că ”tehnologia pe care se bazează SafeLayer PKI este integrată la nivelul librăriilor criptografice accesate cu componenta Digisigner, aceasta din urma acţionând ca o interfaţă pentru soluţia SafeLayer PKI propusă”.

Contradicţiile sunt evidente întrucât, în cadrul aceluiaşi paragraf sunt precizate următoarele:

”[…] răspunsurile noastre [...] unde se regăseşte certificarea solicitată cu privire la soluţia SafeLayer PKI [...] şi asupra modului în care soluţia SafeLayer PKI acţionează ca o interfaţă pentru componenta Digisigner.” Rezultă faptul că nici la momentul contestaţiei nu este clar pentru contestatoare relaţia dintre elementele ofertate şi rolul lor în asigurarea funcţionalităţilor solicitate prin documentaţia de atribuire.

Totodată în cadrul contestației este ofertat un nou produs al companiei SafeLayer, respectiv ”TrustedX Electric Signature”, conform paragrafului de mai jos:

Afirmaţia c): „TrustedX nu are nicio legătură cu funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură” – Afirmaţia este falsă, iar captura de ecran prezentată de autoritatea contractantă nu este menită decât să inducă în eroare în mod grosolan. Captura în cauză nu are cum

să ilustreze funcţinalităţile enunţate, pentru că ea prezintă funcţionalitatea de autentificare a TrustedX, oferită prin intermediul platformei TrustedX Authentication Platform, însă subscrisa nu ne-am referit la această funcţionalitate şi nu am invocat capabilităţile acestei platforme. Funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură oferite de TrustedX pot fi dovedite prin accesarea site-ului web al producătorului, secţiunea „TrustedX Electric Signature" sens în care prezentăm cu titlu ilustrativ următoarea captură de ecran:

Autoritatea contractantă susţine că a constatat că acest produs este unul distinct, aşa cum reiese din captura de ecran următoare care prezintă lista a 5 produse SafeLayer care conţin denumirea TrustedX:

- TrustedX eIDAS Platform
- TrustedX Authentication Platform
- TrustedX Electronic Signature
- TrustedX Encryption Key Management

În oferta tehnică înaintată a fost inclus numai produsul TrustedX Adaptive Authentication/ Autentificare Adaptiva TrustedX, aşa cum reiese din:

- Enumerarea produselor SafeLayer livrate, la pagina 287 a ofertei tehnice

  "Sistemul este produs de compania SafeLayer platforma livrată fiind compusă din:
  - TrustedX Adaptive Authentication
  - KeyOne Certification Authority
  - KeyOne Registration Authority
  - KeyOne Validation Authority
  - Mobile PKI"
- Documentaţia produselor Safelayer de la paginile 447-508, în care pagina 502 este pagină albă include:
  - KeyOne Certification Authority: paginile 447 – 448
  - Mobile PKI Speaker – Date: paginile 449 – 469
  - KeyOne Registration Authority: paginile 470 – 471
  - TrustedX Adaptive Authentication: paginile 472-473
  - KeyOne Validation Authority: paginile 474 – 475
  - KeyOne Autoritate de Certificare: paginile 476 – 477
  - SOLUŢII MOBILE PKI: paginile 478 – 501
  - Autoritatea de Inregistrare KeyOne: paginile 503 – 504
  - Autentificare Adaptiva TrustedX: paginile 505 – 506
  - Autoritatea de Validare KeyOne: paginile 507 – 508

Totodată, autoritatea contractantă consideră că este necesar de precizat faptul că:

1) Produsul TrustedX Electronic Signature nu a fost inclus în oferta tehnică fiind menţionat exclusiv în prezenta contestaţie şi reprezintă completare a ofertei înaintate. Pentru produsul TrustedX Electronic Signature nu au fost incluse în ofertă manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul şi prin care să demonstreze îndeplinirea cerinţei din documentaţia de atribuire "Toate funcţionalităţile referitoare la utilizarea certificatelor

digitale trebuie să fie implementate de către aplicaţii disponibile comercial la momentul ofertării. Interfaţa aplicaţiilor va fi cel puţin în limba română. În acest sens se vor ataşa ofertei manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul, precum şi orice alte documente care să vină în susţinerea conformităţii cu specificaţiile solicitate";

2) În pagina producătorului nu se regăsesc informaţii cu privire la capabilitatea TrustedX Electronic Signature de a cripta/decripta documente sau de a asigura ştergerea sigură a acestora.

3) Afirmaţia „*Mai mult decât atât, în aceeaşi pagină web, dar de altfel şi în oferta tehnică la pag 290 este prezentată tehnologia TrustedX în cadrul unei arhitecturi posibile şi este specificat faptul că funcţionalităţile TrustedX pot fi accesate (utilizate) fie prin interfaţa web (ca web service), fie în interfaţă cu diverse aplicaţii (cum este aplicaţia Digisigner) fie prin combinaţia dintre aceste două metode*" este complet falsă întrucât în oferta tehnică la pagina 290 este prezentată o arhitectură în care produsul TrustedX Authentication Platform poate fi utilizat pentru "verificarea suplimentară a identităţii utilizatorului" şi nu pentru semnare, criptare/decriptare, ştergere sigura, aşa cum reiese din captura de ecran de mai jos. Arhitectura este preluată din documentaţia tehnică a produsului TrustedX Adaptive Authentication, prezentă şi în ofertă la pagina 473.

Aşa cum s-a menţionat anterior, produsul TrustedX Authentication Platform este diferit de produsul TrustedX Electronic Signature, pentru care este prezentat în cadrul contestaţiei exemplul de arhitectură disponibil pe site-ul producătorului SafeLayer la adresa www.safelayer.com/en/trustedx-electronic-signature.

Contestatoarea continuă să modifice şi prin contestaţie oferta tehnică înaintată, introducând produse noi, cu scopul de a induce în eroare atât Consiliul cât şi autoritatea contractantă.

Totodată se arată că prin argumentaţia adusă, contestatoarea pe de o parte, nu îşi cunoaşte propria ofertă, şi pe de altă parte nu are cunoştinţele minime raportate la cerinţele din documentaţia de atribuire.

În concluzie, autoritatea contractantă învederează că:

1. Cerinţa privind certificarea de securitate este îndeplinită de aplicaţiile Safelayer pentru care nu se demonstrează în oferta tehnică depusă îndeplinirea funcţionalităţilor privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura). Aplicaţiile Safelayer ofertate sunt aplicaţii de tip server, care nu implementează funcţionalităţile solicitate pe staţiile de lucru ale utilizatorilor.

2. În cadrul răspunsurilor la întrebările de clarificare cerinţele privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura) sunt îndeplinite de aplicaţia Digisigner, astfel producându-se o modificare a ofertei, dar, chiar şi în aceste condiţii, nu este demonstrată certificarea din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional pentru acest produs.

3. Oferta tehnică nu descrie eventuala integrare dintre produsele Safelayer şi Digisigner, făcând din soluţia propusă una care nu respectă condiţia de a fi matură.

4. Răspunsurile la solicitările de clarificare aduc completări ofertei tehnice depuse

5. Argumentele din contestaţie modifică oferta tehnică depusă prin introducerea în arhitectură a unui produs nou, TrustedX Electronic Signature. Produsul TrustedX Electronic Signature nu a fost inclus în ofertă tehnică fiind menţionat exclusiv în prezenta contestaţie şi reprezintă completare a ofertei înaintate. Pentru produsul TrustedX Electronic Signature nu au fost incluse în ofertă manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul şi prin care să demonstreze îndeplinirea cerinţei din documentaţia de atribuire ”Toate funcţionalităţile referitoare la utilizarea certificatelor digitale trebuie să fie implementate de către aplicaţii disponibile comercial la momentul ofertării. Interfaţa aplicaţiilor va fi cel puţin în limba română. În acest sens se vor ataşa ofertei manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul, precum şi orice alte documente care să vină în susţinerea conformităţii cu specificaţiile solicitate”.

Având în vedere motivele enumerate mai sus, autoritatea contractantă susţine că oferta tehnică înaintată este neconformă.

II. În ceea ce priveşte aplicaţia de generare a cheilor criptografice direct pe telefonul mobil (motivul 2 de neconformitate), autoritatea contractantă menţionează că cerinţa este prevăzută în cadrul capitolului 3.3.7.2 Certificate digitale, şi este enunţată astfel:

În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele:

- Să realizeze şi să transmită către furnizorul de servicii de certificare cererea standard PKCS#10 necesară procesului de emitere a certificatului digital
- Perechea de chei (publica/privată) vor fi generate:
  - Software, direct pe dispozitivul mobil
  - Pe un dispozitiv criptografic de tip smartcard, conectat la terminalul mobil
- Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta.

Autoritatea contractantă susţine că în oferta tehnică a contestatoarei, la pagina 305, se precizează următoarele:

„În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele digitale simple emise de către Autoritatea de Certificare DigiSign pot fi stocate în format .p12[35] pe terminale mobile de tip smartphone sau tabletă.

Referinţe:

[35]*Broşur_CDS_DigiSign.pdf*

Prin Intermediul aplicaţiei Mobile PKI ce lucrează în tandem cu KeyOne Certificate Authority şi KeyOne Registration Authority se realizează generarea de chei atât pe terminalul mobil cât şi pe dispozitive criptografice de tip smartcard".

Urmare a analizei ofertei tehnice s-au constatat următoarele:

- Nu se regăseşte în ofertă versiunea de produs ofertată pentru această aplicaţie
- Link-ul http://www.safelayer.com/en/solutions/mobile-pki redirecţionează navigarea către o altă pagina, http://www.safelayer.com/en/solutions/ mobile-identification în care se prezintă conceptul de utilizare, neidentificând în mod clar aplicaţia ofertată
- Nu se regăseşte modalitatea de îndeplinire a cerinţei de „generare a cheilor criptografice direct pe terminalul mobil".

Având în vedere cele precizate anterior, autoritatea contractantă susţine că i-a adresat contestatoarei următoarea întrebare de clarificare.

24. Având în vedere cerinţa:

„În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphon sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele" (...)

Precum şi informaţiile prezentate în oferta dvs. la pag. 305 s-au constatat următoarele:

- Nu se regăseşte în ofertă versiunea de produs ofertată pentru această aplicaţie
- Link-ul http://www.safelayer.com/en/solutions/mobile-pki redirecţionează navigarea către o altă pagina, http:// www.safelayer.com/en/solutions/ mobile-identification în care se prezintă conceptul de utilizare, neidentificând în mod clar aplicaţia ofertată
- Nu se regăseşte modalitatea de îndeplinire a cerinţei de „generare a cheilor criptografice direct pe terminalul mobil".

Având în vedere cele menţionate anterior, vă rugăm să precizaţi unde anume în propunerea tehnică, prin precizarea exactă a paragrafului şi paginii, se găseşte descrierea cu privire la îndeplinirea cerinţei:

Utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil", pentru care contestatoarea a formulat următorul răspuns:

Răspuns 24.

Referitor la solicitarea dumneavoastră privind modul de îndeplinire a cerinţei:

„În vederea asigurării mobilităţii şi ergonomiei de utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele" (...).

Menţionăm că aplicaţia mobilă de emitere de certificate digitale este Mobile PKi, aşa cum este evident în oferta la pagina 305, paragraful 2 şi la adresa *http://www.safelayer.com/en/solutions/mobile-pki* inclusă de asemenea în răspuns. Această aplicaţie este capabilă să emită certificate, fapt atestat pe pagina oficială a producătorului, la adresa *http://www.safelayer.com/en/solutions/mobile-pki-platform: „Mobile PKI – Digital Certificates Issuance for mobile devices".* De asemenea, această funcţionalitate poate fi asigurată de platforma PKI KeyOne de pe dispozitivele mobile online.

Autoritatea contractantă afirmă că din răspunsul contestatoarei se reţine faptul că ofertantul nu răspunde la întrebarea formulată, întrucât răspunsul relevă faptul că "aplicaţia mobilă de emitere de certificate digitale este Mobile PKI", în timp ce întrebarea se referea la aplicaţia care generează cheile criptografice direct pe terminalul mobil.

De asemenea, aplicaţia Mobile PKI indicată de către ofertant, nu există. Link-ul http://www.safelayer.com/en/solutions/mobile-pki redirectează navigarea către o altă pagină, http://www.safelayer.com/en/solutions/mobile-identification în care se prezintă conceptul de utilizare, şi nu descrierea unei aplicaţii.

De altfel, generarea cheilor este prima etapă din procesul de emitere a certificatelor digitale. Aceasta etapă poate fi derulată atât la client (adică pe terminalul mobil aşa cum este solicitat), cât şi la nivelul unui server de tip Autoritate de certificare. Generarea cheilor direct pe dispozitivul mobil asigură faptul că utilizatorii au controlul exclusiv al cheilor criptografice şi nu există o copie a acestora. În cazul existenţei unei copii a cheilor, o altă persoană poate impersona utilizatorul legitim, folosind cheile copiate, şi poate, în acest fel, să aibă acces la resurse informatice, în numele utilizatorului.

Prin urmare, ofertantul nu precizează care este aplicaţia ofertată pentru implementarea funcţionalităţii solicitate, respectiv de generare a cheilor criptografice direct pe terminalul mobil.

Având în vedere necesitatea clarificării, s-a adresat contestatoarei o nouă întrebare, pentru care autoritatea contractantă a primit răspunsuri evazive şi neconcludente, astfel:

- Denumirea aplicaţiei Mobile PKI, aşa cum a fost inclusă în oferta tehnică iniţială, a fost modificată în Mobile ID. Denumirea Mobile ID nu apare nicăieri în oferta tehincă iniţială, nici independent şi nici ca subcomponentă a Mobile PKI.

Deşi întrebările sunt simple şi la obiect, vizând nominalizarea exactă a aplicaţiei de generare a cheilor criptografice direct pe terminalul mobil, evident o aplicaţie instalată pe terminalul mobil, contestatoarea aduce în discuţie, pe rând, diverse elemente amintite în oferta sa tehnică, astfel:

- Iniţial, în oferta tehnică se prezintă Mobile PKI, componentă a platformei SafeLayer KeyOne, evident o componentă de tip server care, eventual, emite certificate digitale pentru terminale mobile şi nu generează chei criptografice pe aceste terminale mobile, neavând acces la acestea;
- În urma întrebărilor de clarificare, contestatoarea susţine că Mobile PKI, componentă a platformei SafeLayer KeyOne, deţine o subcomponentă,

Mobile ID, nemenţionată însă în oferta sa tehnică, care se instalează pe terminalul mobil prin descărcare de pe Apple AppStore. Se remarcă faptul că pentru Google Android aplicaţia la care se face referire este ”aplicaţia pentru Google Android”, fără a se menţiona denumirea acesteia. Oricum, aşa cum reiese din captura de ecran ataşată contestaţiei, aplicaţia SafeLayer Mobile ID furnizează protecţie împotriva furtului de identitate fără a necesita elemente de autentificare adiţionale (de ex: matrix card, dispozitiv OTP sau smart card).

- În răspunsurile la întrebările de clarificare transmise prin adresa nr. .../DAPITA/4498/03.03.2015 ofertantul ataşează în anexa II declaraţia producătorului Safelayer în care se afirmă că aplicaţia Mobile ID este disponibilă în iTunes App Store şi în Google Play Store.

- Cerinţa din documentaţia de atribuire stabilea că ”Toate funcţionalităţile referitoare la utilizarea certificatelor digitale trebuie să fie implementate de către aplicaţii disponibile comercial la momentul ofertării. Interfaţa aplicaţiilor va fi cel puţin în limba română. În acest sens, se vor ataşa ofertei manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul, precum şi orice alte documente care să vină în susţinerea conformităţii cu specificaţiile solicitate”. Totuşi, în ciuda faptului că aplicaţiile trebuiau să fie disponibile comercial la momentul ofertării, respectiv în august 2014, declaraţia SafeLayer este datată 5 martie 2015, iar aplicaţia nu este prezentă nici la data de 31 martie 2015 în Google Play Store.

În susţinerea afirmaţiilor sale, autoritatea contractantă prezintă o captură de imagine cu rezultatele obţinute după căutare în Google Play (play.google.com) folosind cuvintele cheie Safelayer și Mobile ID. Astfel, se observă că aplicaţia nu este disponibilă pentru descărcare, în totală contradicţie cu declaraţia depusă de contestatoare.

- Aplicaţia Mobile ID nu se regăseşte nicăieri în oferta tehnică depusă, nici la pagina 287 a ofertei tehnice unde sunt enumerate produsele Safelayer ofertate *”Sistemul este produs de compania SafeLayer platforma livrată fiind compusă din:*

- *TrustedX Adaptive Authentication*
- *KeyOne Certification Authority*
- *KeyOne Registration Authority*
- *KeyOne Validation Authority*
- *Mobile PKI”* şi nici în documentaţia privind Mobile PKI (Mobile PKI Speaker – Date: paginile 449 – 469 şi SOLUŢII MOBILE PKI: paginile 478 – 501).

Referitor la afirmaţia contestatoarei: *„Subscrisa am confirmat autorităţii în scris, atât prin adresa nr. nr. MFE/DAPITA/4598/06.03.2015 cât şi prin adresa nr. anterioară de clarificări nr. MFE/DAPITA/3696/20.10.2014 că produsul oferit nu este comercializat cu un model de versionare, acesta fiind motivul pentru care în ofertă nu se regăseşte versiunea de produs ofertată*”, autoritatea contractantă face precizarea că SafeLayer Mobile ID se regăseşte în Apple AppStore, fiind publicate până în acest moment 4 (patru) versiuni, cea mai nouă fiind 1.3.1.

Astfel, prin mai multe declaraţii succesive contestatoarea face afirmaţii false atât cu privire la disponibilitatea şi existenţa aplicaţiilor.

Se reţin astfel următoarele elemente:

- Aplicaţia Mobile ID nu este disponibilă în Google Play, deşi contestatara afirmă contrariul
- Aplicaţia Mobile ID este versionată de către producător, fiind disponibilă în prezent în App Store cu versiunea nr. 1.3.1, deşi contestatoarea afirmă contrariul
- În oferta tehnică nu se demonstrează modul în care aplicaţia Mobile ID îndeplineşte cerinţele solicitate.

Toate aceste aspecte arată fără echivoc faptul că ... a furnizat în cadrul acestei proceduri informaţii eronate şi induce în eroare autoritatea contractantă.

În ceea ce priveşte invocarea concluziei de la punctul 3 al sesiunii demonstrative, din 13.11.2014, consemnată în procesul verbal nr.4198/13.11.2014, autoritatea contractantă face precizarea că aceasta nu a atestat decât faptul că ”aplicaţia ofertată pentru generarea cheilor şi a cererilor de certificate este prezentă în App store. Pentru Android a fost prezentată versiunea de autentificare din browser.”

Prin această afirmație nu se demonstrează nici că aplicaţia Mobile ID este prezentă în Google Play și nici că funcţionalităţile de generare a cheilor pe sistemul de operare Android, utilizând o aplicaţie instalată pe telefon, au fost prezentate în cadrul demonstraţiei.

Este evident faptul că aplicaţia ofertată pentru generarea cheilor şi a cererilor de certificate pentru Android nu a fost prezentată, întrucât aceasta nu este prezentă în Google Play, fapt care ridică semne de întrebare referitoare la veridicitatea informaţiilor prezentate de către contestatoare în cadrul declaraţiilor de la producătorul SafeLayer, anexe la răspunsurile aferente întrebărilor de clarificări transmise prin adresa nr. MFE/DAPITA/4498/03.03.2015.

Afirmaţiile că autoritatea contractantă a luat act de demonstrarea acestor funcţionalităţi este eronată, întrucât, aşa cum este precizat chiar în cadrul contestaţiei, în cadrul sesiunii demonstrative autoritatea contractantă a luat act doar de existenţa aplicaţiei ofertate în App store.

Având în vedere cele precizate anterior, autoritatea contractantă conchide că:

1. Aplicaţia Mobile PKI indicata de către ofertant în oferta depusă, nu există.

Link-ul http://www.safelayer.com/en/solutions/mobile-pki redirecteaza navigarea către o altă pagină, http://www.safelayer.com/en/solutions/mobile-identification, în care se prezintă conceptul de utilizare, şi nu descrierea unei aplicaţii. De altfel, conceptul de Mobile PKI este folosit de toţi furnizorii similari, reprezentând o tehnologie, şi nu o aplicaţie. SafeLayer prezintă acest concept în cadrul platformei, din care se observă componentele aplicaţii ale platformei: CA, RA, VA şi Time-Stamping Authority. Mobile PKI este o tehnologie (certificates inssuance), folosită, probabil, de componenta de Registration Authority (RA).

2. Prin răspunsurile la întrebările de clarificare, ofertantul aduce

completări ofertei, modificând denumirea aplicaţiei Mobile PKI, aşa cum a fost inclusă în oferta tehnică depusă, folosind numele Mobile ID. Denumirea Mobile ID nu apare nicăieri în oferta tehnică iniţială, ca aplicaţie independentă sau ca subcomponentă a Mobile PKI, nici la pagina 287 a ofertei tehnice unde sunt enumerate produsele Safelayer ofertate. *"Sistemul este produs de compania SafeLayer platforma livrată fiind compusă din:*

- *TrustedX Adaptive Authentication*
- *KeyOne Certification Authority*
- *KeyOne Registration Authority*
- *KeyOne Validation Authority*
- *Mobile PKI"* şi nici în documentaţia privind Mobile PKI (Mobile PKI Speaker – Date: paginile 449 – 469 şi SOLUŢII MOBILE PKI: paginile 478 – 501).

3. În răspunsurile la întrebările de clarificare transmise prin adresa nr. MFE/DAPITA/4498/03.03.2015 ofertantul face declaraţii neadevarate, afirmând că aplicaţia Mobile ID este disponibilă în iTunes App Store şi în Google Play Store. La o căutare a aplicaţiei Mobile ID şi a producătorului SafeLayer în Google Play se observă că aplicaţia nu este disponibilă pentru descărcare, în totală contradicţie cu declaraţia depusă de contestară.

Având în vedere motivele enumerate mai sus contestatoarea nu a demonstrat îndeplinirea cerinţei "În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil" neindicând cu exactitate în oferta tehnică înaintată aplicaţia disponibilă pentru sistemele de operare iOS și Andoid pentru generarea cheilor criptografice direct pe terminalul mobil. Din acest motiv oferta tehnică înaintată este neconformă.

III. În ceea ce priveşte îndeplinirea cerinţelor privind accesul unui utilizator de pe PC în sistem (motivul 3 şi motivul 5 de neconformitate), autoritatea contractantă menţionează că cerinţa este prevăzută în cadrul capitolului 3.3.7.3. Utilizarea certificatelor digitale, subcapitolul 3.3.7.3.1. Autentificarea la sistem, şi este enunţată astfel:

„Accesul unui utilizator la sistem de pe PC se va putea realiza utilizand certificatul digital propriu, astfel:

a) *în format PKCS #12, importat la nivelul sistemului de operare, in propriul PC; astfel procesul de autentificare se realizeaza direct intre PC si sistem.*
b) *stocat pe dispozitivul criptografic propriu, conectat la PC, pe care sunt disponibile driverele aferente dispozitivului criptografic; astfel procesul de autentificare se realizează direct între PC şi sistem.*
c) *stocat pe dispozitivul criptografic propriu, conectat la terminalul mobil propriu, sau stocat pe terminalul mobil propriu. Aceasta situaţie este aplicabilă în următoarele situaţii:*
    - *pe respectivul PC nu este importat certificatul digital în format PKCS #12*

- *driverele dispozitivului criptografic nu sunt instalate sau utilizatorul nu este în posesia propriului dispozitiv.*

În cazul folosirii certificatului digital stocat pe dispozitivul criptografic propriu, conectat la terminalul mobil propriu, sau stocat pe terminalul mobil propriu procesul de autentificare necesita un mecanism de tip „challenge-response" pentru identificarea cu exactitate a utilizatorului care doreşte a se autentifica la sistem. Mecanismul de tip „challenge-response" va utiliza tehnologia PKI pentru semnarea digitală a unui mesaj codificat în mod standardizat, de către ambele entităţi implicate în procesul de autentificare, respectiv componenta de server şi utilizatorul. Fiecare dintre cele două entităţi va semna mesajul cu propriul certificat digital. Mesajul codificat trebuie să fie vizibil utilizatorului şi să includă informaţii despre timpul de expirare al procesului de autentificare. Sistemul de autentificare trebuie să fie capabil şi să permită operaţiunile de semnătură cu certificate stocate în memoria terminalului mobil, cu certificate stocate pe Secure SD conectat la terminal, şi cu certificate stocate pe dispozitive de tip smartcard (standard FIPS 140-2 level 2) cu interfaţa standard PKCS #11 conectate la terminal".

Pentru îndeplinirea cerinţelor, contestatoarea a indicat în oferta tehnică depusă, utilizarea aplicaţiei KeyOneXRA.

Având în vedere faptul că autoritatea contractantă a constatat că KeyOneXRA reprezintă componenta de RA (Registration Authority) a soluţiei SafeLayer PKI şi nu deţine funcţionalităţi în ceea ce priveşte accesul utilizatorilor în sistem, a adresat contestatoarei următoarea solicitare de clarificare:

28. Având în vedere cerinţele din caietul de sarcini cu privire la accesul unui utilizator de pe PC la sistem, precum şi informaţiile prezentate în oferta dvs la pag. 308-310, s-a constatat că KeyOne XRA reprezintă componenta de RA (Registration Authority) a soluţiei SafeLayer PKI şi nu deţine funcţionalităţi în ceea ce priveşte accesul utilizatorilor în sistem. Având în vedere cele menţionate anterior, vă rugăm să specificaţi unde anume în propunerea tehnică, prin precizarea exactă a paragrafului şi a paginii, se regăseşte descrierea cu privire la îndeplinirea cerinţelor definite în documentaţia de atribuire cu privire la accesul unui utilizator de pe PC la sistem", la care a primit următorul răspuns:

Răspuns 28.

Referitor la solicitarea dvs. privind modul de îndeplinire a cerinţelor din caietul de sarcini cu privire la accesul unui utilizator de pe PC la sistem:

În răspunsurile la care face referire prezenta solicitare de clarificare, operatorul economic face trimitere la componenta KeyOne XRA acesta evidenţiind clar interacţiunea terminalelor mobile, dar şi desktop (prin intermediul browser-ului web) cu soluţia PKI. Trebuie menţionat faptul că, aşa cum este specificat şi în oferta tehnică, autoritatea de înregistrare este componenta de sistemul PKI care verifică cererile de emitere/revocare certificate digitale venite de la utilizatori şi îi transmite autorităţii de certificare dacă trebuie emis sau nu certificatul solicitat,

acesta fiind practic una din primele interacţiuni ale platformei PKI cu utilizatorul, în faza de emitere certificare. Astfel, cum majoritatea cerinţelor în discuţie se referă la emiterea şi stocarea certificatelor, dar şi faptul că în acest document: KeyOne Registration Authority prezentat în ofertă la pag. 470 şi 471 se atestă capabilităţile soluţiei în relaţie cu dispozitivele mobile şi dispozitivele PC este motivul pentru care acesta a fost dat ca referinţă.

De asemenea, pe parcursul ofertei se evidenţiază o sumă de alte adrese de internet care atestă capabilitatea soluţiei, care în tandem cu explicaţiile propuse pentru fiecare răspuns explică în totalitate îndeplinirea cerinţei. Astfel:

Cerinţa: Accesul unui utilizator la sistem de pe PC se va putea realiza utilizând certificatul digital propriu, astfel:

a) în format PKCS #12, importat la nivelul sistemului de operare, în propriul PC, astfel procesul de autentificare se realizează direct între PC şi sistem.

b) Stocat pe dispozitivul criptografic propriu, conectat la PC, pe care sunt disponibile drivere-le aferente dispozitivului criptografic, astfel procesul de autentificare se realizează direct între PC şi sistem.

c) Stocat pe dispozitivul criptografic propriu, conectat la terminalul mobil propriu sau stocat pe terminalul mobil propriu. Această situaţie este aplicabilă în următoarele situaţii:

- *pe respectivul PC nu este importat certificatul digital în format PKCS #12*
- *driverele dispozitivului criptografic nu sunt instalate sau utilizatorul nu este în posesia propriului dispozitiv.*

Managementul utilizatorilor în KeyOneXRA este independent de mediul de lucru. Acesta permite implementarea autentificării PKI, semnăturii electronice şi criptarea pentru aplicaţii compatibile PKI din sisteme de operare PC (WINDOWS, Mac and Linux), sau echipamente mobile (Google Android şi Apple Ios).

Accesul unui utilizator la sistem de pe PC se va putea realiza utilizând certificatul digital propriu, specificat în documentul KeyOneRegistration Authority prezentat în ofertă la paginile 470 şi 471.

Coroborând acest răspuns cu faptul că soluţia include tehnologiile înglobate în TrustedX Adaptive Authentication, evidenţiate în oferta tehnică paginile 287, 289 şi 290 şi adresa oficială de internet prezentată în ofertă, evidenţiată la pagina 287 şi 289 dar şi cu faptul că soluţia oferă suport pentru standardul PKCS#12, fapt atestat în adresa de internet prezentat în ofertă, propusă în oferta tehnică la pagina 306, se evidenţiază în mod clar că cerinţele sunt îndeplinite în totalitate, şi anume accesul unui utilizator la sistem se realizează în mai multe feluri, aşa cum se evidenţiază în secţiune „functions”, dar şi secţiunea „Architecture” din cadrul prezentării KeyOneRA. Evidenţiem faptul că scenariile sunt multiple şi nu toate sunt evidenţiate în documentaţie, dar menţionate ca posibilităţi în secţiunea „Architecture” a documentului KeyOneRegistration

Authority prezentat în ofertă la paginile 470-471.

Trebuie menţionat că inclusiv şi interacţiunea cu KeyOneRA prezintă accesul la „sistem", acesta fiind practic prima secvenţă de acces în sistem".

Ofertantul face referire, prin răspunsul la această întrebare, la componenta de RA a soluţiei SafeLayer PKI, care este componentă de tip server ce implementează funcţionalităţile de înregistrare a utilizatorilor în sistemul PKI.

Ofertantul nu detaliază capabilităţile sistemului informatic ce va fi livrat de a asigura accesul utilizatorilor, implementând funcţionalităţile solicitate, detaliind, în schimb, capabilităţile de acces la propriile funcţionalităţi ale componentei de RA. Prin documentaţia de atribuire, nu a fost solicitată implementarea unei infrastructuri PKI în cadrul sistemului, ci emiterea certificatelor digitale de către un furnizor de servicii de certificare. La paginile 285, 300, 302 şi 303, ofertantul precizează explicit furnizorul, Digisign, şi autoritatea sub care sunt emise certificatele digitale – Root CA al Digisign. Oferta tehnică nu prezintă nicăieri integrarea între furnizorul de servicii de certificare Digisign şi KeyOne XRA.

De asemenea, funcţionalităţile de a emite certificate digitale nu au nicio legătură cu modalitatea de utilizare a certificatelor de către modulul de autentificare şi autorizare care este distinct de componenta de emitere. În oferta tehnică şi în răspunsul său la întrebările de clarificare ofertantul descrie modalitatea de emitere a certificatelor digitale şi soluţia utilizată în acest sens dar nu prezintă în niciun fel modulul de autentificare şi autorizare a utilizatorilor. Prin urmare, funcţionalităţile de autentificare şi autorizare nu sunt realizate de oferta tehnică propusă în conformitate cu cerinţele documentaţiei de atribuire.

În urma unei noi solicitări de clarificare, cu nr. MFE/DAPITA 4498/03.03.2015, prin răspunsul înregistrat cu nr. MFE/DAPITA 4598/06.03.2015 ofertantul precizează că soluţie de autentificare şi autorizare TrustedX, menţiune ce nu a fost făcută nici în oferta scrisă, la pagina 308, paragrafele 1,2,3,4 şi pagina 309, paragrafele 1 şi 2, şi nici în primul răspuns la întrebările de clarificare.

Produsul KeyONE XRA este un produs de tip server care realizează, conform specificaţiilor tehnice furnizate pe site-ul producătorului, următoarele funcţii:

KeyOne XRA is part of the Safelayer Public Key Infrastructure (PKI) solution.

It provides the Registration Authority (RA) functions and it is designed to:

- User registration and digital certificate lifecycle management through interaction with KeyOne CA.
- Certificate life-cycle management for PKI services and applications that require authentication, signature and data encryption.
- Digital certificate management for a wide range of user platforms and devices.

- Simplified PKI deployment thanks to a complete range of face-to-face and remote registration mechanisms.
- Registration system integration in corporate processes using the JSON/REST and XML/ SOAP standard interfaces.

Se constată astfel că:

- cerinţa "Accesul unui utilizator la sistem de pe PC se va putea realiza utilizând certificatul digital propriu" este neîndeplinită
- ultimul răspuns referitor la aceasta cerinţă modifică oferta depusă prin referirea unei noi componente, TrustedX, care să fie utilizată în procesul de autentificare şi pentru îndeplinirea cerinţelor din capitolul 3.3.7.3.1. Autentificarea la sistem. Utilizarea componentei TrustedX este suplimentară faţă de oferta tehnică înaintată unde, la paginile 308-310 pentru îndeplinirea cerinţelor a fost indicată aplicaţia KeyOne XRA.

Autoritatea contractantă menţionează că atât pentru cerinţa generală "Accesul unui utilizator la sistem de pe PC se va putea realiza utilizând certificatul digital propriu" cât şi pentru paragrafele subsecvente acestei cerinţe (până la pagina 309, paragraful 3 din oferta scrisă, Ofertantul nu a furnizat informaţii despre felul în care soluţia oferită satisface cerinţa, lăsând, practic, autoritatea contractantă să construiască aproape de la zero o soluţie, plecând de la exprimări succcinte şi simple linkuri către manuale şi specificaţii tehnice, autoritatea contractantă constatând că aceste linkuri se referă, într-o proporţie foarte mare, pe parcursul acestei cerinţe, la acelaşi produs, care este un server de Registration Authority, fără nicio legătură cu cerinţa solicitată prin documentaţia de atribuire.

În ceea ce priveşte criticile contestatoarei referitoare la aspectele de neconformitate comunicate, contestatoarea se află într-o gravă confuzie, necunoscând elementele ofertate, astfel:

i) rolul componentei KeyONE XRA este cât se poate de evident şi reiese din oferta tehnică şi din paginile oficiale de Internet ale producătorului, respectiv cel de serviciu de înregistrare în platforma PKI pentru obţinerea/revocarea de certificate digitale,

ii) componenta KeyONE XRA ofertată nu are nicio legătură cu procesul de autentificare al utilizatorilor la sistemul informatic. Ea reprezintă exclusiv interfaţa prin care utilizatorii solicită şi, eventual, obţin credenţialele de acces la sistem (certificatele digitale).

iii) rolul componentei TrustedX în procesul de autentificare al utilizatorilor la sistem este iniţial de suport pentru mecanismul de tip "challenge-response" (oferta tehnică pagina 310), apoi intervine prin componenta ofertată "TrustedX Adaptive Authentication" (răspunsul la întrebarea 28 din primul set de întrebări de clarificare), apoi furnizează strategii pentru integrarea autentificării (răspunsul la întrebarea 7 din al doilea set de întrebări de clarificare) şi, în sfârşit în cadrul contestaţiei reprezintă componenta de autorizare (control acces);

iv) anexa 3 la adresa MFE/DAPITA/4598/06.03.2015 stipulează faptul că "SafeLayer acceptă să primească informaţii de la

Autoritatea de Certificare Digisign referitoare la validitatea certificatelor digitale către soluţia Safelayer KeyOne solution" şi totodată că "DigiSign […] consimte să ofere serviciul de interogare a valabilităţii certificatelor digitale emise de Autoritatea de Certificare DigiSign către serverul SafeLayer KeyOne", fără însă a preciza componenta de SafeLayer KeyOne la care se face referire şi dacă este cea ofertată, sau mecanismul de validare utilizat;

v) dacă certificatele digitale sunt emise de către Autoritatea de Certificare DigiSign, este evident faptul că SafeLayer KeyOne CA, componenta de Autoritate de Certificare ofertată în cadrul platformei SafeLayer PKI este redundantă, dar, în principiu, nu este neconformă. În schimb, ridică semne de întrebare cu privire la faptul că ar exista o soluţie coerentă, eficientă şi matură în momentul ofertării, prezenţa a două tipuri de servere de Registration Authority fiind o dovadă de confuzie în ce priveşte arhitectura soluţiei.

Având în vedere cele precizate anterior, autoritatea contractantă apreciază că autoarea contestaţiei nu a demonstrat îndeplinirea cerinţei din subcapitolul 3.3.7.3.1 Din acest motiv oferta tehnică înaintată este neconformă.

IV. În ceea ce priveşte îndeplinirea cerinţelor privind înscrierea certificatului digital pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta (motivul 4 de neconformitate), autoritatea contractantă susţine că cerinţa este prevăzută în cadrul capitolului 3.3.7.2. certificate digitale, şi este enunţată astfel:

„În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispozitie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele:

[…]

Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta".

În oferta tehnică, la pagina 307, sunt precizate următoarele:

„Înscrierea certificatului digital se poate realiza atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta.
http://www.safelayer.com/en/solution/mobile-pki
http://www.safelayer.com/imagines/stories/pdf/trustedxvirtualcard.pdf".

Contestatoarea nu a indicat prin oferta tehnică înaintată aplicaţia utilizată pentru înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta, aşa cum a fost solicitat prin cerinţa "Toate funcţionalităţile referitoare la utilizarea certificatelor digitale trebuie să fie implementate de către aplicaţii disponibile comercial la momentul ofertării. Interfaţa aplicaţiilor va fi cel puţin în limba română. În acest sens se vor ataşa

ofertei manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul, precum şi orice alte documente care să vină în susţinerea conformităţii cu specificaţiile solicitate".

Având în vedere ambiguitatea ofertei în ceea ce priveşte îndeplinirea cerinţei, autoritatea contractantă a formulat şi adresat următoarea solicitare de clarificări:

27. Având în vedere cerinţa:

„Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil, cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta", pentru aplicaţia de generare a cheilor criptografice direct pe terminalul mobil, precum şi informaţiile prezentate în oferta dvs la pag 307 s-a constatat faptul că nu se regăseşte modalitatea de îndeplinire a cerinţei.

Având în vedere cele menţionate anterior, vă rugăm să specificaţi unde anume în propunerea tehnică, prin precizarea exactă a paragrafului şi paginii, se găseşte descrierea cu privire la îndeplinirea cerinţei:

Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta", de către aplicaţia de generare a cheilor criptografice direct pe terminalul mobil", la care s-a primit următorul răspuns:

Răspuns 27.Referitor la solicitarea dvs. privind modul de îndeplinire a cerinţei:

„Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta".

În răspunsurile la cerinţele caietului de sarcini, răspunsuri propuse la paginile 306 şi 307, se indică modalitatea în care soluţia poate genera şi manipula cheile în funcţie de necesităţi, prin intermediul funcţiei smart card, oferind posibilitatea de a stoca certificatul, fie pe dispozitivul mobil, fie pe orice dispozitiv ataşat terminalului mobil, transformându-l într-un smart card autentic, dar şi chiar într-un spaţiu centralizat şi securizat în vederea eliminării oricăror necesităţi de elemente mobile suplimentare. De asemenea, prin funcţionalităţile soluţie Mobile PKI prezentate la adresa http://www.safelayer.com/en/products/keyone-pki-platform şi evidenţiată în propunerea tehnică în cadrul răspunsurilor la cerinţele în discuţie, paginile 306 şi 307, se dovedeşte clar că toate acestea se realizează de pe terminalul mobil. În sprijinul clarificării acestora vă propunem studierea documentului http://www.safelayer.com/images/stories/pdf/Safelayer_KeyOne_XRA_EN.pdf, document ce oferă detalii despre funcţionalităţile care susţin cererea , emiterea şi revocarea certificatelor digitale.

Astfel subliniem faptul că soluţia propusă este mult superioară cerinţelor, oferind capabilităţi multiple şi configurabile de manipulare a certificatelor digitale, îndeplinind inclusiv cerinţele menţionate în prezenta solicitare de clarificare.

Ofertantul face referire, prin răspunsul la această întrebare, la componenta SafeLayer KeyOne PKI, care este componenta de tip server

ce implementează funcţionalităţile de management a certificatelor digitale (emitere, revocare, emitere CRL, validare), neexplicând modalitatea prin care certificatele sunt înscrise pe terminalul mobil sau pe dispozitivul criptografic conectat la terminalul mobil şi cum este îndeplinită cerinţa.

În special, componenta XRA este în mod cu totul şi cu totul inoportun amintita ca soluţie în cadrul acestei cerinţe, neavâdn nicio legătură cu funcţionalităţile invocate de aceasta.

De altfel ofertantul nu răspunde la întrebarea formulată, în sensul că aceasta făcea referire la facilitatea (de înscriere a certificatului [...]) pe care trebuie să o deţină chiar aplicaţia de pe terminalul mobil, şi nu soluţia în ansamblul său.

Din documentul sugerat a fi studiat, respectiv http://www.safelayer.com/images/stories/pdf/Safelayer_KeyOne_XRA_EN.pdf, reies capabilităţile Autorităţii de Inregistrare KeyOne (KeyOne Registration Authority) referitoare la emiterea certificatelor digitale, şi nu capabilităţile aplicaţiei de pe terminalul mobil, de a stoca şi folosi certificatul digital.

Prin urmare, soluţia propusă nu include o aplicaţie instalată pe terminalul mobil, care să permită înscrierea cheilor criptografice direct pe terminalul mobil şi pe un dispozitiv criptografic de tip smartcard, conectat la terminalul mobil.

Din conţinutul propunerii tehnice şi al răspunsurilor ofertantului la clarificările solicitate rezultă că nu este îndeplinită cerinţa minimă a caietului de sarcini, respectiv: „să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta”.

În ceea ce priveşte criticile contestatoarei referitoare la aspectele menţionate în cazul acestui motiv de neconformitate, acestea sunt complet neîntemeiate, în opinia autorităţii contractante deoarece:

i) Prin răspunsul la adresa MFE/DAPITA/4598/06.03.2015 contestatoarea aduce completări ofertei tehnice indicând utilizarea produsului Mobile ID pentru înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta.

ii) Producătorul SafeLayer declară în documentul prezentat în anexa 2 la adresa MFE/DAPITA/4598/06.03.2015 că ”Mobile ID […] poate genera chei în terminale mobile sau dispozitive de tip smart card”, nefăcând referire la ”înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta”, aşa cum a fost solicitat prin documentaţia de atribuire. Prin urmare afirmaţia contestatoarei şi în ceea ce priveşte acest aspect este incompletă şi neadevărată;

iii) La fel de neadevărată este şi afirmaţia că autoritatea contractantă a confirmat că cerinţa este îndeplinită ca urmare a sesiunii demonstrative din 13.11.2014, întrucât extrasul din procesul verbal nr. 4198/13.11.2014 referit în cadrul contestaţiei relevă faptul că ”a fost făcută o demonstraţie în cadrul sesiunii de prezentare a autentificării cu dispozitiv criptografic conectat la terminal mobil Android”, deci o cu totul

altă funcţionalitate decât cea solicitată, respectiv de ”înscriere a certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta”.

Neconformităţile ofertei subliniate în cadrul punctului 2 de mai sus cu privire la Mobile PKI şi aplicaţia Mobile ID sunt valabile şi în acest caz.

Având în vedere motivele enumerate mai sus contestatoarea nu a demonstrat îndeplinirea cerinţei ”În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele: […] Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta.” neindicând cu exactitate în oferta tehnică înaintată aplicaţia disponibilă pentru sistemele de operare iOS şi Andoid pentru înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta. Din acest motiv oferta tehnică înaintată este neconformă.

V. În ceea ce priveşte îndeplinirea cerinţelor privind accesul unui utilizator la sistem de pe terminalul mobil (motivul 6 de neconformitate), autoritatea contractantă afirmă că cerinţa este prevăzută în cadrul capitolului 3.3.7.3. Utilizarea certificatelor digitale, subcapitolul 3.3.7.3.1. Autentificarea la sistem, şi este enunţată astfel:

Accesul unui utilizator la sistem se va putea realiza şi de pe propriul terminal mobil utilizând certificatul digital propriu, stocat astfel:

- *pe dispozitivul criptografic propriu, conectat la terminalul mobil*
- *pe terminalul mobil*

În ambele situaţii, procesul de autentificare se realizează direct între terminalul mobil şi sistem.

În oferta tehnică la pagina 310 sunt precizate următoarele:

Accesul unui utilizator la sistem se va putea realiza şi de pe propriul terminal mobil utilizând certificatul digital propriu, stocat astfel:
http://www.safelayer.com/en/products/keyone-pki-platform

- pe dispozitivul criptografic propriu, conectat la terminalul mobil

http://www.safelayer.com/images/stories/pdf/Safelayer_keyone_xra_en.pdf

- pe terminalul mobil

http://www.safelayer.com/images/stories/pdf/keyone_xra_en.pdf

În ambele situaţii, procesul de autentificare se realizează direct între terminalul mobil şi sistem.
http://www.safelayer.com/images/stories/pdf/ keyone_xra_en.pdf

Pentru îndeplinirea cerinţelor contestatoarea a indicat în oferta tehnică depusă utilizarea aplicaţiei KeyOne XRA. Autoritatea contractantă a constatat ca KeyOne XRA reprezintă componenta de RA (Registration Authority) a soluţiei SafeLayer PKI, şi nu deţine funcţionalităţi în ceea ce priveşte accesul utilizatorilor în sistem.

Prin urmare s-a adresat următoarea solicitare de clarificare.

29. Având în vedere cerinţele din caietul de sarcini cu privire la

accesul unui utilizator la sistem de pe propriul terminal mobil utilizând certificatul digital propriu, precum şi informaţiile prezentate în oferta dvs. la pag. 310, s-a constatat că KeyOne XRA reprezintă componenta de RA (Registration Authority) a soluţiei SafeLayer PKIşi nu deţine funcţionalităţi în ceea ce priveşte accesul utilizatorilor în sistem. Având în vedere cele menţionate anterior, vă rugăm să specificaţi unde anume în propunerea tehnică, cu precizarea exactă a paginii şi a paragrafului, se găseşte descrierea cu privire la îndeplinirea cerinţelor definite în documentaţia de atribuire cu privire la accesul unui utilizator la sistem de pe propriul terminal mobil utilizând certificatul digital propriu,

la care s-a primit următorul răspuns:

Răspuns 29.

Referitor la solicitarea dumneavoastră privind modul de îndeplinire a cerinţei precizăm:

Aşa cum s-a menţionat şi în răspunsurile anterioare, KeyOne XRA reprezintă componenta RA, componenta ce este parte din sistem. Accesul la acesta evidenţiază (ca modalitate de acces) o mostră a modului în care se realizează accesul la sistem. Ofertantul a evidenţiat în propunerea tehnică, la paginile 287, 289 şi 290 şi adresa oficială de internet http://www.safelayer.com/en/products/trustedx-adaptive-authentication, prezentată în oferta evidenţiată la pagina 287 şi 289, modul concret în care cerinţele sunt îndeplinite.

Astfel, accesul unui utilizator la sistem se realizează în funcţie de scenariu, aşa cum se evidenţiază în secţiunea „Functions" dar şi secţiunea „Architecture" din cadrul prezentării KeyOneRA.

Trebuie menţionat că inclusiv şi interacţiunea cu KeyOneRA prezintă accesul la „sistem" acesta fiind practic prima secvenţă de acces în sistem.

Astfel, considerăm că evidenţierea modului de acces la componenta KeyOne RA componenta parte din sistem, se evidenţiază clar modul de acces al utilizatorului la sistem dar si că a cest fapt oferă o sumă de scenarii şi capabilităţi ce sunt mult superioare cerinţelor evidenţiate în caietul de sarcini.

Ofertantul face referire, prin răspunsul său la această întrebare, din nou, la componenta de RA (Registration Authority) a soluţiei SafeLayer PKI, care este componenta de tip server ce implementează funcţionalităţile de înregistrare a utilizatorilor în sistemul PKI.

În urma unei noi solicitări de clarificare, cu nr. MFE/DAPITA 4498/03.03.2015, prin răspunsul înregistrat cu nr. MFE/DAPITA 4598/06.03.2015 ofertantul, pentru a justifica prezenţa componentei KeyOne XRA precizează că "procesul de autentificare începe ca prima secvenţa cu KeyOne XRA prin înrolarea certificatelor utilizatorilor, corelată cu funcţionalităţile oferite de platforma TrustedX Adaptive Authentication", afirmaţie care întăreşte impresia de lipsă de expertiză a experţilor ofertantului. Autentificarea reprezintă procesul prin care se determină dacă cineva sau ceva este, de fapt, cine sau ce se declară a fi. Din punctul de vedere al unui sistem informatic, autentificarea reprezintă procesul prin care sistemul informatic determină dacă un utilizator sau un proces este chiar cel care se pretinde a fi, ceea ce evident înseamnă

verificarea unor credenţiale de acces la sistemul informatic de către utilizatorul/procesul respectiv. Aceste credenţiale pot fi username şi parola, certificat digital, elemente hardware de autentificare (dispozitive OTP – One Time Password, smart card-uri), precum şi combinaţii ale acestora, şi sunt prezentate de utilizator la începutul procesului de autentificare. În speţa în cauză, autentificarea reprezintă verificarea certificatului digital deţinut de utilizator/existent în posesia utilizatorului.

Modalitatea prin care certificatul digital a ajuns în posesia utilizatorului reprezintă un subiect separat și nu are legătură cu autentificarea ci doar cu obținerea certificatului digital de la Infrastructura PKI, parcurgând etapele de emitere care încep, în cazul SafeLayer PKI, cu KeyOne XRA. Trebuie precizat ca autoritatea contractantă nu a solicitat implementarea unei Infrastructuri PKI, ci a solicitat doar certificatele digitale, care reprezintă rezultatul activității unei Infrastructuri PKI.

Mai mult decât atât, aparent, ofertantul a înțeles această cerință oferind inițial 300 de certificate digitale emise de Digisign, furnizor acreditat de servicii de certificare, pentru ca, ulterior, să mai ofere o întreagă infrastructura paralelă, infrastructura care nu este necesară în contextul în care produsul acestei infrastructuri este ofertat deja de Digisign.

Din nou se poate remarca lipsa de consecvență și modalitatea în care contestatoarea își modifică răspunsurile în funcție de întrebările și remarcile autorității contractante, apelând la diverse funcționalități ale produselor ofertate. Astfel, dacă inițial în oferta tehnică îndeplinirea cerinței era realizată exclusiv de către componenta SafeLayer XRA, în urma răspunsului la întrebarea 8 din setul de clarificări inregistrat cu nr. MFE/DAPITA 4598/06.03.2015, indelinirea cerinței este relizată de produsul Mobile ID, aducând prin această afirmație completări ofertei tehnice depuse:

Pentru conformitate în oferirea unui răspuns clar fără echivoc la solicitarea dumneavoastră, autentificarea de pe terminalele mobile se realizează folosind certificatele digitale stocate fie pe dispozitive mobile fie pe dispozitive criptografice conectate direct la terminalul mobil, fie de pe smartcardurile conectate cu cititoare la aceste terminale mobile. Prin intermediul aplicaţiei Mobile ID (menţionată în răspunsul nr. 4) care la rândul său apelează platforma TrustedX Adaptive Authentication integrată cu KeyOne RA utilizatorilor li se verifică credenţialele şi li se permite accesul la aplicaţiile solicitate prin maparea acestor credenţiale pe drepturile şi rolurile asociate.

Autoritatea contractantă menţionează că autoarea contestaţiei încearcă să inducă în eroare Consiliu prin:

i) invocarea diverselor funcţionalităţi ale aplicaţiilor ofertate, modificând de fiecare dată soluţia care asigură implementarea cerinţelor definite în documentaţia de atribuire;
ii) confuzia deliberată sau generată de neştiinţă referitoare la procesele de autentificare şi autorizare, întrucât cerinţa se referă la ”accesul în sistem”, fără a face referire la autorizarea accesului la resursele acestuia.

Având în vedere motivele enumerate mai sus, autoritatea contractantă apreciază că autoarea contestaţiei nu a demonstrat îndeplinirea cerinței din subcapitolul 3.3.7.3.1. Autentificarea la sistem de către aplicația KeyOne XRA, aşa cum a fost descris în oferta tehnică depusă. Din aceste motive şi coroborat cu argumentele la punctul 3 anterior, oferta tehnică înaintată este neconformă.

VI. În ceea ce priveşte îndeplinirea cerinţelor ca soluţia de securitate propusă să permită contexte diferite de securitate în funcţie de secţiunea din sistem accesată de catre utilizator (motivul 7 de neconformitate), autoritatea contractantă menţionează că cerința este prevăzută în cadrul capitolului 3.3.7.3. Utilizarea certificatelor digitale, subcapitolul 3.3.7.3.1. Autentificarea la sistem, şi este enunțată astfel:

Modulul de autentificare şi autorizare trebuie sa ofere urmatoarele functionalităţi:

- să permită contexte diferite de securitate în funcţie de secţiunea din sistem accesată de către utilizator. Soluţia trebuie să permită prin configurare conexiuni http (publice, care nu necesită autentificare) si https (cu autentificare) în functie de aceste contexte.

În oferta tehnică, la pagina 311 sunt precizate următoarele:

Sistem informatic, prin intermediul soluţiei de securitate şi Microsoft Active Directory permite contexte diferite de securitate în funcţie de secţiunea din sistem accesată de către utilizator. Soluţia permite prin configurare conexiuni http (publice, care nu necesită autentificare) şi http (cu autentificare) în funcţie de aceste contexte.
http://technet.microsoft.com/en-us/library/cc753531(v=ws.10).aspx

Având în vedere faptul că „soluţia de securitate" menţionată în răspunsul la cerinţă este neclară (nu este nomnalizată) s-a adresat contestatoarei următoarea întrebare de clarificare:

32. Având în vedere cerinţele din caietul de sarcini, cap. 3.3.7.3.1, respectiv cele referitoare la Modul de autentificare şi autorizare, vă rugăm să precizaţi, indicând cu exactitate numărul paginii, precum şi litera/paragraful, unde se regăseşte în oferta tehnică şi în ce constă „soluţia de securitate", care în conformitate cu răspunsul dvs. din matricea de conformitate, împreună cu Microsoft Active Directory răspunde cerinţelor referitoare la Modulul de autentificare şi autorizare.

La care contestatoarea a formulat următorul răspuns:

Răspuns 32. Referitor la solicitarea dumneavoastră privind modul de îndeplinire al cerinţelor din caietul de sarcini, cap. 3.3.7.3.1, respectiv cele referitoare la Modulul de autentificare şi autorizare:

Menţionăm că „soluţia de securitate" la care faceţi referire constă în infrastructura de tip PKI, adică soluţia SafeLayer propusă, aceasta fiind constituită, printre altele, din componentele evidenţiate la pagina 287.

PKI constă într-o sumă de tehnici criptografice care permite utilizatorilor o comunicare sigură cu sistemul oferind un strat suplimentar de Securitate care verifică identitatea acestora.

Astfel, ofertantul precizează faptul că soluţia de securitate constă în infrastructura de tip PKI, adică soluţia SafeLayer propusă.

În urma unei noi solicitări de clarificare, cu nr. MFE/DAPITA

4498/03.03.2015: "Vă rugăm să precizaţi care sunt produsele software, componente ale infrastructurii SafeLayer PKI, care, împreună cu Microsoft Active directory asigură "contexte diferite de securitate în funcţie de secţiunea din sistem accesată de utilizator"", prin răspunsul înregistrat cu nr. MFE/DAPITA 4598/06.03.2015 ofertantul, precizează că aplicaţia TrustedX realizează cerinţa.

Conform capturii din pagina oficială a producătorului, serverul TrustedX nu face parte din SafeLayer PKI Platform (de fapt, produsul se numeste SafeLayer KeyOne PKI Platform), ci este un produs distinct din portofoliul SafeLayer.

Ambele răspunsuri modifică oferta tehnică depusă, ultimul conţinând şi o informaţie neadevărată (faptul că serverul TrustedX ar face parte din SafeLayer PKI KeyOne Platform), conform capturii de ecran de mai jos, preluată de pe site-ul producătorului SafeLayer.

În ceea ce privește criticile contestatoarei cu privire la motivele pentru care oferta sa a fost declarată neconformă se poate observa inconsecvența acesteia în ceea ce privește nominalizarea componenţei care îndeplinește cerința. Pe de-o parte (în urma primei întrebări de clarificare), cerința este îndeplinită global de "infrastructura PKI adică soluția SafeLayer propusă", fără a detalia care dintre componentele ofertate asigură îndeplinirea cerinței. Pe de altă parte, urmare a celei de-a doua întrebări, "componenta" responsabilă cu îndeplinirea cerinței este TrustedX.

În niciun moment, însă, contestatoarea nu indică modalitatea prin care cerința este îndeplinită, ci doar invocă capabilitățile TrustedX ca "server de alocare şi gestionare de roluri utilizatori". Din niciun material, link sau precizare nu reiese capabilitatea vreuneia dintre componentele prezentate în pagina 287 a ofertei de a îndeplini cerinţa din documentația de atribuire.

În contestaţia depusă contestatoarea reţine în mod corect, cu privire la conceptele de autentificare/autorizare preluate de pe site-ul wikipedia (http://en.wikipedia.org/wiki/Authentication), faptul că: "În realitate, autentificarea are rolul de a valida identitatea unor utilizatori, iar autorizarea are rolul de a-i acorda acestuia dreptul de acces la resurse, conform drepturilor sale de acces" . Imediat, însă, vine cu o interpretare originală şi eronată, prin care afirmă faptul că "În mod concret, procesul de autentificare este procesul de a asigna un set de credenţiale unui anumit utilizator, iar procesul de autorizare este procesul prin care se acordă dreptul acelui utilizator la resurse".

Pentru o clarificare exactă a conceptelor, aşa cum sunt cunoscute acestea în literatura de specialitate, în aceeaşi pagină prezentată de contestatoare (http://en.wikipedia.org/wiki/Authentication) este dat următorul exemplu "For example, a client showing proper identification credentials to a bank teller is asking to be authenticated that he really is the one whose identification he is showing. A client whose authentication request is approved becomes authorized to access the accounts of that account holder, but no others." în traducere "spre exemplu, un client arată unei bănci credențialele care îl identifică prin care atestă că el este

cine pretinde a fi. După ce procesul de autentificare este aprobat, clientul este autorizat să îşi acceseze numai conturile sale”.

Interpretarea contestatarei este din nou originală şi proprie afirmând că, în fapt, procesul de autentificare presupune emiterea credenţialelor de acces (în exemplele de mai sus credenţialele de acces în bancă respectiv permisul de conducere) lucrul total neadevărat în opinia autorităţii contractante, deoarece credenţialele respective trebuie să existe în prealabil pentru a fi verificate în procesul de autentificare. Credenţialele sunt emise în urma procesului de înregistrare, şi nu în timpul procesului de autentificare. Iar procesul de autorizare presupune stabilirea nivelului de acces al entităţii care a fost autentificată.

Cu alte cuvinte, credenţialele de acces ale utilizatorilor (adică certificatele digitale în speţa de faţă) trebuie să existe şi să fie emise pentru ca utilizatorii să fie autentificaţi şi autorizaţi pentru a accesa resurse specifice. Astfel, chiar dacă emite credențialele utilizatorilor, infrastructura PKI nu oferă funcționalităţi de autentificare şi autorizare, aşa cum în mod eronat susține contestatoarea.

Având în vedere motivele enumerate mai sus contestatoarea nu a demonstrat îndeplinirea cerinței din subcapitolul 3.3.7.3.1. Autentificarea la sistem de către Soluția de securitate şi microsoft Active Directory, aşa cum a fost descris în oferta tehnică depusă. Din aceste motive oferta tehnică înaintată este neconformă.

VII. În ceea ce priveşte îndeplinirea cerinţelor ca soluţia de securitate propusă să permită autentificarea utilizatorilor exclusiv pe baza certificatului digital X.509 v3 personal (motivul 8 de neconformitate), autoritatea contractantă afirmă că cerința este prevăzută în cadrul capitolului 3.3.7.3. Utilizarea certificatelor digitale, subcapitolul 3.3.7.3.1. Autentificarea la sistem, şi este enunţată astfel:

Modulul de autentificare şi autorizare trebuie să ofere următoarele funcţionalităţi:

- *[...]*
- *să permită autentificarea utilizatorilor exclusiv pe baza certificatului digital X.509 v3 personal. Certificatele digitale pot fi emise de multiple Autoritati de certificare definite de incredere, iar modulul trebuie să fie configurabil să se integreze cu oricare dintre ele folosind interfete şi protocoale standard.*

În oferta tehnică, la pagina 311 sunt prezentate următoarele:

Microsoft Active Directory şi soluţia de securitate permit realizarea şi autentificarea utilizatorilor exclusiv pe baza certificatului digital X.509 v3 personal. Certificatele digitale pot fi emise de multiple Autorităţi de certificare definite de încredere, iar modulul este configurabil să se integreze cu oricare dintre ele folosind interfeţe şi protocoale standard;

Având în vedere faptul că „soluţia de securitate” menţionată în răspunsul la cerinţă este neclară (nu este nominalizată) s-a adresat contestatoarei întrebarea de clarificare nr. 32, referită la punctul precedent, la care contestatoarea a formulat răspunsul de asemenea prezentat.

Prin urmare, ofertantul precizează faptul că solutia de securitate

consta în infrastructura de tip PKI împreuna cu Microsoft Active Directory.

Infrastructura KeyONE PKI asigură, conform descrierii de pe siteul producătorului:

- Certification Authority/Registration Authority (CA/RA) – digital certificate management functions
- Validation Authority (VA) – online certificate status information
- Time Stamping Authority (TSA) - electronic time-stamping services
- Mobile PKI – digital certificates issuance for mobile devices

Comunicarea şi integrarea dintre oricare dintre componentele SafeLayer KeyONE PKI şi Microsoft Active Directory nu este atestată în niciun fel, întrucât nu există în oferta scrisă niciun document care să ateste această integrare, iar de pe siteurile producatorilor nu rezultă acest lucru. Prin urmare lipsa explicitării modului de integrare dintre cele două compoenente nu este deloc ”ipotetică”, așa cum eronat afirma contestatoarea, ci este cât se poate de reală. De altfel, contestatoarea prin oferta tehnică şi răspunsurile la întrebările de clarificare ar fi trebuit să scoată în evidenţă această integrare ca şi modul în care înţelege că soluţia să îndeplinească cerinţa, şi nu să lase comisia să caute în toate documentatiile şi specificaţiile tehnice de pe internet dacă cele două produse se pot integra într-o soluţie.

Confuzia în care persistă contestatoarea este evidentă, întrucât nu face distincție între o infrastructura PKI și certificatele digitale, care reprezintă produsul operării unei infrastructuri PKI. Pe de-o parte ofertează o Soluție PKI – SafeLayer KeyOne și pe de altă parte furnizează certificatele digitale solicitate prin DigiSign. Mai mult platforma TrustedX, ”prin intermediul KeyOne XRA, poate lucra cu Digisign […] și cu orice altă Autoritate de certificare”, combinând din nou facilități, produse, tehnologii componente şi platforme într-o manieră cu totul originală.

Mai mult, contestatoarea nu cunoaște care este Autoritatea de certificare care va emite certificatele digitale ale utilizatorilor, respectiv:

1) Autoritatea de certificare Digisign, cu care ”prin intermediul KeyOne XRA” (adică a componentei de înregistrare a utilizatorilor din SafeLayer PKI platform) ”platforma de control acces TrustedX” poate lucra, SAU

2) instanţa de SafeLayer PKI platform (cu componentele sale XRA, CA, VA) ofertată în vederea instalării la autoritatea contractantă, aşa cum reiese din următorul paragraf din contestaţie: *„Răspuns la întrebarea nr. 2: Referitor la întrebarea nr. 2, în care solicitaţi specificarea rolului componentei ADSS OCSP Server, răspunsul nostru este precizat în Oferta tehnică la pag. 315 şi 316. ADSS OCSP Server răspunde cerinţelor AC cu privire la funcţionalitatea Intelling routing, astfel încât să poată fi validate certificate digitale emise de alte CA-uri decât cea din prezenta Soluţie de securitate, implementată în prezentul proiect, iar KeyOne VA este soluţia de verificare a validităţii certificatelor digitale aferente acestui sistem”.*

Având în vedere motivele enumerate mai sus contestatara nu a demonstrat îndeplinirea cerinței din subcapitolul 3.3.7.3.1. Autentificarea la sistem de către Soluția de securitate și microsoft Active Directory, așa cum a fost descris în oferta tehnică depusă. Din aceste motive oferta

tehnică înaintată este neconformă.

VIII. În ceea ce privește îndeplinirea cerințelor cu privire la modul de realizare a criptării (motivul 9 de neconformitate), autoritatea contractantă susţine că cerințele privind mecanismele de asigurare a confidențialității datelor sunt descrise în secțiunea Criptarea documentelor din capitolul 3.3.7.3. Utilizarea certificatelor digitale din modificarea nr. 8 și sunt reproduse în continuare:

Confidentialitatea datelor va fi asigurată prin criptarea documentelor/informatiilor, utilizând tehnologiile PKI şi algoritmi standard, şi prin ştergerea documentelor utilizând algoritmi recunoscuţi la nivel internaţional.

Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici şi asimetrici, astfel:

- *Criptarea asimetrică, utilizând certificatele X509v3 şi algoritmul RSA*
- *Criptarea simetrică folosind algoritmii 3DES si AES*

În aceeaşi secţiune este inclusă şi:

Criptarea trebuie să poată fi realizată astfel:

La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată;

Prin urmare este evident că produsul care realizează criptarea ”La nivel de sistem de operare, prin crearea unei partiţii criptate” trebuie să respecte mecanismele de criptare menţionate:

a) *Criptarea asimetrică, utilizând certificatele X509v3 şi algoritmul RSA*
b) *Criptarea simetrică folosind algoritmii 3DES şi AES*

Cu privire la îndeplinirea cerinţei

Mecanismele de criptare in tehnologiile PKI se bazeaza pe algoritmi criptografici standard simetrici si asimetrici, astfel:

a) *Criptarea asimetrica, utilizand certificatele X509v3 si algoritmul RSA*
b) *Criptarea simetrica folosind algoritmii 3DES si AES,* în oferta tehnică la pagina 319 sunt precizate următoarele:

Aplicaţia DigiSigner propusă integrează în tehnologii PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici şi asimetrici după cum urmează:

Referinţe:

Brosura_DigiSigner.pdf

Criptarea asimetrică se realizează utilizând certificatele X509v3 şi algoritmul RSA.

Criptarea simetrică se realizează utilizând algoritmii 3DES şi AES

Cu privire la îndeplinirea cerinţei:

Criptarea trebuie să poată fi realizată astfel:

a) La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată, în oferta tehnică la pagina 320 sunt precizate următoarele:

„Acest lucru se realizează prin configurarea criptării Bitlocker la nivel de disc (partiţie), astfel încât să se asigure criptarea la nivelul sistemului de operare. La nivelul „Key Management", Bitlocker se va configura pentru a permite utilizarea smartcard-urilor în vederea accesării/deblocării partiţiei criptate, în cazul în care acest smartcard este decontat de la staţia de lucru, sistemul de operare va bloca accesul la informaţia aflată pe această partiţie criptată...".

În oferta tehnică înaintată nu a fost precizat că produsul BitLocker folosește pentru criptare simetrică algoritmul 3DES. Prin urmare, s-a adresat contestatoarei următoarea întrebare de clarificare:

„37. Având în vedere cerinţa din caietul de sarcini referitoare la Asigurarea confidenţialităţii datelor, cap. 3.3.7.3.2:

Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici şi asimetrici, astfel:

Criptarea asimetrică utilizând certificatele X509v3 şi algoritmul RSA.

Criptarea simetrică utilizând algoritmii 3DES şi AES", vă rugăm să precizaţi, indicând cu exactitate numărul de pagini, precum şi litera/paragraful unde este menţionat în oferta tehnică, prin indicarea paginii respectiv literei sau paragrafului, faptul că BitLocker suportă algoritmul criptografic simetric 3DES", la care s-a primit următorul răspuns:

Răspuns 37. Referitor la solicitarea dumneavoastră (...), conform informaţiilor prezentate la pagina 319 a ofertei tehnice şi în pagina 2 a documentaţiei componentei DigiSigner, acesta integrează în tehnologia PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici (3des şi AES) şi asimetrici. Astfel, produsul BitLocker suportă algoritmul criptografic simetric 3DES atât prin intermediul componentei client DigiSigner, care integrează algoritmul criptografic simetric 3DES, cât şi prin dispozitivele criptografice securizate SafeNet e-Teken PRO care suportă algoritmul 3DES conform informaţiilor prezentate la pagina 304 a ofertei tehnice.

Astfel contestatoarea precizează în răspunsul său faptul că aplicaţia Digisigner "integrează în tehnologiile PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici (3DES si AES) şi asimetrici. Astfel, produsul BitLocker suportă algoritmul criptografic simetric 3DES atât prin intermediul componentei client DigiSigner, care integrează algoritmul criptografic simetric 3DES, cât şi prin dispozitivele criptografice securizate SafeNet e-Token PRO [..]" Aplicația DigiSigner nu este menționată în cadrul soluției la această cerință, în propunerea tehnică, deci această afirmație nu poate fi luată în considerare.

De altfel, contestatoarea îşi confirmă strategia de ofertare, indicând soluții informatice care să răspundă unor cerinţe din documentaţie şi apoi "inventând" componente şi integrări între produse, în funcţie de întrebările autorităţii contractante.

În mod evident, se constată următoarele:

1. BitLocker este componenta de tip client care se furnizează odată cu sistemul de operare Microsoft Windows, (Vista şi versiunile ulterioare), fiind inclus în acesta. BitLocker nu are nicio o altă componentă de tip

client. Prin urmare DigiSigner nu are cum să fie "componenta client" pentru BitLocker.

2. BitLocker nu implementează algoritmul 3DES, implementând doar algoritmul AES în modul CBC (128 si 256 biti), aşa cum reiese din documentaţia oficială a producatorului, http://download.microsoft.com/download/0/2/3/0238acaf-d3bf-4a6d-b3d6-0a0be4bbb36e/BitLocker Cipher200608.pdf

3. Dispozitivele securizate SafeNet e-Token PRO suportă algoritmul 3DES, dar realizează această criptare doar dacă aplicaţia care solicită criptarea implementeaza acest algoritm.

Referitor la partea a doua a cerinţei, autoritatea contractantă a adresat următoarea întrebare de clarificare:

38. Având în vedere cerinţa din caietul de sarcini referitoare la Asigurarea confidenţialităţii datelor, cap. 3.3.7.3.2:

„Criptarea trebuie să poată fi realizată astfel:

- La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcadrului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată",, vă rugăm să precizaţi unde este menţionat în oferta tehnică, prin indicarea paginii respectiv literei sau paragrafului, faptul că produsul BitLocker implementează funcţionalitatea de blocare a aceesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului de la staţia de lucru, pentru care contestatoarea a furnizat următorul răspuns:

Răspuns 38. Referitor la solicitarea dumenavoastră privind modul de îndeplinire al cerinţei din caietul de sarcini referitoare la Asigurarea confidenţialităţii datelor, cap. 3.3.7.3.2: (...) menţionă, că aşa cum este evidenţiat în clar în oferta tehnică la pagina 320 paragraful 3, produsul BitLoker, implementează funcţionalitatea de blocare a accesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului de la staţia de lucru.

Contestatoarea precizează astfel faptul că produsul BitLocker implementează funcţionalitatea de blocare a accesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului de la staţia de lucru iar acest aspect este evidenţiat în oferta tehnică la pagina 320, paragraful 3.

Datele prezentate la pagina 320, paragraful 3 prezintă faptul că accesul la partiţia criptată, respectiv operațiunea de deblocare a acesteia, poate fi realizat prin utilizarea unui smartcard, fără a detalia modalitatea de indeplinire a cerinţei, respectiv blocarea la deconectarea unui smartcard.

În opinia autorităţii contractante, criticile formulate de către contestatoare sunt complet neîntemeiate, întrucât:

i) Deși autoritatea contractantă a referit în motivul 9 de neconformitate numărul întrebării de clarificare ca fiind 32, textul menționat este evident cel din cadrul întrebării numărul 37. Aşadar singura diferenţă este numărul întrebării, aspect exclusiv formal, fără a aduce atingere fundamentării neconformităţii ofertei.

ii) Mecanismele de asigurare a confidenţialităţii datelor sunt explicate la începutul subcapitolului Asigurarea confidenţialităţii documentelor.

Prin urmare este evident că produsul care realizeaza criptarea ”la nivel de sistem de operare, prin crearea unei partiţii criptate” trebuie să respecte mecanismele de criptare menționate, cerințele fiind subscrise aceluiași obiectiv, respectiv Asigurarea confidenţialității documentelor. Ceea ce este demn de remarcat este faptul că ”aplicația care realizează funcțiile de criptare este Digisigner” așa cum afirmă în clar contestatoarea, care suportă toți algoritmii criptografici solicitați, fără a mai face referire la tehnologia TrustedX a cărei componentă contestatoarea a declarat că este, ceea ce denotă, încă o dată inconsecvența contestatoarei și necunoașterea propriei oferte.

Cele două paragrafe, respectiv cel în care se prezintă mecanismele și algoritmii de criptare şi cel în care se prezintă funcționalitățile ce trebuie îndeplinite în ceea ce privește criptarea nu pot fi disociate, ele fiind parte a aceluiaşi subcapitol, respectiv Asigurarea confidenţialităţii documentelor.

În opinia autorităţii contractante, este evident cum contestatoarea îşi modifică, de fiecare dată, explicaţiile referitoare la implementarea acestei cerinţe, respectiv:

a. Initial (în oferta tehnică) funcţionalitatea este îndeplinită de către BitLocker;
b. Urmare a intrebărilor de clarificare, funcţionalitatea este îndeplinită de către BitLocker prin ”componenta sa client Digisigner”;
c. În contestaţie funcţionalitatea nici măcar nu mai este nevoie să fie îndeplinită, întrucât cerinţa de funcţionalitate nu are legătură cu mecanismele de criptare şi algoritmii solicitaţi, în cadrul aceluiaşi paragraf.

iii) Menționarea unui paragraf din cadrul procesului verbal nr. 4198/13.11.2014 care nu are nicio legătură cu funcționalitatea de blocare a accesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului este complet irelevantă. Punctul 8 al procesului verbal relevă exclusiv prezentarea algoritmilor criptografici, fără legătură cu funcționalitatea de blocare a accesului.

În concluzie autoritatea contractantă învederează următoarele:

1) Aplicaţia BitLocker propusă pentru îndeplinirea cerinţei ”Criptarea trebuie să poată fi realizată astfel […] La nivel de sistem de operare, prin crearea unei partiţii criptate” nu utilizează algoritmul 3DES pentru criptare şi astfel cerinţa ”Mecanismele de criptare in tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici şi asimetrici, astfel: […] Criptarea simetrică folosind algoritmii 3DES şi AES” nu este îndeplinită de această aplicaţie.

2. În oferta tehnică înaintată nu este descrisă modalitatea de îndeplinire de către BitLocker a cerinţei de blocare a accesului la informațiile aflate pe partiția criptată la deconectarea unui smartcard.

Având în vedere motivele enumerate mai sus contestatara nu a

demonstrat îndeplinirea cerinței de criptare folosind algoritmul 3DES și de blocare a accesului la informațiile aflate pe partiția criptată la deconectarea unui smartcard de aplicația BitLocker, ofertată pentru realizarea criptării la nivel de sistem de operare prin crearea unei partiții criptate. Din aceste motive oferta tehnică înaintată este neconformă.

IX. În ceea ce priveşte îndeplinirea cerinţelor cu privire la Componenta de comunicare cu arhiva electronică legală din capitolul 3.3.8.1 (motivul 10 de neconformitate), autoritatea contractantă susţine că cerinţele documentaţiei de atribuire referitoare la "Modulul 8: Modulul de arhivare a documentelor", subcapitolul "3.3.8.1 - Componenta de Comunicare cu Arhiva Electronica Legala" includ:

- *"această componentă de arhivare electronică va fi capabilă să aplice semnături digitale ..., iar aplicarea de semnături digitale va trebui să ofere următoarele capabilitati minime:[…]"*
- *"Semnătură electronică va fi în conformitate cu următoarele standarde [...]"*
- *"Marca temporala care va fi aplicată semnăturii electronice va avea următoarele functionalitati si caracteristici:[...]"*

Aceste cerințe se referă la o componentă integrată, care să asigure Comunicarea cu Arhiva Electronică Legală și care să îndeplinească cumulativ cerințele subcapitolului 3.3.8.1.

În oferta înaintată contestatarea a răspuns astfel:

- la cerinţa: "această componentă de arhivare electronică va fi capabilă să aplice semnături digitale ..., iar aplicarea de semnături digitale va trebui să ofere următoarele capabilităţi minime:" oferta tehnică specifică faptul că soluţia cuprinde modulul StarSign, componentă a SEAL, care asigură aplicarea de semnături digitale şi mărci temporale;

- la cerinţa: "Semnătură electronică va fi în conformitate cu următoarele standarde" oferta tehnică specifică faptul că semnătură electronica va fi aplicată prin intermediul aplicaţiei DigiSigner;

- la cerinţa: "Marca temporală care va fi aplicată semnăturii electronice va avea următoarele functionalităţi şi caracteristici:" oferta tehnică specifică ca marca temporală va fi aplicată semnăturii electronice prin intermediul aplicaţiei DigiSigner.

Nu este descrisă în oferta tehnică înaintată modalitatea de integrare între aplicația DigiSigner și SEAL/ StarSign şi nici faptul că pentru Componenta de Comunicare cu Arhiva Electronică Legală se va utiliza pentru integrare un SDK.

Prin urmare a fost adresată contestatoarei următoarea solicitare prin adresa nr. 3600/14.10.2014:

43. Având în vedere precizările ofertei tehnice referitoare la următoarele cerinţe din caietul de sarcini "Modulul 8: Modulul de arhivare a documentelor", subcapitolul 3.3.8.1. – Componenta de comunicare cu Arhiva Electronică Legală", respectiv faptul că:

a) la cerinţa: „această componentă de arhivare electronică va fi capabilă să aplice semnături digitale..., iar aplicarea de semnături digitale va trebui să ofere următoarele capabilităţi minime: oferta tehnică specifică faptul că soluţia cuprinde modulul StartSign componentă a SEAL

care asigură aplicarea de semnături digitale şi matrici temporale;

b) la cerinţa: „Semnătura electronică va fi în conformitate cu următoarele standarde", oferta tehnică specifică faptul că semnătura electronică va fi aplicată prin intermediul aplicaţiei DigiSigner,

c) la cerinţa: „Marca temporală care va fi aplicată semnăturii electronice va avea următoarele funcţionalităţi şi caracterisitici", oferta tehnică specifică că marca temporală va fi aplicată semnăturii electronice prin intermediul aplicaţiei DigiSigner, vă rugăm să precizaţi indicând cu exactitate în oferta tehnică numărul paginii, precum şi litera/paragraful, unde este menţionată cu exactitate aplicaţia care implementează cerinţele din documentaţia de atribuire legate de semnarea electronică şi marcarea temporală a documentelor în cadrul componentei de Comunicare cu Arhiva Electronică Legală, la care a fost primit următorul răspuns:

Răspuns 43.

Referitor la solicitarea dumneavoastră privind modul de îndeplinire a cerinţei privitoare la funcţionalităţile Modulul 8: „Modulul de arhivare a documentelor", subcapitolul „3.3.8.1 – Componenta de Comunicare cu Arhiva Electronică Legală" mai sus menţionate.

- Cerinţa este îndeplinită de soluţia ofertată prin intermediul proiectării, dezvoltării, configurării şi implementării componentei SEAL. Modulul StarSign inclus în SEAL asigură aplicarea de semnături digitale şi mărci temporale prin intermediul componentei client DigiSigner. Descrierile detaliate apar în cadrul ofertei tehnice la răspunsurile tehnice la cerinţe la paginile 312 – 330 şi paginile 331-338 şi cuprind toate detaliile solicitate de îndeplinire a cerinţelor.

Menţionăm că răspunsurile ofertantului la solicitarea de clarificare nu aduc modificări ofertei înaintate ci doar clarifică aspectele solicitate.

Ofertantul precizează în răspunsul său faptul că "cerinţa este îndeplinită de soluţia ofertată prin intermediul proiectarii, dezvoltării, configurării şi implementării componentei SEAL. Modulul StarSign inclus în Seal asigură aplicarea de semnături electronice şi mărci temporale prin intermediul componentei client DigiSigner. Descrierile detaliate apar în cadrul ofertei tehnice la răspunsurile tehnice la cerinţe la paginile 312-330, şi paginile 331-338 şi cuprind toate detaliile solicitate de îndeplinire a cerintelor".

La întrebarea precisă a autorității contractante "vă rugăm să precizaţi, indicând cu exactitate în oferta tehnică numărul paginii, precum şi litera/paragraful, unde este menţionată cu exactitate aplicaţia care implementează cerinţele din documentaţia de atribuire legate de semnarea electronică şi marcarea temporală a documentelor în cadrul componentei de Comunicare cu Arhiva Electronica Legală" răspunsul face o referire generală în ceea ce priveste răspunsurile la cerinţele tehnice menţionate, acoperind întregul capitol de semnătură electronică (aferent modulului 7) şi întregul Modul 8 al caietului de sarcini.

Nu se regăseşte în oferta depusă nicio precizare cu privire la integrarea dintre StarSign şi DigiSigner. Mai mult, răspunsul precizează că "cerinţa este îndeplinită de soluţia ofertată prin intermediul proiectării,

dezvoltării, configurării şi implementării", ceea ce induce necesitatea unui proces de proiectare şi dezvoltare în vederea îndeplinirii cerinţei, în condiţiile în care în documentația de atribuire nu au fost solicitate servicii de dezvoltare software pentru Componenta de Comunicare cu Arhiva Electronică Legală.

Soluţia propusă nu prezintă cu exactitate aplicaţia care implementează cerinţele din documentaţia de atribuire legate de semnarea electronică şi marcarea temporală a documentelor în cadrul componentei de Comunicare cu Arhiva Electronică Legală.

Atât prin răspunsul la întrebarea 43 din solicitarea de clarificări nr. 3600/14.10.2014, cât şi în răspunsul la întrebarea nr. 10 din solicitarea de clarificari nr. MFE/DAPITA/4498/03.03.2015, ofertantul aduce modificări şi completări ofertei tehnice înaintată afirmând că aplicaţia SEAL este integrată cu DigiSigner SDK, şi mai mult, încearcă să inducă în eroare autoritatea contractantă.

În oferta tehnică la paginile 317-319, pentru indeplinirea cerinţelor din capitolul „Verificarea documentelor", este indicată aplicaţia SEAL Compliance Edition împreună cu componenta StarSign şi este precizată utilizarea unui SDK, fara a fi mentionata denumirea acestuia si nici produsul DigiSigner.

În conformitate cu cerinţele fişei de date capitolul IV.4.1) Modul de prezentare a propunerii tehnice, se precizează „În cadrul ofertei tehnice se va detalia de către prestator conformitatea soluţiei ofertate cu tote cerintele specificate în documentaţia de atribuire. Furnizorul trebuie să răspundă punctual la toate cerinţele cuprinse în documentaţia de atribuire şi să detalieze în propunerea sa tehnică modul şi mijloacele prin care soluţia ofertată îndeplineşte aceste cerinţe astfel încât comisia de evaluare să aibă posibilitatea evaluarii acesteia în mod cât mai informat".

Având în vedere cerinţa „Aplicaţia trebuie să fie oferită şi sub forma unui SDK care va permite verificarea semnăturilor documentelor electronice. SDK-ul va permite realizarea următoarelor operaţiuni către aplicaţiile care îl apelează" precum şi răspunsul ofertantului „Componenta Star Sign inclusă în produsul SEAL Compliance Edition ofertat permite verificarea documentelor, după cum urmează: [...] Se va oferi un SDK ce va permite verificarea semnăturilor documentelor electronice. SDK-ul oferit va permite realizarea următoarelor operaţiuni către aplicaţiile care îl apelează, după cum urmează: [...]" este evident că DigiSigner SDK nu a fost descris în oferta tehnică ca îndeplinind aceste cerinţe.

Astfel, răspunsul la întrebarea nr. 10 din solicitarea de clarificari nr. MFE/DAPITA/ 4498/ 03.03.2015 aduce completări ale ofertei tehnice.

În opinia contestatoarei, nominalizarea unor produse enumerate în oferta tehnică, fără a fi descrise și fără a se prezenta modul de integrare reprezintă, în mod eronat, modalitatea de îndeplinire a cerințelor documentației de atribuire.

Astfel, la paginile 36, 37 şi 40 din oferta tehnică, sunt prezentate denumirile produselor SEAL Compliance Edition și DigiSigner SDK precum și serverele pe care acestea se vor instala. Totuși, mai mult decât instalarea pe același server, nu este descrisă nicăieri integrarea dintre

cele două aplicații nici în această secțiune a ofertei și nici ulterior.

La paginile 317-318 din ofertă este prezentată furnizarea unui SDK pentru îndeplinirea cerințelor din secțiunea Verificarea documentelor aflat în subcapitolul 3.3.7.3. Utilizarea certificatelor digitale din capitolul 3.3.7. Modulul 7: Componenta de Securizare Acces si Documente. Acest capitol este diferit de Modulul 8: Modulul de arhivare a documentelor în care se află capitolul 3.3.8.1 Componenta de Comunicare cu Arhiva Electronică Legală. Și funcționalitățile solicitate în secțiunea Verificarea documentelor, sunt evident diferite iar SDK-ul care îndeplinește cerințele:

- "Aplicatia trebuie să fie oferită şi sub forma unui SDK care va permite verificarea semnăturilor documentelor electronice. SDK-ul va permite realizarea următoarelor operaţiuni către aplicaţiile care îl apelează:

- *Extragerea informaţiilor privind semnătura electronică şi certificatul semnatarului;*
- *Extragerea datelor în clar din documentul semnat.*

- Pentru SDK se va oferi documentaţia tehnică necesară pentru a permite integrarea în aplicaţiile care vor utiliza documente semnate electronic".

Nu îndeplineşte, în mod automat cerinţele privind:

- "această componentă de arhivare electronică va fi capabilă să aplice semnături digitale ..., iar aplicarea de semnături digitale va trebui să ofere următoarele capabilităţi minime:[…]"
- "Semnătură electronică va fi în conformitate cu următoarele standarde [...]"
- "Marca temporală care va fi aplicată semnăturii electronice va avea următoarele funcţionalităţi şi caracteristici:[...]", deoarece funcţionalităţile de creare a unei semnături electronice şi de marcare temporală sunt diferite de funcţionalităţile de verificare a semnăturii.

De asemenea, contestatoarea nu precizează în oferta tehnică depusă, că DigiSigner SDK că îndeplinește aceste funcționalități și nici modalitatea prin care DigiSigner SDK răspunde cerințelor din secțiunea Verificarea documentelor aflat în subcapitolul 3.3.7.3. Utilizarea certificatelor digitale, precum și a celor din capitolul 3.3.8.1 Componenta de Comunicare cu Arhiva Electronică Legală.

DigiSigner SDK nu este prezentat nici în documentaţia aferentă produsului DigiSigner, aflată la paginile 386-388 ale ofertei tehnice.

De asemenea, în documentaţia de atribuire nu au fost solicitate servicii de dezvoltare pentru Componenta de Comunicare cu Arhiva Electronică Legală.

Aşa cum reiese din cerinţele autorităţii contractante, din capitolul 2.1. OBIECTUL CONTRACTULUI: *„În vederea realizării obiectivelor contractului se vor achiziţiona următoarele:*

- Servicii de prelucrare arhivistică, inventariere şi digitizare a documentelor;

- Servicii de arhivare electronică;

- Servicii de depozitare fizică a documentelor după prelucrarea arhivistică;

- Soluţie de gestiune a documentelor şi a fluxurilor de lucru, cu serviciile de implementare aferente;

- Servicii de dezvoltare portal, inclusiv licenţele aferente;
- Servicii de certificare a semnăturii electronice, inclusiv dispozitive securizate de generare a semnăturii electronice;
- Soluţie de securizare a statiilor de lucru, inclusiv licentele aferente", singurele servicii de dezvoltare solicitate sunt aferente componentei portal şi nu se solicită servicii de dezvoltare pentru Componenta de Comunicare cu Arhiva Electronică Legală.

În concluzie, autoritatea contractantă învederează că:

1. În oferta tehnică înaintată, nu se regăseşte nicio precizare cu privire la integrarea dintre SEAL Compliance Edition cu componenta sa StarSign şi DigiSigner sau cu privire la utilizarea DigiSigner SDK de către aplicaţiile SEAL Compliance Edition sau StarSign.
2. Singurul SDK descris nu este denumit şi oferă exclusiv funcţionalităţi de verificare a documentelor semnate electronic, fără să se descrie funcţionalităţile acestui SDK privind crearea de semnături electronice şi de mărci temporale
3. În descrierea DigiSigner din matricea de conformitate şi în documentaţia aferentă acestui produs, aflată la paginile 386-388 ale ofertei tehnice, nu este menţionată existenţa DigiSigner SDK şi care sunt funcţionalităţile pe care acesta le are.
4. Prin răspunsul la întrebarea 43 din solicitarea de clarificari nr. 3600/ 14.10.2014, cât şi în răspunsul la întrebarea nr. 10 din solicitarea de clarificări nr. MFE/DAPITA/4498/03.03.2015, ofertantul aduce modificări şi completări ofertei tehnice înaintată, afirmând că aplicaţia SEAL este integrată cu DigiSigner SDK.

Având în vedere motivele enumerate mai sus, contestatoarea nu a descris în oferta depusă care este componenta integrată care să asigure Comunicarea cu Arhiva Electronică Legală şi să răspundă la cerinţele:
- "această componentă de arhivare electronică va fi capabilă să aplice semnături digitale ..., iar aplicarea de semnături digitale va trebui să ofere următoarele capabilităţi minime:[…]"
- "Semnătură electronică va fi în conformitate cu următoarele standarde [...]"
- "Marca temporală care va fi aplicată semnăturii electronice va avea următoarele funcţionalităţi şi caracteristici:[...]" şi nu a prezentat în oferta tehnică înaintată modalitatea de integrare între aplicaţia DigiSigner şi SEAL/StarSign şi nici faptul că pentru Componenta de Comunicare cu Arhiva Electronică Legală se va utiliza pentru integrare un SDK.

Astfel, autoritatea contractantă menţionază că din aceste motive, oferta tehnică înaintată este neconformă.

În final, se arată că oferta tehnică înaintată de Asocierea formată din ... demonstrează îndeplinirea cerințelor cu privire la gestionarea etichetelor cu coduri de bare RFID pasive şi la monitorizarea on-line a fluxului operațional.

Susţinerile contestatoarei sunt nefondate, nefiind bazate pe niciun argument concret. Aceste susţineri sunt simple presupuneri, întreaga contestaţie având ca scop tergiversarea încheierii procedurii de atribuire şi semnarea contractului, putând conduce, astfel, la pierderea fondurilor

alocate realizării proiectului.

Prin adresa nr. T/1142/09.04.2015, înregistrată la Consiliu sub nr. 5501/09.04.2015... formulează concluzii scrise faţă de susţinerile prezentate în cererea de intervenţie depusă de ....

I. Cu privire la excepţia lipsei de interes invocate de către intervenientă, contestatoarea susţine că este, în mod evident, vătămată prin actele autorităţii contractante de a respinge oferta sa şi de a declara drept câştigătoare o ofertă care prezintă elemente clare de inadmisibilitate, cu încălcarea principiului tratamentului egal.

De asemenea, contestatoarea susţine că are interes în a contesta oferta declarată câştigătoare, prin prisma faptului că, dacă şi această ofertă va fi declarată drept inadmisibilă ori se va constata că procedura de atribuire este grav afectată, iar aceasta va fi anulată, ... va putea participa cu ofertă la noua procedură; interesul unui ofertant a cărui ofertă a fost declarată neconformă în situaţii similare a fost reţinut şi în jurisprudenţa anterioară a instanţelor de judecată, sens în care de menţionează:

- Decizia civilă nr. 328 din 26 ianuarie 2012 a Curţii de Apel Bucureşti „pe de altă parte, petenta, a cărei ofertă a fost respinsă de autoritate ca neconformă, a criticat oferta câştigătoare, susţinând că […]. Curtea a analizat şi acest motiv al plângerii legat de conformitatea ofertei câştigătorului, întrucât petenta are un interes mediat, în contextul în care se constată că ambele oferte erau inacceptabile sau neconforme, autoritatea contractantă fiind obligată să anuleze procedura de atribuire, iar petenta ar avea posibilitatea în cazul în care se demarează o nouă procedura de licitaţie să participe cu o altă ofertă” (s.n.);
- Sentinţa civilă nr. 1529 din 30 aprilie 2013 a Curţii de Apel Bucureşti, potrivit căreia „în ceea ce priveşte excepţia lipsei de interes, instanţa observă că, deşi oferta petentei a fost calificată de autoritatea contractantă ca inacceptabilă (…), se apreciază de către instanţă că petenta are un interes mediat în soluţionarea cauzei, în contextul în care, dacă ar fi apreciate ca întemeiate argumentele prezentate în susţinerea acestui capăt de cerere, autoritatea contractantă ar fi obligată să anuleze procedura de atribuire, iar petenta ar avea posibilitatea, în cazul în care s-ar demara o nouă procedură de licitaţie, să participe cu o altă ofertă. În consecinţă, reţinând că petenta justifică un interes în soluţionarea cauzei, instanţa va respinge excepţia lipsei de interes ca neîntemeiată” (s.n.).

Având în vedere cele precizate anterior, contestatoarea conchide că are în mod evident interes pentru formularea criticilor cu privire la oferta declarată câştigătoare, excepţia lipsei de interes formulată de intervenientă urmând a fi respinsă.

II. Cu privire la respingerea ofertei sale, faţă de care intervenienta susţine că a identificat în contestaţie o serie de elemente care ar denota „neînţelegerea de către ofertantul ... a cerinţelor documentaţiei de atribuire”, contestatoarea afirmă că în realitate, aceste „elemente” nu fac decât să releve neînţelegerea de către intervenientă a cerinţelor aceleiaşi documentaţii, ridicând semne serioase de întrebare asupra modului în care Asocierea ... a abordat elaborarea ofertei tehnice.

Contestatoarea afirmă că soluţia propusă este un ansamblu de componente mature, fiecare în parte îndeplinind cerinţele din documentaţia de atribuire în considerarea cărora a fost propusă, componentele fiind disponibile comercial şi cu largă utilizare atât la nivel naţional, cât şi internaţional la momentul ofertării.

Prin separarea şi analizarea punctuală şi superficială a componentelor ofertate, cu ignorarea voită a contextului soluţiei globale în care acestea se integrează, intervenienta ... încearcă decredibilizarea soluţiei propuse de ....

... precizează că a ofertat un sistem 100% corespunzător cerinţelor autorităţii contractante, deşi format din mai multe componente, lucru care nu a fost interzis prin documentaţia de atribuire, ci dimpotrivă. Integrarea unor componente multiple este obiectiv necesar pentru a pune la dispoziţie sistemul solicitat şi este o precondiţie a asigurării unei concurenţe între mai mulţi producători, dat fiind că sistemul prezintă o complexitate aparte (accesarea şi manipularea documentelor utilizând o gamă largă de dispozitive şi aplicaţii), iar soluţii unitare, de la acelaşi producător, care să asigure simultan şi integral îndeplinirea cerinţelor autorităţii, sunt disponibile pe scară extrem de limitată. În mod aproape miraculos, singura soluţie unitară/integrată disponibilă pe teritoriul Romaniei care îndeplineşte până la virgulă cerinţele din documentaţia autorităţii, aparţine unuia din membrii asocierii al cărei reprezentant este Siveco şi care solicită să fie intervenient în această speţă.

Critica I: Această primă critică a intervenientei ... se referă la primul motiv de neconformitate invocat de autoritatea contractantă în comunicarea rezultatului procedurii, respectiv Motivul 1.

Contestatoarea precizează că, în esenţă, autoritatea susţine prin comunicarea rezultatului procedurii că din informaţiile prezentate de ..., s-a constatat că:

- Soluţia PKI Safe Layer reprezintă o soluţie de management a certificatelor digitale şi nu implementează funcţionalităţile de semnare, criptare/decriptare, ştergere sigură a fişierelor;
- În cadrul paragrafelor din ofertă care descriu soluţiile de semnare (pag. 312), criptare/decriptare, ştergere sigură a fişierelor (pag. 319-321) care se instalează pe staţiile de lucru, este prezentată soluţia DigiSigner, pentru care nu reiese din ofertă că este certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional.

Faţă de cerinţa pretins neîndeplinită de oferta ..., intervenienta consideră că „nu este clar care este rolul unei soluţii PKI (SafeLayer KeyOne) în cadrul ofertei tehnice, din moment ce nu s-a solicitat o astfel de soluţie, iar din contestaţie reiese că certificatele digitale solicitate în cadrul procedurii sunt furnizate de către Autoritatea de Certificare DigiSign. Introducerea unei soluţii PKI distincte în ofertă presupune că:

1. Autoritatea contractantă urmează să gestioneze singură certificatele digitale simple solicitate;

2. Pentru a putea emite certificate digitale simple, conform cerinţelor din documentaţia de atribuire, autoritatea contractantă trebuie să se

declare ca furnizor de servicii de certificare şi să îndeplinească cerinţele definite prin Legea nr. 455/2001 privind semnătura electronică. Niciunul dintre aceste lucruri nu au fost solicitate prin documentaţia de atribuire (…)”.

În ceea ce priveşte aceste alegaţii ale intervenientei, contestatoarea afirmă că atitudinea oscilantă a autorităţii contractante cu privire la specificaţiile referitoare la certificatele digitale, acestea fiind neclare şi suferind multiple modificări în urma rundelor de întrebări de clarificare şi a contestaţiilor anterioare depunerii ofertelor, ... (inclusiv subcontractanţii săi) a intenţionat să ofere autorităţii contractante o soluţie superioară cerinţelor exprimate, tocmai pentru a evita posibilitatea unei interpretări cu rea-voinţă a ofertei sale şi a unei eventuale concluzii asupra neconformităţii acesteia.

Oferirea posibilităţii autorităţii contractante de a emite certificatele digitale nu contravine în nici un fel cerinţelor din documentaţie şi, mai mult, asigură integrarea între 2 soluţii software, şi anume a Autorităţii de înregistrare KeyOne cu Autoritatea de certificare (Root CA) a Digisign.

In plus, aceşti termeni tehnici reprezintă numele unor componente ale soluţiei unitare pentru: „Servicii de arhivare fizică şi servicii de arhivare electronică a documentelor elaborate/gestionate în cadrul Ministerului Fondurilor Europene”.

De asemenea, contestatoarea menţionează că este complet eronată şi răuvoitoare concluzia intervenientei conform căreia autoritatea contractantă urmează să gestioneze singură certificatele digitale. Fiind vorba de certificate digitale simple, o Autoritate de Certificare poate fi implementată on-premise (la client) pentru a facilita distribuirea certificatelor digitale integrate în cadrul sistemului informatic, însă operaţiunile de gestionare vor fi asigurate, în conformitate cu informaţiile specificate în oferta tehnică, de către furnizorul acestor certificate digitale, respectiv de către Autoritatea de Certificare Rădăcină (Root CA) a DigiSign, căreia Autoritatea de Certificare implementată on-premise îi va fi subordonată.

Nicăieri în oferta tehnică nu este specificat faptul că gestiunea certificatelor digitale cade în sarcina autorităţii contractante, astfel că nu se poate susţine, sub acest aspect, niciun motiv de neconformitate a ofertei cu documentaţia de atribuire. Pentru construirea unei Autorităţi de Certificare subordonate Autorităţii de Certificare Rădăcină (Root CA), în vederea emiterii certificatelor digitale, poate fi utilizat orice sistem tehnologic de tip PKI (proprietar, comercial sau open-source). În acest caz s-a optat pentru soluţia PKI SafeLayer KeyOne, alegerea soluţiei optime fiind lăsată la latitudinea ofertantului.

Totodată, în opinia contestatoarei este profund eronată susţinerea intervenientei conform căreia autoritatea contractantă trebuie să se declare ca furnizor de servicii de certificare şi să îndeplinească cerinţele definite prin Legea nr. 455/2001 privind semnătura electronică, nefiind cazul ca autoritatea contractantă să gestioneze certificatele digitale.

Actualmente, există în România atât instituţii de stat, cât şi companii private care au implementate sisteme PKI şi nu apar declaraţi public ca şi

furnizori de servicii de certificare. De fapt, singurele autorităţi de certificare declarate public pe site-ul Autoritatii de Reglementare şi Supraveghere din cadrul MSI pot fi consultate la adresa: http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Tehnologia - Informatiei/Servicii-electronice/Semnatura-electronica.

Consultand registrul disponibil, se constată că apar 10 furnizori de servicii de certificare, 6 acreditaţi, 2 cu activitatea încetată şi 2 neacreditaţi. Ar fi absurd să se concluzioneze faptul că doar 10 companii/instituţii au implementat sistem PKI în România.

Mai mult, intervenienta susţine, din nou în mod eronat şi tendenţios, că „Utilizarea la implementarea proiectului a altor certificate digitale decât cele emise de o soluţie PKI care nu este a furnizorului DigiSign, sub Root CA DigiSign, aşa cum este indicat în oferta tehnică contravine cerinţelor minime ale autorităţii contractante şi este neconformă".

Afirmaţia antemenţionată, în opinia contestatoarei, presupune eronat că fiecare furnizor de servicii de certificare are propriul sistem tehnologic PKI de emitere a certificatelor digitale. Cerinţa solicită prezentarea următoarelor informaţii despre furnizorul certificatelor: (i) denumirea acestuia; (ii) dacă este sau nu furnizor acreditat în conformitate cu Legea nr. 455/2001 şi (iii) informaţii referitoare la certificatul rădăcină sub care sunt emise certificatele digitale simple.

Tratarea de către ... a cerinţei din documentaţia de atribuire îndeplineşte în totalitate şi respectă cerinţele minime ale autorităţii contractante. Orice organizaţie sau furnizor de servicii de certificare poate avea un număr nelimitat de Autorităţi de Certificare Rădăcină şi Autorităţi de Certificare subordonate, iar sistemele PKI utilizate pentru emiterea certificatelor digitale simple pot fi proprietare, comerciale sau open-source.

A doua critică a intervenientei ... – „Nu rezultă în mod explicit care este soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) şi care trebuie să fie certificată din punct de vedere al securităţi informatice de către un organism abilitat la nivel naţional, european sau internaţional, prezentată în cadrul ofertei ..." – se referă tot la primul motiv de neconformitate invocat de autoritatea contractantă în comunicarea rezultatului procedurii.

Astfel, contestatoarea susţine că cerinţa enunţată este îndeplinită integral de soluţia propusă, formată din componentele la care ...face referire în cererea de intervenţie: (i) componenta DigiSigner; (ii) componenta SafeLayer KeyOne; (iii) componenta TrustedX.

... a segmentat însă soluţia în momentul în care a descris-o într-o manieră care să faciliteze procesul de discreditare a soluţiei complete şi conforme propuse de ... deşi ... nu îşi poate forma o opinie pertinentă în lipsa tuturor informaţiilor detaliate în cadrul ofertei tehnice.

Contestatoarea menţionează că în oferta depusă a indicat cu claritate că înţelege să probeze îndeplinirea cerinţei prin soluţia SafeLayer PKI, care prin tehnologia TrustedX implementează funcţionalităţile solicitate (semnare, criptare/decriptare, ştergere sigură a fişierelor) şi deţine

certificarea din punct de vedere al securităţii informatice emisă de către un organism abilitat la nivel internaţional, respectiv certificarea Common Criteria EAL 4+, care răspunde întrutotul cerinţei menţionate. Aşa cum a fost prezentat şi consemnat în cadrul sesiunii demonstrative, DigiSigner este componenta client care realizează funcţiile de semnare, criptare/decriptare, ştergere sigură prin integrarea la nivelul librăriilor criptografice cu TrustedX, soluţie certificată Common Criteria EAL 4+, aceasta certificare fiind conformă cerinţei exprimate în documentaţia de atribuire.

De asemenea, se afirmă că sunt disponibile 2 variante de produs DigiSigner, una disponibilă gratuit pentru descărcare pentru medii non-enterprise (personal, home, non-commercial) şi una pentru mediile enterprise, aşa cum este şi cazul soluţiei oferite în cadrul prezentei proceduri, aceasta fiind cea demonstrată în faţa comisiei de evaluare.

Contestatoarea reiterează că funcţionalităţile de semnare, criptare/decriptare, ştergere sigură au fost demonstrate în cadrul sesiunii demonstrative, fiind efectiv prezentate tuturor membrilor comisiei de evaluare. Pentru confirmarea afirmaţiilor de mai sus, contestatoarea prezintă capturi de ecran ale aplicaţiei DigiSigner pentru mediul enterprise.

A treia critică a intervenientei ... – „admiţând faptul că există o componentă «client» - DigiSigner şi o componentă «server» - TrustedX, nu se poate invoca exclusiv certificarea componentei de tip server pentru a justifica certificarea întregii soluţii, în condiţiile în care pe staţiile de lucru se instalează componenta «client», care nu deţine nicio certificare” – vizează tot primul motiv de neconformitate invocat de autoritatea contractantă în comunicarea rezultatului procedurii.

Înţelegerea intervenientei asupra noţiunii de „soluţie” este eronată şi tendenţioasă, neexistând o cerinţă în cadrul documentaţiei de atribuire în care să fie specificat, în mod explicit, faptul că atât componenta de tip server, cât şi componenta de tip client, trebuie să fie certificată din punct de vedere al securităţii informaţiei de către un organism abilitat la nivel naţional, european sau internaţional.

Mai mult, aspectele învederate de intervenientă cu privire la aplicaţia DigiSigner fac referire la versiunea publică a software-ului DigiSigner, care este oferită gratuit, în regim freeware. Este absurdă şi nefondată opinia acesteia conform căreia programul DigiSigner nu este oferit şi în regim comercial de către producătorul DigiSign, înscris în Registrul Naţional al Programelor pentru Calculator pentru a desfăşura activităţi de producere, comercializare şi distribuire a acestui program. În plus, decizia de a restricţiona accesul la toate funcţionalităţile specificate de ..., respectiv de integrare a componentei TrustedX sau a altei componentei tehnologice, de ştergere sigură a informaţiilor şi de configurare a acestor funcţionalităţi priveşte strict politica producătorului DigiSign de comercializare a programului software DigiSigner.

De asemenea, contestatoarea precizează că, deşi produsele software sunt disponibile comercial, acestea necesită configurări şi parametrizări pentru a lucra împreună, aşa cum s-a demonstrat în cadrul sesiunii

demonstrative folosind un mediu de test în care aceste componente au fost configurate să lucreze împreuna, precum şi faptul că în ofertă se indică o perioadă de 8 luni pentru implementarea proiectului ca ansamblu de activităţi, inclusiv integrarea dintre DigiSigner şi TrustedX – în mod nefondat considerată neverosimilă de către ..., în ciuda faptului că membrii comisiei de evaluare au putut asista la prezentarea tuturor acestor funcţionalităţi în cadrul sesiunii demonstrative.

A patra critică a intervenientei ... – „prin contestaţia înaintată ... furnizează Autorităţii contractante şi onoratului Consiliu informaţii false cu privire la lipsa versiunilor pentru aplicaţia SafeLayer MobileID" – se raportează la al doilea motiv de neconformitate învederat de autoritatea contractantă în comunicarea rezultatului procedurii.

Autoritatea se bazează între altele pe „argumentul" că în oferta ... nu s-ar regăsi versiunea de produs ofertată pentru aplicaţia SafeLayer MobileID. Intervenienta constată că în AppStore această aplicaţie este prezentă cu versiunea 1.3.1 şi că tot în AppStore utilizatorii pot consulta informaţii privind istoricul versiunilor anterioare.

Faţă de cele susţinute de intervenientă, ca şi de Autoritatea contractantă, contestatoarea învederează că a respectat cerinţa autorităţii de a oferta „versiuni actuale" ale produselor software, în condiţiile în care a declarat că se vor oferi versiuni actuale, în ciuda faptului că nu a exprimat în clar numărul versiunii software. În condiţiile în care acest argument nu este de natură să atragă declararea ofertei ... ca neconformă, afirmaţia ...potrivit căreia lipsa versiunilor conduce la furnizarea de informaţii false, fiind doar o altă acuzaţie lipsită de fundament.

A cincea critică a intervenientei ... – „prin contestaţia înaintată ... furnizează autorităţii contractante şi onoratului Consiliu informaţii false cu privire la disponibilitatea SafeLayer MobileID în Google Play" – se referă tot la al doilea motiv de neconformitate identificat de autoritatea contractantă în comunicarea rezultatului procedurii.

Faţă de această alegaţie a intervenientei, fiind general cunoscut faptul că se pot instala aplicaţii în cadrul sistemului de operare Google Android fără a se utiliza un repository de tip Google Play, contestatoarea precizează că a specificat că există aplicaţii pentru Google Android, fără ca în ofertă sau în contestaţie să fi afirmat că Mobile ID este disponibilă în Google Play.

În acest sens, contestatoarea afirmă că în contestaţie a făcut referire la concluzia de la punctul 3 al sesiunii demonstrative din 13.11.2014, consemnată în procesul verbal nr. 4198/13.11.2014 din care a reprodus în extras pasajul relevant:

3. Aplicatia pentru generarea cheilor si a cererilor de certificate este prezenta in Google Play/App store sau in alt store de aplicatii?

Răspuns ofertant: Da,ofertantul a demonstrat că aplicația ofertată pentru generarea cheilor şi a cererilor de certificate este prezentă în App store. Pentru Android a fost prezentata versiunea de autentificare din browser

Aşadar, contestatoarea susţine că în contestaţie a arătat că pentru sistemul de operare Google Android în sesiunea demonstrativă a fost prezentată versiunea de autentificare din browser, Autoritatea contractantă confirmând că a luat act de această demonstraţie. Nu a susţinut însă că Mobile ID este disponibilă în Google Play. Oricum, prin documentaţia procedurii nu s-a solicitat ca aplicaţia să fie disponibilă în Google Play, ci doar compatibilă cu Android, fapt confirmat de broşura de la producător a aplicaţiei ofertate de ..., prezentată şi în oferta tehnică.

În concluzie, afirmaţia intervenientei ... cu privire la furnizarea de informaţii false de către ... nu poate fi catalogată altfel decât tendenţioasă şi nu are decât scopul de a induce autorităţii contractante o falsă percepţie cu privire la oferta depusă.

A şasea critică a intervenientei ... – „din contestaţie … reiese faptul că aplicaţia SafeLayer Mobile ID «furnizează protecţie împotriva furtului de identitate fără a utiliza produse de autentificare adiţionale (matrix card, OTP device sau smart card)». Prin urmare, este neverosimilă conformitatea acestei aplicaţii cu specificaţiile solicitate, respectiv capabilitatea de a se integra cu dispozitive criptografice de tip smartcard (pentru generare de chei criptografice şi înscriere de certificate digitale pe acestea)” – se referă tot la al doilea motiv de neconformitate identificat de autoritatea contractantă în comunicarea rezultatului procedurii.

Susţinerea intervenientei este falsă, fiind bazată pe o traducere distorsionată a textului redat de ... în contestaţie sub forma unei capturi de ecran de pe pagina http://www.safelayer.com/en/solutions/mobile-identification.

Din captura de ecran reluată de intervenientă la pag. 13 din cererea de intervenţie nu reiese faptul că aplicaţia SafeLayer Mobile ID „furnizează protecţie împotriva furtului de identitate fără a utiliza produse de autentificare adiţionale (matrix card, OTP device sau smart card)”. Afirmaţia intervenientei ... se bazează pe o traducere subiectivă din limba engleză a capturii de ecran, care nu redă întreaga funcţionalitate a aplicaţiei, ci doar o capabilitate a acesteia.

Pentru conformitate, contestatoarea redă textul original în limba engleză care a fost în mod tendenţios denaturat la traducere de către .. *„SafeLayer Mobile ID is an innovative identification system based on intelligent mobile devices (telephones and tablets). It provides protection against identity fraud without REQUIRING an ADDITIONAL authenticator (matrix card, OTP device, smart card” (s.n.).*

Traducerea corectă ar fi fost următoarea:

„SafeLayer Mobile ID este un sistem inovativ de identificare, bazat pe dispozitive mobile inteligente (telefoane sau tablete). Acesta furnizează protecţie împotriva furtului de identitate, fără a solicita/necesita produse de autentificare adiţionale (matrix card, OTP device, smart card)”.

Prin urmare, SafeLayer este un sistem care furnizează protecţie împotriva furtului de identitate, fără a impune utilizatorilor achiziţionarea de produse de autentificare adiţionale, asigurând, aşadar, acestora şi funcţionalităţile oferite de asemenea produse, ceea ce vine în avantajul clienţilor care nu doresc să achiziţioneze produse de autentificare

adiţionale. Din această frază reiese faptul că SafeLayer Mobile ID este o soluţie care oferă funcţionalităţi superioare faţă de cerinţele minime solicitate de autoritatea contractantă.

Capabilitatea de a se integra cu dispozitive criptografice de tip smartcard, despre care în mod tendenţios intervenientul afirmă că ar fi neverosimilă, este prezentată atât pe site-ul producătorului la adresa http://www.safelayer.com/en/compliance/technical-standards, unde este specificată în mod clar compatibilitatea produselor SafeLayer cu standardul PKCS#11, cât şi în datasheet-ul componentei KeyOne (http://www.safelayer.com/images/stories/pdf/keyone_xra_en.pdf).

A şaptea critică a intervenientei ... – „Componenta KeyOne XRA ofertată nu reprezintă o componentă de autentificare a utilizatorilor, ci este interfaţa de Autoritate de Înregistrare (RA – Registration Authority), interfaţa prin care sunt înregistraţi utilizatorii pentru emiterea certificatelor digitale" – se referă la al treilea motiv de neconformitate identificat de autoritatea contractantă în comunicarea rezultatului procedurii.

Identic cu autoritatea contractantă, intervenienta consideră că ... ar fi invocat componenta KeyOne XRA a soluţiei SafeLayer PKI, respectiv componenta de „Registration Authority" („RA") a soluţiei enunţate, care în viziunea autorităţii nu face dovada îndeplinirii cerinţelor referitoare la accesul unui utilizator de pe PC în sistem, deoarece ar avea numai funcţionalităţi de înregistrare a utilizatorilor în sistem, nu şi de acces al utilizatorilor la sistem.

În replică la cele susţinute de intervenienta ..., contestatoarea susţine că aceasta presupune în mod eronat faptul că Autoritatea de Certificare a DigiSign are o singură componentă de înregistrare a utilizatorilor, prezentând în mod tendenţios interfaţa web pusă la dispoziţie de DigiSign pentru înregistrarea clienţilor de certificate digitale calificate, care nu fac obiectul prezentei proceduri.

Funcţionalităţile de autentificare a componentei KeyONE XRA sunt specificate chiar în datasheet-ul produsului, din care contestatoarea citează:

„This enables deploying PKI authentication, e-signing and encryption for a wide range of PKI-compatible applications and platforms: Windows, Mac and Linux desktop environments and mobile devices with Google Android and Apple iOS operating systems are supported" şi

„Certificate life-cycle management for PKI services and applications that require authentication, signature and data encryption."

Contestatoarea menţionează că soluţia ofertată este superioară celei solicitate prin documentaţia de atribuire, prin faptul că au fost ofertate atât Autoritate de Înregistrare („Registration Authority" sau „RA"), respectiv KeyOne XRA, cât şi Autoritate de certificare sub Root CA DigiSign, oferta fiind din toate punctele de vedere conformă cu cerinţele din documentaţia de atribuire. Rolul KeyOne XRA rezultă cu claritate din arhitectura PKI şi din explicaţiile prezentate în oferta tehnică.

A opta critică a intervenientei ... – „Specificaţiile prevăzute în capitolul Asigurarea confidenţialităţii documentelor trebuie tratate în

integralitatea lor, în sensul că aplicaţiile ofertate pentru asigurarea funcţionalităţilor de criptare trebuie să implementeze aceste funcţionalităţi prin mecanismele de criptare prevăzute în documentaţie (…) Aplicaţia BitLocker propusă de ..., disponibilă pentru sistemele de operare Microsoft Windows (…) nu poate reprezenta o soluţie de criptare la nivel de operare prin crearea unei partiţii criptate care respectă cerinţele Autorităţii Contractante, întrucât BitLocker utilizează ca algoritm de criptare simetrică doar unul dintre algoritmii solicitaţi, respectiv AES" – se referă la motivul 9 de neconformitate din comunicarea rezultatului procedurii.

Contestatoarea reaminteşte că autoritatea contractantă a susţinut că prin clarificările pe care le-a furnizat referitoare la cerinţa din caietul de sarcini privind „Asigurarea confidenţialităţii datelor", cap. 3.3.7.3.2, ... ar fi arătat că „Aplicaţia DigiSigner propusă integrează în tehnologiile PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici si asimetrici. Astfel, produsul BitLocker suportă algoritmul criptografic simetric 3DES atât prin intermediul componentei client DigiSigner, care integrează algoritmul criptografic simetric 3DES, cât şi prin dispozitivele criptografice securizate SafeNet e-Token PRO (…)".

Autoritatea însă pretinde că a constatat că dispozitivele securizate SafeNet e-Token PRO suportă algoritmul 3DES, dar realizează această criptare numai dacă aplicaţia care solicită criptarea implementează acest algoritm. Or, BitLocker nu implementează algoritmul 3DES, ci doar AES, conform documentaţiei producătorului.

Autoritatea este în eroare, deoarece în caietul de sarcini nu există o cerinţă privitoare la „Asigurarea confidenţialităţii datelor" având cuprinsul menţionat de autoritate, respectiv: *„Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici si asimetrici, astfel:*

- *Cripratea asimetrică, utilizând certificatele X509v3 şi algoritmul RSA,*
- *Criptarea simetrică folosind algoritmii 3DES şi AES".*

Cerinţa cu conţinutul enunţat se află în subcapitolul „Asigurarea confidenţialităţii documentelor". La acest punct, răspunsul ... la cerinţa menţionată este următorul: *„Aplicatia DigiSigner propusă integrează în tehnologiile PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici şi asimetrici, după cum urmează: (Referinţe: Broşura_DigiSigner.pdf):*

Criptarea asimetrica se realizează utilizând certificatele X.509 v3 şi algoritmul RSA.

Criptarea simetrică se realizează utilizând algoritmii 3DES şi AES."

Astfel, contestatoarea afirmă că răspunsul său a fost aşadar conform cerinţei caietului de sarcini, aplicaţia prin care se realizează funcţiile de criptare fiind DigiSigner. Cum referirea la cerinţa suportului pentru algoritmul 3DES se află în capitolul dedicat „Asigurării confidenţialităţii documentelor", răspunsul ... este conform cerinţei câtă vreme aplicaţia DigiSigner suportă toţi algoritmii criptografici solicitaţi.

Pe de altă parte, produsul BitLocker răspunde cerinţelor caietului de sarcini, dar nu are nicio legătură cu tehnologia PKI şi nici cu necesitatea criptării utilizând algoritmul 3DES, aferentă capitolului „Asigurarea confidenţialităţii documentelor”.

Astfel, BitLocker realizează criptarea partiţiilor şi răspunde la cerinţelor referitoare la criptarea aplicaţiilor, conform cărora „Criptarea trebuie să poată fi realizată astfel: a. La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată ”. În cuprinsul cerinţei citate nu se precizează algoritmul criptografic 3DES, deci prin documentaţie nu s-a cerut ca BitLocker să implementeze acest algoritm.

Este complet eronată din punct de vedere tehnic şi arhitectural concluzia intervenientei conform căreia un produs ce realizează criptare de partiţii ar putea intra în categoria soluţiilor de PKI. În vederea clarificării confuziei în care intervenienta se află, contestatoarea reiterează în cele ce urmează câteva aspecte de bază accesibile atât în domeniul public, cât şi în literatura de specialitate, pe care orice integrator de soluţii de securitate ar trebui sa le cunoască, mai ales în situaţia în care propune o soluţie de PKI la nivelul de complexitate cerut în cazul prezentului proiect.

Astfel, o Infrastructură de Chei Publice („PKI”) se referă la un sistem format din hardware, software, politici necesare pentru crearea, gestionarea, distribuţia, utilizarea, stocarea şi revocarea certificatelor digitale. Aceasta are 3 scopuri principale:

- publicarea cheilor / certificatelor publice;
- certificarea faptului că o cheie este legată de un individ sau de o entitate,
- verificarea validităţii unei chei publice.

Pe de altă parte, criptarea discului (sau a partiţiilor) este o tehnologie ce protejează informaţiile existente pe un suport fizic de stocare, convertindu-le într-un format indescifrabil de către persoane neautorizate, în lipsa unei chei de criptare.

Nicăieri în documentaţiile de specialitate nu se specifică existenţa vreunei legături directe prin care o soluţie de criptare de disc ar putea intra în categoria soluţiilor PKI. Intervenienta comite aşadar o confuzie tehnică inacceptabilă pentru nivelul de profesionalism şi experienţă pe care aceasta îl invocă în cadrul prezentei proceduri de atribuire.

Mai mult decât atât, cele două soluţii îndeplinesc principii de securitate diferite, principalul scop al PKI fiind de a asigura confidenţialitatea, autentificarea şi non-repudierea, în timp ce o soluţie de criptare de disc serveşte scopului protejării integrităţii datelor stocate pe o anumita maşină.

În concluzie:

- produsul BitLocker este o soluţie de criptare de disc care răspunde cerinţei enunţată: *„Criptarea trebuie să poată fi realizată astfel: a. La nivel de sistem de operare, prin crearea unei partitii criptate (…);”*

- aplicaţia DigiSigner răspunde cerinţei conform căreia *„Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici şi asimetrici, astfel: Criptarea asimetrica, utilizand certificatele X509v3 si algoritmul RSA; Criptarea simetrica folosind algoritmii 3DES si AES*", conform precizărilor din oferta tehnică privind această aplicaţie: *„Aplicatia DigiSigner propusă integrează în tehnologiile PKI mecanismele de criptare care se bazează pe algoritmi criptografici standard, simetrici şi asimetrici, după cum urmează: (Referinţe: Brosura_DigiSigner.pdf)*

- *Criptarea asimetrica se realizeaza utilizand certificatele X.509 v3 si algoritmul RSA.*
- *Criptarea simetrica se realizeaza utilizand algoritmii 3DES si AES."*

A noua critică a intervenientei ... se referă la următoarele motive de neconformitate identificate de autoritate în comunicarea rezultatului procedurii:

- motivul 2: Autoritatea contractantă susţine că nu este îndeplinită cerinţa: „utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil";

- motivul 4: Autoritatea contractantă consideră că ... nu a probat îndeplinirea cerinţei ca aplicaţia de generare a cheilor criptografice direct pe terminalul mobil să realizeze „înscrierea certificatului digital atât pe dispozitivul mobil, cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta";

- motivul 9, prin care autoritatea contractantă susţine că oferta ... nu îndeplineşte cerinţa privitoare la modul de realizare a criptării, respectiv: „Criptarea trebuie să poată fi realizată astfel: a. La nivel de sistem de operare, prin crearea unei partiţii criptate".

În susţinerea poziţiei sale, intervenienta citează concluziile sesiunii sesiunii demonstrative din 13.11.2014, consemnate la pct. 3, 5 şi 8 din procesul verbal nr. 4198/13.11.2014, susţinând că acestea nu confirmă că s-ar fi demonstrat îndeplinirea cerinţelor caietului de sarcini.

Contestatoarea precizează că .. face afirmaţii pe care le scoate cu rea-voinţă din contextul prezentării concluziilor sesiunii demonstrative, în care funcţionalităţile din modulul 7 au fost demonstrate conform solicitărilor comisiei de evaluare din cadrul autorităţii contractante.

Astfel, intervenienta susţine că:

- Răspunsul de la pct. 3 din procesul verbal citat mai jos demonstrează, în opinia intervenientei, că ... nu a ofertat o aplicaţie client instalată pe terminalele mobile cu sistem Android, care să răspundă la cerinţa: „utilizatorii trebuie să aibă la dispozitie o aplicatie de generare a cheilor criptografice direct pe terminalul mobil", deoarece „arată doar faptul că a fost realizată o autentificare, nu şi că a fost prezentată aplicaţia care să realizeze generare a cheilor criptografice direct pe terminalul mobil cu sistem de operare Android":

3. Aplicatia pentru generarea cheilor si a cererilor de certificate este prezenta in Google Play/App store sau in alt store de aplicatii?

Răspuns ofertant: Da,ofertantul a demonstrat că aplicația ofertată pentru generarea cheilor şi a cererilor de certificate este prezentă în App store. Pentru Android a fost prezentata versiunea de autentificare din browser

Contestatoarea îşi exprimă nedumerirea privind evaluarea soluţiei sale şi a interpretării procesului verbal al sesiunii demonstrative, mai ales că autoritatea contractantă nu a consemnat niciun aspect de neconformitate a soluţiei prezentate.

- Răspunsul de la pct. 5 din procesul verbal citat mai jos demonstrează în opinia intervenientei că ... nu a ofertat o aplicaţie client instalată pe terminalele mobile cu sistem Android, care să realizeze „înscrierea certificatului digital atât pe dispozitivul mobil, cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta" deoarece „arată doar faptul că a fost realizată o autentificare, nu şi că a fost prezentată aplicaţia care să realizeze înscrierea certificatului digital pe terminalul mobil cu sistem de operare Android":

5. Demonstratia include utilizarea certificatelor digitale pe terminalele mobile stocate pe dispozitivul criptografic propriu, conectat la terminalul mobil?

Răspuns ofertant: Da, a fost făcută o demonstrație în cadul sesiunii de prezentare a autentificarii cu dispozitiv criptografic conectat la terminal mobil Android.

Având în vedere cele antemenţionate, contestatoarea precizează că din declaraţia de la producătorul Safelayer (Anexa nr. 2 la adresa ... nr. MFE/DAPITA/4598/06.03.2015) reiese clar şi fără echivoc că aplicaţia care implementează partea de înscriere certificate pentru echipamente mobile este "Mobile PKI" (aceeaşi cu „Safelayer Mobile ID", aşa cum am arătat anterior, susţinut de declaraţia Safelayer – Anexa nr. 1 la adresa ... nr. MFE/DAPITA/4598/06.03.2015). Conform declaraţiei de la producător, soluţia propusă permite înscrierea cheilor criptografice direct pe terminalul mobil şi pe dispozitive criptografice de tip smartcard, conectat la terminalul mobil.

- Răspunsul de la pct. 8 din procesul verbal citat mai jos demonstrează în opinia intervenientei că oferta ... nu îndeplineşte cerinţa de blocare a accesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului, întrucât din procesul verbal nu reiese „care au fost aplicaţiile utilizate în cadrul demonstraţiei şi nici că aplicaţia BitLocker permite blocarea accesului la partiţiile criptate":

8. Sunt prezentati algoritmii criptografici folositi pentru criptare fisiere si criptare partiții?

Răspuns ofertant: Da, ofertantul a făcut o demonstrație pe fişiere criptate şi pe partiții criptate.

Contestatoarea menţionează că dovada funcţionalităţii de blocare a accesului la informaţiile aflate pe partiţia criptată la deconectarea smartcard-ului a fost făcută cu prisosinţă în cadrul sesiunii demonstrative din 13.11.2014, cu prilejul demonstraţiei pe care ... a făcut-o pe fişiere criptate şi pe partiţii criptate, despre care se face menţiune la punctul 8 din procesul verbal.

Totodată se arată că abordarea cerinţei enunţate la pag. 320 paragraful 3 din oferta tehnică, dublată de demonstraţia practică

susţinută, este întrutotul conformă caietului de sarcini, în cadrul căruia nu s-a impus ofertanţilor un mod specific în care să detalieze sau să probeze modalitatea de îndeplinire a cerinţei în cauză.

În final contestatoarea apreciază că argumentele învederate de intervenientă nu ţin seama de faptul că nu i se poate îngrădi dreptul de a critica acele aspecte de admisibilitate ale ofertei câştigătoare de care a luat cunoştinţă cu ocazia consultării dosarului achiziţiei. În acest sens, contestatoarea invocă motivarea Deciziei CNSC nr. 2558/C8/2544,2582/18.07.2013.

Prin adresa nr. 276/17.04.2015, înregistrată la Consiliu sub nr. 6053/17.04.2015, ... formulează note scrise faţă de concluziile scrise ale contestatoarei nr. T/1142/09.04.2015.

Faţă de răspunsul contestatoarei cu privire la excepţia lipsei de interes, intervenienta afirmă că prin demersul său, contestatoarea nu a înteles să evidenţieze „elementele clare de inadmisibilitate" ale ofertei sale, astfel că interesul acesteia nu poate fi unul personal şi direct, în sensul că folosul practic trebuie să o vizeze pe contestatoare.

Mai mult, trecând peste faptul că prin contestaţie ... nu a solicitat şi anularea procedurii de atribuire, este fără tagadă că interesul contestatoarei în cadrul procedurii de atribuire a contractului de achizitie publică nu poate fi constituit decât de folosul practic al adjudecării contractului, iar nu de anularea procedurii de atribuire, întrucât interesul trebuie să fie clar şi născut şi actual – existent în cadrul procedurii derulate, ci nu eventual, constând în participarea la o nouă procedură de atribuire cu privire la care nu are certitudinea că va mai fi organizată.

Intervenienta invocă Decizia civila nr. 51/CA din 21 februarie 2013 a Curtii de Apel Constanta – Sectia a II-a civila, de contencios administrativ si fiscal, din cuprinsul căreia rezultând următoarele:

„Referitor la soluţia dată de Consiliu exceptiei lipsei de interes in formularea contestatiei de catre N.S.C. Ltd., Curtea constata ca nu este fondata. Nu poate fi primita motivarea Consiliului in sensul ca societatea ar avea un interes pornind de la calitatea sa de ofertant in cadrul procedurii de atribuire, prin aceasta manifestandu-si vointa de a se angaja din punct de vedere juridic in contractul de achizitie publica, urmarind atribuirea lui in favoarea sa.

Oferta depusa de societate a fost considerata inacceptabila de catre autoritatea contractanta, intrucat valoarea ofertei reprezenta 262% din valoarea estimata a contractului. Criticand raportul procedurii, contestatoarea nu a adus in fata Consiliului vreun argument in sustinerea netemeiniciei solutiei adoptate de autoritatea contractanta in privinta sa. In aceste conditii, solutia ramanand definitiva, societatea nu mai poate participa in atribuirea contractului si, in aceasta cauza, nu ii serveste niciunui interes personal si direct, nascut si actual anularea procedurii de atribuire.

Avand in vedere ca interesul sau poate fi considerat nascut si actual doar in legatura cu procedura actuala, in care a participat, nu poate fi primit argumentul conform caruia anularea procedurii actuale da contestatoarei posibilitatea de a participa din nou la licitatie, ca urmare a

reluarii ei, tocmai pentru ca interesul verificat in cauza nu poate fi raportat la un eveniment viitor si incert.

(…)

Prin urmare, fata de cele de mai sus, Curtea apreciaza ca fiind intemeiata exceptia lipsei de interes in formularea contestatiei de catre (…) si va respinge contestatia acesteia ca fiind formulata de o persoana lipsita de interes."

În considerarea celor de mai sus, odata reţinută neconformitatea ofertei contestatoarei, intervenienta solicită să se constate lipsa de interes a ... în formularea criticilor referitoare la oferta Asocierii ...

Cu privire la motivele care au stat la baza respingerii ofertei sale, intervenienta afirmă că prin intermediul concluziilor scrise, contestatoarea face dovada neconformităţii ofertei sale, prin afirmaţii contrare documentelor de la dosarul achizitiei, respectiv a răspunsurilor la solicitările de clarificări venite din partea autorităţii contractante, chiar contrare celor aratate în cuprinsul contestaţiei, fiind evident că ... fie nu are cunoştinţă despre conţinutul propunerii sale tehnice, fie încearcă să dea o aparenţă de conformitate ofertei sale, prin modificarea propunerii tehnice iniţiale.

Astfel, la o simplă analiză a punctului de vedere al autorităţii contractante, precum şi a răspunsurile la clarificări, transmise de către autoarea contestaţiei pe parcursul etapei de evaluare a ofertei, se poate constata cu uşurinţă inconsecvenţa declaraţiilor acesteia, răspunzând de cele mai multe ori neconcludent solicitărilor comisiei de evaluare şi, mai mult, procedând inclusiv la modificarea propunerii tehnice, aspect contract dispozitiilor imperative ale art. 79 alin. (1) si (2) din HG nr. 925/2006, cu modificarile si completarile ulterioare.

În susţinerea celor de mai sus, intervenienta prezintă în continuare o expunere punctuală a neconformităţilor ofertei contestatoarei, precum şi un răspuns la afirmaţiile nefondate şi neîntemeiate arătate în concluziile scrise, care confirmă legalitatea şi temeinicia deciziei autorităţii contractante de a respinge oferta ... ca fiind neconformă.

Cu privire la primul motiv de respingere a ofertei contestatoarei, intervenienta menţionează următoarele:

1. Soluţia „certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional" este SafeLayer. Această soluţie nu oferă funcţionalităţi, aşa cum reiese de pe site-ul producatorului, cu privire la "utilizarea certificatelor digitale pe statiile de lucru (semnare, criptare/decriptare, stergere sigura)".

2. Produsele descrise în secţiunea în care se arată îndeplinirea cerinţelor privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura), respectiv capitolul 3.3.7.3.2. Semnătura electronică şi sectiunea Asigurarea confidentialităţii documentelor sunt DigiSigner şi BitLocker, care nu fac parte din portofoliul de produse SafeLayer. Pentru aceste produse nu se demonstrează faptul că se deţine o certificare de securitate sau că,

impreuna cu produsele SafeLayer, se formează un ansamblu care să respecte cerinţele de certificare.

3. Prin răspunsurile la întrebările de clarificare, contestaţie şi Concluzii scrise autoarea contestataţie încearcă să prezinte, în mod forţat, o integrare între DigiSigner şi produsele SafeLayer. Această integrare nu este susţinută de niciun fel de informaţii, de niciun alt document disponibil pe site-ul Common Criteria (entitatea care a emis certificatea EAL pentru produsele SafeLayer) şi nici de alte documente disponibile pe site-ul producatorului SafeLayer.

4. Mai mult decât atât, o certificare a unui produs presupune identificarea exactă a denumirii acestuia, a versiunii de produs, a componentelor acestuia, precum şi a condiţiilor operaţionale în care acesta funcţionează. În aceste conditii, nu reiese în niciun fel faptul că Digisigner se integrează cu componentele KeyONE, respectiv TrustedX şi asigură respectarea nivelului de certificare.

5. ... încearcă să inducă în mod evident în eroare autoritatea contractantă aducând informaţii noi atât prin răspunsurile la întrebările de clarificare, cât şi prin contestaţie. În acest ultim document, ... introduce un nou produs, aşa cum reiese din afirmaţia autorităţii contractante ”Produsul TrustedX Electronic Signature nu a fost inclus în oferta tehnică fiind menţionat exclusiv în prezenta contestaţie şi reprezintă completare a ofertei înaintate. Pentru produsul Trusted.X Electronic Signature nu au fost incluse în ofertă manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul” din punctul de vedere transmis la data de 03.04.2015, aspect ce contravine prevederilor art. 79 alin. (2) din HG nr. 925/2006, reprezentand, practic, o modificare de propunere tehnică.

Interveneinta menţionează că soluţia, în fapt tehnologia, TrustedX este o soluţie de tip server ce nu implementează cerinţele din documentaţia de atribuire referitoare la utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura).

În fapt, soluţia ofertată de către ... pentru îndeplinirea acestor cerinţe este Digisigner. Modalitatea prin care ... înţelege să forţeze acreditarea aplicaţiei Digisigner prin motivarea ca cerinţă este îndeplinită ca urmare a integrării la nivelul librăriilor criptografice cu TrustedX este total eronată şi are scopul de a induce în eroare autoritatea contractanta. Susţinerea faptului că dacă o aplicaţie utilizează resursele unei alte aplicaţii certificate atunci este şi ea certificată este în mod evident falsă. Aşa cum bine a observat autoritatea contractantă, în răspunsul la contestaţia ..., urmărind această logică, orice virus este certificat din punct de vedere al securităţii informatice dacă rulează pe un sistem de operare certificat, lucru în mod evident, total neadevarat şi fals. Mai mult decat atât, în portalul Common Criteria (https://www.commoncriteriaportal.org/ products/) nu există niciun fel de informaţii referitoare la aplicaţia Digisigner.

Pentru a explica mai bine şi în mod clar de ce o terţă aplicaţie ce utilizează librării criptografice acreditate nu poate fi de la sine acreditată din punct de vedere al securităţii informatice, intervenienta prezintă

următorul exemplu ipotetic elocvent: se dă o aplicaţie ce utilizează o librarie criptografică acreditată pentru a proteja prin criptare un document. După criptare, aplicaţia are o funcţionalitate prin care documentul criptat este transmis prin email destinatarului legitim. În acelaşi timp însă aplicaţia criptează documentul, folosind aceeaşi librărie criptografică certificată şi pentru o terţă persoană neautorizată şi transmite documentul şi către aceasta. Se observă astfel că, în aceste condiţii, deşi aplicaţia utilizează o librarie criptografică, certificată ea poate realiza ”în spate” o serie de acţiuni rău intenţionate la adresa utilizatorilor. Rolul unei certificări de securitate este acela de a arăta că aplicaţia, în ansamblul său, oferă un grad de protecţie adecvat utilizatorilor.

Mai mult decât atât, în concluziile scrise, ... prezintă o cu totul altă aplicaţie (DigiSigner Enterprise) decât cea care a fost prezentată în oferta tehnică, respectiv DigiSigner, al cărei datasheet se regăseşte în oferta tehnică la paginile 386-388, fapt care constituie în mod evident o modificare de ofertă tehnică, modificare care nu poate fi sancţionată decât cu respingerea ofertei ca neconformă.

De asemenea, intervenienta subliniază lipsa de transparenţă a ofertantului care afirmă că aplicaţia este o variantă de produs Enterprise, deşi nu se regăseşte nicăieri în dosarul achiziţiei această nouă denumire, iar în răspunsurile la întrebările de clarificare, ... afirmă că aplicaţia nu este versionabilă.

Faţă de cele de mai sus, intervenientasusţine că argumentele prezentate susţin decizia autorităţii contractante de a declara neconformă oferta tehnică a ... în ceea ce priveşte neîndeplinirea cerinţei ”Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional”.

Cu privire la cel de-al doilea motiv de respingere a ofertei contestatoarei, intervenienta susţine următoarele:

1. ... afirmă faptul că, pentru terminalele mobile, Autoritatea de Certificare DigiSign poate emite certificate digitale simple ce pot fi stocate în format .p12 pe aceste dispozitive. Formatul .p12 este o modalitate prin care sunt păstrate într-un container atât cheile (publică şi privată), cât şi certificatul. În cazul în care perechea de chei publică/privată sunt generate pe un dispozitiv criptografic de tip smartcard, conectat la terminalul mobil, cheia privată nu poate fi extrasă de pe smart card, astfel că nu mai poate fi creat containerul .p12.
2. Aplicaţia Mobile PKI realizează generarea de chei pe terminale mobile şi dispozitive de tip smartcard. Mobile PKI lucrează în tandem cu KeyOne certification Authority si KeyOne registration Authority. Nu a fost indicată versiunea aplicaţiei Mobile PKI.
3. Nu este descrisă integrarea între Autoritatea de Certificare DigiSign, care a fost indicată ca emite certificatele digitale, şi KeyOne certification Authority si KeyOne registration Authority cu privire la emiterea certificatelor digitale.

4. Prin răspunsurile la întrebările de clarificare, contestaţie şi Concluzii scrise Star Storage SA introduce o nouă componentă, Mobile ID şi indică un link nou către site-ul producătorului SafeLayer. Nu este indicată o versiune nici pentru Mobile ID şi nici pentru Mobile PKI.

5. Nu reiese în niciun fel modul în care Mobile ID respectă cerinţele din documentaţia de atribuire. Modul în care ... înţelege să prezinte o soluţie care, în mod evident nu utilizează dispozitive de tip smartcard, ca fiind superioară cerinţelor din documentaţia de atribuire se înscrie în aceeaşi linie cu declaraţiile referitoare la disponibilitatea produsului în Google Play sau cu cele legate de versiunea aplicaţiei. O soluţie de tip software nu poate fi superioară din punct de vedere al securităţii unei soluţii care asigură protecţia cheilor prin utilizarea de dispozitive hardware de tip smartcard certificate FIPS sau Common Criteria.

Spre exemplu, este bine cunoscut faptul că, în conformitate cu cerintele legale, certificatele digitale emise de către furnizorii de servicii de certificare din România se emit folosind numai dispozitive criptografice de tip smartcard. Astfel, apare întrebarea "cum poate o solutie software să implementeze funcţionalităţi superioare în ceea ce priveşte stocarea de chei şi operaţiuni criptografice în raport cu un smartcard?".

Intervenienta consideră afirmatia ... ca neadevarată, nefundamentată şi în totală contradicţie cu bunele practici şi standarde în domeniul securităţii informatice.

Mai mult, ... încearcă să inducă din nou în eroare Consiliul afirmând că la adresa http://safelayer.com/en /compliance/technical-standards este specificată în mod clar compatibilitatea produselor SafeLayer cu standardul PKCS#11 (conform cerinţei din documentaţia de atribuire). Vizitând respectivul link care are denumirea de "Standarde Tehnice" se poate constata, chiar la începutul secţiunii, faptul că respectiva pagină este o "Colecţie a tuturor standardelor de securitate şi recomandări suportate de către produsele SafeLayer". Nu se precizează însă nicăieri în site-ul safelayer faptul că aplicaţia Mobile ID suportă integrarea cu dispozitive de tip smartcard folosind standardul PKCS#11.

Un exemplu concludent asupra faptului că nu toate standardele enumerate în respectiva pagină sunt suportate de toate soluţiile SafeLayer se poate vedea în datasheet-ul aplicaţiei KeyOneVA disponibil la adresa http://safelayer.com/images/stories/pdf/Safelayer_KeyOne_VA_EN.pdf.

Astfel, soluţia implementează următoarele standarde: Online validation protocol: IETF RFC2560. • Cryptographic devices: RSA PKCS #11. • Connectivity: SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, REST and SOAP Web Services, POP3, SMTP and I/O standard. • Update mechanism: ITU-T X509.v3 CRL and/or the KeyOne CertStatus Server module. Supports multiple CAs. • Event monitoring: SNMP v1, v2c and v3. • SIEM integration and audit: Syslog protocol or Windows Event Log, dar nu implementează alte standarde referite la adresa http://safelayer.com/en/compliance/technical-standards cum ar fi:

- RFC 3161: Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)
- RFC 5280, RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)
- RFC 3739, RFC 3039: Internet X.509 Public Key Infrastructure. Qualified Certificates Profile
- RFC 5652, RFC 3852: Cryptographic Message Syntax (CMS) etc…

Având în vedere cele precizate anterior, intervenienta învederează modul total tendenţios şi neprofesionist în care contestatoarea ... foloseşte frânturi de informaţii de pe site-ul producătorului SafeLayer, în încercarea de a-şi susţine conformitatea ofertei.

6. Prin răspunsurile la întrebările de clarificare, contestaţie şi Concluzii, ... furnizează informaţii contradictorii şi eronate:

a. Sustine că ”produsul oferit nu este comercializat cu un model de versionare, acesta fiind motivul pentru care în ofertă nu se regăseşte versiunea de produs ofertat.” – afirmaţie neadevarată, deoarece Safelayer Mobile ID este prezent cu versiunea 1.3.1 în App Store şi, mai mult, atât Apple App Store, cât si Google Play cer ca aplicaţiile publicate să fie versionate.

b. Susţine, inclusiv printr-o declaraţie a Safelayer, că Mobile ID este prezentă în Google Play – afirmaţie neadevarată, aşa cum a arătat autoritatea contractantă prezentând rezultatele căutărilor în Google Play.

c. Prin concluzii, revine la punctul anterior afirmând ”... a specificat că există aplicaţii pentru Google Android fără ca în ofertă sau în contestaţie să fi afirmat că mobile ID este în Google Play”. Din analiza documentelor reiese clar că autoritatea contractantă nu a solicitat niciodată ca aplicaţiile să fie prezente în Google Play. Întrebarea acesteia din sesiunea demonstrativă ”Aplicaţia pentru generarea cheilor şi a cererilor de certificate este prezentă în Google Play/App store sau în alt store de aplicatii?” da posibilitatea indicării oricărui store de aplicaţii sau descrierea modalitatii prin care aplicaţia pentru Android ajunge pe telefoanele utilizatorilor. Cu toate acestea, nici în sesiunea demonstrativă şi nici în răspunsurile la clarificări nu este descrisă această modalitate.

... afirmă, pentru a susţine conformitatea cu cerinţele, atât în răspunsurile la întrebările de clarificare din 06.03.2016, printr-o declaraţie a SafeLayer, cât şi în contestaţie că SafeLayerMobile ID este prezent în iTunes App Store şi Google Play.

7. Prin răspunsul nr. 21 la solicitările la clarificări nr. 3600 din 14.10.2014, ... afirmă faptul că aplicaţiile ofertate nu sunt versionabile. Prin răspunsul nr. 1 la solicitările la clarificări nr. MFE/DAPITA/4498 din 03.03.2015 afirmă că ”produsele oferite nu sunt versionabile”. Şi totuşi, prin concluziile scrise acceptă faptul că aplicaţiile sunt versionabile. Această nouă aplicaţie (SafeLayer MobileID) nu este referită nicăieri în dosarul achiziţiei studiat, cu excepţia ultimelor răspunsuri la întrebările de clarificare şi nu s-a identificat nicio referinţă la modul în care această nouă aplicaţie îndeplineşte cerinţele de clarificare.

Mai mult, studiind site-ul producătorului SafeLayer, rezultă în mod clar că această aplicaţie nu îndeplineşte cerinţele specificate în documentaţia de atribuire.

Intervenienta învederează, în acest sens, că era obligaţia ... de a prezenta modul în care aplicaţiile ofertate îndeplinesc cerinţele autorităţii contractante. Astfel, ... nu o ofertat versiunea concretă de produs pentru a permite autorităţii contractante să poată evalua cu celeritate modul în care soluţia ofertată răspunde cerinţelor din documentaţia de atribuire.

Având în vedere informaţiile cu privire la prezenţa produselor Safelayer în Google Play:

- În Anexa 2 din răspunsurile la clarificări cu numărul MFE/DAPITA/4498 din 03.03.2015, ... a înaintat către autoritatea contractantă declaraţia producătorului SafeLayer prin care acesta afirmă în clar faptul că "[…] SafeLayer Mobile ID, disponibilă în iTunes App Store şi în Google Play Store […]".
- În concluziile scrise, ... afirmă faptul că "precizăm că ... a specificat că există aplicaţii pentru Google Android, fără ca în ofertă sau în contestaţie să fi afirmat că Mobile ID este disponibilă în Google Play", intervenienta subliniază atât afirmaţiile contradictorii, cât şi încercările de inducere în eroare ale ... care, în mod evident, îşi schimbă declaraţiile în funcţie de problemele identificate de autoritatea contractantă sau de aceasta.

Totodată, având în vedere cele prezentate mai sus, intervenienta îşi exprimă îndoiala rezonabilă cu privire la legalitatea declaraţiilor producătorului SafeLayer transmise prin ... către autoritatea contractantă.

În aceste condiţii, în mod temeinic şi legal autoritatatea contractantă a declarat neconformă oferta tehnică a ... în ceea ce priveşte cerinţa *"În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele:*

- *Să realizeze şi să transmită către furnizorul de servicii de certificare cererea standard PKCS#10 necesară procesului de emitere a certificatului digital*
- *Perechea de chei (publică/privată) vor fi generate:*
  - *Software, direct pe dispozitivul mobil*
  - *Pe un dispozitiv criptografic de tip smartcard, conectat la terminalul mobil*

Să realizeze înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta".

Argumentele prezentate anterior susţin decizia autorităţii contractante de a declara neconformă oferta tehnică a SC ... şi în ceea ce priveste cerinţa "Toate funcţionalităţile referitoare la utilizarea certificatelor digitale trebuie să fie implementate de către aplicaţii disponibile comercial la momentul ofertării. Interfaţa aplicaţiilor va fi cel

puţin în limba română. În acest sens se vor ataşa ofertei manuale de utilizare, fişe tehnice de produs din care să reiasă versiunea actuală de produs şi producătorul, precum şi orice alte documente care să vină în susţinerea conformităţii cu specificaţiile solicitate”.

Cu privire la cel de-al treilea motiv de respingere a ofertei contestatoarei, intervenienta susţine că pentru îndeplinirea cerinţelor, ... a indicat că utilizează aplicaţia SafeLayer KeyOne XRA. KeyOne XRA reprezintă componenta de RA (Registration Authority) a soluţiei SafeLayer PKI, şi nu deţine funcţionalităţi în ceea ce priveste accesul utilizatorilor în sistem.

Funcţionalitaţile componentei TrustedX cu privire la autentificare sunt prezentate treptat, pe măsură ce sunt transmise întrebări de clarificare. Contestatoarea nu este consecventă în afirmaţii, astfel că rolul componentei TrustedX în procesul de autentificare al utilizatorilor la sistem este iniţial de suport pentru mecanismul de tip "challenge-response", apoi intervine prin componenta ofertată "TrustedX Adaptive Authentication" (răspunsul la întrebarea nr. 28 din primul set de întrebări de clarificare), apoi furnizează strategii pentru integrarea autentificării (răspunsul la întrebarea 7 din al doilea set de întrebări de clarificare) şi, în sfârşit, în cadrul contestaţiei, reprezintă componenta de autorizare (control acces).

Şi de această dată, autoritatea contractantă a respins în mod temeinic şi legal oferta tehnică a ... în ceea ce priveşte cerinţele capitolului 3.3.7.3.1. Autentificarea la sistem.

Cu privire la cel de-al patrulea motiv de respingere a ofertei contestatoarei, intervenienta susţine următoarele:

1. Neconformităţile identificate în acest motiv au strânsă legătură cu neconformităţile identificate la motivul 2 în ceea ce priveşte aplicaţia utilizată pentru înscrierea certificatului digital pe dispozitivul mobil şi pe dispozitivul criptografic de tip smart card. Nu este indicată în mod clar aplicaţia utilizată (Mobile PKI este redenumită Mobile ID) şi versiunea acesteia pentru sistemele de operare iOS şi Android.
2. Susţinerea conformităţii se realizează indicându-se informaţii nerelevante, care nu au legătură cu subiectul. Astfel, producătorul SafeLayer declară în documentul prezentat în anexa 2 la adresa MFF/DAPITA/4598/06.03.2015 ca ''Mobile ID [...] poate genera chei în terminale mobile sau dispozitive de tip smart card". Documentul SafeLayer nu face referire la "înscrierea certificatului digital atât pe dispozitivul mobil cât şi, după caz, pe dispozitivul criptografic de tip smartcard conectat la acesta", aşa cum a fost solicitat prin documentaţia de atribuire, iar generarea cheilor şi înscrierea certificatului sunt operaţiuni diferite.
3. Sesiunea demonstrativă nu a dovedit îndeplinirea cerinţei, iar afirmaţia ”5. Demonstratia include utilizarea certificatelor digitale pe terminalele mobile stocate pe dispozitivul criptografic propriu, conectat la terminalul mobil? Răspuns ofertant: Da, a fost făcută o demonstraţie în cadul sesiunii de prezentare a autentificării cu dispozitiv criptografic conectat la terminalul Android” arată doar faptul că a fost realizată o

autentificare, nu şi faptul că a fost prezentată aplicaţia care realizează înscrierea certificatului digital pe terminalul mobil cu sistem de operare Android.

Astfel, intervenienta afirmă că argumentele prezentate anterior susţin decizia autorităţii contractante de a declara neconformă oferta tehnică a ... în ceea ce priveşte cerinţa ”utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil”.

Cu privire la cel de-al cincilea motiv de respingerea ofertei contestatoarei, intervenienta afirmă că,

1. Arhitectura soluţiei de acces a unui utilizator de pe PC în sistem descrisă nu este clară. ... a prezentat mai multe game de produse: certificate digitale simple emise de DigiSign, familia de produse SafeLayer KeyOne PKI şi familia de produse SafeLayer TrustedX, fără a arăta modul în care acestea funcţionează împreună. În funcţie de întrebările de clarificare adresate sau de conformităţile identificate a realizat diverse combinaţii între aceste produse. Mai mult, prin răspunsurile la întrebările de clarificare a indicat produse noi, din familiile menţionate mai sus.
2. Prin ,,Concluzii scrise’’ înaintate pe 09.04.2015, ... descrie o arhitectură eterogenă care include SafeLayer keyOne PKI şi Autoritatea de Certificare DigiSign. Aceasta arhitectură nu a fost prezentată în oferta tehnică şi, pe de altă parte, implementarea acesteia nu este permisă de modul de funcţionare al DigiSign aşa cum este descris în documentele Codul de Practici şi Proceduri şi Politica de Certificare disponibile la adresa www.digisign.ro
3. Pe de o parte, ... furnizeaza certificate digitale simple emise de DIGISIGN S.A., iar pe de altă parte, oferă o altă soluţie PKI, SafeLayer Key One, subordonată DIGISIGN S.A, care să emită certificate digitale simple.

Mai mult, ... susţine faptul că implementarea acestei soluţii are ca scop “distribuirea certificatelor digitale”, iar operaţiunile de gestionare ale acestei soluţii vor fi asigurate de catre SC DIGISIGN SA.

Intervenienta subliniază starea de confuzie în care persistă .... deoarece, chiar şi în urma schimbului de informaţii aferent sesiunilor de întrebări şi răspunsuri legate de oferta tehnică, nu este deloc clar cine va opera soluţia PKI, cine va emite în fapt certificatele digitale şi dacă soluţia PKI va fi instalată sau nu la sediul autorităţii contractante.

Practic, operatiunea de “distribuire a certificatelor digitale” nu are niciun fel de legătură cu soluţia PKI utilizată. Urmând logica ... ar însemna ca orice utilizator care foloseşte un certificat digital emis de ... ar putea să îşi implementeze propria soluţie PKI subordonată ..., aspect evident neadevarat.

Intervenienta consideră că ... încearcă să definească o soluţie coerentă chiar şi în acest moment, încercând să combine diverse elemente ofertate într-un concept ale cărui caracteristici variază funcţie de informaţiile colectate din documentele aferente procedurii de licitaţie.

Drept urmare, argumentele prezentate anterior susţin decizia autorităţii contractante de a declara neconformă oferta tehnică a ... în ceea ce priveste cerinţele capitolului 3.3.7.3.1. Autentificarea la sistem.

Cu privire la cel de-al şaselea motiv de respingere a ofertei contestatoarei, intervenienta menţionează următoarele:

1. ... propune pentru realizarea autentificării, atât în ofertă cât şi în răspunsul la întrebarea 29 din clarificări tehnice 1, aplicaţia KeyOne XRA care, nu oferă funcţionalităţi pentru aceste operatiuni.

2. Prin răspunsurile la întrebările de clarificare ... revine şi modifică arhitectura propusă, indicând şi componenta TrustedX Adaptive Authentication ca fiind cea care realizează autentificarea. Pentru a nu elimina KeyOne XRA este facută o descriere teoretică în care ... face confuzii între procesele de identificare a utilizatorilor, emitere a credenţialelor de acces, autentificarea, autorizarea şi accesul la sistem. Descrierea teoretică are rolul de a masca neconformitatea aplicaţiei KeyOne XRA în ceea ce priveşte realizarea procesului de acces la utilizatorilor.

3. Sesiunea demonstrativă nu a făcut dovada îndepliniri cerinţei, iar afirmaţia ”5. Demonstraţia include utilizarea certificatelor digitale pe terminalele mobile stocate pe dispozitivul criptografic propriu, conectat la terminalul mobil?

Raspuns ofertant: Da, a fost făcută o demonstraţie în cadul sesiunii de prezentare a autentificăfii cu dispozitiv criptografic conectat la terminalul Android”, arată doar faptul că a fost realizată o autentificare cu dispozitiv criptografic conectat la un terminal Andoid, nu şi faptul că a fost realizată o demonstraţie cu terminale iOS care utilizează pentru autentificare un dispozitiv criptografic conectat la terminal.

Argumentele prezentate anterior susţin decizia autorităţii contractante de a declara neconformă oferta tehnică a ... în ceea ce priveşte cerinţele capitolului 3.3.7.3.1. Autentificarea la sistem.

Cu privire la cel de-al şaptelea motiv de respingerea ofertei contestatoarei, intervenienta menţionează următoarele:

1. ... afirmă ca cerinţa ”să permită contexte diferite de securitate în funcţie de secţiunea din sistem accesată de către utilizator. Soluţia trebuie să permită prin configurare conexiuni http (publice, care nu necesită autentificare) şi https (cu autentificare) în funcţie de aceste contexte” este indeplinită ”prin intermediul soluţiei de securitate şi Microsoft Active Directory”, iar soluţia de securitate este descrisă, prin răspunsul la întrebarea nr. 32 din Clarificari tehnice 1 că fiind ”infrastructura de tip PKI adică soluţia Safelayer propusă„

2. Prin răspunsul la întrebare de clarificare nr. 9 din Clarificări tehnice 2, este indicat produsul TrustedX ca îndeplinind cerinţa;

3. Astfel, pe de-o parte (în urma primei întrebări de clarificare), cerinţa este îndeplinită global de "infrastructura PKI adică soluţia SafeLayer propusă", fără a detalia care dintre componentele ofertate asigură îndeplinirea cerinţei. Pe de altă parte, urmare a celei de-a doua întrebări, "componenta" responsabilă cu îndeplinirea cerinţei este TrustedX. În niciun moment, însă, contestatoarea nu indică modalitatea prin care

cerinţa este îndeplinită, ci doar invocă capabilităţile TrustedX ca "server de alocare şi gestionare de roluri utilizatori". Din niciun material, link sau precizare nu reiese capabilitatea vreuneia dintre componentele prezentate în pagina nr. 287 a ofertei, asa cum reiese din punctul de vedere al autorităţii contractante de a îndeplini cerinţa din documentaţia de atribuire.

Astfel, argumentele prezentate anterior sustin decizia autorităţii contractante de a declara neconformă oferta tehnică a SC STAR STORAGE SA, în ceea ce priveşte cerinţele capitolului 3.3.7.3.1. Autentificarea la sistem.

Cu privire la cel de-al optulea motiv de respingere a ofertei, intervenienta susţine că ... nu a descris modul în care se realizează integrarea dintre Microsoft Active Directory şi soluţia Safelayer propusă, iar autoritatea contractantă nu deţine suficiente elemente pentru a verifica conformitatea celor descrise.

Fişa de date a achiziţiei precizează în mod explicit ”Furnizorul trebuie să răspundă punctual la toate cerinţele cuprinse în documentaţia de atribuire şi să detalieze în propunerea sa tehnică modurile şi mijloacele prin care soluţia ofertată îndeplineşte aceste cerinţe, astfel încât comisia de evaluare să aibă posibilitatea evaluarii acesteia în mod cât mai informat. În cazul în care oferta nu oferă informaţii complete prin detalierea răspunsului la cerinţe sau nu îndeplineşte cerinţele exprimate în documentaţia de atribuire, comisia de evaluare poate să declare oferta ca fiind inacceptabilă/neconformă”.

Cu privire la cel de-al nouălea motiv de respingere a ofertei contestatoarei, intervenienta afirmă că aplicaţia BitLocker ofertată pentru îndeplinirea cerinţei ”Criptarea trebuie să poată fi realizată astfel: La nivel de sistem de operare, prin crearea unei partiţii criptate;” nu foloseşte algoritmul de criptare 3DES, aşa cum reiese din documentaţia oficială a producătorului Microsoft.

Specificaţiile prevăzute în capitolul Asigurarea confidentialităţii documentelor trebuie tratate în integralitatea lor, în sensul că aplicaţiile ofertate pentru asigurarea funcţionalităţilor de criptare trebuie să implementeze aceste funcţionalităţi prin mecanismele de criptare prevăzute în documentaţie. Astfel, inclusiv aplicaţia care realizează criptare *”La nivel de sistem de operare, prin crearea unei partiţii criptate”* trebuie să raspundă cerinţelor:

”Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici şi asimetrici, astfel:

- *Criptarea asimetrică, utilizând certificatele X509v3 şi algoritmul RSA*
- *Criptarea simetrică folosind algoritmii 3DES si AES*

(...)

Certificatele care vor fi utilizate in procesul de criptare trebuie sa fie disponibile local, pe statia de lucru pe care se realizeaza criptarea, sau prin publicarea intr-un serviciu de directoare standard LDAPv3. Criptarea va trebui sa poata fi realizata pentru mai multi utilizatori simultan, iar

pentru utilizatorul care a initiat procesul de criptare, documentul trebuie sa poata fi criptat in mod automat.

Certificatele necesare decriptarii pot fi stocate atât pe smart card compatibil cu standardul PKCS #11, cât şi in format software conform cu standardul PKCS#12."

Aplicaţia DigiSigner, care realizează criptarea folosind algoritmul 3DES nu îndeplineşte cerinţele "Criptarea trebuie să poată fi realizată astfel: La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţile aflate pe partiţia criptată;"

... nu a descris modul cum produsul BitLocker îndeplineşte cerinţa "Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată".

Afirmatia din PV sesiune demo: *"8. Sunt prezentati algoritmii criptografici utilizati pentru criptarea fisiere si criptarea partitii?*

Răspuns ofertant: Da. Ofertantul a făcut o demonstraţie pe fişiere criptate şi pe partiţii criptate" dovedeşte, în cel mai bun faptul că au fost prezentaţi „algoritmii criptografici folosiţi pentru criptare fişiere şi criptare partiţii", nereieşind care au fost aplicaţiile utilizate în cadrul demonstraţiei şi nici că aplicaţia BitLocker permite blocarea accesului la partitiile criptate.

Cu privire la cel de-al zecelea motiv de respingere a ofertei contestatoarei, intervenienta afirmă că nu a identificat nicio precizare cu privire la integrarea dintre SEAL Compliance Edition cu componenta sa StarSign si DigiSigner sau cu privire la utilizarea DigiSigner SDK de catre aplicatiile SEAL Compliance Edition sau StarSign.

Singurul SDK descris nu este denumit şi oferă exclusiv funcţionalităţi de verificare a documentelor semnate electronic, fără să se descrie funcţionalităţile acestui SDK privind crearea de semnături electronice.

În descrierea DigiSigner din matricea de conformitate şi în documentaţia aferentă acestui produs aflată la paginile 386-388 ale ofertei tehnice nu este menţionată existenţa DigiSigner SDK şi care sunt funcţionalităţile pe care acesta le are, aşa cum reiese din punctul de vedere al MFEUR.

Prin răspunsul la întrebarea 43 din solicitarea de clarificări nr. 3600/14.10.2014 cât şi în răspunsul la întrebarea nr. 10 din solicitarea de clarificari nr. MFE/DAPITA 4498/03.03.2015, ofertantul aduce modificări şi completări ofertei tehnice înaintată afirmând că aplicaţia SEAL este integrată cu DigiSigner SDK.

Fişa de date a achiziţiei precizează în mod explicit că "Furnizorul trebuie să răspundă punctual la toate cerinţele cuprinse în documentaţia de atribuire şi să detalieze în propunerea sa tehnică modurile şi mijloacele prin care soluţia ofertată îndeplineşte aceste cerinţe, astfel încât comisia de evaluare să aibă posibilitatea evaluării acesteia în mod cât mai informat. În cazul în care oferta nu oferă informaţii complete prin detalierea răspunsului la cerinţe sau nu îndeplineşte cerinţele exprimate

în documentaţia de atribuire, comisia de evaluare poate să declare oferta ca fiind inacceptabilă/neconformă".

Având în vedere cele precizate anterior, intervenienta menţionează că toate aceste aspecte fac ca decizia autorităţii contractante de a declara neconformă oferta tehnică a ... în ceea ce priveşte cerinţele:

- " această componentă de arhivare electronică va fi capabilă să aplice semnături digitale ... , iar aplicarea de semnături digitale va trebui să ofere următoarele capabilităţi minime:[...]"
- "Semnătura electronică va fi în conformitate cu următoarele standarde [...]"
- "Marca temporală care va fi aplicată semnăturii electronice va avea următoarele funcţionalităţi şi caracteristici:[...]", să fie temeinică şi legală.

Prin adresa nr. T/1162/16.04.2015, înregistrată la Consiliu sub nr. 6042/17.04.2015, ... formulează răspuns la punctul de vedere al autorităţii contractante

Referitor la susţinerile şi criticile punctuale ale autorităţii contractante, suplimentar argumentelor invocate prin contestaţie, contestatoarea face următoarele menţiuni:

Referitor la Motivul 1:

Autoritatea contractantă prezintă iniţial o cerinţă care se află în cadrul unui capitol, respectiv 3.3.7.1. Principii de securitate iar pe urmă face trimitere către o cerinţă din cadrul unui alt capitol, respectiv 3.3.7.3.2. Semnătura electronică, cu scopul de a induce în eroare Consiliul.

Cerinţa care face scopul prezentului punct este exact următoarea: „soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau international".

Astfel, într-un mod lipsit de echivoc, cerinţa mai-sus menţionată se referă la o soluţie. Autoritatea contractantă are o înţelegere greşită asupra termenului "soluţie", confundându-l intenţionat cu termenul "componentă" pentru a segmenta în mod eronat soluţia complexă propusă, astfel încât să creeze confuzie şi să încerce desfiinţarea soluţiei propuse de ....

Mai mult, autoritatea contractantă ulterior prezintă doar o parte din cerinţă, omiţând în mod voit prima parte a cerinţei, cu scopul de a lăsa în mod deliberat o concepţie greşită.

De asemenea, concluzia formulată de aceasta după ce transcrie modalitatea de rezolvare a cerinţei este complet eronată, aşa cum se poate observa prin simpla citire a frazei. Nicăieri nu este specificat faptul că „aplicaţiile Safelayer îndeplinesc cerinţa privind certificarea din punct de vedere al securităţii informatice….." însă este specificat în mod clar implementarea tehnologiei TrustedX la nivelul staţiilor de lucru, tehnologie care în conformitate cu răspunsul la clarificări nr. MFE/DAPITA 4598/06.03.2015, este integrată la nivelul librăriilor criptografice accesate de componenta DigiSigner, toate componentele lucrând în comuniune în cadrul solutiei SafeLayer propusă, care este certificată

ISO/IEC 15408 EAL4+, şi care în mod unitar răspund şi îndeplinesc atât cerinţele de funcţionare cât şi de conformitate solicitate de catre autoritatea contractantă.

Referitor la modalitatea de integrare solicitată în repetate rânduri în cadrul punctului de vedere de către autoritatea contractantă, nicăieri în cadrul documentaţiei de atribuire nu este solicitată detalierea modului de integrare a componentelor soluţiei.

Astfel, contestatoarea consideră atitudinea autorităţii contractante abuzivă şi insinuantă, solicitând, practic, dezvăluirea unor detalii clasificate, tocmai ale unei soluţii de securitate informaţională, fapt ce contravine dreptului de proprietate intelectuală al producătorului soluţiei.

Cu privire la alegaţiile nefondate ale autorităţii privind documentaţia aferentă componentei DigiSigner, capabilităţile de integrare cu aplicaţii de management de documente, de securizare a tranzacţiilor şi de interoperabilitate cu servicii de tip PKI sunt prezentate în mod clar chiar pe prima pagină a documentului.

Este absurd ca în prezent, într-un timp în care aplicaţiile software apar, sunt upgradate sau sunt înlocuite de versiuni mult mai fiabile, există vaste posibilităţi standardizate de comunicaţie, autoritatea contractantă să fie de părere că în documentaţia unui produs este necesar să apară integrarea cu un anumit produs comercial.

Contestatoarea susţine că nicăieri în cadrul documentatiei de atribuire nu este solicitată detalierea modului de integrare a componentelor soluţiei, întrucât această cerinţă ar contraveni bunului simţ şi ar încălca dreptul de proprietate intelectuală al producatorului soluţiei.

Percepţia autorităţii contractante este alterată întrucat din cele trei motive enunţate în punctul de vedere, respectiv:

Este evident faptul că, în oferta tehnică, ofertantul a propus o soluţie incompletă şi neconformă:

- *Cerinţa privind certificarea de securitate este îndeplinită de aplicaţiile Safelayer pentru care nu se demonstrează îndeplinirea funcţionalităţilor privind utilizareacertificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură).*
- *Cerinţele privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) sunt îndeplinite de aplicaţia DigiSigner pentru care, însă nu este demonstrată certificarea din punct de vedere al securităţii informatice de către un organism abilitate la nivel naţional, european sau international.*
- *Oferta tehnică nu descrie enetuala integrare dintre produsele Safelayer şi DigiSigner.*

Ca un rezumat al celor de mai sus, sunt evidente următoarele aspecte:

- Autoritatea încearcă prin cuvinte să manipuleze termenii şi introduce în mod eronat sintagma „aplicaţiile Safelayer”, sintagma nefolosită, dar mai departe, neputând contesta faptul că cerinţa privind îndeplinirea certificării de securitate este îndeplinită, atestă ea însăşi îndeplinirea acestei cerinţe;

- în continuare, autoritatea atestă faptul că cerinţele privind utilizarea certificatelor digitale pe staţiile de lucru sunt îndeplinite de componenta DigiSigner;
- în final, autoritatea introduce în mod abuziv şi insinuant, în punctul de vedere, susţinerea că ... nu a respectat cerinţa de descriere a integrării dintre componentele SafeLayer şi DigiSigner, cerinţă care nu există în cadrul documentaţiei de atribuire.

De asemenea, contestatoarea afirmă că autoritatea solicită în mod flagrant şi abuziv să prezinte modalitatea de integrare a aplicaţiilor, acest aspect nefiind solicitat nicăieri în cadrul documentaţiei de atribuire detalierea modului de integrare a componentelor soluţiei, precum şi faptul că autoritatea contractantă se contrazice, întrucât demonstrarea îndeplinirii funcţionalităţilor privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura) fiind atestate de către aceasta atât la pag. 11 a punctului de vedere, cât şi în cadrul sesiunii demonstrative din data de 13.11.2014, din 13.11.2014 consemnată prin procesul verbal nr. 4198/13.11.2014.

Se mai arată că în ofertă la pagina 292, paragraful 2 este prezentat în mod clar faptul că implementarea tehnologiei TrustedX la nivelul staţiilor de lucru, tehnologie care în conformitate cu răspunsul la clarificări nr. MFE/DAPITA 4598/06.03.2015, este integrată la nivelul librăriilor criptografice accesate de componenta DigiSigner, toate componentele lucrând în comuniune în cadrul soluţiei SafeLayer propusă, care este certificată ISO/IEC 15408 EAL4+, şi care în mod unitar răspund şi îndeplinesc atât cerinţele de funcţionare cât şi de conformitate solicitate de către autoritatea contractantă.

Se poate observa atitudinea răuvoitoare a autorităţii contractante, de inducere în eroare, care a solicitat indicarea certificării solicitate în cadrul documentaţiei în capitolul 3.3.7.1. Principii de securitate, pentru a face trimitere către o componentă din cadrul unui alt capitol, respectiv 3.3.7.3.2. Semnătura electronică şi pentru a concluziona ulterior, în mod eronat, faptul că prin răspunsul de clarificare ... a adus completări ofertei tehnice înaintate.

În mod clar şi vădit este ignorată precizarea din cadrul frazei indicate în care este specificată clar implementarea tehnologiei TrustedX la nivelul staţiilor de lucru, tehnologie care, în conformitate cu răspunsul la clarificări nr. MFE/DAPITA 4598/06.03.2015, este integrată la nivelul librăriilor criptografice accesate de componenta DigiSigner.

Astfel, contestatoarea conchide că ambiguitatea însuşită de autoritatea contractantă denotă lipsa de interes şi intenţia clară de a o descalifica pe motiv că nu înţelege o soluţie informatică complexă, în speţa cea ofertata de ..., în favoarea asocierii concurente, folosind exemple menite să inducă în eroare de genul celui de mai jos:

În acest fel, urărind logica contestatoarei prin care un produs care se integrează cu un alt produs certificat înseamnă că este şi el certificat, înseamnă că orice produs/aplicaţie care se integrează de exemplu cu un sistem de operare certificat (cum ar fi Microsoft Windows Vista ce deţine CC EAL 1) este şi el certificat. Pe cale de consecinţă, un virus sau un

program malware ce în mod evident rulează pe un sistem de operare va fi şi el certificat din punct de vedere al securităţii, aspect evident neadevărat. Se observă, astfel, confuzia gravă în care este contestatoarea precum şi lipsa dovezilor tehnice care să vină în justificarea argumentelor sale.

Contestatoarea atrage atenţia asupra faptului că exemplul prezentat de autoritatea contractantă este exagerat şi dat numai cu scopul de a perturba şi confuziona opinia şi decizia Consiliu. Componenta unei soluţii informatice, respectiv DigiSigner, în primul rând nu „rulează" (înfăşoară, rostogoleşte sau roteşte), aşa cum susţine autoritatea contractantă, ci este integrată în cadrul soluţiei SafeLayer, certificată ISO/IEC 15408 EAL4+ din punct de vedere al securităţii informatice.

Aşadar, îndeplinirea cerinţei privind certificarea din punct de vedere al securităţii informatice pentru soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional este demonstrată şi atestată de însăşi autoritatea contractantă.

Referitor la următoarea afirmaţie a acesteia, respectiv: *„Totodată în cadrul contestaţiei este ofertat un nou produs al companiei SafeLayer respectiv TrustedX Electronic Signature, conform paragrafului de mai jos"*, contestatoarea menţionează că autoritatea contractantă face o confuzie inexplicabilă între termenul tehnologie şi termenul produs, cu scopul de a induce în eroare Consiliul, fiind prezentat, în mod clar, faptul că au fost prezentate funcţionalităţile tehnologiei TrustedX, respectiv de autentificare şi semnare electronică cu scopul de a lămuri ambiguitatea consacrată a autorităţii contractante, nu de a modifica sau completa oferta.

Concluzionând, în contradicţie cu motivele enumerate de autoritatea contractantă, care refuză cu orice preţ să înţeleagă, să accepte şi să prezinte situaţia de fapt, admiţând că o soluţie este formată dintr-o suită de componente, contestatoarea precizează următoarele:

(i) componetele ofertate de aceasta atestă îndeplinirea cerinţelor privind certificarea de securitate şi utilizarea certificatelor digitale pe staţiile de lucru, însă autoritatea ignoră în mod voit faptul că este specificat clar în oferta tehnică implementarea tehnologiei TrustedX la nivelul staţiilor de lucru, tehnologie care în conformitate cu răspunsul la clarificări nr. MFE/DAPITA 4598/06.03.2015, este integrată la nivelul librăriilor criptografice accesate de componenta DigiSigner, astfel, toate componentele lucrând în comuniune în cadrul soluţiei SafeLayer propusă, care este certificată ISO/IEC 15408 EAL4+, şi care în mod unitar răspund şi îndeplinesc atât cerinţele de funcţionare cât şi de conformitate solicitate de către autoritatea contractantă;

(ii) ... nu a completat oferta aşa cum insinuiază autoritatea contractantă, prin menţionarea şi prezentarea pe larg a funcţionării aplicaţiei, în acest sens, menţionând şi produsul TrUstedX – varianta Electronic Signature – component a aplicaţiei ofertate.

(iii) atitudinea autorităţii contractante este abuzivă, întrucât solicită dezvăluirea unor detalii clasificate vizând soluţia de securitate informaţională, reluând în cadrul punctului de vedere critica sub forma detalierii modului de integrare a componentelor soluţiei ofertate, deşi această cerinţă, nu se regăseşte nicăieri în cadrul documentaţiei de atribuire.

(iv) informaţiile furnizate în cadrul răspunsurilor de clarificare nu modifică oferta în niciun fel, acestea având strict rolul de a limpezi înţelegerea închisă şi unilaterală a autorităţii contractante prin explicarea în detaliu a funcţionalităţilor oferite de componentele ce o formează acestea contribuind la desăvârşirea soluţiei unitare conformă cerinţelor documentaţie.

Referitor la Motivul 2, contestatoarea face următoarele precizări:

- Safelayer Mobile ID (referită în ofertă şi ca Mobile PKI, descrisă în fişa de produs aflată la adresa http://www.safelayer.com/images/stories/pdf/Safelayer_Mobile_ID_EN.pdf), este o aplicaţie flexibilă şi versatilă destinată terminalelor mobile care funcţionează pe sisteme de operare iOS şi Android, ce poate fi folosită pentru autentificare şi/sau semnare în orice browser sau aplicaţie, putând fi integrată rapid prin intermediul standardelor Web curente folosind Web API şi WDK (Widget Development Kit).

Aplicaţia Safelayer Mobile ID, prin componenta sa de PKI, permite generarea şi inregistrarea certificatelor digitale direct pe terminalul mobil. Procesul de generare a cheilor criptografice este un proces subsidiar procesului de generare a certificatului digital, ceea ce presupune în mod evident generarea cheilor criptografice direct în containerul securizat specific terminalului mobil sau într-un echipament criptografic ataşat prin intermediul unui cititor (de smartcard, sau SD). Schema de mai jos ilustrează interacţiunile dintre aplicaţia Safelayer Mobile ID, aplicaţii terţe şi componente de infrastructură:

- Safelayer TrustedX furnizează funcţionalităţi de autentificare şi verificare a semnăturii;
- serverul de credenţiale este bazat pe PKI şi certificate digitale;
- aplicaţiile terţe pot fi browser web, aplicaţii dezvoltate de parteneri şi alte aplicaţii executate de pe alte echipamente.

Referitor la Motivul 3, contestatoarea susţine că este necesar să clarifice diferenţele dintre: „controlul accesului”, „autentificare” şi „autorizare”, redând în continuare următoarele definiţii şi precizări:

➢ Autentificarea este procesul prin care se verifică dacă un utilizator este cine pretinde că este. În mod normal, aceasta implică faptul că utilizatorul introduce un nume şi o parolă, dar poate include orice altă metodă de a demonstra identitatea, spre exemplu un smartcard, un PIN, o amprentă digitală etc.

Pentru a realiza autentificarea, un utilizator trebuie fie să aibă un cont creat într-un sistem ce poate fi interogat de mecanismul de

autentificare, fie este necesară crearea unui cont de utilizator ca parte a procesului primei autentificări.

➢ Autorizarea este procesul prin care unui utilizator deja autentificat i se permite sau nu accesul la o anumită resursă. Autorizarea determină ce îi este permis unui utilizator şi ce nu.

Nivelul de autorizare acordat unui utilizator este determinat prin examinarea metadatelor asociate contului său. Autorizarea include o componentă de management al autorizării, care este un sistem care furnizează funcţionalitatea de a crea reguli de autorizare.

➢ Controlul accesului la resurse este procesul de punere în practică a regulilor de securitate implicate pentru o anumită resursă, şi poate fi văzut ca o combinare între autentificare şi autorizare, plus eventual un set de măsuri suplimentare.

Pentru o înţelegere mai bună, contestatoarea detaliază:

➢ Protocolul de control al accesului, denumit şi protocolul AAA (authentication, authorization, accounting) în cadrul soluţiei propuse este realizat de o integrare a KeyONE XRA şi TrustedX.

- KeyONE XRA este componenta primordială de realizare a autentificării prin înscrierea şi validarea unui set de credenţiale de utilizator, iar TrustedX are rolul de a face managementul autorizării, prin interogari adresate KeyONE XRA.
- TrustedX se comportă ca un agent între aplicaţiile utilizatorului şi serviciile de furnizare a identităţii, în cazul de faţă KeyONE XRA. Accesul unui utilizator în sistem de pe PC folosind certificatul digital propriu este posibila prin cel puţin una din cele trei modalităţi oferite de TrustedX:
  - folosind interfaţa nativă de autentificare a TrustedX;
  - incluzând procedura de autentificare în interfaţa aplicatiei terţe;
  - externalizat cu alţi furnizori de identitate agreaţi, complementar cu TrustedX şi functionalităţi de tip single sign-on;
  - interfaţa de autentificare prezentă în Safelayer Mobile ID;

➢ Serviciile de furnizare a identitatii sunt:

- servere LDAP (Active Directory);
- servere de baze de date;
- servere RADIUS;
- servicii PKI (KeyONE);

Astfel, contestatoarea menţionează că accesul unui utilizator de pe PC folosind certificatul digital propriu se realizează, în funcţie de necesităţi, folosind interfaţa proprie a TrustedX sau integrând autentificarea TrustedX cu aplicaţiile prezente sau ce urmează a fi dezvoltate, oferind un grad maxim de flexibilitate în vederea oferirii unei soluţii adaptabile la necesităţile prezente şi viitoare.

Referitor la Motivul 4, contestatoarea susţine că din fişa tehnică a produsului Safelayer Mobile ID: http://www.safelayer.com/images/

stories/pdf/Safelayer_Mobile_ID_EN.pdf reiese că: "When the user downloads Mobile ID from the Apple App Store or Google Play, the app automatically initializes with the creation and registration of the cryptographic credentials that will be used for identifying the user".

În traducere: "Când utilizatorul descarcă Mobile ID din Apple App Store sau Google Play, aplicaţia iniţializează automat crearea şi înregistrarea credenţialelor criptografice ce vor fi utilizate pentru a identifica utilizatorul".

Mai mult, conform declaraţiei de la producător, este specificat în mod clar că aplicaţia Safelayer Mobile ID este parte din componenta Mobile PKI inclusă în suita de produse Safelayer KeyONE PKI şi poate genera cheile criptografice direct în echipamente mobile sau echipamente smartcard ataşate acestora.

Refuzul de a lua în considerare declaraţia unui producător de renume mondial, dar care nu preproduce integral cerinţa din documentaţie aşa cum sunt declaraţiile furnizorului CertSign este un abuz din partea autorităţii.

Aplicaţia Safelayer Mobile ID, conform declaraţiei de producător, stochează fie pe echipamentul mobil, fie pe un echipament criptografic ataşat acestuia, certificatul digital în vederea folosirii acestuia pentru acces sau semnare.

Soluţia propusă permite înscrierea cheilor criptografice direct pe terminalul mobil sau pe un dispozitiv criptografic de tip smartcard, conectat la terminalul mobil.

Referitor la Motivul 5, contestatoarea reiterează alegaţiile de la Motivul 3.

Referitor la Motivul 6, unde autoritatea contractantă afirmă că „În ceea ce priveşte îndeplinirea cerinţelor ca soluţia de securitate propusă să permită contexte diferite de securitate în funcţie de secţiunea din sisntem accesată de către utilizator (motivul 7 de neconformitate), contestatoarea menţionează că cerinţa exprimată în documentaţia de atribuire a fost:

Cerinţa este prevăzută în cadrul capitolului 3.3.7.3. Utilizarea certificatelor digitale, subcapitolul 3.3.7.3.1 Autentificarea la sistem şi este enunţată astfel:

Modulul de autentificare şi autorizare trebuie să ofere următoarele funcţionalităţi:

- *să permită contexte diferite de securitate în funcţie de secţiunea din sistem accesată de către utilizator. Soluţia trebuie să permită prin configurare conexiuni http (publice, care nu necesită autentificare) şi https (cu autentificare) în funcţie de aceste contexte.*

Cu privire la acest aspect, contestatoarea precizează că soluţia PKI SafeLayer face parte din ansamblul licenţelor din infrastructura PKI descris în ofertă, acestea funcţionând ca un tot unitar, împreună cu KeyOne şi TrustedX. Atât licenţele KeyOne, cât şi TrustedX, au fost menţionate în ofertă. La pag. 287 sunt prezentate componentele soluţiei PKI Safelayer care asigură conformitatea cu cerinţa exprimată în documenţatie.

De asemenea, contestatoarea prezintă răspunsul său la întrebarea nr. 9, adresată în setul de întrebări MFE/DAPITA/4498/03.03.2015, răspuns care în opinia contestatoarei a fost scos din context şi prezentat după bunul plac al autorităţii contractante:

„9. Prin intermediul produsului TrustedX Authentication Platform se administrează şi gestionează rolurile de utilizatori http://www.safelayer.com/en/products/trustedx-adaptive-authentication TrustedX se comportă ca un agent între aplicaţiile utilizatorilor şi serviciile de furnizare a identităţii. Pentru a invoca TrustedX aplicaţiile folosesc protocoalele Oauth 2.0 sau SAML 2.0, iar ca servicii de furnizare a identităţii sunt suportate LDAP/Active Directory, RADIUS şi servicii PKI.

Platforma TrustedX furnizează o serie de strategii pentru integrarea autentificării:

- standard, care foloseşte interfaţa de autentificare furnizată de TrustedX;

- interfaţa grafică delegată, care furnizează o experienţă de utilizare care este omogena si armonioasa cu aplicaţiile;

- externalizată către alţi furnizori de identitate complementări cu TrustedX şi functionalităţi de tip SSO.

Contestatoarea învederează că în vederea asigurării acestor functionalităţi, TrustedX este o componentă a infrastructurii SafeLayer PKI şi are rolul de a administra drepturile şi permisiunile utilizatorilor, impreună cu Microsoft Active Directory, aşa cum reiese clar atât din răspunsul la intrebarea nr. 32 şi aşa cum este prezentat în pag. 286, 287, 288, 289, cât şi pag. 311 din oferta tehnică.

În susţinerea celor antemenţionate, contestatoarea reiterează extrasul din răspunsul său din oferta tehnică şi paginile unde se pot găsi:

Pag. 286-287 – unde a fost definită soluţia de securitate cu toate componentele specifice solicitate pentru acoperirea cerinţelor din caietul de sarcini:

Sistemul va avea un sistem de securitate care permite protejarea informatiei, atat fata de accesul neautorizat intern, cat si fata de accesul neautorizat extern. Protectia va fi asigurata atat la nivel hardware cat si software.	***DA***	*Sistemul incorporeaza componente de securitate pe mai multe nivele, avand la baza un modul de tip LDAP (Microsoft Active Directory) ce asigura desemnarea si propagarea drepturilor pentru fiecarui utilizator, rol, grup etc.* *Acesta se integreaza nativ cu elementele de securitate propuse oferind capabilitati de protejare a datelor atat la nivel software cat si la nivel hardware.* *Astfel Active Directory atribuie drepturile si realizeaza efectiv autorizarea accesului la nivel de sistem de operare si retea de calculatore impunand strict regulile de securitate ale sistemului asa cum acestea sunt definite de administrator.* *Sistemul de tip PKI propus, este un sistem complex, capabil sa adauge straturi de securitate suplimentare prin aplicare unor*

		*reguli de autentificare suplimentare, bazate pe **certificate digitale** si **dispozitive hardware cu suport criptografic certificat** FIPS 140-2 level 2 (minim 500 de operatiuni criptografice RSA 1024 / secunda) pentru stocarea cheilor utilizate pentru semnarea raspunsurilor trimise catre client, asigurand astfel protectia atat la nivel hardware cat si software.* *Sistemul este produs de compania **SafeLayer** platforma livrata fiind compusa din :* *TrustedX Adaptive Authentication* *KeyOne Certification Authority* *KeyOne Registration Authority* *KeyOne Validation Authority* *Mobile PKI* *Aceasta este capabila de realizarea autentificarilor in diverse moduri fiind o platforma adaptiva si flexibila. Mai multe detalii legate de acesta platforma se pot gasi la adresa oficiala a producatorului :* *http://www.safelayer.com/en/products/keyone-pki-platform* *http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx* *http://www.safelayer.com/en/products/trustedx-adaptive-authentication*

Pagina 288:

Utilizatorii vor avea acces numai la aplicatiile si documentele pentru care au drepturi.	***DA***	*Pe baza celor doua componente (Microsoft Active Directory si SafeLayer KeyOne PKI Platform) se creaza un mecanism centralizat de control si audit ce permite ca factorii de autentificare sa fie flexibili si creati in functie de necesitatile de acces ale fiecarui grup de utilizatori (angajati, colaboratori, clienti, etc.) sau aplicatii. Mecanismul de single sign-on este administrat conform cu nivelul de acces cerut.* *Astfel, utilizatorii vor avea acces numai la aplicatiile si documentele pentru care au drepturi.* *http://www.safelayer.com/en/products/trustedx-adaptive-authentication* *http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx*

Pagina 288-289:

Se vor asigura autentificarea, verificarea drepturilor si	***DA***	*Modulul de autentificare numit TrustedX permite urmatoarele facilitati:*

permisiunilor printr-un sistem de securitate, se vor oferi facilitati extinse de autentificare si autorizare a utilizatorilor si a terminalelor folosite.		*furnizarea identitatii ca nivel suplimentar de siguranta, evaluand in mod transparent gradul de risc luand in calcul profilul utilizatorului, comportament si referinte biometrice* *mecanismul centralizat de control si audit ce permite ca factorii de autentificare sa fie flexibili si creati in functie de necesitatile de acces ale fiecarui grup de utilizatori (angajati, colaboratori, clienti, etc.) sau aplicatii.* *Sistemul va asigura autentificarea, verificarea drepturilor si permisiunilor, si va oferi facilitati extinse de autentificare si autorizare a utilizatorilor si a terminalelor folosite.* *http://www.safelayer.com/en/products/trustedx-adaptive-authentication*

Pagina 311:

sa permita contexte diferite de securitate in functie de sectiunea din sistem accesata de catre utilizator. Solutia trebuie sa permita prin configurare conexiuni http (publice, care nu necesita autentificare) si https (cu autentificare) in functie de aceste contexte. *sa permita autorizarea utilizatorilor pe baza listelor de acces definite la nivelul modulului;*	***DA***	*Sistemul informatic, prin intermediul solutiei de securitate si Microsoft Active Directory permite contexte diferite de securitate in functie de sectiunea din sistem accesata de catre utilizator. Solutia permite prin configurare conexiuni http (publice, care nu necesita autentificare) si https (cu autentificare) in functie de aceste contexte.* *http://technet.microsoft.com/en-us/library/cc753531(v=ws.10).aspx* *Microsoft Active Directory si solutia de securitate permit autorizarea utilizatorilor pe baza listelor de acces definite la nivelul modulului;* *http://technet.microsoft.com/en-us/library/cc785913(v=ws.10).aspx* *http://www.safelayer.com/en/products/keyone-pki-platform*

Contestatoarea menţionează că accesul unui utilizator la sistem se face prin intermediul produsului TrustedX care furnizează capabilităţi de interfaţare şi acces, atât pentru echipamente de tip PC sau laptop (prin interfaţa nativă TrustedX, sau interfaţa TrustedX inclusă în aplicaţiile dezvoltate ulterior) cât şi pentru terminale mobile care operează în sistemele iOS sau Android (prin aplicaţia mobilă Safelayer Mobile ID).

Însă, conform celor prezentate în continuare, contestatoarea susţine că autoritatea contractantă face o confuzie gravă de termeni între „server” şi „aplicaţie” prin afirmaţia:

„TrustedX nu este un "server", ci o soluţie de autentificare compatibilă atât cu browsere Web, cât şi cu aplicatii mobile (prin integrararea Safelayer Mobile ID). O aplicaţie Web este componentă client a unui server de aplicaţie, ce facilitează interfaţarea între utilizator şi resursele serverului, şi poate fi accesată prin intermediul unui browser.

În plus, generarea cheilor criptografice direct pe terminalul mobil este o activitate subsidiară şi premergătoare generării şi înrolării certificatului digital direct pe terminalul mobil, producătorii luând decizia de a nu include această informaţie redundantă în prezentarea comercială a produsului Safelayer Mobile ID, însă afirmând acest fapt în declaraţia de producător.

Astfel, contestatoarea consideră abuziv refuzul autorităţii de a lua în considerare declaraţiile unui producător de renume mondial.

În plus, concluzia autorităţii este că: „...reţine în mod corect, cu privire la conceptele de autentificare/autorizare preluate de pe site-ul wikipwdia..” în realitate. Autentificarea are rolul de a valida identitatea unui utilizator, iar autorizarea are rolul de a-i acorda acestuia dreptul de acces la resurse, conform drepturilor sale de acces”.

Referitor la Motivul 7, contestatoarea afirmă că TrustedX este un produs distinct faţă de KeyONE PKI doar în ceea ce priveşte aspectele comerciale, în cazul contractării unei soluţii (fie TrustedX, fie KeyONE PKI) producătorul Safelayer recomandând integrarea cu cealaltă soluţie, deoarece sunt produse complementare. Chiar dacă produsele pot fi vândute şi/sau folosite separat, în toate implementările lor, producătorul oferă suita de soluţii compusă.

Din descrierea tehnică a produsului: http://www.safelayer.com/images/stories/pdf/Safelayer_TrustedX_Adaptive_Auth_EN.pdf) reiese în clar integrarea produsului TrustedX atât cu servicii PKI (KeyONE PKI), cât şi cu protocoale LDAP (Active Directory) în vederea oferirii de contexte diferite de securitate în funcţie de secţiunea de sistem accesată de utilizator.

Safelayer KeyONE PKI, la fel ca şi TrustedX, nu este un produs, ci o platformă de produse ce poate (şi este recomandat) să fie integrată cu produsele complementare oferite de Safelayer.

În concluzie, o soluţie PKI oferită de Safelayer va include atât produse din gama KeyONE, cât şi produse din gama TrustedX, iar o soluţie de control acces oferită de Safelayer va include atât produse din gama TrustedX cât şi produse din gama KeyONE.

Referitor la Motivul 8, privind îndeplinirea cerinţelor referitoare la modul de realizare a criptării, contestatoarea afirmă că în documentaţia iniţială a acestei proceduri, în secţiunea de criptare a informaţiilor la nivelul sistemului de operare, a fost solicitat ca aplicaţia respectivă să permită atât criptare simetrică cât şi asimetrică.

Ca urmare a numeroaselor contestaţii depuse pe acest subiect, aceste cerinţe au fost eliminate. În pofida obligaţiei de a respecta decizia Consiliului, în continuare, autoritatea contractantă susţine necesitatea ca aplicaţiile care implementează tehnologiile PKI să realizeze atât criptare simetrică cât şi asimetrică, adică exact aşa cum a fost solicitat iniţial.

În continuare, contestatoarea redă argumentaţia autorităţii contractante:

„Cerinţele privind mecanismele de asigurare a confidenţialităţii datelor sunt descrise în secţiunea Criptarea documentelor din capitolul

3.3.7.3 Utilizarea certificatelor digitale din modificarea nr. 8 şi sunt reproduse în continuare:

Certificarea datelor va fi asigurată prin criptarea documentelor/informaţiilor, utilizând tehnologii PKI şi algoritmi standard şi prin ştergerea documentelor utilizând algoritmi recunoscuţi la nivel internaţional.

Mecanismele de criptare în tehnologiile PKI se bazează pe algoritmi criptografici standard simetrici şi asimetrici astfel;

- *Criptarea asimetrică, utilizând certificatele X509v3 şi algoritmul RSA*
- *Criptarea simetrică folosind algoritmii 3DES şi AES.*

În aceeaşi secţiune este inclusă şi:

(...)

Criptarea trebuie să poată fi realizată astfel:

a) La nivel desistem de operare, prin crearea unei partiţii criptate;

Decontarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată".

(...)

Prin urmare este evident că produsul care realizează criptarea „La nivel de sistem de operare, prin crearea unei partiţii criptate" trebuie să respecte mecanismele de criptare menţionate:

- *Criptarea asimetrică, utilizând certificatele X509v3 şi algoritmul RSA*
- *Criptarea simetrică folosind algoritmii 3DES şi AES*

Având în vedere cele precizate anterior, contestatoarea învederează faptul că autoritatea contractntă a creat cerinţe sinonime şi identice, tocmai pentru a favoriza unul dintre potenţialii ofertanţi, eludând punerea în practică a deciziilor Consiliului.

Contestatoarea menţionează că autoritatea contractantă conectează la nivel logic două cerinţe distincte astfel încât induce cerinţe artificiale la nivelul criptării partiţiilor de pe staţiile de lucru, tocmai pentru a favoriza anumiţi producători:

- Pentru îndeplinirea cerinţei „asigurarea confidentialităţii documentelor folosind tehnologii PKI" – ... a ofertat produsul Digisigner şi a descris procedurile prin care se realizează operaţiunile de semnare, criptare, aplicare marca temporală etc. asigurând astfel îndeplinirea integrală a cerinţei exprimate în documentaţie
- Referitor la criptarea de disc, produsul Microsoft Bitlocker, propus îndeplineşte integral cerinţele autorităţii contractante:

  a. La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţile aflate pe partiţia criptată;"

În plus, contestatoarea subliniază şi conexarea artificială a algoritmilor cu care se realizează criptarea directă a documentelor cu cerinţa pentru realizarea criptării partiţiilor de disc din punctul de vedere al MFE. Nu au fost ceruţi în clar algoritmi pentru criptarea partiţiilor de disc cum de altfel ar reiesi din decizia Consiliului de modificare a documentaţiei.

În sprijinul presupunerii referitoare la restrângerea de competiţie prin conexarea acestor algoritmi, contestatoarea menţionează că algoritmul AES este net superior lui 3DES, mai mult decât atât, algoritmul 3DES nu mai este recomandat de către autorităţi internaţionale precum NIST şi nici folosit de producători în produsele lor (majoritatea produselor ce realizează criptare de disc folosesc AES şi nu 3DES).

http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

Table 2: Comparable strengths (p.64)

Table 4: Security-strength time frames (p.67)

Documentul oficial NIST, în care 3DES este referit ca TDEA (Triple DEA) evidenţiază în clar că folosirea acestuia după anul 2014 nu mai este recomandată.

Astfel, alăturarea cerinţelor 3DES cu AES şi criptarea de disc nu poate să demonstreze decât intenţia autorităţii şi restrangerea competiţiei.

În schimb, produsul BitLocker, realizează criptarea partiţiilor, care nu are nicio legătură cu cerinţa mai sus menţionată, care se referă la „Asigurarea confidentialităţii documentelor".

BitLocker răspunde la cerinţa referitoare la criptarea aplicaţiilor, pretins neîndeplinită, conform căreia *„Criptarea trebuie să poată fi realizată astfel:*

a. La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la statia de lucru trebuie sa poata conduce la blocarea accesului la informatiile aflate pe partitia criptata". De remarcat că în cuprinsul cerinţei menţionate nu se specifică nimic despre algoritmul criptografic 3DES. Prin urmare, caietul de sarcini nu impune ca BitLocker să implementeze algoritmul 3DES.

În concluzie, produsul BitLocker răspunde la cerinţa pretins neîndeplinită, însă nu are nicio legătură cu tehnologia PKI şi nici cu cerinţa de asigurare a confidentialităţii documentelor aceasta din urmă fiind cea în care se specifică necesitatea criptării utilizând algoritmul 3DES".

Contestatoarea reaminteşte că singurele certificate digitate cerute sunt cele simple, iar acestea includ chei de criptare asimtemtrice dar nu includ şi chei de criptare simetrice. Aşa cum a fost indicat în contestaţiile asupra documentaţiei de atribuire, cerinţele de criptare cu chei simetrice şi asimtrice nu făceau altceva decât restrângeau competiţia şi nu aduceau vreun plus de funcţionalitate autorităţii contractante.

Referitor la afirmaţia:

„Cu privire la îndeplinirea cerinţei

Criptarea trebuie să poată fi realizată astfel:

c) La nivel de sistem de operare, prin crearea unei partiţii criptate. Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată..", contestatoarea afirmă că a demonstrat în cadrul sesiunii demonstrative din 13.11.2014 cum se blochează accesul la o partiţie în urma

deconectării smartcardului de la staţia de lucru. Omiterea acestui aspect în cadrul evaluării nu poate induce decât relele intenţii ale autorităţii cât şi favorizarea făţişă a celuilalt competitor.

Contestatoarea reiterează faptul că a fost solicitată o perioadă de implementare pentru acest proiect, perioadă la capătul căreia funcţionalităţile demonstrate deja vor fi disponibile utilizatorilor soluţiei.

Referitor la Motivul 9, contestatoarea menţionează că prin aprecierea autorităţii contractante cu privire la îndeplinirea cerinţelor referitoare la componenta de comunicare cu arhiva electronică legală din capitolul 3.3.8.1 transpusă ca motivul 10 de neconformitate, răspunsurile ... au fost scoase din context, reiterând în susţinerea afirmaţiilor sale, cele menţionat în contestaţie în acest sens.

De asemenea, contestatoarea afirmă că autoritatea contractantă a dorit să afle într-un mod semnificativ de amănunţit, atipic pentru procedurile de evaluare, modul în care componentele tehnice fucţionează sau interfaţează pentru îndeplinirea funcţionalităţilor solicitate, în ciuda faptului că acestea au fost demonstrate în faţa comisiei de evaluare în 13.11.2014.

Astfel, asa cum s-a răspuns în oferta tehnică, componenta care asigură funcţionalităţile cerute este StarSign, ca parte a soluţiei software de arhivă electronică aparţinând Star Storage:

- *la cerinţa „această componentă de arhivare electronică va fi capabilă să aplice semnături digitale ..., iar aplicarea de semnături digitale va trebui să ofere următoarele capabilităţi minime" oferta tehnică specifică faptul că soluţia cuprinde modulul StarSign, componentă a SEAL, care asigură aplicarea de semnături digitale şi mărci temporale,*
- *la cerinţa „Semnătura electronică va fi în conformitate cu următoarele standarde" oferta tehnică specifică faptul că semnătura electronică va fi aplicată prin intermediul aplicaţiei DigiSigner;*
- *la cerinţa „Marca temporală care va fi aplicată semnăturii electronice va avea următoarele funcţionalităţi şi caracterisitici, ofertatehnică specifică ca marcă temporală va fi aplicată semnăturii electronice prin intermediul aplicaţiei DigiSigner.*

Funcţionalităţile de semnare şi aplicare de mărci temporale în interiorul arhivei electronice legale sunt asigurate de către modulul StarSign din soluţia de arhiva SEAL.

Contestatoarea învederează în acest faptul că soluţia sa de arhivă şi securitate logică este rezultatul integrării mai multor tehnologii aparţinând unor producători diferiţi:

- ✓ Star Storage – arhiva electronică SEAL;
- ✓ DigiSign – client semnare şi autoritate de certificare şi marcare temporală;
- ✓ SafeLayer pentru soluţia de securitate logică la nivel server, autentificare, autorizare şi mobile PKI;

Această integrare a fost necesară ca urmare a cerinţelor de securitate elaborate, sau complexe aşa cum însăşi autoritatea constată.

Astfel, punctul tangent al modului StarSign din arhiva electronică cu soluţia PKI propusă este componenta Digisigner. Integrarea tehnică între Digisigner şi StarSign este realizată cu ajutorul unui SDK – Software Development Kit, pus la dispoziţie de către Digisign.

Contestatoarea îşi exprimă surpinderea deoarece îndeplinirea acestei cerinţe a fost declarată drept neconformă, în condiţiile în care aceastasusţine că a insistat prezentarea funcţionalităţii solicitate în cadrul sesiunii demonstrative din 13.11.2014 în faţa întregii comisii de evaluare.

Mai mult, aşa cum reiese clar şi fără echivoc din răspunsul său din 06.03.2015, inclusiv SDK-ul a fost prezentat în oferta sa tehnică, fiind alocate atât resurse hardware virtuale pentru SDK, respectiv prezentat în schema de licenţiere, respectiv explicitat în detaliu în oferta tehnică.

Contestatoarea precizează că singurul SDK ofertat în oferta tehnică este SDK Digisigner, pe cale de consecinţă este singurul SDK decris în ofertă. Aprecierea autorităţii contractante potrivit căreia s-au adus completări la ofertă, în contextul în care s-au menţionat paginile din oferta tehnică la care se regăsesc informaţiile solicitate, nu poate fi decât rău-voitoare.

Referitor la afirmaţia „De asemenea, în documentaţia de atribuire nu au fost solicitate servicii de dezvoltare pentru Componenta de Comunicare cu Arhiva Electronică Legală”, contestatoarea menţionează că nu este necesară vreo dezvoltare, ci o parametrizare a unor produse comerciale astfel încât să funcţioneze între ele, existând o perioadă de implementare e soluţiei de 8 luni, tocmai pentru a putea parametriza toate componentele soluţiei de arhivă electronică şi cele de securitate astfel încât să funcţioneze ca un tot unitar.

Totodată, contestatoarea menţionează că StarSign este un modul de sine stătător al arhivei electronice SEAL, prezentat ca atare atât la nivel documentar în oferta tehnică cât şi în cadrul sesiunii demonstrative. Singurul SDK ofertat şi licenţiat este Digisigner, însă clarificările oferite fie nu au fost luate în considerare, fie cu rea voinţă au fost interpreatate drept o completare la ofertă;

Funcţionalităţile de semnare electronică, la fel ca şi cele de marcare temporală presupun aplicarea unor algoritmi criptografici standard sau a unor funcţii standard, iar aprecierea autorităţii cum că acestea nu au fost suficient de detaliat expuse induce un caracter excesiv la nivel de evaluare, tocmai pentru a putea respinge oferta subscrisei. De neînţeles este faptul că a fost trecută cu vederea sau uitată sesiunea demonstrativă, unde aceste funcţionalităţi au fost efectiv demonstrate, ceea ce poate conduce la ideea că acest punct de vedere al autorităţii contractante nu a fost redactat de către comisia de evaluare.

Cerinţa autorităţii a fost oferirea unui SDK, iar prin răspunsul său, contestatoarea afirmă că nu a făcut altceva decât să confirme că oferă acest SDK, numele acestuia fiind precizat în clar în tablelul de licenţiere software la pagina 40 din oferta tehnică;

Aplicaţia SEAL a fost proiectată pentru a lucra cu mai mulţi furnizori de identitate electronică şi marcare temporală iar facilitatea acestuia de a se integra la nivel de SDK cu aceşti furnizori nu poate fi apreciat decât ca

un plus de flexibilitate în soluţie. Este de inteles de ce anume autoritatea contractantă refuză să accepte explicaţiile ... asupra elementelor de ofertă şi le cataloghează ca şi modificări de ofertă.

Cu privire la afirmaţia autorităţii contractante *„Motivul respingerii ofertei îl reprezintă neconformitatea tehnică, incapacitatea ofertantului de a prezenta şi susţine o ofertă care să îndeplinească cerinţele documentaţiei de atribuire şi completarea ofertei cu informaţii suplimentare transmise prin răspunsurile la întrebările de clarificare. Prin răspunsurile la întrebările de clarificare ofertantul face incluisiv declaraţii eronate",* contestatoarea face următoarele precizări:

a) Documentaţia de atribuire a favorizat încă de la lansare anumite companii care fac parte din Asocierea formată din ...;

b) Documentaţia de atribuire a fost de natură a limita competiţia prin cerinţele excesive, în special cele referitoare la soluţiile PKI (Public Key Infrastructure) acestea fiind reformulate ca urmare a deciziilor CNSC nr. 244S/C8/1201/07.04.2014; nr. 1584/C8/1201/28.05.2014; nr. 557 S/C3/2606/03.07.2014; nr. 2326/C3/2601-2606/04.08.2014; nr. 16s/ C6/159/16.02.2015; nr. 203/ C6 /159/23.02.2015.

c) Aprecierea la adresa ofertei Star Storage ca „incapacitate" denotă o rea-intenţie, mai ales că proiectul este unul de arhivare fizică şi electronică, domeniu în care ... este unul dintre cele mai importante companii în domeniu, având o experienţă de peste 14 ani, implementand proiecte similare atât la instituţii publice cât şi la companii private.

d) Au fost introduse cerinţe excesive de securitate, acestea fiind şi cele care au fost subiectul principal al contestaţiilor asupra documentaţiei de atribuire şi asupra clarificărilor la aceasta. Scopul acestor cerinţe excesive, care în fapt nu reprezintă scopul principal al proiectului, nu au făcut decât să limiteze competiţia în proiectul în care ponderea componentei de securitate, motiv de descalificare, o reprezintă numai 1% restul fiind arhivare fizică şi electronică;

Pentru acoperirea cerinţelor legate de soluţii PKI, ... a ales să lucreze cu subcontractorii declaraţi în oferta sa, aceştia fiind:

.... – unul dintre cei 5 furnizori de identitate digitală din România;

..., cei din urmă reprezentând producătorul SafeLayer, printre ai cărui acţionari se numară Orange, Indra sau Bull, companii cu reputaţie în IT si telecomunicaţii iar printre clienţii Safelayer se numără: NATO, Ministerul de Interne, Ministerul de Justiţie din Spania, Guvernul Portugaliei, bănci de prestigiu de pe 4 continente.

Astfel a fost nevoie ca unul dintre cei 5 furnizori de identitate digitală şi PKI din România să completeze portofoliul reputaţei companii SafeLayer pentru a răspunde acestor cerinţe care îngrădesc artificial competiţia.

Contestatoarea susţine că atitudinea comisiei de evaluare a fost schimbată total după susţinerea sesiunii demonstrative. Astfel, aceasta afirmă că a susţinut o sesiune demonstrativă, al cărei scop declarat în documentaţie a fost chiar prezentarea modulului de securitate PKI, şi nu cum ar fi fost de aşteptat întreaga soluţie, adică şi cea de arhivă electronică.

În cadrul acestei sesiuni, deşi echipa ... a fost formată din circa 20 de specialişti care au acoperit toate aspectele soluţiei, nu numai cele de securitate, comisia de evaluare a primit răspunsuri pentru toate întrebările şi toate funcţionalităţile modului de securitate. Ba chiar, a insistat întrebând comisia dacă este necesar să detalieze anumite funcţionalităţi pe care le-a văzut demonstrate.

Contestatoarea afirmă că soluţia propusă de ... este un ansamblu de componente mature, fiecare în parte îndeplinind cerinţele din documentaţia de atribuire în considerarea cărora a fost propusă, componentele fiind disponibile comercial şi cu largă utilizare atat la nivel naţional, cât şi internaţional la momentul ofertării.

Prin separarea şi analizarea punctuală şi superficială a componentelor ofertate, cu ignorarea voită a contextului soluţiei globale în care acestea se integrează, prin punctul de vedere transmis, auroritatea încearcă decredibilizarea soluţiei propuse de ...

În final, contestatoarea susţine că a ofertat un sistem 100% corespunzator cerinţelor autorităţii contractante, deşi format din mai multe componente, lucru care nu a fost interzis prin documentaţia de atribuire, ci dimpotrivă. Integrarea unor componente multiple este necesară pentru a pune la dispoziţie sistemul solicitat şi este o precondiţie a asigurării unei concurenţe între mai mulţi producători, dat fiind că sistemul prezintă o complexitate aparte (accesarea şi manipularea documentelor utilizand o gamă largă de dispozitive şi aplicaţii), iar soluţii unitare, de la acelaşi producător, care să asigure simultan şi integral îndeplinirea cerinţelor autorităţii, sunt disponibile pe scara extrem de limitată.

Prin adresa nr. T/1171/17.04.2015, înregistrată la Consiliu sub nr. 6043/17.04.2015, ... formulează concluzii scrise ca urmare a studierii dosarului, în care reiterează cele precizate în cadrul contestaţiei nr.T/1179/20.04.2015 şi de asemenea menţionează că atitudinea răuvoitoare a expertului tehnic, preluată şi de comisia de evaluare, rezultă dintr-un exemplu, legat de pretinsa neîndeplinire a cerinţei caietului de sarcini care constituie Motivul 2 de neconformitate „sesizat" de autoritatea contractantă, respectiv *„În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele: (...)".*

În acest caz, evaluarea modului de respectare a cerinţei este vădit distorsionată, prin conexarea a 2 operaţiuni distincte, fără legătură logică: generarea de certificate pe telefoane mobile şi autentificare de pe telefoane mobile. În acest sens, expertul tehnic argumentează neîndeplinirea cerinţei caietului de sarcini astfel (pag. 19 din raportul de expertiza tehnică revizuit înregistrat cu nr. 4461/02.03.2015):

Autentificarea din browser de pe sistemul de operare Android demonstrază că nu există o aplicaţie comercială ofertată care să genereze chei criptografice şi cereri de certificate pentru acest sistem de operare. Folosirea browserului implică faptul că acestea sunt generate pe un

server şi nu pe dispozitivul mobil, aşa cum s-a solicitat prin caietul de sarcini.

Faţă de aceste susţineri, contestatoarea învederează următoarele:

- Prin caietul de sarcini s-a solicitat ca generarea de certificate să se facă sub sistemele de operare iOS/Android, fără a se preciza dacă operatorul logic în această cerinţă este „şi” sau „sau”;
- ... a prezentat generarea de certificate pe iOS folosind aplicaţia Mobile ID, arătând corespondenţa cu Mobile PKI;
- ... nu i s-a solicitat în cadrul sesiunii demonstrative să prezinte generarea de certificate sub sistemul de operare Google Android;
- A arătat prin declaraţii de la producător că există aplicaţie pentru Google Android. Aplicaţiile pentru Google Android pot fi prezente în Google Play, magazinul oficial Google pentru aplicaţii pentru Android, sau se pot instala separat, direct pe terminalul mobil, sub formă de fişiere de tip.apk;
- Procesul de autentificare cu certificate digitale este total diferit de cel de generare de certificate. Practic, un utilizator cu certificate deja generate sau emise le poate folosi pentru a accesa o aplicaţie potrivit schemei sale de drepturi. Autentificarea la soluţia de portal şi implicit la arhivă se realizează folosind un browser, aceste module fiind web based, aşa cum însăşi autoritatea a solicitat in documentaţie;
- Browser-ele sunt folosite atât pe telefoanele mobile cu sisteme de operare iOS şi Android, cât şi pe staţiile de lucru. Autentificarea se poate realiza prin interfaţa nativă a soluţiei SafeLayer sau prin integrarea interfeţei de autentificare cu aplicaţii terţe. În cazul ofertei ...:
    - pe staţiile de lucru, autentificarea se face în browser;
    - pe telefoanele mobile cu sistem de operare Apple iOS autentificarea se poate face atât cu aplicaţie care integrează interfaţa de autentificare, cât şi direct cu browser;
    - Pe telefoanele mobile cu sistem de operare Google Android, autentificarea se face doar prin browser.
- Nu a fost exprimată vreo cerinţă ca autentificarea să fie făcută atât cu aplicaţii, cât şi cu browser, ci doar să poată fi făcută de pe telefoanele mobile;

În concluzie, atât generarea de certificate pe telefoane mobile, cât şi autentificarea de pe telefoane mobile au fost demonstrate, însă autoritatea a decis să constate neîndeplinirea cerinţelor caietului de sarcini.

Contestatoarea reaminteşte în acest context că cerinţa iniţială a autorităţii contractante a fost generarea de certificate pentru telefoanele mobile cu sisteme de operare Apple iOS/Google Android.

De asemenea, contestatoarea învederează că în rapoartele expertului tehnic sunt prezentate eronat şi cu distorsionarea vădită a realităţii concluziile sesiunii demonstrative susţinute de .... Astfel, în cadrul acestei sesiuni au fost efectiv demonstrate la nivel practic funcţionalităţile modulului 7 şi nu a avut loc o simplă iteraţie de întrebări şi răspunsuri, aşa cum susţine expertul tehnic, sens în care sunt

exemplificate următoarele pasaje din raportul de expertiză tehnică revizuit înregistrat cu nr. 4461/02.03.2015:

Pag. 26: În cadrul sesiunii demonstrative comisia de evaluare a întrebat „Demonstraţia include utilizarea certificatelor digitale pe terminalele mobile stocate pe terminalul mobil? Iar ofertantul a răspuns „Da, a fost făcută o demonstraţie în cadrul sesiunii de prezentare".

Pag. 34: În cadrul sesiunii demonstrative comisia de evaluare a întrebat „Sunt prezentaţi algoritmii criptografici folosiţi pentru criptare fişiere şi criptare partiţii? iar ofertantul a răspuns "Da". Ofertantul a făcut o demonstraţie pe fişiere criptate şi pe partiţii criptate".

Cu privire la cel de-al doilea exemplu, contestatoarea precizează că acesta priveşte Motivul 9 de respingere a ofertei ..., prin care autoritatea contractantă susţine că oferta sa nu îndeplineşte cerinţa caietului de sarcini privitoare la modul de realizare a criptării, respectiv: „Criptarea trebuie să poată fi realizată astfel: a. La nivel de sistem de operare, prin crearea unei partiţii criptate; Deconectarea smartcardului de la staţia de lucru trebuie să poată conduce la blocarea accesului la informaţiile aflate pe partiţia criptată".

Aşadar, deşi procesul verbal al sesiunii demonstrative atestă că ... şi subcontractanţii săi au demonstrat efectiv ceea ce a solicitat comisia, indicând algoritmii cu care se realizează criptarea, totuşi, la acel moment, comisia de evaluare nu a mai ridicat alte întrebări, ci s-a mulţumit să concluzioneze că nu s-au prezentat algoritmii de criptare deşi a putut constata în mod practic cum se realizează criptarea partiţiilor –la pag. 35 din raportul de expertiză tehnică revizuit înregistrat cu nr. 4461/02.03.2015 se arată:

Demonstraţia nu a prezentat algoritmii criptografici folosiţi de Bitlocker.

În al doilea rând, dacă oferta subscrisei a fost respinsă ca neconformă pe motiv că în oferta depusă şi/sau răspunsurile oferite la întrebările de clarificare nu s-au regăsit informaţii care să demonstreze îndeplinirea cerinţelor Caietului de sarcini şi, în plus, că prin unele din răspunsurile de clarificare am modificat propunerea tehnică, în schimb, oferta Asocierii ... a fost declarată conformă, constatându-se în toate cazurile că informaţiile solicitate s-ar regăsi în cadrul ofertei tehnice şi/sau că în urma răspunsurilor la clarificări nu s-au adus completări acestei oferte.

De asemenea, contestatoarea arată că oferta sa a fost respinsă ca neconformă pe motiv că în oferta depusă şi/sau răspunsurile oferite la întrebările de clarificare nu s-au regăsit informaţii care să demonstreze îndeplinirea cerinţelor caietului de sarcini şi, în plus, că prin unele din răspunsurile de clarificare s-a modificat propunerea tehnică, în schimb, oferta Asocierii ... a fost declarată conformă, constatându-se în toate cazurile că informaţiile solicitate s-ar regăsi în cadrul ofertei tehnice şi/sau că în urma răspunsurilor la clarificări nu s-au adus completări acestei oferte.

Având în vedere cele precizate anterior, contestatoarea reiterează că autoritatea contractantă a procedat cu rea-credinţă la ignorarea atât a

elementelor conţinute în oferta ..., cât şi a precizărilor furnizate prin răspunsurile de clarificare transmise. Mai mult, răspunsurile de clarificare nu au făcut altceva decât să indice elementele din oferta ... care se corelează, rezumându-se aşadar la a indica doar informaţii deja prezentate în ofertă, inclusiv în descrierile din broşurile anexate acesteia, şi nu au introdus elemente sau componente noi. Prin urmare, concluzia autorităţii contractante în sensul că s-ar fi procedat la o modificare a ofertei este nelegală şi abuzivă, iar în condiţiile în care Asocierea ... şi-a completat pe cale de clarificări propunerea tehnică prezentând informaţii ce lipseau cu desăvârşire constituie o altă încălcare gravă şi evidentă a principiului tratamentului egal.

Prin urmare, declararea drept admisibilă a ofertei Asocierii ..., în condiţiile în care aceasta şi-a completat propunerea tehnică prin clarificări, ar avea drept consecinţă defavorizarea în mod nejustificat a subscrisei şi crearea unui avantaj indiscutabil Asocierii. O asemenea defavorizare este cu atât mai gravă cu cât ... a ofertat preţul cel mai scazut, cu aproximativ 12.000.000 lei mai puţin faţă de preţul ofertat de Asocierea ....

Prin declararea drept conformă a ofertei Asocierii ..., autoritatea contractantă se face vinovată şi de încălcarea prevederilor art. 201 alin. (2) din O.U.G. nr. 34/2006.

În acest sens, contestatoarea invocă motivarea Hotărârii Curţii de Apel Bucureşti nr. 3195/17.04.2014, în sensul că „prevederile art. 201 alin. (2) invocate sunt încălcate întrucât numai ca urmare a solicitării de clarificări a fost posibilă completarea ofertei petentei, iar avantajul evident este reprezentat de declararea ofertei ca şi câştigătoare dar numai în acest context, şi anume al clarificărilor/completărilor solicitate de autoritatea contractantă".

Astfel, în considerarea celor de mai sus, este indubitabil că oferta Asocierii ..., în măsura în care a fost completată prin răspunsurile la solicitările de clarificări, trebuie declarată neconformă de către autoritatea contractantă, în virtutea prevederilor art. 36 alin. (2) lit. a) din HG nr. 925/2006 şi art. 79 alin. (2) din HG nr. 925/2006.

Totodată, contestatoarea susţine că oferta financiară a Asocierii ... a fost evaluată în mod ilegal.

În acest sens, arată că în Raportul procedurii (pag. 345) se precizează că: *„evaluarea propunerii financiare a fost efectuată exclusiv de către expertul tehnic cooptat, conform prevederilor Ordinului Ministrului Fondurilor Europene nr. 854 din data de 01.08.2014 modificat prin Ordinul Ministrului Fondurilor Europene nr. 861 din data de 08.08.2014".*

În opinia contestatoarei această modalitate de evaluare este vădit ilegală, în raport de dispoziţiile legale care statuează că atributul evaluării ofertelor aparţine exclusiv comisiei de evaluare, iar nu expertilor externi. Nelegalitatea modului de evaluare a ofertelor transpare cu claritate din prevederile:

- art. 72 alin. (2) lit. g) din HG nr. 925/2006 care stabilesc în mod clar în sarcina comisiei de evaluare verificarea propunerilor financiare prezentate de ofertanţi,
- art. 73 alin. (1), (4) nr. 925/2006, numai membrii comisiei de evaluare au dreptul de vot, experţii cooptaţi având rolul exclusiv de a sprijini activităţile de evaluare.

Astfel, sensul dispoziţiilor legale invocate este acela de a consfinţi rolul consultativ, de suport al experţilor tehnici cooptaţi, care însă nu se pot substitui membrilor comisiei de evaluare, singurii cu drept de vot.

Prin contestaţia nr. T/1179/20.04.2015, ... menţionează că oferta Asocierii ...nu îndeplineşte cerinţa din fişa de date cu privire la atestarea situaţiei datelor la bugetul de stat/bugetele locale.

Contestatoarea arată că prin fişa de date a achiziţiei, pct. III.2.1.a) Situaţia personală a candidatului sau ofertantului s-au cerut următoarele:

„7. Documente privind îndeplinirea obligaţiilor exigibile de plată a impozitelor şi taxelor:

Condiţie de calificare: certificatele de atestare fiscală emise de organul fiscal competent, conf. art. 112 si art. 113 din Ordonanţa nr. 92/2003, care să ateste că ofertantul nu are datorii scadente la nivelul lunii anterioare celei în care este prevăzut termenul limită de depunere a ofertelor".

Data limită de depunere a ofertelor a fost stabilită (astfel cum a fost modificat pe cale de erată) pentru 13.08.2014. În aceste condiţii, cerinţa de calificare din fişa de date impunea prezentarea unor certificate de atestare fiscală eliberate de Administraţia Finanţelor Publice din care să reiasă că operatorul economic nu are datorii către bugetul de stat/bugetele locale, scadente la nivelul lunii iulie 2014.

Conform art. 112 din Codul de Procedură Fiscală:

„(1) Certificatul de atestare fiscală se emite de organul fiscal competent la solicitarea contribuabililor. Certificatul se emite şi din oficiu sau la solicitarea altor autorităţi publice, în cazurile şi în condiţiile prevăzute de reglementările legale în vigoare (…).

(2) Certificatul de atestare fiscală se eliberează pe baza datelor cuprinse în evidenţa pe plătitor a organului fiscal competent şi cuprinde creanţele fiscale exigibile, existente în sold în ultima zi a lunii anterioare depunerii cererii, denumită lună de referinţă, şi neachitate până la data eliberării acestuia.

(3) În situaţia în care se emit certificate de atestare fiscală în primele 5 zile lucrătoare ale lunii, acestea vor cuprinde creanţele fiscale exigibile, existente în sold la sfârşitul lunii anterioare lunii de referinţă şi neachitate până la data eliberării acestora.

(4) Certificatul de atestare fiscală se emite în termen de 5 zile lucrătoare de la data depunerii cererii şi poate fi utilizat de persoana interesată pe o perioadă de până la 30 de zile de la data eliberării (…). Pe perioada de utilizare, certificatul poate fi prezentat de contribuabil, în original sau în copie legalizată, oricărui solicitant".

Aşadar, coroborând cerinţa din fişa de date cu dispoziţiile sus-citate ale Codului de Procedură Fiscală, rezultă că Asocierea ... trebuia să

prezinte un certificat eliberat de Administraţia Finanţelor Publice din care să reiasă absenţa datoriilor către bugetul de stat/bugetele locale scadente (exigibile) la 31.07.2014.

Din Raportul procedurii rezultă că Asocierea ... nu a depus în ofertă certificatele de atestare fiscală pentru toţi membrii Asocierii din care să rezulte că aceştia nu aveau obligaţii de plată către bugetele locale exigibile la nivelul lunii iulie 2014, aşa cum s-a solicitat prin fişa de date. În consecinţă, autoritatea contractantă a adresat Asocierii ... o solicitare de clarificări, cu adresa nr. 3149/12.09.2014, fiind reprodus mai jos pasajul relevant, preluat din Raportul procedurii:

„3) Pentru liderul de asociere ... şi pentru asociaţii ... vă solicităm să ne transmiteţi Certificatele privind taxele şi impozitele locale pentru toate punctele de lucru/filiale/sucursale/reprezentanţe menţionate în Certificatele constatatoare emise de ONRC în conformitate cu art. 25, 26 şi 34 din OUG nr. 92/2003 privind Codul de procedură fiscală”.

De asemenea, contestatoarea arată că potrivit raportului procedurii, prin adresa nr. 12408/18.09.2014, înregistrată la MFE cu nr. 3232/DAPITA/18.09.2014, Asocierea ... a transmis răspunsul la solicitarea de clarificări a autorităţii contractante, prezentând o serie de certificate de atestare fiscală privind plata taxelor şi impozitelor locale pentru asociaţii ...., ... şi ... datate septembrie 2014, care reflectă inexistenţa obligaţiilor de plata exigibile la nivelul lunii august 2014.

Aşadar, deşi conform fişei de date trebuiau prezentate certificate care să reflecte faptul că asociaţii nu aveau obligaţii de plată către bugetele locale exigibile la nivelul lunii anterioare depunerii ofertelor (la nivelul iulie 2014), Asocierea ...a prezentat pentru trei dintre asociaţi certificate care nu îndeplineau această cerinţă. Cu toate acestea, comisia de evaluare s-a declarat satisfăcută de răspunsul primit la cererea de clarificare adresată Asocierii ... şi a admis oferta acesteia.

Aşa cum o demonstrează şi practica decizională a Consiliului, dovada îndeplinirii acestui tip de cerinţă trebuia analizată în mod foarte strict de comisia de evaluare, în sensul că se impunea verificarea îndeplinirii a două cerinţe cumulative (şi nu alternative):

- operatorii economici trebuie să prezinte certificate de atestare fiscală care să ateste că şi-au îndeplinit obligaţiile de plată a impozitelor şi taxelor; şi
- îndeplinirea acestor obligaţii de plată trebuie să fie anterioară lunii în care se depun ofertele.

Aşa fiind, chiar dacă membrii Asocierii ... au demonstrat că nu aveau obligaţii scadente la nivelul lunii august 2014, acest lucru nu poate suplini absenţa dovezilor privind lipsa acestor datorii la 31.07.2014. Aceasta deoarece este posibil ca datoriile să fi existat la 31.07.2014 şi să fi fost achitate ulterior, până la data emiterii certificatelor, ceea ce nu înseamnă că Asocierea a îndeplinit cerinţa fişei de date – ar fi trebuit ca membrii Asocierii ... să nu aibă datorii neachitate la nivelul lunii anterioare depunerii ofertelor, ceea ce Asocierea nu a demonstrat.

Mai mult, certificatul de atestare fiscală se emite în 5 zile lucrătoare şi, dat fiind că data limită de depunere a ofertelor a fost 13.08.2014,

emiterea acestuia pentru data de 31.07.2014 putea fi solicitată după primele 5 zile lucrătoare ale lunii iulie, astfel încât certificatul să fie obţinut în timp util pentru a fi depus în cadrul ofertei.

În susţinerea afirmaţiilor sale, contestatoarea invocă practica Consiliului, respectiv decizia CNSC publicată în BO2014_0753:

„Consiliul analizând înscrisurile depuse în ofertei, prin propria voinţă, de către ... constată că operatorul economic contestator, la data depunerii/deschiderii ofertelor nu a îndeplinit condiţiile cumulative impuse de către autoritatea contractantă şi acceptate de către contestator prin necontestarea lor în termenul legal, în speţă nu a făcut dovada că nu figurează în evidenţele fiscale cu obligaţii de plată exigibile la data de 31.01.2014.

Din cele de mai sus rezultă că acest contestator nu a îndeplinit această cerinţă de calificare.

Având în vedere că invitaţia de participare a fost publicată în data de 06.02.2014, iar data limită de depunere a ofertelor a fost 21.02.2014, ... putea şi avea timp suficient ca să solicite la autorităţile legale competente un alt certificat de atestare fiscală prin care să se ateste că nu are obligaţii de plată a impozitelor şi taxelor către bugetul general consolidat, la data de 31.01.2014, întrucât conform prevederilor art. 112 alin. (4) din OUG nr. 92/2003 Codul de procedură fiscală, actualizat, «certificatul de atestare fiscală se emite în termen de 5 zile lucrătoare de la data depunerii cererii» şi «la solicitarea contribuabililor»”.

În concluzie, Asocierea ... nu a îndeplinit cerinţa de calificare din fişa de date referitoare la prezentarea unor certificate de atestare fiscală din care să reiasă că operatorul economic nu are datorii către bugetul de stat/bugetele locale, scadente la nivelul lunii anterioare celei în care este prevăzut termenul limită de depunere a ofertelor, motiv pentru care oferta sa trebuia respinsă ca inacceptabilă, în temeiul art. 36 alin. (1) lit. b) din HG nr. 925/2006.

Totodată, contestatoarea apreciază că respingerea ofertei Asocierii ... se impune şi în virtutea art. 201 alin. (2) şi a principiului tratamentului egal prevăzut la art. 2 alin. (2) lit. b) din OUG nr. 34/2006.

În susţinerea afirmaţiilor sale, contestatoarea precizează că autoritatea contractantă a încălcat flagrant principiul tratamentului egal între ..., pe de o parte, şi Asocierea ..., pe de altă parte, în privinţa modului de analiză a ofertelor şi a solicitărilor de clarificări adresate celor doi ofertanţi.

În acest sens, contestatoarea învederează că a primit 52 de întrebări de clarificare, comparativ cu 6 întrebări câte au fost adresate Asocierii .... Pe baza informaţiilor incluse din prezentarea Asocierii ... susţinută cu ocazia sesiunii demonstrative, unde au fost prezentate pasaje din matricea de răspuns a Asocierii la cerinţele caietului de sarcini, se constată că, deşi nivelul de detalii furnizate de Asocierea ... este limitat, solicitările de clarificare ale autorităţii contractante referitoare la detalierea modului în care se implementează funcţionalităţile tehnice au fost adresate exclusiv ....

Contestatoarea redă în continuare unele pasaje ilustrative din

prezentarea Asocierii ..., ce demonstrează gradul redus de detaliu al abordării cerinţelor caietului de sarcini.

Se mai arată că atitudinea răuvoitoare a autorităţii contractante reiese şi din faptul că, deşi în cazul unora dintre cerinţele tehnice, Asocierea ... nici nu a oferit vreun răspuns, autoritatea nu a solicitat clarificări, ci pur şi simplu a ignorat lipsa răspunsului.

Faptul că furnizarea unui volum ridicat de detalii a fost considerată necesară doar în cazul ... relevă în mod explicit atitudinea părtinitoare a autorităţii contractante faţă de Asocierea ... Pe când nivelul de detaliu furnizat de Asocierea ... a fost considerat unul satisfăcător în cazul tuturor cerinţelor caietului de sarcini, în ceea ce o priveşte pe ... concluzia fost că nu au existat suficiente detalii şi nu s-au prezentat screenshot-uri (capturi de ecran) ale aplicaţiilor. Această atitudine este cu atât mai revoltătoare cu cât însuşi expertul cooptat ..., care semnează raportul de evaluare, a putut constata în cadrul sesiunii demonstrative ceea ce se presupunea necesar a fi probat prin capturi de ecran. Mai mult, aceste capturi de ecran nu au fost solicitate în documentaţie, rolul sesiunii demonstrative fiind tocmai acela de a proba existenţa aplicaţiilor comerciale solicitate, dincolo de broşurile prezentate in oferta tehnică.

În acest context contestatoarea aminteşte că prin Modificarea nr. 8/17.06.2014 s-a renunţat la solicitarea de capturi de ecrane, aspect ignorat de către expertul tehnic pe „expertiza” căruia s-a bazat comisia de evaluare. În acest sens este reprodus un extras din raportul expertului tehnic Răzvan Pop:

„Ofertantul nr. 2....

Oferta tehnică a companiei ... conţine o descriere detaliată a produselor şi serviciilor oferite după cum urmează:

- Descrierea tehnică generală a soluţiei oferite şi abordării propuse;

- Arhitectura soluţiei oferite şi a diagramei funcţionale şi modelului de componente,

- Prezentarea componentelor software pentru soluţia ofertată;

- Prezentarea modului de îndeplinire a (1) cerinţelor specifice, (2) cerinţelor de raportare, (3) cerinţelor privind managementul proiectului şi (4) activităţilor solicitate din caietul de sarcini:

- Alte informaţii considerate semnificative de ofertant pentru evaluarea corespunzătoare a propunerii tehnice.

Răspunsurile la o parte din cerinţele din caietul de sarcini au fost neconcludente şi deşi au fost solicitate întrebări de clarificare, răspunsurile la aceste cerinţe nu au fost detaliate şi/sau nu au fost însoţite de screenshot-uri sau explicaţii complete acolo unde s-a considerat relevant.

Deşi ofertantul a făcut o corespondenţă punct cu punct între aceste cerinţe (aşa cum au fost ele listate în tabelul de conformitate) şi funcţionalităţile ofertate, anumite cerinţe din tabelul de conformitate nu au fost îndeplinite. În concluzie, oferta ... nu respectă întru totul cerinţele tehnice minime formulate de către autoritatea contractantă în caietul de sarcini iar ofertantul va fi considerat ca fiind descalificat din punct de vedere tehnic....”.

Contestatoarea susţine că încălcarea principiului tratamentului egal este demonstrată cu prisosinţă de modul de evaluare a îndeplinirii cerinţei caietului de sarcini referitoare la certificarea soluţiei care implementează funcţionalităţile privind utilizarea certificatelor digitale - Motivul 1 de declarare a ofertei ... ca neconformă.

Astfel, autoritatea contractantă a susţinut prin comunicarea rezultatului procedurii că oferta ... nu îndeplineşte cerinţa enunţată la cap. 3.3.7 din caietul de sarcini, respectiv: „Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificate din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional".

Astfel, autoritatea contractantă susţine că nerespectarea cerinţei menţionate rezultă atât din oferta tehnică a ..., cât şi din răspunsurile de clarificare oferite. Astfel, autoritatea arată că analizând oferta tehnică a ... (pag. 292, 312 şi 319-321) a constatat următoarele:

- Soluţia PKI Safe Layer reprezintă o soluţie de management a certificatelor digitale şi nu implementează funcţionalităţile de semnare, criptare/decriptare, ştergere sigură a fişierelor;
- În cadrul paragrafelor care descriu soluţiile de semnare (pag. 312), criptare/decriptare, ştergere sigură a fişierelor (pag. 319-321) care se instalează pe staţiile de lucru, este prezentată soluţia DigiSigner, pentru care nu reiese din ofertă că este certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional.

Contestatoarea menţionează că temeiurile de respingere invocate de autoritate nu au niciun suport în prevederile caietului de sarcini. De asemenea, în oferta tehnică (pag. 292) s-a prezentat în mod neechivoc modul în care soluţia ofertată răspunde cerinţelor caietului de sarcini, precizând că probează îndeplinirea cerinţei prin soluţia SafeLayer PKI, care prin tehnologia TrustedX implementează funcţionalităţile solicitate prin caietul de sarcini (semnare, criptare/decriptare, ştergere sigură a fişierelor) şi deţine certificarea din punct de vedere al securităţii informatice emisă de către un organism abilitat la nivel internaţional, respectiv certificarea Common Criteria EAL 4+, care răspunde întrutotul cerinţei menţionate.

În răspunsul său (adresa ... nr. MFE/DAPITA/3696/20.10.2014) la întrebarea 23 din solicitarea de clarificare nr. MFE/DAPITA/3597/14.10.2014, contestatoarea afirmă că a confirmat că înţelege să îndeplinească cerinţa caietului de sarcini prin soluţia SafeLayer PKI şi a explicat că DigiSigner este doar o aplicaţie, o componentă utilizată la nivel de client, adică al staţiilor de lucru/PC-urilor, pentru a apela funcţionalităţile disponibile la nivelul soluţiei SafeLayer PKI.

Ulterior, în cadrul răspunsurilor sale (adresa ... nr. MFE/DAPITA/4598/06.03.2015) la solicitarea de clarificări nr. MFE/DAPITA/4498/03.03.2015, contestatoarea susţine că a precizat în mod clar faptul că tehnologia pe care se bazează SafeLayer PKI este

integrată la nivelul librăriilor criptografice accesate cu componenta DigiSigner, aceasta din urmă acţionând ca o interfaţă pentru soluţia SafeLayer PKI propusă. Aşadar, în condiţiile în care soluţia SafeLayer PKI este certificată ISO/IEC 15408 EAL4+ din punct de vedere al securităţii informatice, este evident că nu este necesar să se demonstreze certificarea şi pentru componenta/aplicaţia DigiSigner.

În acelaşi timp, componenta DigiSigner nu este nou introdusă în ofertă, ci se regăseşte menţionată la pag. 312 şi 319-321 din aceasta, răspunsurile de clarificare având rolul de a indica autorităţii paginile unde se regăseşte certificarea solicitată cu privire la soluţia SafeLayer PKI şi de a preciza modul în care componenta DigiSigner acţionează ca o interfaţă pentru această soluţie.

Întrucât autoritatea contractantă nu poate aplica reguli discreţionare în privinţa ofertei Asocierii ..., se impunea ca acelaşi mod de analiză a îndeplinirii cerinţei aflate în discuţie care a fost aplicat ofertei depuse de ... să îşi găsească aplicare şi în cazul ofertei Asocierii.

În aceste condiţii, contestatoarea arata în continuare că autoritatea contractantă nu ar fi putut considera cerinţa de calificare îndeplinită de Asocierea ....

Astfel, conform prezentării Asocierii ... susţinute cu ocazia sesiunii demonstrative, soluţia ofertată pentru implementarea funcţionalităţilor privind utilizarea certificatelor digitale pe staţiile de lucru – semnare, criptare/decriptare şi stergere sigură – este suita shellSafe.

Contestatoarea prezintă, în acest sens, pasajele relevante din prezentarea susţinută cu ocazia sesiunii demonstrative şi învederează faptul că Asocierea ... a prezentat certificarea exclusiv pentru soluţia shellSafe, nu şi pentru componentele care implementează pe staţiile de lucru funcţionalităţile de semnare, criptare/decriptare şi stergere sigură, şi anume componentele clickSign sau sendSAFE. ClickSign şi sendSAFE sunt individualizate drept componente chiar de către producător pe site-ul său conform capturii prezentate în continuare în cadru contestaţie.

Astfel contestatoarea arată că acest exemplu relevă cu claritate atitudinea părtinitoare a autorităţii contractante faţă de Asocierea SIVECO, vădit defavorabilă ..., care s-a manifestat pe întreg parcursul evaluării ofertelor. Astfel, în cazul ..., autoritatea a solicitat clarificări în mod repetat, respectiv prin întrebarea 23 din solicitarea de clarificare nr. MFE/DAPITA/3597/14.10.2014, ulterior şi prin solicitarea de clarificare nr. MFE/DAPITA/4498/ 03.03.2015, referitoare la certificarea componentei DigiSigner, şi deşi ... a explicat de fiecare dată că soluţia SafeLayer PKI este cea certificată, nefiind necesară certificarea unei componente (în speţă DigiSigner), autoritatea a procedat în cele din urmă la respingerea ofertei ... sub pretextul absurd că orice componentă a soluţiei trebuie să aibă o certificare. Prin contrast, în cazul ofertei Asocierii ... autoritatea contractantă nu a solicitat nicio clarificare în privinţa certificării pentru vreuna din componentele soluţiei.

În acest sens, contestatoarea precizează că în jurisprudenţa europeană s-a reţinut că:

„principiile menţionate (n.n. principiul egalităţii de tratament şi principiul transparenţei), care au drept semnificaţie în special faptul că ofertanţii trebuie să se afle pe o poziţie de egalitate atât în momentul în care îşi pregătesc ofertele, cât şi în momentul în care acestea sunt evaluate de către autoritatea contractantă, constituie, într-adevar, temeiul directivelor privind procedurile de atribuire a contractelor de achiziţii publice, iar obligaţia autorităţilor contractante de a asigura respectarea acestora corespunde chiar esenţei acestor directive”.

„Astfel, potrivit unei jurisprudenţe constante, autoritatea contractantă are obligaţia la fiecare fază a unei proceduri de cerere de ofertă, de a respecta principiul egalităţii de tratament faţă de ofertanţi şi, pe cale de consecinţă, de a respecta egalitatea de şanse a tuturor ofertanţilor”.

Necesitatea respectării acestui principiu apare cu atât mai stringentă cu cât încălcarea sa atrage aplicarea de corecţii financiare – prezentul contract fiind finanţat din fonduri externe nerambursabile.

Potrivit pct. 8 din Capitolul 1 din Ghidul privind principalele riscuri identificate în domeniul achiziţiilor publice şi recomandările Comisiei Europene ce trebuie urmate de autorităţile de management/organismele intermediare în procesul de verificare a procedurilor de achiziţii publice aprobat prin Ordinul nr. 543/2013, este considerată un risc solicitarea de clarificări în timpul procesului de evaluare a candidaturilor/ofertelor care se realizează în mod discriminatoriu (cu nerespectarea principiului tratamentului egal). Astfel, Ghidul precizează următoarele: „În procesul de evaluare a documentelor de calificare/selecţie şi/sau a ofertelor, comisia de evaluare trebuie să asigure respectarea principiului tratamentului egal între candidaţii/ofertanţii participanţi la procedura de atribuire”.

Cu titlu de exemplu, contestatoarea menţionează că, în cadrul proiectului „Sistem integrat de management al deşeurilor în judeţul Botoşani”, Cod SMIS 16992, autoritatea contractantă a fost sancţionată pentru încălcarea principiului tratamentului egal, arătându-se că „în exercitarea prerogativei de analiză a ofertelor, autoritatea contractantă are obligaţia să trateze ofertanţii în mod egal, astfel încât unul sau mai mulţi dintre aceştia să nu fie favorizaţi sau, din contră, defavorizaţi prin solicitările de clarificări”.

De asemenea, potrivit Normelor de aplicare a OUG nr. 66/2011, aprobate prin HG nr. 875/2011, „cel mai frecvent indicator al oferirii de mită şi comisioane ilegale este tratamentul favorabil nejustificat acordat unui contractant de către un responsabil pentru contractare într-o perioadă de timp”.

În al doilea rând, dacă oferta ... a fost respinsă ca neconformă pe motiv că în oferta depusă şi/sau răspunsurile oferite la întrebările de clarificare nu s-au regăsit informaţii care să demonstreze îndeplinirea cerinţelor caietului de sarcini şi, în plus, că prin unele din răspunsurile de clarificare s-a modificat propunerea tehnică, în schimb, oferta Asocierii ... a fost declarată conformă, constatându-se în toate cazurile că informaţiile

solicitate s-ar regăsi în cadrul ofertei tehnice şi/sau că în urma răspunsurilor la clarificări nu s-au adus completări acestei oferte.

Contestatoarea reiterează că autoritatea contractantă a procedat cu rea-credinţă la ignorarea atât a elementelor conţinute în oferta sa cât şi a precizărilor furnizate prin răspunsurile de clarificare transmise. Mai mult, răspunsurile de clarificare nu au făcut altceva decât să indice elementele din oferta ... care se corelează, rezumându-se aşadar la a indica doar informaţii deja prezentate în ofertă, inclusiv în descrierile din broşurile anexate acesteia, şi nu au introdus elemente sau componente noi. Prin urmare, concluzia autorităţii contractante în sensul că s-ar fi procedat la o modificare a ofertei este nelegală şi abuzivă, iar în condiţiile în care Asocierea ... şi-a completat pe cale de clarificări propunerea tehnică prezentând informaţii ce lipseau cu desăvârşire constituie o altă încălcare gravă şi evidentă a principiului tratamentului egal.

Prin urmare, declararea drept admisibilă a ofertei Asocierii ..., în condiţiile în care aceasta şi-a completat propunerea tehnică prin clarificări, ar avea drept consecinţă defavorizarea în mod nejustificat a ... şi crearea unui avantaj indiscutabil Asocierii. O asemenea defavorizare este cu atât mai gravă cu cât ... a ofertat preţul cel mai scăzut, cu aproximativ 12.000.000 lei mai puţin faţă de preţul ofertat de Asocierea ....

Prin declararea drept conformă a ofertei Asocierii ..., autoritatea contractantă se face vinovată şi de încălcarea prevederilor art. 201 alin. (2) din OUG nr. 34/2006.

În acest sens, contestatoarea invocă motivarea Hotărârii Curţii de Apel Bucureşti nr. 3195/17.04.2014, în sensul că „prevederile art. 201 alin. 2 invocate sunt încălcate întrucât numai ca urmare a solicitării de clarificări a fost posibilă completarea ofertei petentei, iar avantajul evident este reprezentat de declararea ofertei ca şi câştigătoare dar numai în acest context, şi anume al clarificărilor/completărilor solicitate de autoritatea contractantă".

În contextul celor precizate anterior, contestatoarea apreciază că oferta Asocierii ..., în măsura în care a fost completată prin răspunsurile la solicitările de clarificări, trebuie declarată neconformă de către autoritatea contractantă, în virtutea prevederilor art. 36 alin. (2) lit. a) din HG nr. 925/2006 şi art. 79 alin. (2) din HG nr. 925/2006.

De asemenea, contestatoarea învederează că oferta financiară a Asocierii ... a fost evaluată în mod nelegal. În raportul procedurii se precizează că „evaluarea propunerii financiare a fost efectuată exclusiv de către expertul tehnic cooptat, conform prevederilor Ordinului Ministrului Fondurilor Europene nr. 854 din data de 01.08.2014 modificat prin Ordinul Ministrului Fondurilor Europene nr. 861 din data de 08.08.2014.

În opinia contestatoarei această modalitate de evaluare este vădit nelegală, în raport de dispoziţiile legale care statuează că atributul evaluării ofertelor aparţine exclusiv comisiei de evaluare, iar nu experţilor externi. Nelegalitatea modului de evaluare a ofertelor transpare cu claritate din prevederile:

- art. 72 alin. (2) lit. g) din HG nr. 925/2006 care stabilesc în mod clar în sarcina comisiei de evaluare verificarea propunerilor financiare prezentate de ofertanţi;
- art. 73 alin.(1) şi (4) din HG nr. 925/2006, numai membrii comisiei de evaluare au drept de vot, experţii cooptaţi având rolul exclusiv de a sprijini activităţile de evaluare.

Astfel, sensul dispoziţiilor legale invocate este acela de a consfinţi rolul consultativ, de suport al experţilor tehnici cooptaţi, care însă nu se pot substitui membrilor comisiei de evaluare, singurii cu drept de vot.

În aceeaşi ordine de idei, art. 2 alin. (4) din HG nr. 925/2006 stipulează principiul asumării răspunderii, potrivit căruia autoritatea contractantă este responsabilă pentru modul de atribuire a contractului de achiziţie publică, cu respectarea tuturor dispoziţiilor legale aplicabile. Or, nu se poate conchide că autoritatea contractantă s-a conformat acestui principiu, în condiţiile în care aceasta nu a trecut prin propriul filtru, astfel cum era obligată, concluziile expertului cooptat.

Totodată, contestatoarea pune în discuţie şi o serie de alte aspecte constatate cu ocazia consultării dosarului, ce relevă potenţiale derapaje suplimentare de la legalitatea procesului de evaluare, astfel:

1. Prin Nota justificativă privind perioada de evaluare a ofertelor datată 02.09.2014 şi semnată de doamna ..., se menţionează:

(a) Faptul că la data de 13.08.2014, în cadrul şedinţei de deschidere a ofertelor, domnul ..., membru cu drept de vot în comisia de evaluare, a depus o declaraţie prin care precizează că se află în imposibilitate de a-şi exercita atribuţiile de membru al comisiei de evaluare deoarece nu garantează imparţialitatea faţă de unul dintre ofertanţii participanţi la procedură. Mai departe, se arată că până la data de 02.09.2014 domnul ... nu fusese înlocuit cu unul dintre membrii de rezervă ai comisiei, deoarece aceştia se aflau fie în concediu de odihnă, fie la cursuri de perfecţionare, propunându-se înlocuirea acestuia cu doamna ... începând cu data de 01.09.2015. Or, în pofida acestei situaţii, din chiar cuprinsul aceleiaşi Note rezultă că în perioada 13.08.2014-02.09.2015 se efectuaseră acte de evaluare a ofertelor depuse în cadrul procedurii, respectiv fusese verificată îndeplinirea cerinţelor documentaţiei privitoare la situaţia personală a candidatului/ofertantului şi capacitatea de exercitare a activităţii profesionale.

În acest sens, contestatoarea redă în cele ce urmează, pasajul relevant din NOTĂ:

„În data de 13.08.2014, în cadrul deschiderii ofertelor, la sediul Ministerului Fondurilor Europene a fost depusă de domnul ..., consilier în cadrul Direcţiei Generale de Coordonare Sistem şi Asistenţă Tehnică, în calitate de membru cu drept de vot în cadrul comisie de evaluare, o declaraţie (document ataşat în copie) prin care acesta menţionează că se află în imposibilitatea de a-şi exercita atribuţiile ce îi revin în cadrul comisiei de evaluare, întrucât nu garantează imparţialitatea faţă de unul dintre ofertanţii participanţi la procedura de atribuire. Până la momentul întocmirii prezentei Note, domnul ... nu a fost înlocuit cu unul dintre membrii de rezervă nominalizaţi în cadrul Ordinului MFE nr. 845/2014,

modificat de Ordinul MFE nr. 861/08.08.2014, deoarece membrii de rezervă din cadrul comisiei de evaluare se aflau, fie în concediu de odihnă, fie la cursuri de perfecţionare. Pe cale de consecinţă, începând cu data de 01.09.2014, domnul ... va fi înlocuit cu unul dintre membrii de rezervă desemnaţi în cadrul ordinului de numire, respectiv cu doamna .... De la data de 01.09.2014, doamna ... va exercita atribuţiile în calitate de membru cu drept de vot în cadrul comisiei.

Până în prezent a fost verificată doar demonstrarea îndeplinirii cerinţelor menţionate în fişa de date şi în anunţul de participare referitoare la:

- *secţiunea II.2.1.a) Situaţia personală a candidatului sau ofertantului,*
- *secţiunea II.2.1.b) Capacitatea de execrcitare a activităţii profesionale"*.

În aceste condiţii este evidentă nelegalitatea actelor de evaluare efectuate în cadrul procedurii de atribuire în perioada 13.08.2014-02.09.2015.

(b) Faptul că doamna ... semnează Nota în data de 01.09.2014 în calitate de preşedinte fără drept de vot al comisiei de evaluare, deşi aceasta avea la data respectivei Note calitatea de preşedinte cu drept de vot, revocarea dreptului de vot al doamnei ... operând abia prin Ordinul MFE nr. 9/13.01.2015.

Această „scăpare" sugerează că respectivul document a fost „fabricat" la o dată ulterioară revocării dreptului de vot al doamnei Valentina Lazăr.

2. Invitaţia adresată domnului ..., expert IT cooptat de a participa la sesiunea demonstrativă susţinută de ... în data de 13.11.2014 este nedatată şi conţine următoarea precizare:

„Ţinând cont de faptul că ofertantul Asocierea ..., ..., ..., ..., ... nu a dorit să beneficieze de această prelungire a termenului şi a susţinut prezentarea demonstrativă în data de 06.11.2014, ora 13.00, fapt consemnat şi în procesul verbal de prezentare a sesiunii demonstrative pentru funcţionalităţile Modulului 7 din caietul de sarcinicu nr. MFE/4077/06.11/2014, vă invităm să participaţi la prezentarea sesiunii demonstrative a ofertantului ..., în data de 13.11.2014, orele 15.00".

Această menţiune indică, practic fără echivoc, că domnul ... era informat cu privire la susţinerea de către Asocierea ... a sesiunii demonstrative în data de 06.11.2014, fapt absolut surprinzător în contextul în care aparent domnul ... a participat la sesiunea demonstrativă susţinută de Asocierea ... şi a semnat Procesul verbal al respectivei sesiuni (Anexa 4 – Proces verbal de prezentare a sesiunii demonstrative pentru funcţionalităţile Modulului 7 din caietul de sarcini pentru ofertantul Asocierea ..., înregistrat cu nr. MFE/DAPITA 4077/06.11.2014).

Acest „detaliu" ridică serioase semne de întrebare cu privire la veridicitatea informaţiilor cuprinse în Procesul verbal al sesiunii demonstrative susţinute de Asocierea ... şi la însăşi autenticitatea acestui înscris.

În final, contestatoarea învederează că în contextul în care procedura a fost marcată de numeroase nereguli, autoritatea contractantă are obligaţia de a anula procedura de atribuire potrivit art. 209 alin. (1) lit. c) din OUG nr. 34/2006. Ipoteza reglementată de legiuitor la acest articol priveşte existenţa unor abateri grave de la prevederile legislative, care afectează procedura de atribuire, iar situaţiile relevate în contestaţiile depuse cu privire la prezenta procedură se încadrează în definiţia „abaterilor grave" prevăzută la alin. (4) al art. 209 din OUG nr. 34/2006, respectiv erori sau omisiuni constatate pe parcursul analizei, evaluării şi/sau finalizării procedurii de atribuire, faţă de care autoritatea contractantă se află în imposibilitate de a adopta măsuri corective fără ca acestea să conducă la încălcarea principiilor prevăzute la art. 2 alin. (2) lit. a)-f) din acelaşi act normativ.

Prin adresa nr. 307/23.04.2015, înregistrată la Consiliu sub nr. 6583/24.04.2015, ... formulează răspuns la concluziile scrise emise de către ..., înregistrate sub nr. T/1171/17.04.2015, în care învederează că argumentele prezetate în cuprinsul concluziilor scrise nu reprezintă altceva decât veritabile completări ale contestaţiei depuse iniţial, completări care nu au fost evidenţiate în termenul legal de contestare reglementat de OUG nr. 34/2006 şi care nu pot fi primite la soluţionarea litigiului dedus judecaţii.

În susţinerea afirmaţiilor sale, intervenienta invocă Decizia civilă nr. 1550 din 10 septembrie 2012, Curtea de Apel Bacau - Secţia a II-a civilă, de contencios administrativ şi fiscal, a reţinut că *„Formularea de critici noi după expirarea termenului de contestare - prin intermediul concluziilor scrise - este tardivă, iar analizarea lor de către Consiliu este inadmisibilă".*

Pentru a decide în acest sens, instanţa de judecată a reţinut că „Procedura contenciosului prescrisă de ordonanţă este supusă unor rigori stricte, subordonate principiului celerităţtii exprimat de art. 276 alin. (1) al acestui act normativ. Imperativul celerităţii defineşte o serie de cerinţe speciale ale procedurii în faţa Consiliului între acestea numărându-se necesitatea sesizării Consiliului într-un termen anume dat de art. 256^2 alin. (1), cu o serie de temeiuri de nelegalitate determinate ce ar putea atrage anularea actului vătămător şi/sau recunoaşterea dreptului pretins de petiţionar; termenul respectiv este unul de decădere, depasirea sa ducând la tardivitatea oricărei completări la acţiune. Aşadar, este lipsită de relevanţă că reclamanta nu şi-a completat capetele de cerere ale contestaţiei iniţiale, atâta vreme cât ea a înţeles să invoce cu totul alte temeiuri de nelegalitate a actelor contestate, cu mult după depăşirea termenului impus de ordonanţă. În mod evident, aceste noi temeiuri reprezintă o modificare a investirii Consiliului care este solicitat să analizeze eventualul caracter fondat al acestora, să ceară autorităţii contractante să prezinte un punct de vedere la ele, să le pună în discuţia celorlalţi participanţi la dispută. Or, o modificare a instirii Consiliului ulterioară expirării termenului prevăzut la art. 256^2 alin. (1) este afectată de tardivitate".

Cât priveşte procedura de a solicita accesul la dosarul achiziţiei publice, urmată de completarea contestaţiei în raport de informaţiile din respectivul dosar, trebuie avut în vedere că ordonanţa prevede calea de atac a contestaţiei pentru motive de nelegalitate şi netemeinicie care îi sunt cunoscute persoanei vătămate la momentul formulării ei, iar nu pentru motive necunoscute. Contestaţia trebuie să cuprindă motivarea integrală a ei, în fapt şi în drept, sens în care dispune art. 270 alin. (1) lit. e) din ordonanţă. Singura ipoteză în care se admite completarea motivării este aceea de la art. 270 alin. (2) - când Consiliul apreciază că în contestaţie nu se regăseşte motivarea ei, ocazie cu care pune în vedere autoarei să îşi regularizeze contestaţia în termen de cinci zile.

Drept urmare, faţă de cele mai sus aratate, luând în considerare inclusiv cele menţionate în cuprinsul cererii de intervenţie, precum şi faptul că toate criticile evidenţiate în cuprinsul concluziilor scrise depuse de autoarea contestaţiei la data de 17.04.2015 sunt noi, nefiind menţionate în cadrul contestaţiei, intervenienta solicită să fie respinse ca inadmisibile.

În eventualitatea în care sunt considerate ca fiind admisibile completările din concluziile scrise, cu toate că în cuprinsul contestaţiei ... nu a adus critici ofertei ... cu privire la modalitatea de îndeplinire a cerinţelor minime de calificare, respectiv la o eventuală încălcare a principiului tratamentului egal, intervenienta învederează următoarele:

1. Cu privire la afirmaţia contestatoarei potrivit căreia oferta Asocierii ... nu îndeplineşte cerinţa din fişa de date cu privire la atestarea situaţiei datoriilor la bugetul de stat/bugetele locale, intervenienta afirmă că certificatele solicitate de autortiatea contractantă au vizat punctele de lucru ale membrilor asocierii, iar nu sediile principale ale acestora, cu privire la care au fost depuse certificate corespunzătoare.

Pe de altă parte, în cadrul ofertei, ... susţine că a depus o declaraţie pe proprie răspundere privind îndeplinirea cerinţelor minime de calificare şi selecţie, întemeiată pe dispoziţiile art. 11 alin. (4) din HG nr. 925/2006, însoţită de o anexă în care a menţionat succint, dar precis, modul concret de îndeplinire a cerinţelor din fişa de date a achiziţiei.

În considerarea celor de mai sus, intervenienta susţine că, potrivit art. 9 alin. (3) din Ordinul ANRMAP nr. 509/2011 privind formularea criteriilor de calificare şi selecţie *„În situaţiile de la art. 11 alin. (4) şi (5) din Hotărârea Guvernului nr. 925/2006 (...), autoritatea contractantă va lua în considerare, la verificarea îndeplinirii cerinţei de calificare privind plata de către ofertant a impozitelor; taxelor şi contribuţiilor de asigurări sociale, atât declaraţia pe propria răspundere prin care se confirmă îndeplinirea cerinţei cât şi acele certificate de atestare fiscală prezentate de ofertant în urma solicitării primite din partea autorităţii contractante, chiar dacă acestea sunt emise de autorităţile competente ulterior datei de deschidere a ofertelor şi, eventual, atestă lipsa datoriilor ulterior respectivei date”.*

Astfel luând în considerare faptul că dispoziţiile art. 11 citat mai sus nu impun ca documentul să fie emis în momentul deschiderii ofertelor, ci doar să reflecte o situaţie de fapt a ofertantului, precum şi interpretarea

ANRMAP exprimată prin Ordinul 509/2011, act care reprezintă poziţia oficială a legiuitorului în concordanţă cu principiile consacrate la art. 2 alin. (2) din ordonanţa, intervenienta afirmă că decizia autorităţii contractante este legală.

De altfel, fiind investită cu o cerere similară, Curtea de Apel Craiova - Secţia contencios administrativ şi fiscal, prin Decizia nr. 1469 din 2 martie 2012, a reţinut că „Este nelegală respingerea unei oferte pe motivul că certificatele de atestare fiscală sunt emise ulterior datei şedinţei de deschidere a ofertelor".

2. Referitor la afirmaţia contestatoarei potrivit căreia „Respingerea ofertei Asocerii ... se impune şi în virtutea art. 201 alin. (2) şi a principiului tratamentului egal prevăzut la art. 2 alin. (2) lit. b) din OUG nr. 34/2006”, intervenienta afimă că aceasta este nefondată.

Totodată, intervenienta menţionează că îndeplinirea cerinţelor minime din caietul de sarcini nu se analizează din perspectiva nivelului de detalii furnizate de un ofertant, fiind evident că autoritatea contractantă este interesată ca propunerea tehnică să răspundă necesităţilor acesteia, iar nu ca propunerea tehnică să fie voluminoasă, cu informaţii irelevante faţă de cele stabilite în caietul de sarcini. Este irelevant cât de detaliată este abordată îndeplinirea cerinţelor din caietul de sarcini, din moment ce informaţiile incluse în propunerea tehnică răspund necesitaţilor achizitorului.

În legătură cu afirmaţiile ... referitor la evaluarea ofertei tehnice a Asocierii ... privind gradul de detaliu al răspunsurilor din matricea de conformitate, intervenienta afirmă că în oferta tehnică a oferit informaţii precise, la obiect, care includ denumirea aplicaţiilor furnizate şi funcţionalităţile îndeplinite. Informaţii detaliate privind fiecare aplicaţie, care să susţină îndeplinirea cerinţelor, sunt prezentate cu un grad de detaliu suficient pentru a demonstra conformitatea cu cerinţele din documentaţia de atribuire. În afară de informaţiile din matricea de conformitate au fost furnizate, în cadrul ofertei înaintate, şi manuale şi fişe tehnice de produs care conţineau detalii privind la caracteristicile tehnice. Exemplele prezentate de contestatoare sunt rupte din contex, paragrafele indicate fiind extrase, de fapt, dintre alte paragrafe în care sunt descrise pe larg funcţionalităţile aplicaţiilor.

Intervenienta învederează că motivele care au condus la declararea ofertei ca ... fiind neconformă nu ţin de gradul de detaliu al ofertei tehnice ci de lipsa informaţiilor privind aplicaţiile şi arhitectura sistemului ofertat şi modul în care acestea funcţionează împreună pentru îndeplinirea cerinţelor.

Astfel, aşa cum reiese din comunicarea privind rezultatul procedurii de atribuire nr. 13760/16.03.2015 şi din răspunsurile la întrebările de clarificare, la motivele de neconformitate următoare contestatoarea declara iniţial că o anumită aplicaţie îndeplineşte cerinţele dar aduce prin răspunsuri completări şi încearcă să realizeze conexiuni între aplicaţii diverse, realizate de producători diferiţi şi pentru care nu sunt furnizate detalii de integrare, invocând ca singur motiv de conformitate faptul că

toate aceste aplicaţii au fost enumerate, la un moment dat, într-o secţiune din oferta tehnică:

- Motivul 1 - certificarea de securitate este deţinută de Soluţia SafeLayer. Răspunsurile la întrebările de clarificare indică îndeplinirea cerinţei privind Soluţia SafeLayer împreuna cu DigiSigner, care este componenta client a SafeLayer. În contestaţie ... indică, pentru îndeplinirea cerinţei, şi produsul TrustedX Electronic Signature care nu a fost inclus în oferta tehnică, aşa cum reiese din punctul de vedere transmis de autoritatea contractantă la data de 03.04.2015
- Motivul 2, motivul 4 - sunt indicate certificatele emise în format .p12 de DigiSign şi SafeLayer Mobile PKI, fără a se preciza o versiune de produs. Răspunsurile la întrebările de clarificare prezintă îndeplinirea cerinţei de către SafeLayer Mobile ID care nu a fost menţionat anterior, pentru care se susţine în mod eronat că nu există versiuni, acesta fiind la versiunea 1.3.1 în App Store, şi pentru care se prezintă declaraţii false din partea SafeLayer, conform cărora Mobile ID ar fi prezent în Google Play (Anexa II la Răspuns la întrebările de clarificare nr T/822/06.03.2015).
- Motivul 3 - este indicată utilizarea aplicaţiei SafeLayer KeyOne XRA. Răspunsurile la întrebările de clarificare prezintă îndeplinirea cerinţei de către TrustedX Adaptive Authentication.
- Motivul 5 - este indicată utilizarea KeyOne XRA. Răspunsurile la întrebările de clarificare prezintă îndeplinirea cerinţei de către SafeLayer TrustedX iar în Concluziile scrise nr. T/1142/09.04.2015 aduc alte completări, fiind indicată integrarea dintre Autoritatea de înregistrare KeyOne cu Autoritatea de certificare (Root CA) a DigiSign.
- Motivul 6 - este indicată utilizarea KeyOne XRA. Răspunsurile la întrebările de clarificare prezintă îndeplinirea cerinţei de către SafeLayer TrustedX.
- Motivul 7, motivul 8 - este indicată utilizarea *„soluţiei de securitate si Microsoft Active Directory".* Răspunsurile la întrebările de clarificare prezintă îndeplinirea cerinţei de către SafeLayer TrustedX.
- Motivul 9 - este indicată utilizarea BitLocker. Răspunsurile la întrebarile de clarificare prezintă îndeplinirea cerinţei de către DigiSigner, care este componenta client a BitLocker, şi SafeNet e-Token PRO.
- Motivul 10 - cu privire la semnătură electronică este indicată când utilizarea componentei SEAL a modulului StarSign, când utilizarea DigiSigner. Răspunsurile la întrebările de clarificare prezintă integrarea dintre SEAL şi DigiSigner SDK, care nu a fost menţionat şi descris anterior.

Cu privire la raportul expertului tehnic cooptat, intervenienta afirmă că declararea motivelor de neconformitate s-a făcut în baza Raportului procedurii. Deoarece decizia de a respinge oferta ... a aparţinut, în mod exclusiv, autorităţii contractante, nu se poate reţine o eventuală încălcare a dispoziţiilor legale care să conducă la concluzia existenţei unor abateri de la legislaţia achiziţiilor publice. Nu a existat niciun motiv de neconformitate care să refere lipsa capturilor de ecran.

De asemenea, intervenienta susţine că în prezenta procedură, producătorul SafeLayer a făcut declaraţii false privind disponibilitatea aplicaţiei Mobile ID în Google Play astfel că orice alte declaraţii din partea acestuia şi a ofertantului ..., care nu sunt insotite de dovezi clare, trebuie privite cu neîncredere.

În legătură cu afirmaţiile ... referitor la evaluarea ofertei tehnice a Asocierii ... privind îndeplinirea cerinţei „Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional european sau internaţional", intervenienta precizează următoarele:

Astfel, după cum reiese din oferta tehnică şi din prezentarea susţinută cu ocazia sesiunii demonstrative, a fost ofertată suita de aplicaţii shelISAFE care conţine componentele (aplicaţiile) clickSIGN, sendSAFE, diskSAFE şi shredSAFE.

Intervenienta susţine că shelISAFE nu este o aplicaţie de sine statoare, ci o colecţie de aplicaţii (ciickSIGN, sendSAFE, diskSAFE şi shredSAFE) care îndeplinesc funcţionalităţi diferite. Faptul că aceste componente fac parte din shelISAFE este menţionat în mod explicit în ofertă, în repetate rânduri, ca de exemplu:

- în matricea de conformitate
- în manualele transmise împreună cu oferta tehnică,
- pe site-ul unde este disponibil Catalogul ...(... INFORMATION ASSURANCE PRODUCT CATALOGUE), indicat şi în oferta tehnică: http://www.ia.nato.int/niapc/Product/shellSAFE476 shelISAFE este inclusă în "CATALOGUL NAŢIONAL CU PACHETE, PRODUSE ŞI PROFILE DE PROTECŢIE INFOSEC - versiunea consolidată iunie 2014", publicat de ORNISS. Catalogul este disponibil la adresa: http://orniss.ro/ro/legislatie/pdf/ordine/catalogulnational/CATALOG INFOSEC v conso lidata iunie2014.pdf.

shelISAFE este inclusă în ... INFORMATION ASSURANCE PRODUCT CATALOGUE pentru protecţia informaţiilor clasificate ale Alianţei, până la nivelul .. RESTRICTED (http://www.ia.nato.int/niapc/Product/shellSAFE 476).

De asemenea, certificarea din punct de vedere al securităţii a fost realizată pentru întreaga suită shelISAFE, implicit, pentru toate componentele sale: clickSIGN, sendSAFE, diskSAFE şi shredSAFE. Acest lucru reiese atât din informaţiile prezentate în oferta tehnică, precum şi din extrasele de mai sus.

La soluţionarea contestaţiei nu poate fi primită afirmaţia conform căreia „Asocierea SIVECO a prezentat certificarea exclusiv pentru soluţia shellSAFE nu şi pentru componentele care implementează pe staţiile de lucru funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură, şi anume componentele clickSIGN sau sendSAFE", aceasta fiind făcută cu scopul de a devia de la neconformităţile ....

Aceasta deoarece, toate aplicaţiile care compun suita shelISAFE (clickSIGN, sendSAFE, diskSAFE şi shredSAFE) sunt dezvoltate de acelaşi

producător, UTI, iar evaluarea shelISAFE a presupus evaluarea fiecărei aplicaţii. Pentru demonstrarea conformităţii au fost prezentate, de fiecare dată, aplicaţiile clickSIGN, sendSAFE, diskSAFE şi shredSAFE, în funcţie de funcţionalităţile care trebuiau îndeplinite şi s-a menţionat faptul că fac parte din suita shelISAFE, aşa cum reiese şi din captura de ecran prezentată de ... la pagina 11 a Concluziilor scrise. În plus, inclusiv ..., în catalogul ... INFORMATION ASSURANCE PRODUCT CATALOGUE, prezintă shellSAFE ca o suită de aplicaţii şi enumeră explicit componentele clickSIGN, sendSAFE, diskSAFE şi shredSAFE, certificate pentru protecţia informaţiilor clasificate ale Alianţei.

În aceste condiţii, este evident că autoritatea contractantă nu a avut niciun motiv de a solicita Asocierii ... clarificări suplimentare deoarece, asa cum a fost indicat în oferta tehnică înaintată, suita shellSAFE care conţine aplicaţiile clickSIGN, sendSAFE, diskSAFE şi shredSAFE este inclusă în NATO INFORMATION ASSURANCE PRODUCT CATALOGUE, pentru protecţia informaţiilor clasificate ale coaliţiei, şi este prezentă în CATALOGUL NATIONAL CU PACHETE, PRODUSE ŞI PROFILE DE PROTECŢIE INFOSEC de pe site-ul ORNISS, ceea ce demonstrează fără echivoc că shellSAFE şi implicit componentele sale este „certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional”, fiind enumerată în secţiunile:

- "A. LISTA PRODUSELOR INFOSEC APROBATE LA NIVELUL NATO", subsecţiunea " 22. Suite de securitate desktop"
- "E. LISTA PRODUSELOR ŞI MECANISMELOR CRIPTOGRAFICE CERTIFICATE LA NIVEL NATIONAL".

Cu privire la motivul 2 de respingere a ofertei SC STAR STORAGE SA, intervenienta susţine următoarele:

- Capitolul *3.3.7.3.1. Autentificarea la sistem* din Modificarea 8 include cerinţa *„Terminalele mobile utilizate în cadrul autorităţii contractante se bazează minim pe sistemele de operare iOS si Android".* Acest capitol descrie functionalităţi care presupun utilizarea certifictelor digitale pe terminalele mobile, cu ambele sisteme de operare, deci este evident faptul că aplicaţia de generare a cheilor criptografice direct pe terminalul mobil trebuie să fie disponibilă atât pentru iOS cât şi pentru Android.
- Sesiunea demonstrativă nu suplineşte detalierea modului de îndeplinire a cerinţelor şi descrierea funcţionalităţiior şi capacităţilor tehnice ale aplicaţiilor în oferta tehnică. Din afirmaţiile ... rezultă că nici măcar în cadrul sesiunii demonstrative nu a prezentat aplicaţia Mobile PKI sau Mobile ID, cu nicio funcţionalitate, pentru sistemul de operare Android.
- în Anexa II la Răspuns la întrebăriie de clarificare nr T/822/06.03.2015 contestatara prezintă declaraţia SafeLayer privind aplicaţia Mobile ID în care afirmă în mod explicit că Mobile ID este disponibil în Google Play. Mobile ID nu este prezent magazinul oficial al Google deşi, până la aceste concluzii scrise ... a susţinut declaraţiile false ale SafeLayer iar acum încearcă să prezinte o altă modalitate de îndeplinire a cerinţei.

Intervenienta susţine că pentru accesul de pe PC, printr-un browser web, trebuie să fie disponibilă o metodă de autentificare a utilizatorului

folosind certificatul digital propriu aflat pe terminalul mobil. ... a prezentat iniţial SafeLayer KeyOne XRA ca fiind aplicaţia utilizată pentru autentificare iar prin contestatie susţine că „Pe telefoanele mobile cu sistem de operare Google Android autentificarea se face doar în browser”.

De asemenea, nu demonstrează că aplicaţia de generare a cheilor criptografice direct pe terminalul mobil este disponibilă pentru Android. Astfel de detalii precum şi modul în care soluţia propusă îndeplineşte cerinţele ar fi trebuit să se găsească în oferta tehnică.

Datorită specificului sistemelor de operare mobile, care nu sunt la fel de flexibile ca sistemele de operare de pe PC, mecanismul de autentificare din browser pentru sistemul de operare Android nu poate asigura îndeplinirea cerinţei referitor la accesul de pe PC:

„În cazul folosirii certificatului digital stocat pe dispozitivul criptografic propriu, conectat la terminalul mobil propriu, sau stocat pe terminalul mobil propriu procesul de autentificare necesita un mecanism de tip „challenge-response" pentru identificarea cu exactitate a utilizatorului care doreşte a se autentifica la sistem. Mecanismul de tip „challenge- response" va utiliza tehnologia PKl pentru semnarea digitala a unui mesaj codificat in mod standardizat, de către ambele entitati implicate in procesul de autentificare, respectiv componenta de server si utilizatorul. Fiecare dintre cele două entităţi va semna mesajul cu propriul certificat digital. Mesajul codificat trebuie să fie vizibil utilizatorului şi să includă informaţii despre timpul de expirare al procesului de autentificare. Sistemul de autentificare trebuie să fie capabil şi să permită operaţiunile de semnătură cu certificate stocate în memoria terminalului mobil, cu certificate stocate pe Secure SD conectat la terminal şi cu certificate stocate pe dispozitive de tip smartcard (standard FIPS140-2 level 2) cu interfaţa standard PKCS #11 conectate la terminal".

Pentru accesul la sistem folosind terminale mobile, intervenienta afirmă că în această situaţie este posibilă autentificarea folosind browserul terminalului mobil, deoarece acesta este utilizat pentru accesul la aplicaţii. Totuşi, îndeplinirea acestei cerinţe nu îndeplineşte şi cerinţa de acces de pe PC şi autentificare folosind terminalul mobil.

Concluzionând, intervenienta reţine cerinţele din documentaţia de atribuire conform cărora:

- utilizatorii trebuiau să poată accesa sistemul de pe PC, folosind un browser web, şi autentificându-se prin intermediul terminalului mobil şi a unei aplicaţii.

- utilizatorii trebuiau să poată accesa sistemul de pe terminalul mobil, folosind un browser web de pe acest terminal

- „Terminalele mobile utilizate în cadrul autorităţii contractante se bazează minim pe sistemele de operare iOS şi Android" iar functionalităţile sistemului *trebuie* să fie disponibile pe acestea. Nu există în documentaţia de atribuire nicio referinţă care să facă distincţia între funcţionalităţile disponibile pe sistemul de operare iOS şi cele disponibile pe sistemul de operare Android. Formularea folosita de contestatară „iOS/Android" nu se regăseşte printre cerinţele capitolului *3.3.7. Modulul 7: Componenta de Securizare Acces şi Documente* din Modificarea 8 iar

prezentarea în contestatie, pentru prima dată, a interpretării conform căreia funcţionalităţile trebuie să fie disponibile pe un sistem de operare sau pe altul este forţată.

În ceea ce priveşte modalitatea de evaluare a propunerii sale financiare, intervenienta susţine că trebuie avut în vedere că, potrivit HG nr. 925/2006, experţii cooptaţi sunt desemnaţi cu scopul de a facilita activitatea de evaluare a ofertelor, iar printre atribuţiile acestora, raportat la competenţele lor, se numără şi analiza situaţiei financiare a ofertanţilor/candidaţilor ori analiza financiară a efectelor pe care le pot determina anumite elemente ale ofertei sau clauze contractuale propuse de ofertant.

Mai mult, trebuie avut în vedere că experţii cooptaţi nu au drept de vot, însă au obligaţia de a elabora un raport de specialitate în care, pe baza expertizei pe care o deţin, îşi exprimă punctul de vedere cu privire la ofertele evaluate, raportul de specialitate fiind destinat să faciliteze comisiei de evaluare adoptarea deciziilor în cadrul procesului de analiză a ofertelor şi de stabilire a ofertei/ofertelor câştigătoare.

Drept urmare, chiar şi în situaţia în care evaluarea propunerii financiare a ... s-a realizat de către expertul cooptat, din moment ce decizia de declarare a admisibilităţii a aparţinut, în mod exclusiv, autorităţii contractante**,** nu se poate reţine o eventuală încălcare a dispoziţiilor legale.

Prin adresa nr. 15384/23.04.2015, înregistrată la Consiliu sub nr. 6546/24.04.2015, Ministerul Fondurilor Europene formulează punct de vedere faţă de contestaţia nr. T/1179/20.04.2015, depusă de ... în care consideră că întrega pledoarie prezentată în cadrul motivului I este nerelevantă din punct de vedere al motivelor de declarare a ofertei contestatoarei ca necâştigătoare.

În ceea ce priveşte susţinerea contestatoarei potrivit căreia oferta Asocierii ... nu îndeplineşte cerinţa din fişa de date cu privire la atestarea situaţiei datoriilor la bugetul de stat/bugetele locale, autoritatea contractantă menţionează că aşa cum rezultă din grila de verificare a cerinţelor de calificare a ofertantului Asocierea dintre ... a constatat ca urmare a analizei documentelor de calificare următoarele:

- referitor la Certificatul de atestare fiscală, eliberat de organul de administrare fiscală al unităţii administrativ teritoriale pe raza căreia societatea îşi are sediul social, din care să rezulte, îndeplinirea obligaţiilor scadente la nivelul lunii anterioare celei în care este prevăzut termenul limită de depunere a ofertelor pentru:

- Liderul asocierii ... a depus în cadrul ofertei o copie „conform cu originalul” a certificatului de atestare fiscală nr.1172645/04.08.2014, eliberat de ANAF, prin care se certifică lipsa obligaţiilor de plată la administraţia fiscală la data de 31.07.2014 (pag.62-64), semnat şi ştampilat.
- ... a depus în cadrul ofertei o copie „conform cu originalul” a certificatului de atestare fiscală nr. 911966/08.08.2014, eliberat de

ANAF, prin care se certifică lipsa obligaţiilor de plată la administratia fiscală la data de 31.07.2014 (pag.65-66), semnat şi ştampilat.
- ... a depus în cadrul ofertei o copie „conform cu originalul” a certificatului de atestare fiscală nr.912010/08.08.2014, eliberat de ANAF, prin care se certifică lipsa obligaţiilor de plată la administraţia fiscală la data de 31.07.2014 (pag.67-68), semnat şi ştampilat.
- ... a depus în cadrul ofertei o copie „conform cu originalul” a certificatului de atestare fiscală nr.228827/22.07.2014, eliberat de ANAF, prin care se certifică lipsa obligaţiilor de plată la administraţia fiscală la 30.06.2014.(pag.71-73), semnat şi ştampilat, declaraţia iniţială şi anexa la aceasta prin care declară pe proprie răspundere că îndeplineşte acest criteriu de calificare şi se obligă ca, în cazul în care va primi solicitare din partea autorităţii contractante, să prezinte documentul edificator.
- ... a depus în cadrul ofertei o copie „conform cu originalul” a certificatului de atestare fiscală nr.1170324/10.07.2014, eliberat de ANAF, prin care se certifică lipsa obligaţiilor de plată la administraţia fiscală la 30.06.2014.(pag.76-78), semnat şi ştampilat, însă nu este valabil la data deschiderii ofertelor aşa cum este mentionat in Documentatia de atribuire pag. 7, si anume: „Toate documentele trebuie să fie valabile la data deschiderii ofertelor”, declaraţia iniţială prin care declara pe proprie răspundere că îndeplineşte acest criteriu de calificare şi se obliga ca, în cazul în care va primi solicitare din partea autoritatii contractante, să prezinte documentul edificator.

Ca urmare, în cadrul solicitării de clarificari înregistrată DAPITA cu nr. 3149/12.09.2014 transmisă Asocierii ..., comisia de evaluare a solicitat clarificarea următoarelor aspecte:

1) Pentru asociatul ...: În cadrul procesului de evaluare comisia de evaluare a constatat că aţi depus Certificatul de atestare fiscală ce atesta datoriile de până la data de 30.06.2014. Ca urmare, vă rugăm să ne retransmiteţi Certificatul constator din care să rezulte îndeplinirea obligaţiilor scadente la nivelul lunii anterioare datei de deschidere a ofertelor, respectiv 31.07.2014, conform cerinţelor din fişa de date.

2) Pentru asociatul ...: În cadrul procesului de evaluare comisia de evaluare a constatat că aţi depus Certificatul de atestare fiscală ce atestă datoriile de până la data de 30.06.2014. Ca urmare, vă rugăm să ne retransmiteţi Certificatul constator din care să rezulte îndeplinirea obligaţiilor scadente la nivelul lunii anterioare datei de deschidere a ofertelor, respectiv 31.07.2014, conform cerinţelor din fişa de date.

Răspunsul la clarificare înregistrat cu nr. 3232/DAPITA/18.09.2014 a fost transmis în termenul solicitat. Ofertantul a transmis Certificatul de atestare fiscală al operatorului ... cu nr.1181211/12.08.2014 (3 pagini), din care reiese că nu are obligaţii de plată exigibile la data de 31.07.2014 şi Certificatul de atestare fiscală al operatorului ... cu nr. 229178/13.08.2014 (3 pagini) din care reiese că nu are obligaţii de plată exigibile la data de 31.07.2014.

- referitor la Certificatul privind plata impozitelor şi taxelor locale din care să rezulte plata obligaţiilor faţă de bugetul local din care să rezulte îndeplinirea obligaţiilor scadente

la plată în luna anterioară celei în care se depune oferta. Se va prezenta Certificatul privind plata impozitelor şi taxelor locale în copie lizibilă, cu ştampila şi semnătura autorizată având menţiunea „conform cu originalul”.

- Liderul asocierii ...a depus în cadrul ofertei o copie a certificatului de atestare fiscală nr. 256448/01.08.2014, eliberată de Directia Impozite şi Taxe Locale Sector 1, prin care se certifică lipsa obligaţiilor de plată privind impozitele şi taxele locale (pag.80), cu ștampila şi semnătura autorizată şi menţiunea conform cu originalul.
- ... a depus în cadrul ofertei o copie a certificatului de atestare fiscală nr. 125822/01.08.2014, eliberată de Direcţia Venituri Buget Local Sector 2, prin care se certifică lipsa obligaţiilor de plată privind impozitele şi taxele locale (pag.83), cu ştampila şi semnătura autorizată şi menţiunea conform cu originalul.
- ... a depus în cadrul ofertei o copie a certificatului de atestare fiscală nr.350407/04.08.2014, eliberată de Direcţia Generală de Impozite şi Taxe Locale Sector 4, prin care se certifică lipsa obligaţiilor de plată privind impozitele şi taxele locale (pag.84-85), cu ștampila şi semnătura autorizată şi menţiunea conform cu originalul.
- ... a depus în cadrul ofertei o copie a certificatului de atestare fiscală nr.6500/01.08.2014, eliberată de Direcţia Economică şi Finanţe Publice Locale a municipiului Iaşi, prin care se certifică lipsa obligatiilor de plata privind impozitele şi taxele locale (pag.88), cu ștampila şi semnătura autorizată şi menţiunea conform cu originalul.
- ... a depus în cadrul ofertei o copie a certificatului de atestare fiscală nr.147-14-27579/01.08.2014 eliberată de Direcţia de Impozite şi Taxe Locale Sector 6, prin care se certifică lipsa obligaţiilor de plată privind impozitele şi taxele locale (pag.91), cu ştampila şi semnătura autorizată şi menţiunea conform cu originalul.

Astfel, autoritatea contractantă afirmă că în cadrul solicitării de clarificări înregistrată DAPITA cu nr. 3149/12.09.2014 transmisă Asocierii SIVECO, comisia de evaluare solicită clarificarea următorului aspect:

- Pentru liderul de asociere ... și pentru asociații ..., ... vă solicităm să ne transmiteți Certificatele privind taxele și impozitele locale pentru toate punctele de lucru/filiale/sucursale/reprezentanțe menționate în Certificatele constatatoare emise de O.N.R.C., în conformitate cu art.25, 26 și 34 din O.G.nr.92/2003 privind Codul de procedură fiscală.

Ofertantul a transmis anexat răspunsului la clarificare înregistrat cu nr. 3232/DAPITA/18.09.2014:

- Certificatul privind taxele şi impozitele locale nr. IF 053405/17.09.2014 pentru operatorul ..., punct de lucru ... eliberat de către Direcţia Fiscală a municipiului ..., din care reiese că nu are obligatii de plata la bugetul local la nivelul lunii august,
- Certificatul privind taxele şi impozitele locale nr. S70365/16.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de către Consiliul Local ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.

- Certificatul privind taxele şi impozitele locale nr. 372829/15.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de către Consiliul Local ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 2844855/17.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de către Consiliul Local ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 6378185/15.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de catre Primăria Municipiului ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 7610/15.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de către Primăria Municipiului ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 287063/01.09.2014 pentru operatorul ... - pct de lucru Sector ..., eliberat de către Consiliul local Sector ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 702110/15.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de către Primăria Municipiului ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 323066/15.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de către Primăria Municipiului ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 1792624/15.09.2014 pentru operatorul ... - pct de lucru ... eliberat de către Primăria Municipiului ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificatul privind taxele şi impozitele locale nr. 5895/15.09.2014 pentru operatorul ... - pct de lucru ..., eliberat de către Primăria Comunei ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificate privind taxele şi impozitele locale nr. 350851/16.09.2014 şi nr.350852/16.09.2014 şi nr. pentru operatorul ... - pctele de lucru din şoseaua ... Sector ... Bucureşti, eliberat de către D.G.I.T.Sector ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.

- Certificat privind taxele şi impozitele locale nr. 147-14-34002/16.09.2014 şi nr. pentru operatorul ... - pct de lucru din Sectorul ... Bucureşti, eliberat de către D.G.I.T.Sector ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august.
- Certificat privind taxele şi impozitele locale nr.147-14-31475/28.08.2014 şi nr. pentru operatorul ... - pct de lucru din Sectorul

... Bucureşti, eliberat de către D.G.I.T.Sector ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii iulie.
- Certificat privind taxele şi impozitele locale nr.47382/01.09.2014 pentru operatorul .... - pct de lucru din ..., eliberat de către Serviciul Finante Publice Locale ..., din care reiese că nu are obligaţii de plată la bugetul local la nivelul lunii august, şi

Având în vedere următoarele prevederi:
- art. 201 alin. (1) din O.U.G. nr. 34/2006 cu modificările şi completările ulterioare, şi anume: „Pe parcursul aplicării procedurii de atribuire, autoritatea contractantă are dreptul de a solicita clarificări şi, după caz, completări ale documentelor prezentate de ofertanţi/candidaţi pentru demonstrarea îndeplinirii cerinţelor stabilite prin criteriile de calificare şi selecţie sau pentru demonstrarea conformităţii ofertei cu cerinţele solicitate."
- art. 9 alin. (2) din Ordinul nr. 509 din 14.09.2011, al preşedintelui Autoritatii Nationale pentru Reglementarea si Monitorizarea Achizitiilor Publice privind formularea criteriilor de calificare si selectie, şi anume: „Raportarea se va face la inexistenta datoriilor fată de bugetul general consolidat, la o dată corelată cu termenul legal al scadentei de plată şi nu la termenul de valabilitate al documentului la data depunerii sau deschiderii ofertelor."
- art. 9 alin. (3) din Ordinul nr. 509 din 14.09.2011, al preşedintelui Autorităţii Naţionale pentru Reglementarea şi Monitorizarea Achiziţiilor Publice privind formularea criteriilor de calificare şi selecţie, şi anume: „În situaţiile de la art. 11 alin. (4) şi (5) din Hotărârea Guvernului nr. 925/2006 (...) autoritatea contractantă va lua în considerare, la verificarea îndeplinirii cerinţei de calificare privind plata de către ofertant a impozitelor, taxelor și contribuțiilor de asigurări sociale, atât declarația pe propria răspundere prin care se confirmă îndeplinirea cerinței, cât și acele certificate de atestare fiscală prezentate de ofertant în urma solicitării primite din partea autorității contractante, chiar dacă acestea sunt emise de autoritățile competente ulterior datei de deschidere a ofertelor și, eventual, atestă lipsa datoriilor ulterior respectivei date".

Răspunsurile primite din partea Asocierii ... au fost considerate concludente şi acceptate de comisia de evaluare. În concluzie, Asocierea ... a îndeplinit cerinţa de calificare din fişa de date referitoare la prezentarea unor certificate de atestare fiscală din care să reiasă că operatorul economic nu are datorii către bugetul de stat/bugetele locale, scadente la nivelul lunii anterioare celei în care este prevăzut termenul limită de depunere a ofertelor.

În ceea ce priveşte critica contestatoarei potrivit căreia respingerea ofertei Asocierii Siveco se impune şi în virtutea art. 201 alin. (2) şi a principiului tratamentului egal prevăzut la art. 2 alin. (2) lit.b) din OUG nr. 34/2006, autoritatea contractantă susţine că autoarea contestaţiei face afirmaţii complet nefondate şi de rea credinta, acuzând autoritatea contractantă de încălcarea articolului 201 alin. (2) şi a) principiului tratamentului egal prevăzut în articolul 2 alin. (2) lit. b) din OUG 34/2006, aducând în susţinerea propriilor afirmaţii argumente

nefundamentate şi vădit rău-intenţionate. Aceste aspecte, coroborate cu atitudinea şi acţiunile contestatoarei de-a lungul întregului proces aferent procedurii şi cu argumentele prezentate anterior în punctele de vedere demonstrează, în mod neechivoc, faptul că ... îşi doreşte exclusiv blocarea procedurii şi, implicit îngreunarea, pe cât posibil, a absorbţiei fondurilor europene din care ar urma să se finanţeze contractul.

Faptul că i s-au adresat mai multe întrebări de clarificare (52) în comparaţie cu celalalt ofertant, în condiţiile în care, oferta ... a fost neclară în ceea ce priveşte produsele ofertate, neputându-se identifica cu exactitate care sunt acestea, ar trebui să demonstreze diligenţa de care autoritatea contractantă a dat dovadă în procesul de evaluare. Întrebările au fost clare şi concise, urmărind exclusiv lămurirea neclarităţilor legate de oferta contestatoarei, neclarităţi care însă au persitat şi în anumite cazuri persistă încă. Mai mult, ..., prin oferta, şi ulterior de-a lungul sesiunilor de clarificare, a încercat cu bună ştiinţă inducerea în eroare a comisiei de evaluare prin furnizarea de informaţii eronate referitoare la versionarea produselor software ofertate.

Referitor la critica contestatoarei potrivit căreia oferta financiară a Asocierii ... a fost evaluată în mod nelegal, autoritatea contractantă susţine că prin Ordinul Ministerului Fondurilor Europene nr. 854 din data de 01.08.2014 modificat prin Ordinul Ministerului Fondurilor Europene nr. 861 din data de 08.08.2014 atribuţiile Expertului IT cooptat - angajat conform contract de servicii nr. 6126/144/29.11.2013 cu titlul „Sprijin pentru Ministerul Fondurilor Europene în realizarea funcţiilor de coordonare a instrumentelor structurale şi de gestionare a Programului Operaţional Asistenţă Tehnică" constau în: „sprijinirea procesului de evaluare a propunerilor tehnice şi financiare depuse în cadrul procedurii menţionate, iar atribuţiile acestuia se vor rezuma după caz, la verificarea şi evaluarea propunerilor tehnice şi financiare, inclusiv acordarea punctajelor aferente acestora. Expertul cooptat nu va avea drept de vot, însă în conformitate cu prevederile art. 73 din H.G. nr. 925/2006, cu modificările şi completările ulterioare, are obligaţia de a elabora un raport de specialitate cu privire la aspectele tehnice asupra cărora, pe baza expertizei pe care o deţine, îşi exprimă punctul de vedere în procesul de evaluare. Raportul de specialitate se ataşează la raportul de atribuire şi devine parte a dosarului achiziţiei publice, iar expertul răspunde solidar alături de membrii comisiei de evaluare".

Astfel, autoritatea contractantă afirmă că la Raportul procedurii nr. 13739/LO/16.03.2015 au fost anexate printre altele şi:

4. Raportul intermediar de expertiză tehnică a expertului cooptat înregistrat la MFE/DAPITA cu nr. 4039/05.11.2014 care conţine ataşat:

a) Grila de verificare a propunerii tehnice pentru ofertantul Asocierea formată din SC ... (lider), SC ... SRL, SC ...SA, SC ... SRL şi SC ... SRL;

b) Grila de verificare a propunerii tehnice pentru ofertantul ...

5. Raportul de expertiză tehnică a expertului cooptat înregistrat la MFE/DAPITA cu nr. 4324/21.11.2014 care conţine ataşat:

a) Grila de verificare a propunerii tehnice pentru ofertantul Asocierea formată din ...;

b) Grila de verificare a propunerii tehnice pentru ofertantul ....

c) Grila de acordare a punctajului aferent ofertei depuse pentru Asocierea formată din ....

[…]

9. Raportul de expertiză tehnică revizuit a expertului cooptat înregistrat la MFE/DAPITA cu nr. 4461/02.03.2015, Anexa - Raportul tehnic nr. 2 în urma desfăşurării sesiunilor demonstrative.

Autoritatea contractantă consideră că această modalitate de evaluare este în conformitate cu legislaţia în vigoare, respectiv art. 73 alin. (4), (5) şi (6) din HG 925/2006, cu modificările şi completările ulterioare.

Mai mult, raportul de evaluare a fost asumat prin semnătură de comisia de evaluare, raport care a fost semnat și de către cei trei observatori desemnați (..., ..., ...), cu mențiunea "fără observații" cu privire la respectarea aspectelor procedurale.

De asemenea, în cadrul secţiunii Aplicarea criteriului de atribuire, la pagina 350, din Raportul procedurii nr. 13739/LO/16.03.2015 este făcută următoarea menţiune „Comisia de evaluare a semnat grila de punctaj", grila de acordare a punctajului care este anexată Raportului procedurii menţionat anterior.

Având în vedere cele precizate anterior, autoritatea contractantă consideră criticile contestatoarei referitoare la aspectele menționate tendenţioase, complet neîntemeiate, nefondate, nefiind bazate pe niciun argument concret.

În ceea ce priveşte critica contestatoarei referitoare la Nota justificativă privind prelungirea perioadei de evaluare a ofertelor nr. 7113/LO/02.09.2014, şi anume:

(a) „nelegalitatea actelor de evaluare efectuate în cadrul procedurii de atribuire în perioada 13.08.2014-02.09.2015", având în vedere prevederile art. 76 alin. (1) şi (2) din HG nr. 925/2006, autoritatea contractantă menţionează că nu identifică „evidenta" nelegalitate a „actelor de evaluare efectuate în cadrul procedurii de atribuire în perioada 13.08.2014-02.09.2015".

b) În ceea ce priveşte semnarea Notei justificative privind prelungirea perioadei de evaluare a ofertelor nr. 7113/LO/02.09.2014 în calitate de preşedinte fără drept de vot al comisiei de evaluare, autoritatea conteractantă afirmă că în cadrul procesului de evaluare, dintr-o eroare de editare, apare Nota justificativă antemenţionată semnată de preşedintele cu drept de vot al comisiei de evaluare, ca fiind fără drept de vot, deşi majoritatea documentelor sunt semnate doar în calitate de preşedinte al comisiei de evaluare.

În ceea ce priveşte critica contestatoarei, şi anume „această „scăpare" sugerează că respectivul document a fost „fabricat" la o dată ulterioară revocării dreptului de vot al doamnei ..." autoritatea contractantă face următoarele precizări:

1) Nota justificativă privind prelungirea perioadei de evaluare a ofertelor nr. 7113/LO/02.09.2014 a fost finalizată în data de 02.09.2014.
2) În data de 04.02.2014 ofertanţii participanţi la procedură au fost informaţi via fax cu privire la prelungirea perioadei de evaluare prin adresa semnată de preşedintele comisiei de evaluare şi înregistrată DAPITA cu nr. 3079/04.09.2014 (Anexa nr. 1 – 3 pagini)
3) În data de 04.02.2014 observatorii UCVAP au fost informaţi via fax cu privire la prelungirea perioadei de evaluare prin adresa semnată de preşedintele comisiei de evaluare şi înregistrată DAPITA cu nr. 3078/04.09.2014 şi le-a fost înaintată Nota justificativă privind prelungirea perioadei de evaluare a ofertelor nr. 7113/LO/02.09.2014 (Anexa nr. 2 – 2 pagini).
4) Modificarea componenţei comisiei de evaluare s-a produs ca urmare a Ordinului Ministerului Fondurilor Europene nr. 9 din data de 13.01.2015.

Referitor la Invitaţia adresată domnului ...., expert IT cooptat, de a participa la sesiunea demonstrativă susţinută de Star Storage în data de 13.11.2014, autoritatea contractantă afirmă că această invitaţie este datată cu nr. 4161/12.11.2014, iar la sesiunile demonstrative din data de 06.11.2014 au fost invitaţi cei 2 ofertanţi, observatorii UCVAP şi expertul IT cooptat.

Cu privire la solicitarea contestatoarei de anulare a procedurii, autoritatea contractantă susţine că aceasta este nefondată, nefiind bazată pe niciun argument concret. Susținerile contestatoarei sunt simple presupuneri, întreaga contestație având ca scop tergiversarea încheierii procedurii de atribuire și semnarea contractului, putând conduce astfel la pierderea fondurilor alocate realizării proiectului.

Prin adresa nr. 311/24.04.2015, înregistrată la Consiliu sub nr. 6625/24.04.2015, ... formulează cerere de intervenţie în care solicită respingerea ca tardiv formulată şi ca fiind lipsită de interes contestaţia, în principal, iar în subsidiar, ca nefondată cu consecinţa menţinerii rezultatului procedurii de atribuire.

De asemenea, intervenienta invocă excepţia tardivităţii contestaţiei în conformitate cu dispoziţiile art. 270 alin. (1) din OUG nr- 34/2006.

În acest sens, intervenienta arată că prin intermediul celor două contestaţii, ... a înţeles să critice aceleaşi decizii ale autorităţii contractante, respectiv decizia de respingere ca nefondată a ofertei acesteia, precum şi decizia prin care oferta Asocierii ... a fost declarată câştigătoare, singura diferenţă constând în aceea că, prin contestaţia care face obiectul prezentului dosar, autoarea căii de atac a încercat să evidenţieze motivele de fapt pentru care consideră că oferta Asocierii ... trebuia declarată inadmisibilă.

Din punctul său de vedere, intervenienta apreciază că demersul societatii contestatoare nu reprezintă altceva decât o completare a contestaţiei depuse iniţial, demers care urmează a fi sancţionat cu tardivitatea/inadmisibilitatea, motivat de faptul că ... avea obligaţia de a

include în contestaţia iniţială motivele de fapt şi de drept relevante în susţinerea acesteia.

O interpretare contrară ar echivala cu eludarea termenelor de 5 zile/10 zile în care trebuie formulată şi motivată o contestaţie.

Astfel, în cazul de faţă, este tardiv şi/sau inadmisibil ca motivarea integrală a unei contestaţii să se facă printr-o altă contestaţie depusă ca urmare a studierii dosarului achizitiei publice, cu eludarea termenului legal imperativ de 10 zile pentru formularea şi implicit motivarea acesteia.

Caracterul tardiv al „motivării" unei contestaţii prin concluzii scrise este în deplină concordanţă cu practica anterioară a Consiliului.

Astfel, prin Decizia nr. 2180 din 30 mai 2011 – publicată în extras şi cu nota de Dumitru Daniel Serban in Curierul Juridic nr. 7-8/2011, pag. 391-397, Consiliul a statuat următoarele:

„(…) completarea contestaţiei cu noi acuzatii la adresa autorităţii, în afara termenului legal de contestare a actului vătămător, este incompatibilă cu dispoziţiile normative în vigoare (…)."

„(…) motivele suplimentare celor din contestaţia (…) formulate de (…) în cuprinsul concluziilor scrise depuse la Consiliu la 19.05.2011 vor fi înlăturate de acesta ca inadmisibile pe calea concluziilor scrise şi nu vor fi reţinute pentru analizare, depăşind cadrul procesual cu care a fost investit."

Important de reţinut este că toate diligenţele pentru includerea tuturor criticilor în cuprinsul contestaţiei şi pentru motivarea corespunzatoare a acesteia, în termenul imperativ de 10 zile reglementat de legislaţia achizitiilor publice, revin în mod exclusiv operatorului economic care depune contestatia.

În sustinerea acestei afirmaţii, relevantă este Decizia nr. 4874 din 3 iulie 2012 pronunţată de Curtea de Apel Alba Iulia, din al cărei conţinut rezultă următoarele:

„În atare conditii, formularea de critici noi după expirarea termenului de contestare era tardivă, iar analizarea acestora de către Consiliu era inadmisibilă. De asemenea, reiterarea acestor critici tardive pe calea plângerii este inadmisibilă, urmând a fi respinse în consecinta".

În acelasi sens s-a pronunţat şi Curtea de Apel Bucureşti în Decizia civilă nr. 1570 din 24 august 2011, reţinând:

„Pe fondul plângerii, Curtea a constatat că susţinerile petentei sunt neîntemeiate. Referitor la cererea de completare a contestaţiei formulată la Consiliul, Curtea a reţinut că este inadmisibilă prezentarea unor noi motive cu nerespectarea termenului de 10 zile de la data comunicării rezultatului procedurii de atribuire, având în vedere că data luării la cunoştinţă cu privire la decizia de respingere a fost cunoscută de petentă prin primirea adresei nr. (…).

Prin urmare, în mod corect Consiliul a considerat că petenta avea obligaţia de a include motivele pe care îşi întemeiază cererea, precum şi dezvoltarea acestora, prin însăşi contestaţia formulată ori în mod separat, însă în cadrul termenului legal de formulare a acestora, respectiv 10 zile

de la data comunicării adresei atacate, cererea completatoare şi modificatoare depusă de petenta fiind astfel inadmisibilă”.

La aceeasi concluzie a ajuns şi Curtea de Apel Ploieşti care, prin Decizia nr. 493 din 17 martie 2010, a reţinut că:

„Din dispoziţiile legale menţionate mai sus rezultă că termenele de la art. 256[2] din ordonanţă trebuie respectate atât pentru formularea contestaţiei, cât şi pentru motivarea în fapt şi în drept a acesteia. Or, completarea motivelor iniţiale ale contestaţiei trebuie să se facă cu respectarea termenelor de la art. 256[2], nu după expirarea lor. În acest caz, Consiliul are posibilitatea să sancţioneze cu tardivitatea completările contestaţiei iniţiale care nu sunt de ordine publică şi au fost făcute peste termenele imperative prevăzute de lege”.

Cât priveşte procedura de a solicita accesul la dosarul achiziţiei publice, urmată de completarea contestaţiei în raport de informaţiile din respectivul dosar, trebuie avut în vedere că ordonanţa prevede calea de atac a contestaţiei pentru motive de nelegalitate şi netemeinicie care îi sunt cunoscute persoanei vătămate la momentul formulării ei, iar nu pentru motive necunoscute.

Contestaţia trebuie să cuprindă motivarea integrală a ei, în fapt şi în drept, sens în care dispune art. 270 alin. (1) lit. e) din ordonanţă. Singura ipoteză în care se admite completarea motivării este aceea de la art. 270 alin. (2) din ordonanţă.

Drept urmare, faţă de cele mai sus aratate, luând în considerare că prin contestaţia care face obiectul raportului juridic litigios, ... a procedat, practic la o completare a contestaţiei analizate în cadrul dosarului nr. 400/C4, intervenienta solicită respingerea contestaţiei ca fiind tardiv formulată.

De asemenea, intervenienta invocă exceptia lipsei de interes a ... în formularea de critici faţă de oferta declarată câştigătoare, menţionând în acest sens că dovedirea interesului legitim trebuie realizată prin intermediul contestaţiei supuse analizei, iar nu prin raportare la o altă cale de atac promovată în cadrul aceleiaşi proceduri de atribuire.

Pe de altă parte, în eventualitatea în care se va proceda la respingerea contestaţiei care face obiectul dosarului nr. 400/2015, va interesul ofertantului respins de a contesta ofertele admisibile nu îndeplineşte cerinţa de a fi născut şi actual.

Astfel, în măsura în care se va reţine legală respingerea ofertei ..., autoarea contestaţiei nu mai poate justifica un interes legitim, născut, actual şi direct pentru criticarea ofertei declarate câştigătoare pe calea contestaţiei ulterioare.

În cazul societăţii contestatoare, culpa pentru nedepunerea unei oferte în conformitate cu documentaţia de atribuire aparţine exclusiv acesteia, astfel că, din această perspectivă, este evident că nu poate pretinde un interes legitim pentru a critica oferta declarată câştigătoare.

Pe fondul cauzei, intervenienta solicită respingerea ca nefondată a contestaţiei reiterând în susţinerea solicitării sale cele menţionate în cadrul adreselor nr. 276/17.04.2015 şi nr. 307/23.04.2015.

Prin adresa nr. T/1271/30.04.2015, înregistrată sub nr. 7112/04.05.2015, ... formulează concluzii scrise prin care aduce o serie de precizări faţă de susţinerile prezentate în răspunsul formulat de ... la concluziile sale scrise înregistrate cu nr. T/1171/17.04.2015, cererea de intervenţie formulată de ... în calitate de lider al asocierii a cărei ofertă a fost declarată câştigătoare a procedurii de atribuire, în dosarul nr. 610/2015, punctul de vedere al autorităţii contractante, în care precizează că nu i se poate îngrădi dreptul de a critica acele aspecte de admisibilitate ale ofertei câştigătoare de care a luat cunoştinţă cu ocazia consultării dosarului achiziţiei.

În acest sens, contestatoarea invocă Decizia Consiliului nr. 2558/C8/2544/2582/18.07.2013 prin care Consiliul a respins excepţia tardivităţii ridicată de autoritatea contractantă într-o speţă similară, în care contestatoarea formulase prin contestaţie critici faţă de oferta declarată câştigătoare, iar apoi expusese motivarea în fapt şi în drept a respectivelor critici în cadrul concluziilor scrise, în urma consultării dosarului achiziţiei.

Astfel, identificând din studierea dosarului noi elemente de nelegalitate în legătură cu decizia autorităţii contractante privind declararea ofertei Asocierii ... ca fiind câştigătoare, prin concluziile scrise au fost aduse o serie de completări şi precizări sub aspectul motivelor ce stau la baza contestaţiei cu privire la modul de evaluare a ofertei Asocierii ....

Contestatoarea susţine că a înţeles să invoce în sprijinul criticilor sale privind modul de evaluare a ofertei Asocierii Siveco, în mod perfect legal, un act de care a luat la cunoştinţă abia cu ocazia consultării dosarului în urma depunerii contestaţiei iniţiale.

A susţine că ... putea să invoce toate motivele de nelegalitate legate de evaluarea ofertei Asocierii ... în termenul de 10 zile de la data la care a aflat că Asocierea a fost declarată câştigătoare, deşi înăuntrul acelui termen nu avea cunoştinţă de conţinutul documentelor relevante aflate la dosarul achiziţiei referitoare la modul de evaluare a ofertei respectivei Asocieri (Raportul procedurii, răspunsuri la clarificări), ar echivala cu negarea liberului acces al ... la justiţie. Aceasta deoarece nu există nicio altă cale legală de a ataca nelegalitatea actelor din cadrul procedurii de atribuire, cu excepţia celei prevăzute la art. 256^2 din OUG nr. 34/2006.

În considerarea celor de mai sus, termenul de precizare/completare a motivelor de contestare a deciziei de declarare drept câştigătoare a ofertei Asocierii ... sub aspectul neîndeplinirii cerinţei din fişa de date cu privire la atestarea situaţiei datoriilor la bugetul de stat/bugetele locale, al încălcării principiului tratamentului egal prevăzut la art. 2 alin. (2) lit. b) din OUG nr. 34/2006 şi al evaluării nelegale a ofertei financiare a Asocierii ... este, în opinia contestatoarei, de 10 zile de la data la care a luat cunoştinţă de conţinutul documentelor din dosarul achiziţiei care au relevat respectivele motive. Faptul că a înţeles să învedereze aceste motive pe calea concluziilor scrise nu îi ştirbeşte în niciun fel îndreptăţirea de a obţine anularea deciziei, atâta vreme cât termenul legal de 10 zile nu a fost depăşit.

Sub acest aspect, în jurisprudenţa Curţii de Apel Bucureşti s-au reţinut următoarele: *„Susţinerea petentei (...) că motivele de recurs dezvoltate de asocierea constatatoare prin notele scrise ar reprezenta, de fapt, o nouă contestaţie, formulată tardiv, este nefondată, întrucât momentul în raport cu care se stabileşte dacă aceste motive au fost depuse în termen este cel la care asocierea a avut acces la dosarul achiziţiei. Atunci a avut posibilitatea, în mod obiectiv şi legal, să ia cunoştinţă în mod real de alte motive de neconformitate a celorlalte oferte depuse în cadrul procedurii, suplimentare faţă de cele invocate în contestaţie. Or, faţă de momentul la care asocierii i-a fost permis accesul la dosarul achiziţiei, aceste motive au fost depuse în termen şi, în mod legal, au fost luate în considerare de către Consiliu la pronunţarea soluţiei" (Curtea de Apel Bucureşti, Decizia Civilă nr. 2103/21.05.2012).*

De asemenea, într-o altă speţă soluţionată de aceeaşi instanţă s-a reţinut că: *„Decizia Consiliului în sensul respingerii ca inadmisibile a motivelor suplimentare de contestaţie (...) este nelegală şi prin raportare la prevederile art. 21 din Constituţie, care garantează accesul liber la justiţie, dar şi la prevederile art. 6 parag. 1 din Convenţia europeană a drepturilor omului, din perspectiva dreptului de acces la instanţă, componentă esenţială a dreptului de la un proces echitabil garantat de Convenţie. Astfel, la data evenimentelor nu exista nicio altă cale procedurală efectivă care sâ permită contestatoarei invocarea aspectelor de neleaalitate si netemeinicie de care a luat cunoştinţă la momentul studierii dosarului achiziţiei publice, iar refuzul Consiliului de analiză a tuturor criticilor formulate a lipsit-o pe aceasta de orice posibilitate clară şi concretă de acces la instanţă, deşi procedura administrativ-jurisdicţională era în curs de desfăşurare, Consiliul având competenţa de a statua asupra tuturor aspectelor cu care a fost sesizat" (Curtea de Apel Bucureşti, Decizia civilă nr. 1780/19.09.2011).*

În ceea ce priveşte pretinsa tardivitate a celei de-a doua contestaţii formulate, contestatoarea susţine că a depus a doua contestaţie pentru a evita ca, în cazul în care completările la prima contestaţie cu critici ce vizează oferta Asocierii ... pe calea concluziilor scrise ar fi totuşi respinse ca tardiv formulate (ori ca inadmisibile), fiind astfel decăzută din dreptul de a supune controlului de legalitate modul în care a fost evaluată oferta Asocierii ....

În ceea ce priveşte excepţia lipsei de interes privind criticarea ofertei Asocierii ..., contestatoarea afirmă că acest interes se relevă nu numai prin prisma capătului de cerere din prima contestaţie privind modul de evaluare a ofertei ..., ci şi în mod autonom, independent de acest capăt.

Aceasta deoarece, chiar dacă, s-ar reţine neconformitatea ofertei depuse de ..., aceasta ar avea în continuare interes pentru a învesti CNSC cu o cerere având ca obiect critici privind inadmisibilitatea ofertei declarate câştigătoare, întrucât, dacă şi această ofertă va fi declarată drept inadmisibilă ori se va constata că procedura de atribuire este grav afectată, iar aceasta va fi anulată, contestatoarea susţine că va putea participa cu ofertă la noua procedură. Interesul unui ofertant a cărui ofertă a fost declarată neconformă în situaţii similare a fost reţinut şi în jurisprudenţa anterioară a instanţelor de judecată, sens în care invocă:

- Decizia civilă nr. 328 din 26 ianuarie 2012 a Curţii de Apel Bucureşti: „pe de altă parte, petenta, a cărei ofertă a fost respinsă de autoritate ca neconformă, a criticat oferta câştigătoare, susţinând că [...]. Curtea a analizat şi acest motiv al plângerii legat de conformitatea ofertei câştigătorului, întrucât petenta are un interes mediat, în contextul în care se constată că ambele oferte erau inacceptabile sau neconforme, autoritatea contractantă fiind obligata să anuleze procedura de atribuire, iar petenta ar avea posibilitatea în cazul în care se demarează o nouă procedură de licitaţie să participe cu o altă ofertă" (s.n.);

- Sentinţa civilă nr. 1529 din 30 aprilie 2013 a Curţii de Apel Bucureşti, potrivit căreia „în ceea ce priveşte excepţia lipsei de interes, instanţa observă că, deşi oferta petentei a fost calificată de autoritatea contractantă ca inacceptabilă (...), se apreciază de către instanţă că petenta are un interes mediat în soluţionarea cauzei, în contextul în care, dacă ar fi apreciate ca întemeiate argumentele prezentate în susţinerea acestui capăt de cerere, autoritatea contractantă ar fi obligată să anuleze procedura de atribuire, iar petenta ar avea posibilitatea. În cazul în care s-ar demara o nouă procedură de licitaţie, să participe cu o altă ofertă. În consecinţă, reţinând că petenta justifică un interes în soluţionarea cauzei, instanţa va respinge excepţia lipsei de interes ca neîntemeiată" (s.n.).

Contestatoarea susţine că este în mod evident vătămată prin actele autorităţii contractante de a respinge oferta ... şi de a declara în acelaşi drept câştigătoare o ofertă care prezintă elemente clare de inadmisibilitate, cu încălcarea principiului tratamentului egal.

În lumina celor de mai sus, contestatoarea afirmă că interesul său de a critica oferta Asocierii ... se relevă independent de criticile privind modul de evaluare a ofertei sale formulate prin prima contestaţie.

În ceea ce priveşte faptul că oferta Asocierii ... nu îndeplineşte cerinţa din fişa de date cu privire la atestarea situaţiei datoriilor la bugetul de stat/bugetele locale, aspect faţă de care ... susţine că autoritatea contractantă a solicitat certificate vizând punctele de lucru, iar nu sediile principale ale membrilor Asocierii ...., contestatoarea afirmă că acest argument nu are nicio relevanţă, faţă de împrejurarea că prin fişa de date a achiziţiei, pct. III.2.1.a) Situaţia personală a candidatului sau

ofertantului s-au cerut „certificatele de atestare fiscală emise de organul fiscal competent (...) care să ateste că ofertantul nu are datorii scadente la nivelul lunii anterioare celei în care este prevăzut termenul limită de depunere a ofertelor", fără a se face nicio distincţie cu privire la faptul că lipsa datoriilor trebuie să vizeze punctele de lucru sau sediile principale.

Alt argument adus de .... este că a depus în ofertă o declaraţie pe propria răspundere privind îndeplinirea criteriilor de calificare şi selecţie, în baza art. 11 alin. (4) şi (5) din HG nr. 925/2006, invocând art. 9 alin. (3) din Ordinul ANRMAP nr. 509/2011 privind formularea criteriilor de calificare şi selecţie, care în viziunea sa i-ar da dreptul să depună certificate emise ulterior datei de deschidere a ofertelor.

Faţă de acest argument, contestatoarea precizează că nu a negat dreptul Asocierii ... de a depune certificate de atestare fiscală emise ulterior datei de deschidere a ofertelor, cu condiţia ca acestea să confirme că operatorul economic nu avea datorii către bugetul de stat/bugetele locale scadente la nivelul lunii iulie 2014 (anterior lunii în care s-a împlinit termenul limită de depunere a ofertelor). A primi o interpretare contrară, chiar bazată pe invocarea dispoziţiilor unui ordin al ANRMAP, înseamnă a nesocoti principiile nediscriminării şi tratamentului egal între ofertanţi prevăzute de OUG nr. 34/2006. Astfel, chiar dacă membrii Asocierii ... au demonstrat că nu aveau obligaţii scadente la nivelul lunii august 2014, ei nu au demonstrat lipsa acestor datorii la 31.07.2014. Or, este perfect posibil ca datoriile să fi existat la 31.07.2014 şi să fi fost achitate ulterior acestei date de membrii Asocierii, până la data emiterii certificatelor, astfel că membrii Asocierii nu mai figurau cu datorii la nivelul lunii august.

Totuşi, a admite că asemenea certificate fac dovada îndeplinirii cerinţelor fişei de date echivalează cu a fi de acord că între un ofertant care îşi achitase toate datoriile către bugetele publice până la data cerută prin documentaţia de atribuire şi unul care şi-a achitat aceste datorii ulterior se poate pune semnul egalităţii, ceea ce evident nu poate fi primit. Ofertantul care şi-a plătit datoriile cu întârziere are în mod evident un avantaj, deoarece s-a folosit mai mult timp de respectivele sume, în dauna bugetelor publice.Cum certificatul de testare fiscală se emite în 5 zile lucrătoare, având în vedere că data limită de depunere a ofertelor a fost 13.08.2014, emiterea acestuia pentru data de 31.07.2014 putea fi solicitată după primele 5 zile lucrătoare ale lunii iulie, astfel încât certificatul să fie obţinut în timp util pentru a fi depus în cadrul ofertei.

Contestatoarea invocă în susţinerea afirmaţiilor sale, Decizia BO2014_0753: *„Consiliul analizând înscrisurile depuse în ofertei, prin proprio voinţă, de către ... constată că operatorul economic contestator, la data depunerii/deschiderii ofertelor nu a îndeplinit condiţiile cumulative impuse de către autoritatea contractantă şi acceptate de către contestator prin necontestarea lor în termenul legal, în speţă nu a făcut dovada că nu figurează în evidenţele fiscale cu obligaţii de plată exigibile la data de 31.01.2014.*

Din cele de mai sus rezultă că acest contestator nu a îndeplinit această cerinţă de calificare.

Având în vedere că invitaţia de participare a fost publicată în data de 06.02.2014, iar data limită de depunere a ofertelor a fost 21.02.2014, ... putea si avea timp suficient ca să solicite la autorităţile legale competente un alt certificat de atestare fiscala prin care să se ateste că nu are obligaţii de plată a impozitelor şi taxelor către bugetul general consolidat,la data de 31.01.2014, întrucât conform prevederilor art. 112 alin. (4) din OUG nr. 92/2003 Codul de procedură fiscală, actualizat, «certificatul de atestare fiscală se emite în termen de 5 zile lucrătoare de la data depunerii cererii» şi «la solicitarea contribuabililor»" (s.n.).

În ceea ce priveşte faptul că respingerea ofertei Asocierii ... se impune şi în virtutea art. 201 alin. (2) şi a principiului tratamentului egal prevăzut la art. 201 alin. (2) şi a principiului tratamentului egal, contestatoarea susţine că autoritatea contractantă a aplicat reguli discreţionare în privinţa evaluării ofertei Asocierii ..., iar un exemplu extrem de uşor de înţeles este modul în care autoritatea a apreciat îndeplinirea cerinţei de la cap. 3.3.7 din caietul de sarcini, respectiv: „Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigura) trebuie sa fie certificată din punct de vedere al securitatii informatice de către un organism abilitat la nivel naţional, european sau internaţional".

Conform prezentării Asocierii ... susţinute cu ocazia sesiunii demonstrative, soluţia din oferta Asocierii ce răspunde acestor cerinţe este suita de aplicaţii shellSafe. Asocierea ... a prezentat certificarea exclusiv pentru soluţia shellSafe, nu şi pentru componentele acesteia care implementează pe staţiile de lucru funcţionalităţile cerute, şi anume componentele clickSIGN şi sendSAFE.

Astfel, a susţine, aşa cum o face ... că toate componentele suitei au fost „implicit" certificate *(certificarea din punct de vedere al securităţii a fost realizată pentru întreaga suită shellSAFE,* implicit pentru toate componentele sale: *clickSIGN, sendSAFE, diskSAFE şi shredSAFE")* echivaiează cu a pretinde legitimarea tratamentului discriminatoriu aplicat de autoritate, care a favorizat vădit Asocierea ... în detrimentul ....

De asemenea, contestatoarea arată că suita shellSAFE beneficiază de certificare din punct de vedere al securităţii numai în mod condiţionat, şi anume sub rezerva îndeplinirii anumitor condiţii foarte stricte, proprii sistemului de protecţie a informaţiilor clasificate naţionale. NATO sau UE, aşa cum rezultă şi din Catalogul naţional cu pachete, produse şi profile de protecţie INFOSEC menţionat de ...

Aceste condiţii se referă la modul/condiţiile de utilizare, la dispozitivele împreună cu care se utilizează această suită, la algoritmii de criptare folosiţi, la certificatele digitale utilizate, etc. Or. aceste condiţii extrem de stricte nu vor fi şi nici nu se cere a fi asigurate (pentru că nu sunt necesare nivelului de securitate aplicabil) în cadrul sistemului ofertat către autoritatea contractantă în cadrul prezentei proceduri, de unde rezultă că în fapt certificarea aferentă soluţiei ofertate nici măcar nu este valabilă în contextul sistemului ce face obiectul procedurii.

Faptul că certificarea proprie sistemului de protecţie a informaţiilor clasificate naţionale, NATO sau UE nu este necesară, fiind o cerinţă excesivă, care excede nevoilor autorităţii, a fost stabilit deja de Consiliu printr-o decizie pronunţată anterior, în urma căreia autoritatea contractantă a emis Modificarea nr. 1 referitoare la procedura de atribuire, prin care s-au stabilit între altele următoarele:

«În cadrul caietului de sarcini publicat în SEAP, cerinţele se vor modifica astfel: 1. La Capitolul 3.3.7. Modulul 7: Componenta de Securizare Acces şi Documente Sistem centralizat pentru autentificarea la aplicaţii - 3.3.7.4. Aplicaţie de securitate pentru statiile de lucru paragraful „Pentru toate aplicaţiile de securitate pentru statiile de lucru se va avea in vedere certificarea naţionala ca produse de securitate la nivel minim Secret de Serviciu de către ORNISS”. Dacă produsul nu este certificat, este obligatoriu ca Ofertantul sa se oblige prin contract sa deruleze procedurile aferente certificării, pana la testarea de acceptanta provizorie si sa puna la dispoziţie documentaţie, scheme, diagrame, cod sursa sau orice alte documente necesare. Obligaţiile de ordin financiar, tehnic si procedural aferente certificării revin in exclusivitate Ofertantului si trebuie sa fie in conformitate cu legislaţia aplicabila in Romania" se va elimina».

Prin adresa nr. 353/06.05.2015, înregistrată la Consiliu sub nr. 7496/07.05.2015, ... formulează răspuns la concluziile scrise înregistrate sub nr. T/1271/30.04.2015 în care învederează că jurisprudenţa în materie nu este unitară, existând decizii contradictorii în acest sens, însă trebuie avut în vedere, pe lângă jurisprudenţa majoritară în domeniu (care este în sensul inadmisibilităţii completării contestaţiei ulterior termenelor legale reglementate la art. 256^2 din OUG nr. 34/2006, cu modificarile si completarile ulterioare), inclusiv jurisprudenţa Curţii de Justiţie a Uniunii Europene, care adoptă aceeaşi poziţie.

Astfel, decăderea din dreptul de a depune completări de acţiune în afara termenului de contestare a fost statuat chiar de CJUE în Hotărârea din 11 octombrie 2007 pronunţată în cauza C-241/06, având ca obiect o cerere de pronunţare a unei hotărâri preliminare formulată în temeiul articolului 234 CE de Hanseatisches Oberlandesgericht in Bremen (Germania) - Lämmerzahl GmbH impotriva Freie Hansestadt Bremen, în cuprinsul acesteia fiind reţinute următoarele:

„45 Prin intermediul primei intrebari formulate, instanta nationala urmareste sa rezolve, in esenta, doua probleme. Pe de o parte, aceasta intreaba in ce conditii dreptul comunitar permite ca dreptul national sa supuna unui termen de decadere caile de atac care privesc alegerea procedurii de atribuire a unui contract de achizitii publice, estimarea valorii contractului sau actele care intervin in primele faze ale unei proceduri de atribuire. Pe de alta parte, in ipoteza in care o astfel de norma de decadere poate fi admisa, aceasta instanta se intreaba daca dreptul comunitar permite ca aceasta sa fie extinsa in mod general asupra cailor de atac privind deciziile autoritatii contractante, inclusiv cele intervenite in cursul fazelor ulterioare ale procedurii de atribuire.

(…)

Aprecierea Curtii

50 În ceea ce priveste prima parte a acestei întrebări, trebuie amintit faptul că Directiva 89/665 nu se opune unei reglementări naţionale care prevede că orice cale de atac împotriva unei decizii a autorităţii contractante trebuie formulată într-un termen prevăzut în acest scop şi că orice neregularitate a procedurii de atribuire invocată în sprijinul acestei căi de atac trebuie invocată în acelasi termen, sub sancţiunea decăderii, astfel încât, după împlinirea acestui termen, nu mai este posibil să se conteste o astfel de decizie sau să se invoce o astfel de neregularitate, în măsura în care termenul respectiv este rezonabil (Hotărârea din 12 decembrie 2002, Universale Bau şi alţii, C-470/99, Rec., p. I-11617, punctul 79, şi Hotararea din 27 februarie 2003, Santex, C- 327/00, Rec., p. I 1877, punctul 50)".

Practic, nu poate fi admisibil şi nici permis ca o contestaţie să fie depusă la Consiliu doar pentru a avea acces autoarea ei la documentele ofertelor celorlalţi şi a le studia în vederea descoperirii motivelor care ar putea să îi susţină contestaţia depusă. Un asemenea comportament din partea operatorilor economici ar fi atât contrar legii, cât şi abuziv, trebuind a fi sancţionat ca atare.

Argumentele de mai sus urmează a fi avute în vedere şi cu privire la tardivitatea celei de-a doua contestaţii formulate de ... prin care sunt contestate aceleaşi acte ale autorităţii contractante, demersul contestatoarei reprezentând, în fapt, o completare a contestaţiei depuse iniţial, fără a putea fi privită ca o contestaţie distinctă, decât în situaţia în care avea ca obiect anularea unor alte acte considerate vătămătoare emise de autoritatea contractantă.

Cât priveşte interesul ... de a critica oferta declarată câştigătoare în condiţiile în care nu face dovada admisibilităţii ofertei sale, nu se poate trece cu vedere modalitatea în care contestatoarea încearcă să îşi suplimenteze şi adaptaze apărările în funcţie de poziţia părţilor adverse, în acelaşi sens procedând şi prin răspunsurile la solicitările de clarificări.

În ceea ce priveşte susţinerile contestatoarei referitoare la îndeplinirea de către ... a cerinţei din fişa de date a achizitiei privitoare la atestarea situaţiei datoriilor la bugetul de stat/bugetele locale, intervenienta afirmă că prin concluziile scrise, ... denaturează scopul cerinţelor minime de calificare pe care le pot solicita autorităţile contractante în cadrul procedurilor de atribuire a contractelor de achiziţie publică, scop care, potrivit art. 7 din HG nr. 925/2006, cu modificarile si completarile ulterioare, constă în „(…) demonstrarea potenţialului tehnic, financiar şi organizatoric al fiecărui operator economic participant la procedură, potenţial care trebuie să reflecte posibilitatea concretă a acestuia de a îndeplini contractul şi de a rezolva eventualele dificultăţi legate de îndeplinirea acestuia, în cazul în care oferta sa va fi declarată câştigătoare".

Or, în cazul datoriilor la bugetul de stat/bugetele locale, este fără tăgadă că un ofertant care poate face dovada situaţiei financiare la o dată cât mai apropiată de cea a semnării contractului, este mult mai fiabil din punct de vedere al posibilităţii concrete de a îndeplini contractul şi de a

rezolva eventualele dificultăţi legate de îndeplinirea acestuia, în cazul în care oferta sa va fi declarată câştigătoare, acesta fiind şi argumentul pentru care ANRMAP, în cuprinsul Ordinului nr. 509/2011 a reţinut că autoritatea contractantă va lua în considerare, la verificarea îndeplinirii cerinţei de calificare privind plata de către ofertant a impozitelor, taxelor şi contribuţiilor de asigurări sociale inclusiv acele certificate de atestare fiscală prezentate de ofertant în urma solicitării primite din partea autorităţii contractante, chiar dacă acestea sunt emise de autorităţile competente ulterior datei de deschidere a ofertelor şi, eventual, atestă lipsa datoriilor ulterior respectivei date.

De asemenea, intervenienta arată că în cazul în care cerinţa din fişa de date ar fi fost în sensul interpretat de către contestatoare, respectiv acela potrivit căruia ofertanţii aveau obligaţia de a depune certificatele fiscale inclusiv pentru punctele de lucru pe care acesţia le-ar deţine, aceasta precizare ar fi trebuit să fie explicit evidenţiată în conţinutul fişei de date.

Cu privire la eventuala încălcare a principiului tratamentului egal de către autoritatea contractantă, în primul rând trebuie reţinut că există dreptul, iar nu obligaţia de a fi solicitate ofertanţilor clarificări şi completările formale sau de confirmare, necesare pentru evaluarea fiecărei oferte, aspect pentru care, dacă autoritatea contractantă a solicitat ... mai puţine clarificări nu poate fi interpretat decât în sensul că propunerea sa tehnică a răspuns necesităţilor acesteia.

În al doilea rând, în opinia intervenientei sunt nefondate afirmaţiile potrivit cărora „autoritatea contractantă a aplicat reguli discreţionare în privinţa evaluării ofertei Asocierii ...”, pentru simplul considerent că soluţia propusă pentru implementarea functionalităţii privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura) este certificată conform cerinţelor din caietul de sarcini.

Totodată, intervenienta afirmă că autoritatea contractantă nu a contestat niciuna dintre certificarile de securitate prezentate de cei doi ofertanţi, dar a identificat neconformităţi în oferta ... şi în răspunsurile la întrebările de clarificare cu privire la îndeplinirea cerinţei, deoarece:

- Soluţia „certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional” este SafeLayer PKI platform. Această soluţie nu oferă functionalităţi, aşa cum reiese de pe site-ul producătorului, cu privire la ”utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura)”.

- Produsele descrise în secţiunea în care se arată îndeplinirea cerinţelor privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura), respectiv capitolul 3.3.7.3.2. Semnătura electronică şi secţiunea Asigurarea confidenţialităţii documentelor sunt DigiSigner şi BitLocker, care nu fac parte din portofoliul de produse SafeLayer. Pentru aceste produse nu se demonstrează faptul că deţin o certificare de securitate sau că, împreună cu produsele SafeLayer formează un ansamblu care să respecte cerinţele de certificare.

Asocierea ... nu trebuia să prezinte certificări individuale pentru produsele care compun suita shellSAFE deoarece:

- shellSAFE nu este un produs în sine, ci o suită de aplicaţii (clickSIGN, sendSAFE, diskSAFE si shredSAFE) realizate de acelaşi producător, UTI. Dacă aceste aplicaţii nu ar fi certificate este evident că nu s-ar putea afirma că suita shellSAFE este certificată din punct de vedere al securităţii. Atunci când un client achiziţionează shellSAFE acesta primeşte o licenţă şi un kit de instalare care, după ce este rulat, instalează pe staţia de lucru a clientului produsele clickSIGN, sendSAFE, diskSAFE şi shredSAFE.
- În oferta tehnică, atunci când a precizat îndeplinirea cerinţei de una dintre aplicaţiile shellSAFE (clickSIGN, sendSAFE, diskSAFE şi shredSAFE), s-a specificat că aceste aplicaţii fac parte din suita shellSAFE
- Din manualele transmise împreună cu oferta tehnică şi de pe site-ul NATO indicat, de asemenea, în ofertă, reiese că suita shellSAFE este compusă din produsele certificate clickSIGN, sendSAFE, diskSAFE şi shredSAFE.
- ORNISS, ca organism de certificare, nu a considerat necesară nominalizarea componentelor shellSAFE decât atunci când, pentru una dintre acestea, se aplicau condiţii diferite faţă de celelalte componente, aşa cum este cazul shredSAFE: „Funcţiile oferite de modulul ShredSAFE nu asigură declasificarea mediilor de stocare clasificate SECRET”.

... a prezentat, de asemenea, pentru îndeplinirea cerinţei o familie de produse, folosind sintagma „Soluţia SafeLayer PKI platform” care, aşa cum este prezentat pe site-ul SafeLayer este compusă din KeyOne Certification Authority, KeyOne Registration Authority, KeyOne Validation Authority şi KeyOne Time-Stamping Authority (http://www.safelayer.com/en/products/keyone-pki-platform).

Niciunul dintre produsele SafeLayer nu îndeplinesc cerinţele privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, stergere sigura), pentru îndeplinirea acestor cerinţe fiind indicate de ... produsele DigiSigner şi Bitlocker, realizate de alţi producători decât SafeLayer şi pentru care nu se prezintă o certificare de securitate.

Având în vedere cele precizate anterior, intervenienta consideră că autoritatea contractantă a procedat în mod corect atunci când a solicitat clarificări pentru lămurirea acestei situaţii, procedând la respingerea ofertei ... nu deoarece componentele individuale ale Soluţiei SafeLayer PKI platform nu deţineau o certificare individuală de securitate ci, pentru că:

- Produsele care implementau cerinţele privind utilizarea certificatelor digitale pe staţiile de lucru aşa cum reiese din dosarul achiziţiei studiat (semnare, criptare/decriptare, stergere sigura), sunt DigiSigner şi BitLocker
- DigiSigner şi BitLocker nu fac parte din Soluţia SafeLayer PKI platform, fiind realizate de alţi producători, DigiSign respectiv Microsoft.

- Pentru DigiSigner şi BitLocker nu se demonstrează faptul că deţin o certificare de securitate.

Cu privire la certificarea shellSAFE, intervenienta afirmă că:

- La nivel naţional, suita este acreditată să protejeze informaţii naţionale clasificate. Pentru aceste informaţii sunt necesare anumite precauţii suplimentare, descrise în mod explicit de către ORNISS. Aceleaşi aplicaţii care protejează informaţiile clasificate pot fi utilizate pentru a proteja şi alte informaţii sensibile dar neclasificate. Nivelul de securitate al aplicaţiior sau taria algoritmilor criptografici nu sunt mai slabe şi, aşa cum se poate observa şi din informaţiile prezentate de ORNISS, cele mai multe precauţii trebuie avute în vedere pentru protecţia cheilor criptografice ale utilizatorilor, chei folosite de aplicaţie pentru protecţia informaţiilor (folosirea de smart card certificat FIPS 140-2 nivel 2, emiterea certificatelor digitale de infrastructuri de chei publice autorizate, cu nivel de clasificare similar). ORNISS indică faptul că suita shellSAFE este certificată din punct de vedere al securităţii iar pentru protecţia informaţiilor clasificate enumeră care sunt măsurile de securitatate suplimentare care trebuie implementate.

- Suita shellSAFE îndeplineşte astfel, fără nici un fel de echivoc, cerinţa menţionată în cadrul dosarului achiziţiei şi anume „Soluţia […] certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional”.

Din examinarea materialului probator administrat, aflat la dosarul cauzei, Consiliul reţine următoarele:

..., în calitate de autoritate contractantă, a iniţiat procedura de licitaţie deschisă în vederea atribuirii contractului de servicii având ca obiect „Servicii de arhivare fizică şi servicii de arhivare electronică a documentelor elaborate/gestionate în cadrul ...”, prin publicarea în sistemul electronic de achiziţii publice (SEAP) a anunţului de participare nr. ... din 02.02.2014. Potrivit acestuia, criteriul de atribuire aplicat a fost „oferta cea mai avantajoasă din punct de vedere economic”, valoarea estimată a contractului fiind de 28.830.000 lei, fără TVA.

De la iniţierea procedurii şi până în prezent, s-au aflat pe rolul Consiliului 10 contestaţii, care au fost soluţionate prin deciziile nr. .../.../.., .., .., .., .., ../..., nr. ../../.../ ..., nr. ../../.../... şi nr. .../../.../ ....

Potrivit deciziei nr. .../.../.../..., Consiliul a dispus următoarele: ,,Cu privire la solicitarea petentei de obligare a autorităţii contractante la anularea adreselor nr. MFE/DAPITA. 2486/02.02.2015, nr. MFE/DAPITA 2753/04.02.2015 şi nr. MFE/DAPITA 3203/10.02.2015, prin care comisia de evaluare, invocând modificarea componenţei comisiei de evaluare şi sub motivarea că *„toţi membri cu drept de vot ai comisiei să poată participa la toate etapele necesare evaluării ofertelor*”, a dispus contestatoarei prezentarea, *„încă o dată*”, a sesiunii demonstrative, în cadrul căreia să fie prezentate funcţionalităţile minime cerute în cadrul Modului 7 din caietul de sarcini şi la care să se asigure participarea, din partea ofertantului, a unor persoane competente care să răspundă la eventualele întrebări tehnice, petenta urmând să asigure şi echipamentele necesare prezentării funcţionalităţilor Modului 7, dar şi predarea unei copii a prezentării ce urmează a fi susţinută, Consiliul are în vedere următoarele aspecte:

- în procesul verbal nr. MFE/DAPITA 4198 din 13.11.2014, încheiat cu ocazia prezentării, de către ... a sesiunii demonstrative a funcţionalităţilor aferente Modulului 7 din caietul de sarcini (…), se regăseşte menţiunea: *„Au fost prezentate **toate sesiunile demonstrative solicitate** pentru demonstrarea **funcţionalităţilor referitoare la utilizarea certificatelor digitale din cadrul Modulului 7** aferente cerinţelor minime solicitate prin documentaţia de atribuire*", precum şi faptul că, din partea ofertantului au participat un număr de 17 specialişti;

- în acelaşi act sunt consemnate un număr de 8 întrebări adresate ofertantului şi răspunsurile afirmative ale acestuia, de maniera: *„Da, toate versiunile sunt actuale (...); Da, include utilizarea (...); Da, s-a făcu demonstraţie (...)*" etc.;

- în procesul verbal este consemnată participarea la demonstraţie, pe lângă membri comisiei de evaluare şi a reprezentanţilor UCVAP, a expertului IT cooptat – Răzvan Pop, persoană care a întocmit şi semnat caietul de sarcini, la finalul căruia se regăseşte menţiunea: "***Întocmit: ...**, Expert IT independent, **angajat conform contract nr. 6126/144/29.11.2013** cu titlul „Sprijin pentru Ministerul Fondurilor Europene în realizarea functiilor de coordonare a instrumentelor structurale si de gestionare a Programului Operational Asistentă Tehnică"*;

- în actul evocat nu s-au reţinut probleme necesar a fi clarificate în urma prezentării sesiunii demonstrative.

Consiliul mai reţine că, nici în anunţul de participare şi nici în fişa de date, nu s-a prevăzut obligativitatea ofertanţilor de a prezenta sesiuni demonstrative pe timpul evaluării ofertelor.

Singurul document care conţine referiri la sesiunea demonstrativă este caietul de sarcini, pct. 3.3.7 – ***„Modulul 7: Componenta de Securizare Acces si Documente"***:

- subpct. 3.3.7.1. Sistem centralizat pentru autentificarea la aplicatii - *„Se va urmari ca solutia pentru dispozitive mobile sa fie una matura si in acest sens **se vor prezenta manuale de utilizare si capturi de ecran care sa demonstreze cerintele mai sus mentionate**. De asemenea, **se va organiza si o sesiune demonstrativa in care se vor prezenta functionalitatile mai sus mentionate***";

- ***subpct. 3.3.7.2. Serviciul de verificare a validitatii certificatelor digitale –*** *"Ofertantul trebuie sa demonstreze implementarea tuturor componentelor intr-un sistem informatic implementat la cel putin un client si pentru un numar de minim 300 de utilizatori.*

*Se va urmari ca solutia sa fie una matura si in acest sens **se vor prezenta manuale de utilizare si capturi de ecran care sa demonstreze cerintele mai sus mentionate**. De asemenea, **se va organiza si o sesiune demonstrativa in care se vor prezenta functionalitatile mai sus mentionate***";

- subpct. 3.3.7.3. ***Aplicatie pentru validarea automata a documentelor semnate electronic –*** "*Ofertantul trebuie sa demonstreze implementarea tuturor componentelor intr-un sistem informatic implementat la cel putin un client si pentru un numar de minim 300 de utilizatori.*

*Se va urmari ca solutia sa fie una matura si in acest sens **se vor prezenta manuale de utilizare si capturi de ecran care sa demonstreze cerintele mai sus mentionate**. De asemenea, **se va organiza si o sesiune demonstrativa in care se vor prezenta functionalitatile mai sus mentionate***".

Prin pct. IV.4.1) "*Modul de prezentare a propunerii tehnice*" al fişei de date au fost menţionate următoarele instrucţiuni: "*In cadrul Ofertei Tehnice **se va detalia de catre Prestator conformitatea solutiei ofertate cu toate cerintele specificate in Documentatia de Atribuire**.*

***Furnizorul** trebuie sa raspunda punctual la toate cerintele cuprinse in Documentatia de Atribuire si **sa detalieze in propunerea sa tehnica modurile si mijloacele prin care solutia ofertata indeplineste aceste cerinte**, astfel incat comisia de evaluare sa aiba posibilitatea evaluarii acesteia in mod cat mai informat. In cazul in care oferta nu ofera informatii complete prin detalierea raspunsului la cerinte sau nu indeplineste cerintele exprimate in Documentatia de Atribuire, comisia de evaluare poate sa declare oferta ca fiind inacceptabila/neconforma.*

Nu vor fi luate in considerare componente ale ofertei tehnice cum ar fi: pliante, diverse materiale promotionale ale firmelor producatoare sau furnizoare de servicii, prezentari, brosuri, etc. care nu au legatura directa cu obiectul, structura si cerintele din prezenta Documentatie de Atribuire.

(...)

Ofertantul trebuie sa justifice acoperirea cerintelor prin prezentarea de: capturi de ecrane si descriere functionala explicita pe fluxuri de lucru".

Faţă de precizările pct. 1.3. din caietul de sarcini intitulat *„**VOLUMUL DE SERVICII SI PRODUSE PENTRU CARE SE OFERTEAZĂ**”*, se reţine că obiectul contractului constituit de ***„Achiziţionarea de servicii de arhivare fizică şi servicii de arhivare electronică aferente documentelor elaborate/ gestionate în cadrul Ministerului Fondurilor Europene”*** include o ***parte de servicii***, constituită de:

Modulul 1 – Servicii de prelucrare fond arhivistic;

Modulul 2 – Serviciu de inventariere a documentelor;

Modulul 3 – Serviciu de digitizare a documentelor;

Modulul 4 – Suport tehnic pentru elaborarea Nomenclatorului arhivistic,

precum şi o componentă de ***furnizare de software***, livrabile constiuite de soluţia informatică conţinând:

Modulul 5 – Portal;

Modulul 6 – Sistemul Informatic de Management al Documentelor;

Modulul 7 – Componenta de Securizare Acces si Documente;

Modulul 8 – Modulul de arhivare a documentelor.

Pentru toate modulele de livrabile/soft au fost solicitate, inclusiv, licentele aferente, urmând ca, pe platforma informatică constituită de livrabilele antemenţionate, să fie prestate serviciile de arhivare electronică.

Prin urmare, sesiunea demonstrativă solicitată de autoritatea contractantă este de natura ***mostrelor*** reglementate de art. 188 alin. (1) lit. e) din OUG nr. 34/2006 potrivit cărora *„În cazul aplicării unei proceduri pentru atribuirea unui contract de furnizare, în scopul verificării capacităţii tehnice şi/sau profesionale a ofertanţilor/candidaţilor, autoritatea contractantă are dreptul de a le solicita acestora, în funcţie de specificul, de cantitatea şi de complexitatea produselor ce urmează să fie furnizate şi numai în măsura în care aceste informaţii sunt relevante pentru îndeplinirea contractului, următoarele: (…)* ***e)*** *mostre, descrieri şi/sau fotografii a căror autenticitate trebuie să poată fi demonstrată în cazul în care autoritatea contractantă solicită acest lucru*", mostra (sesiunea demonstrativă) îndeplinind astfel un dublu rol, respectiv: de criteriu de calificare privind *capacitatea tehnică şi/sau profesională a ofertanţilor*, concomitent cu rolul de confirmare a conformităţii funcţionalităţii soluţiei informatice de arhivare electronică a documentelor cu specificaţiile tehnice impuse prin caietul de sarcini pentru modulul nr. 7.

În raport de dispoziţiile art. 33 alin. (3) din OUG nr. 34/2006 conform cărora *„**Cerinţele/Criteriile de calificare** şi/sau selecţie, **care se regăsesc în caietul de sarcini** ori documentaţia descriptivă **şi care nu sunt preluate în fişa de date/invitaţia de participare/anunţul de participare**, sunt considerate **clauze nescrise***" şi ţinând cont de faptul că cerinţa minimă de calificare de prezentare a mostrei/demo-ului vizând funcţionalitatea ***„Modulului 7: Componenta de Securizare Acces si Documente”*** NU a fost preluată în fişa de date şi anunţul de participare, se constată că respectiva cerinţă ***este clauză nescrisă*** care, în sensul interpretat de CSM prin Hotărârea nr. 638 din 2 aprilie 2009, dar şi cel reglementat de art. 1402 din C.civ. – *„**Condiţia** imposibilă, **contrară legii** sau bunelor moravuri **este considerată nescrisă** (…)*", este o clauză/cerinţă/convenţie contrară dispoziţiei legale (art. 33 alin. (3) din ordonanţă), care nu produce niciun efect, nefiindu-i astfel opozabilă societăţii contestatoare împotriva voinţei acesteia.

Reţinând că autoritatea contractantă se află în proces de evaluare a ofertelor, Consiliul determină că stabilirea, de către comisia de evaluare, a conformităţii ofertelor se poate face respectarea dispoziţiilor art. 1255 alin. (2) din C.civ – *„(...) clauzele nule sunt înlocuite de drept cu dispoziţiile legale aplicabile*", prin aplicarea întocmai a regulii instituite prin pct. IV.4.1) "Modul de prezentare a propunerii tehnice" al fişei de date

conform cărora "*Ofertantul trebuie sa justifice acoperirea cerintelor prin prezentarea de: capturi de ecrane si descriere functionala explicita pe fluxuri de lucru*".

Mai mult, pe lângă faptul că cerinţa de prezentare a sesiunii demonstrative este o clauză nescrisă prin impunerea acesteia doar prin caietul de sarcini, fără a fi fost preluată în fişa de date şi anunţul de participare, justificarea sub care autoritatea contractantă a solicitat prezentarea, *„încă o dată*", a sesiunii demonstrative, motivată doar prin înlocuirea unuia dintre membrii comisiei de evaluare şi că astfel *„toţi membri cu drept de vot ai comisiei să poată participa la toate etapele necesare evaluării ofertelor*", este contrară dispoziţiilor art. 72 alin. (4) teza a II-a din HG nr. 925/2006 – "*După producerea înlocuirii, **calitatea de membru al comisiei de evaluare este preluată** de către membrul de rezervă, **care îşi va exercita atribuţiile aferente până la finalizarea procedurii de atribuire***", text legal care nu dispune în sensul susţinut de autoritatea contractantantă, cum că, la înlocuirea unui membru al comisiei de evaluare, s-ar impune reluarea întregii activităţi de evaluare a ofertelor (toate etapele de evaluare).

Un considerent de ordinul celui invocat de autoritatea contractantă este contrar şui normelor art. 76 alin. (1) din HG nr. 925/2006 conform cărora: "*Modul de lucru al comisiei de evaluare este stabilit de comun acord între membrii acesteia, **urmând a se avea în vedere calendarul estimativ de aplicare a procedurii** şi perioada solicitată pentru valabilitatea ofertelor*", calendar care oricum este în mod vizibil eludat, devreme ce, în urma prezentării, de către S.C. STAR STORAGE S.A., a sesiunii demonstrative din data de 13.11.2014, autoritatea contractantă revine cu o solicitare de repetare a acesteia în data de 02.02.2015, la distanţă de aprox. 80 de zile, fiind încălcate astfel dispoziţiile art. 200 din OUG nr. 34/2006 – "***În termen de 25 de zile de la data deschiderii ofertelor**, autoritatea contractantă stabileşte oferta câştigătoare, pe baza criteriului de atribuire precizat în invitaţia de participare/anunţul de participare şi în documentaţia de atribuire, dacă oferta respectivă îndeplineşte toate condiţiile de admisibilitate care rezultă din documentaţia de atribuire şi actele anexate. **În cazuri temeinic motivate, autoritatea contractantă poate prelungi <u>o singură dată perioada de evaluare</u>**, cu excepţia situaţiilor în care autoritatea contractantă reevaluează ofertele ca urmare a unei decizii a Consiliului, a unei hotărâri judecătoreşti sau a recomandărilor observatorilor Unităţii pentru Coordonarea şi Verificarea Achiziţiilor Publice*".

Întrucât expertul tehnic cooptat – «***...**, Expert IT independent, **angajat conform contract nr. 6126/144/29.11.2013** cu titlul „Sprijin pentru Ministerul Fondurilor Europene în realizarea functiilor de coordonare a instrumentelor structurale si de gestionare a Programului Operational Asistentă Tehnică"*» a rămas în aceeaşi calitate pe toată durata procedurii, solicitarea autorităţii contractante este nejustificată şi în raport de dispoziţiile art. 73 alin. (5)-(6) din HG nr. 925/2006 – *„(5) Experţii cooptaţi nu au drept de vot, însă **au obligaţia de a elabora un raport de specialitate cu privire la aspectele tehnice**, financiare sau juridice asupra cărora, pe baza expertizei pe care o deţin, îşi exprimă punctul de vedere. (6) **Raportul de specialitate prevăzut la alin. (5) este destinat să faciliteze comisiei de evaluare adoptarea deciziilor în cadrul procesului de analiză a ofertelor** şi de stabilire a ofertei/ofertelor câştigătoare. Raportul de specialitate se ataşează la raportul de atribuire şi devine parte a dosarului achiziţiei publice*", la dosarul cauzei neregăsindu-se vreun raport de specialitate din care să rezulte aspecte vădit neclare, care să revendice întemeiat solicitarea autorităţii contractante de reluare a sesiunii demonstrative.

Luând act de faptul că cerinţa de prezentare a sesiunii demonstrative este:

- clauză nescrisă în înţelesul dispoziţiilor art. 33 alin. (3) din OUG nr. 34/2006;

- excesivă faţă de regula instituită prin pct. IV.4.1) "Modul de prezentare a propunerii tehnice" al fişei de date conform cărora "*Ofertantul trebuie sa justifice acoperirea cerintelor prin prezentarea de: capturi de ecrane si descriere functionala explicita pe fluxuri de lucru*";

- solicitarea autorităţii contractante de repetare a respectivei sesiuni motivată doar prin invocarea faptului că, în cazul înlocuirii unui membru al comisiei de evaluare,

„toţi membri cu drept de vot ai comisiei să poată participa la toate etapele necesare evaluării ofertelor", considerent contrar dispoziţiilor art. 72 alin. (4) teza a II-a din HG nr. 925/2006;

- expertul tehnic cooptat participant la sesiunea demonstrativă a rămas neschimbat, precum şi faptul că, la dosar nu se regăseşte niciun act de natura "***raportului de specialitate cu privire la aspectele tehnice***", prin care să se revendice vreo eventuală necesitate de reluare a sesiunii demonstrative,

Consiliul constată că cererea petentei de anulare a adreselor autorităţii contractante nr. MFE/DAPITA. 2486/02.02.2015, nr. MFE/DAPITA 2753/04.02.2015 şi nr. MFE/DAPITA 3203/10.02.2015, precum şi a actelor subsecvente acestora este întemeiată.

Prin urmare, în eventualitatea în care comisia de evaluare nu este pe deplin edificată asupra conformităţii ofertelor cu cerinţele şi specificaţiile caietului de sarcini, aceasta are la dispoziţie procedura reglementată de art. 78 din HG nr. 925/2006, respectiv de stabilire a clarificărilor şi completărilor formale sau de confirmare necesare pentru evaluarea fiecărei oferte, pe care le va formula clar, precis si prin care se va defini în mod explicit şi suficient de detaliat în ce constau solicitarile comisiei de evaluare, în strictă corelare cu conţinutul precizărilor şi regulilor documentaţiei de atribuire''.

Prin contestaţia în analiză, contestatoarea ... critică raportul procedurii nr. .../16.03.2015, solicitând Consiliului reevaluarea ofertelor, atât a celei proprii, cât şi a celei depuse de competitoarea sa, asocierea ...

În urma depunerii contestaţiei, a formulat cerere de intervenţie ... în calitate de lider al asocierii ... întemeiată pe prevederile art. 61 alin. (3) din Noul cod de procedură civilă. Văzând că ... în calitate de lider al asocierii ..., a fost desemnată câştigătoare a procedurii, este interesată în menţinerea actelor întocmite de autoritatea contractantă, Consiliul, în temeiul art. 61 din Codul de procedură civilă va admite, în principiu, cererea de intervenţie formulată de societatea respectivă.

Cu privire la excepţia lipsei de interes a contestatoarei, invocată de ..., Consiliul constată că aceasta este nefondată. Pentru a ajunge la această concluzie, Consiliul are în vedere că argumentele intervenientei în sprijinul admiterii excepţiei sunt, de fapt, tocmai cele care îi justifică interesul. Astfel, aceasta arată că potrivit art. 255 alin. (1) din OUG nr. 34/2006, interesul unui ofertant respins de a contesta ofertele admisibile nu îndeplineşte cerinţa ca interesul să fie născut şi actual. Aceasta mai arată că în măsura în care se va respinge oferta ..., autoarea contestaţiei nu mai poate justifica un interes legitim, născut, actual şi direct pentru criticarea ofertei declarate câştigătoare. Astfel cum rezultă din contestaţia dpusă, contestatoarea critică măsura respingerii ofertei sale, şi, în egală măsură, declararea drept admisibilă a ofertei .... Deci, până în acest moment, ambele decizii (cea de respingere a ofertei contestatoarei şi cea de admitere a ...) nu au caracter definitiv. Modul în care ... argumentează excepţia, conduce la concluzia că organul de soluţionare nu poate verifica nimic, deoarece drept de contestaţie ar avea doar ofertanţii admisibili, în situaţia de faţă singura ofertă admisibilă fiind oferta proprie. Rezultă, astfel, că ofertantul respins nu are posbilitatea să se plângă în niciun fel, nici în legătură cu respingerea propriei oferte, nici în legătură cu admiterea ofertei concurente, concluzii desprinse în urma unor raţionamente incorecte. Practica judecătorească invocată de petentă

este, astfel, interpretată eronat, aceasta referindu-se la oferte respinse definitiv în urma unor etape anterioare ale procedurilor de atribuire.

În situaţia de speţă, dintre cele două oferte participante la procedură, oferta contestatoarei a fost respinsă, fiind declarată câştigătoare cealaltă ofertă considerată neconformă de către petentă, interesul acesteia fiind direct, născut şi actual.

Pe fondul contestaţiei, în legătură cu motivele de neconformitate invocate de autoritatea contractantă pentru respingerea ofertei ..., Consiliul observă că în urma deciziei citate mai sus, s-a stabilit necesitatea înlocuirii sesiunii demonstrative pentru dovedirea conformităţii cerinţelor cu ,,procedura reglementată de art. 78 din HG nr. 925/2006, respectiv de stabilire a clarificărilor şi completărilor formale sau de confirmare necesare pentru evaluarea fiecărei oferte, pe care le va formula clar, precis si prin care se va defini în mod explicit şi suficient de detaliat în ce constau solicitarile comisiei de evaluare, în strictă corelare cu conţinutul precizărilor şi regulilor documentaţiei de atribuire''.

Astfel cum rezultă din conţinutul deciziei nr. .../../.../ ... nu se poate organiza o sesiune demonstrativă, deoarece ,,cerinţa minimă de calificare de prezentare a mostrei/demo-ului vizând funcţionalitatea „Modulului 7: Componenta de Securizare Acces si Documente" NU a fost preluată în fişa de date şi anunţul de participare'', motiv pentru care ,,se constată că respectiva cerinţă este clauză nescrisă''. Pentru acest motiv, deşi anterior acestei decizii a mai avut loc o sesiune demostrativă, invocată de petentă în cuprinsul contestaţiei, ea nu poate fi luată în considerare de comisia de evaluare, întrucât fiind clauză nescrisă, or potrivit art. 33 alin. (3) din OUG nr. 34/2006, ,,Cerinţele/Criteriile de calificare şi/sau selecţie, care se regăsesc în caietul de sarcini ori documentaţia descriptivă şi care nu sunt preluate în fişa de date/invitaţia de participare/anunţul de participare, sunt considerate clauze nescrise''. Având acest caracter, rezultă că această clauză nu are niciun efect. Prin urmare, ofertanţii au obligaţia de a-şi demonstra conformitatea ofertei prin documente, şi nu prin prezentarea unei sesiuni demonstrative. Întrucât decizia anterioară a Consiliului este pronunţată ca urmare a unei contestaţii depuse tot de ..., aceasta nu poate invoca în favoarea sa procesul verbal al primei sesiuni demonstrative, deoarece, aşa cum s-a arătat, demostrarea confoirmităţii ofertelor se face în baza documentelor, capturilor de pe ecran, în niciun caz a sesiunilor demonstrative. Mai mult, în procesul verbal nr. ...DAPITA/4198/13.11.2014, nu se reţine conformitatea ofertei ori anumite consideraţii/constatări ale comisiei de evaluare sau experţilor cooptaţi, ci doar întrebări adresate de experţi şi răspunsurile contestatoarei ca urmare a prezentării anumitor componente. Nicăieri nu se menţionează, aşa cum susţine contestatoarea, că pe parcursul sesiunii demonstrative s-ar fi consemnat anumite concluzii ale experţilor sau comisiei de evaluare din care să rezulte conformitatea ofertei, aceasta menţionând explicit în cuprinsul contestaţiei, că ,,În acelaşi sens este, de altfel, şi **concluzia de la punctul 3 al sesiunii demonstrative** din 13.11.2014, consemnată în

procesul verbal nr. 4198/13.11.2014 din care este reprodus mai jos un extras:

3. Aplicaţia pentru generarea cheilor şi a cererilor de certificare este prezentă în Google Play/App store sau în alt store de aplicaţii?

Răspuns ofertant: Da, ofertantul a demonstrat că aplicaţia ofertată pentru generarea cheilor şi a cererilor de certificare este prezentă în APP store. Pentru Android a fost prezentată versiunea de autentificare din browser".

Contestatoarea susţine în repetate rânduri în cuprinsul contestaţiei (pag. 13, pag. 17, pag. 19, pag. 20, pag. 27), că în cuprinsul procesului verbal al sesiunii demonstrative nr. 4198/13.11.2014, autoritatea ar fi consemnat o serie de concluzii referitoare la conformitatea anumitor elemente ale ofertei, elemente care, ulterior, ar fi fost considerate neconformităţi, exprimându-şi, în repetate rânduri, nedumerirea cum este posibil ca autoritatea să îşi nege propriile conclzii din acel document. Din lectura documentului în cauză, Consiliul observă că societatea contestatoare interpretează eronat documentul respectiv. Pe tot parcursul documentului, sunt consemnate, la fel ca în paragraful citat mai sus, întrebările experţilor şi răspunsurile ofertantului. Răspunsul ofertantului ,,*Da, ofertantul a demonstrat că…..*" nu poate fi considerat drept concluzie a comisiei de evaluare, aşa cum susţine contestatoarea pe tot parcursul contestaţiei. De altfel, nici nu era posibil ca experţii în cauză să stabilească conformitatea ofertei în cadrul sesiunii demonstrative, şi, chiar dacă în procesul verbal s-ar fi consemnat conformitatea ofertei, concluzia experţilor nu este obligatoriu să fie însuşită de comisia de evaluare.

Deci, procesul verbal respectiv nu poate fi luat în considerare, aşa cum susţine contestatoarea, în verificarea conformităţii ofertei. Rezultă, astfel, că membrii comisiei de evaluare şi experţii cooptaţi trebuie să se raporteze exclusiv la documentele prezentate de ofertanţi şi la răspunsurile la solicitările de clarificări, deşi este posibil ca tocmai o sesiune demonstrativă să fi fost de natură să conducă la edificarea comisiei în legătură cu dovedirea de către ofertanţi a conformităţii ofertelor, inclusiv a conformităţii ofertei contestatoarei. În momentul de faţă, conformitatea ofertei contestatoarei trebuie să rezulte exclusiv din documente, deci funcţionalitatea fiecărei componente a sistemului trebuie dovedită prin capturi de ecran, cărţi tehnice, broşuri şi alte asemenea. Chiar dacă societatea contestatoare susţine importanţa sesiunii demonstrative în concluziile depuse şi în cea de-a doua contestaţie, arătând că prin modificarea nr. 8 s-a renunţat la solicitarea capturilor de ecran, astfel cum rezultă din decizia anterioară a Consiliului, tocmai de aceste documente trebuie să se ţină seama, şi nu de sesoiunea demonstrativă. Decizia Consiliului nr. .../../.../... nu a fost atacată cu plângere, şi, mai mult decât atât, tocmai contestatoarea s-a opus sesiunii demonstrative.

Cu privire la Motivul 1 de respingere a ofertei contestatoarei, autoritatea contractantă a reţinut că ... nu îndeplineşte cerinţa enunţată la cap. 3.3.7 din caietul de sarcini, respectiv: „Soluţia care

implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional". Această cerinţă a fost introdusă în caietul de sarcini prin Modificarea nr. 8, emisă în data de 17.06.2014 în urma Deciziei Consiliului nr. .../...C10/..., ..., ..., ..., ..., .../..., regăsindu-se în documentul publicat pe SEAP la pagina 29.

Din analiza ofertei tehnice şi a solicitărilor de clarificări, autoritatea a reţinut că societatea contestatoare a prezentat Soluţia PKI Safe Layer, care reprezintă o soluţie de management a certificatelor digitale şi nu implementează funcţionalităţile de semnare, criptare/decriptare, ştergere sigură a fişierelor, iar în cadrul paragrafelor care descriu soluţiile de semnare (pag. 312), criptare/decriptare, ştergere sigură a fişierelor (pag. 319-321) care se instalează pe staţiile de lucru, **este prezentată soluţia DigiSigner,** pentru care nu reiese din ofertă că este certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional.

Conform apărărilor prezentate pe larg de contestatoare, autoritatea contractantă excede prevederile documentaţiei de atribuire atunci când pretinde ca şi soluţiile de semnare, criptare/decriptare, ştergere sigură a fişierelor care se instalează pe staţiile de lucru, să fie certificate de către un organism abilitat la nivel naţional. Astfel, aceasta susţine că înţelege să probeze îndeplinirea cerinţei **prin soluţia SafeLayer PKI, care prin tehnologia TrustedX, implementează funcţionalităţile solicitate prin caietul de sarcini (semnare, criptare/decriptare, ştergere sigură a fişierelor) şi deţine certificarea din punct de vedere al securităţii informatice emisă de către un organism abilitat la nivel internaţional, respectiv certificarea Common Criteria EAL 4+, care răspunde întrutotul cerinţei menţionate. Această certificare menţionată în extrasul de la pag. 292 din oferta tehnică este listată public la adresa: http://www.commoncriteriaportal.org., unde de altfel sunt listate toate certificările obţinute de SafeLayer PKI.**

Cu privire la modul de îndepinire a acestei cerinţe, autoritatea a transmis contestatoarei solicitarea de clarificări nr. MFE/DAPITA/3597/14.10.2014, iar la întrebarea nr. 23, s-a cerut **identificarea cu exactitate a soluţiei care implementează funcţionalităţile menţionate**, respectiv Soluţia PKI Safe Layer sau soluţia DigiSigner La aceasta, ... a răspuns prin adresa nr. MFE/DAPITA/3696/20.10.2014, platforma SafeLayer este certificată ISO/IEC 15408 EAL 4+ şi, împreună cu componenta client DigiSigner, asigură funcţionalităţile de semnare, criptare/decriptare, ştergere, sigură cerute prin caietul de sarcini. Contestatoarea preciază ca greşită interpretarea dată de autoritatea contractantă că soluţia care se instalează pe staţiile de lucru pentru a implementa funcţionalităţile solicitate (semnare, criptare/decriptare, ştergere sigură) este, de fapt, soluţia DigiSigner pentru care nu există menţiuni în ofertă privind certificarea acesteia din punct de vedere al securităţii informatice,

conform cerinţelor caietului de sarcini, iar nu SafeLayer PKI. Autoritatea a solicitat prin adresa nr. MFE/DAPITA/4498/03.03.2015, un nou set de clarificări pentru lămurirea acestui aspect, la care ... a răspuns prin adresa nr. MFE/DAPITA/4598/06.03.2015, precizând că platforma SafeLayer este certificată şi, împreună cu componenta client DigiSigner, asigură funcţionalităţile de semnare, criptare/decriptare, ştergere, sigură cerute prin caietul de sarcini.

Cu toate acestea, autoritatea se declară nemulţumită de clarificarea oferită, apreciind în continuare că nu se prezintă niciun document care să ateste certificarea cerută pentru DigiSigner şi că răspunsurile la solicitările de clarificare ar modifica oferta depusă, prin menţionarea produsului.

Consiliul reţine că autoritatea contractantă a dat dovadă de diligenţă, făcând demersuri repetate pentru a da posibilitatea ofertantului să dovedească îndeplinirea specificaţiei tehnice citate. Aşa cum s-a arătat, autoritatea a cerut ca soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional. Este adevărat că societatea contestatoare a prezentat o soluţie complexă, din care face parte şi soluţia DigiSigner. Astfel, chiar dacă soluţia SafeLayer PKI care, prin tehnologia TrustedX, implementează funcţionalităţile solicitate prin caietul de sarcini (semnare, criptare/decriptare, ştergere sigură a fişierelor) şi deţine certificarea din punct de vedere al securităţii informatice emisă de către un organism abilitat la nivel internaţional, respectiv certificarea Common Criteria EAL 4+, aceasta trebuie să prezinte un astfel de certificat şi pentru soluţia DigiSigner. Aşa cum este scrisă cerinţa, soluţia trebuie să fie certificată în întregime. Din oferta depusă, rezultă cu certitudine că se foloseşte componenta DigiSigner referiri la acesta regăsindu-se la pag. 312, 313, 314, 415, 316, 319, 320 şi altele din ofertă.

Deşi contestatoarea susţine că în răspunsul la întrebarea 23 din solicitarea de clarificare nr. MFE/DAPITA/3597/14.10.2014, a confirmat că înţelege să îndeplinească cerinţa caietului de sarcini prin soluţia SafeLayer PKI şi a explicat că DigiSigner este doar o aplicaţie, o componentă utilizată la nivel **de client**, adică al staţiilor de lucru/PC-urilor, pentru a apela funcţionalităţile disponibile la nivelul soluţiei SafeLayer PKI, în realitate, răspunsul 23 este de natură a convinge Consiliul că autoritatea contractantă a procedat corect respingând oferta, deoarece certificarea se referă şi la staţiile de lucru de tip client. În specificaţia a cărei nerespectare este invocată de autoritate, se vorbeşte clar de utilizarea certificatelor digitale pe staţiile de lucru, şi nu doar de server.

Consiliul mai reţine că este eronată susţinerea contestatoarei potrivit căreia este ,,evident, în aceste condiţii, că nu este necesar să se demonstreze certificarea şi pentru componenta/aplicaţia DigiSigner'', fiind necesar acest lucru, fiind expres solicitat în caietul de sarcini astfel cum a fost modificat în urma deciziei Consiliului. De asemenea, este eronată

susţinerea contestatoarei conform căreia autoritatea ar fi pretins în comunicarea rezultatului procedurii cu privire la componenta DigiSigner că ar fi nou introdusă în ofertă, ci dimpotrivă, chiar autoritatea contractantă întreabă despre certificarea acestei componente.

Consiliul reţine că nu poate fi acceptată drept relevantă în cauză nici explicaţia contestatoarei din setul de răspunsuri de clarificare din 06.03.2015 cu privire la diferenţa dintre o soluţie certificată şi o aplicaţie/componentă care asigură interfaţa cu aceasta (sau, în limbaj tehnic, „o apelează") folosind standarde de comunicaţii Web Service. Nu aceasta este problema în discuţie în prezenta cauză, ci îndeplinirea cerinţei referitoare la certificarea soluţiei, or, aşa cum s-a arătat, însăşi contestatoarea recunoaşte că soluţia DigiSigner nu este certificată, susţinând că nici nu era necesar. Autoritatea contractantă nu a pus în discuţie certificarea soluţiei SafeLayer PKI, deci toate explicaţiile contestatoarei pe acest aspect sunt lipsite de relevanţă, din moment ce acest aspect nu este motiv de respingere a ofertei.

Cu privire la analiza realizată de contestatoare asupra conţinutului adresei autorităţii contractante nr. MFE/DAPITA/13760/16.03.2015, respectiv argumentele expuse la lit. a)-d) a motivului de la pct. 1, Consiliul observă că motivul de respingere menţionat de autoritate, nu este, în niciun caz, neindicarea exactă a locului din ofertă unde se regăseşte descris Produsul Digi Signer. Astfel, afirmaţia că ,,Produsul Digisigner nu este prezent în locul menţionat" are la bază răspunsul contestatoarei la o solicitare de clarificări potrivit căruia referiri în cadrul ofertei la componenta Digi Signer s-ar găsi la pag. 292. Nu există niciun temei a considera că autoritatea nu şi-ar fi îndeplinit obligaţia de a examina oferta în ansamblul său.

În ceea ce priveşte afirmaţia b) potrivit căreia „TrustedX nu face parte din platforma KeyOne" şi care, în opinia contestatoarei, este irelevantă şi nu poate justifica respingerea ofertei, Consiliul observă că şi aceasta este interpretată în afara contextului prezentat. Autoritatea contractantă se referă strict la răspunsul 23 prin care contestatoarea a menţionat că prin intermediul Platformei Safe Layer Key One realizează semnarea, criptarea, decriptarea şi stergerea sigură cu tehnologia TrustedX, or, aşa cum şi contestatoarea recunoaşte, TrustedX nu face parte din platforma respectivă. Autoritatea menţionează că TrustedX nu este menţionat în cadrul ofertei în cadrul Modulului 7 – Componenta de Securizare Acces si Documente. Contestatoarea mai precizează că referiri la TrustedX sunt la pag. 37 din ofertă, deci nu a modificat soluţia tehnică. Mergând la pagina respectivă, Consiliul observă că se găseşte o schemă intitulată Arhitectura PKI, unde apare menţionat şi TrustedX, dar şi Digi Signer. Din lectura schemei respective, rezultă că acestea au în vedere componenta de autentificare, şi nu de semnare, criptare/decriptare, ştergere sigură a fişierelor. De asemenea, la pagina 38 a propunerii tehnice, se menţionează expres că Digi Signer se va instala pe staţiile de lucru fiind utilizat în procesul de certificat calificat se va instala pe staţiile de lucru fiind utilizat în procesul de semnare cu certificat calificat. Deci, chiar şi la paginile indicate de contestatoare şe menţionează clar că Digi

Signer se utilizează pentru semnare, şi nu TrustedX, cum susţine contestatoarea în cuprinsul contestaţiei şi în răspunsul la solicitarea de clarificări.

Şi în legătură cu afirmaţia c) („TrustedX nu are nicio legătură cu funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură", care, în opinia contestatoarei falsă, iar captura de ecran prezentată de autoritatea contractantă este menită să inducă în eroare, deoarece aceasta ilustrează funcţionalităţile de autentificare a TrustedX, oferită prin intermediul platformei TrustedX Authentication Platform), Consiliul nu va reţine ca fiind concludente afirmaţiile contestatoarei funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură oferite de TrustedX pot fi dovedite prin accesarea site-ului web al producătorului, secţiunea „TrustedX Electronic Signature", deoarece, pe de o parte, nu autoritatea contractantă trebuie să dovedească conformitatea ofertei contestatoarei prin căutare pe site-uri, această obligaţie revenindu-i ofertantei. Aceasta nu şi-a valorificat posibilităţile oferite de autoritatea contractantă cu ocazia solicitărilor de clarificări, de a-şi dovedi conformitatea ofertei. Pe de altă parte, este clar că societatea contestatoare mizează, în contestaţia de faţă, pe dificultatea de înţelegere a obiectului procedurii atunci când, la afirmaţia b, susţine că la pagina 37 face referire la TrustedX, în realitate făcând referire la TrustedX Authentication Platform, iar la aprecierea răspunsului 23 la solicitarea de clarificări susţine că autoritatea a apreciat în mod greşit că TrustedX nu are nicio legătură cu funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură, folosind în sprijinul afirmaţiilor sale o captură a TrustedX Authentication Platform, când, în realitate, trebuia să caute pe site-urile producătorului pentru a verifica secţiunea TrustedX Electronic Signature, despre care, însă, nu face vorbire nici în ofertă, nici în răspunsul la solicitările de clarificări. Astfel, analiza celor două afirmaţii realizată de contestatoare conduce, în mod clar la concluia, că nu a menţionat nicăieri în conţinutul ofertei că va folosi TrustedX Electronic Signature pentru semnare, criptare/decriptare şi ştergere sigură, ci dimpotrivă, că va folosi Digi Signer, în legătură cu care nu a prezentat certificare.

Contestatoarea mai susţine că în oferta tehnică la pag. 290 este prezentată tehnologia TrustedX în cadrul unei arhitecturi posibile şi este specificat faptul că funcţionalităţile TrustedX pot fi accesate (utilizate) fie prin interfaţă web (ca web service), fie în interfaţă cu diverse aplicaţii (cum este aplicaţia Digisigner), fie prin combinaţia dintre aceste două metode. La pagina indicată de contestatoare se vorbeşte exclusiv de mecanisme de autentificare TrustedX Authentication Platform, şi nu de semnare, criptare/decriptare şi ştergere sigură TrustedX Electronic Signature, deci, chiar şi cu această ocazie, contestatoarea face afirmaţii inexacte.

Referitor la afirmaţia d): „În continuare, nu prezentaţi niciun document care să ateste certificarea produsului DigiSigner, colaborarea acestuia cu platforma SafeLayer nefiind suficientă în acest sens", contestatoarea susţine că DigiSigner este doar o componentă, o aplicaţie

care accesează funcţionalităţile asigurate de soluţia SafeLayer PKI prin tehnologia TrustedX, certificările acesteia în domeniul securităţii informatice emise de o entitate abilitată la nivel internaţional fiind disponibile public la adresa https://www.commoncriteriaportal.org, aşa cum s-a indicat în oferta tehnică la pag. 292. Pentru acest motiv, nu este necesară prezentarea unei certificări şi pentru DigiSigner, certificarea care răspunde integral cerinţelor caietului de sarcini fiind cea emisă pentru soluţia SafeLayer PKI. Consiliul nu îşi însuşeşte punctul de vedere prezentat de contestatoare, întrucât cerinţa din caietul de sarcini este clară, fiind necesară prezentarea certificării pentru DigiSigner, or contestatoarea nu a depus dovezi în acest sens. De asemenea, Consiliul constată că nu este suficientă în dovedirea cerinţei a cărei nerespectare este invocată de autoritatea contractantă, colaborarea dintre produsul DigiSigner şi platforma SafeLayer, deoarece oferta contestatoarei nu a fost respinsă penru o eventuală incompatibilitate între cele două produse, ci pentru inexistenţa certificării pentru DigiSigner.

Este neîndoielnic faptul că ofertantul, în urma solicitării de clarificări şi-a modificat propunerea tehnică, menţionând că funcţionalităţile de semnare, criptare/decriptare şi ştergere sigură se realizează prin intermediul tehnologiei TrustedX, deşi pe tot parcursul propunerii tehnice menţionează pentru aceste funcţionalităţi DigiSigner. De asemenea, este de remarcat că societatea contestatoare nu menţionează nici în răspunsul la solicitarea de clarificări că va folosi TrustedX Electronic Signature pentru funcţionalităţile respective, ci va folosi tehnologia TrustedX, fapt considerat a nu fi de natură a modifica propunerea tehnică, întrucât a menţionat la capitolul arhitectura sistemului TrustedX Authentication Platform, platformă în legătură cu care ea însăşi susţine că este diferită de TrustedX Electronic Signature, legătura dintre ele fiind producătorul SafeLayer. Toate argumentele prezentate de contestatoare în combaterea acestui motiv sunt, de fapt, interpretări proprii, bazate pe diverse fragmente din adresa de comunicare a rezultatului procedurii rupte din context, avalanşa de informaţii prezentate având rolul de a îngreuna afdlarea adevărului.

Referitor la cel de-al doilea motiv de respingere a ofertei contestatoarei, respectiv neîndeplinirea specificaţiei tehnice „În vederea asigurării mobilităţii şi ergonomiei în utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tabletă. Prin urmare, utilizatorii trebuie să aibă la dispoziţie o aplicaţie de generare a cheilor criptografice direct pe terminalul mobil care să permită următoarele: (...)”.

Verificând Modificarea nr. 8, emisă în data de 17.06.2014 în urma Deciziei Consiliului nr. .../.../..., ..., ..., ..., ..., .../..., Consiliul observă că la pagina 32, se menţionează următoarele:

,,In vederea asigurarii mobilitatii si ergonomiei in utilizare, certificatele pot fi stocate pe terminale mobile de tip smartphone sau tableta. Prin urmare, utilizatorii trebuie sa aiba la dispozitie **o aplicatie** de generare a cheilor criptografice direct pe terminalul mobil care sa permita urmatoarele:

-Sa realizeze si sa transmita catre furnizorul de servicii de certificare cererea standard PKCS#10 necesara procesului de emitere a certificatului digital

- Perechea de chei (publica/privata) vor fi generate:

o Software, direct pe dispozitivul mobil

o Pe un dispozitiv criptografic de tip smartcard, conectat la terminalul mobil

-Sa realizeze inscrierea certificatului digital atat pe dispozitivul mobil cat si, dupa caz, pe dispozitivul criptografic de tip smartcard conectat la acesta.''

În justificarea acestui motiv, autoritatea a luat în considerare următoarele argumente considerate de contestatoare drept nefondate:

- În oferta ... (pag. 305) nu s-ar regăsi versiunea de produs ofertată pentru această aplicaţie;
- Linkul http://www.safelayer.com/en/solutions/mobile-pki redirecţionează către o altă pagină, respectiv http:// www.safelayer.com/en/solutions/mobile-identification, care, susţine autoritatea, ar prezenta doar „conceptul de utilizare", nu şi aplicaţia ofertată;
- În oferta .... nu se regăseşte modalitatea de îndeplinire a cerinţei de „generare a cheilor criptografice direct pe terminalul mobil";
- Adresa nr. MFE/DAPITA/4598/06.03.2015, conţinând răspunsul ... la întrebarea nr. 24 din solicitarea de clarificări nr. MFE/DAPITA/4498/03.03.2015, unde a indicat o aplicaţie denumită „Mobile PKI", care în opinia autorităţii contractante „nu există".

... susţine că a confirmat autorităţii în scris, atât prin adresa nr. MFE/DAPITA/4598/06.03.2015, cât şi prin adresa anterioară de clarificări, nr. MFE/DAPITA/3696/20.10.2014, că produsul oferit nu este comercializat cu un model de versionare, acesta fiind motivul pentru care în ofertă nu se regăseşte versiunea de produs ofertată.

- Aplicaţia de generare a cheilor criptografice direct pe terminalul mobil, care este menţionată în ofertă, poartă denumirea completă de „Safelayer Mobile ID", aşa cum de altfel s-a explicat în adresa nr. MFE/DAPITA 4598/06.03.2015, la care se face referire şi sub denumirile de „Mobile ID" sau „Mobile PKI", având în vedere capabilităţile oferite, aspect susţinut prin declaraţia producătorului Safelayer, ataşată ca Anexa nr. 1 la adresa mai sus menţionată. În mod evident, fiecare producător are libertatea de a-şi denumi sau supranumi propriul produs după cum consideră de cuviinţă (evident, în limitele legale), iar Safelayer a decis să se refere la aplicaţia de generare a cheilor criptografice pentru terminale mobile sub denumirea "Mobile PKI", fapt atestat şi de declaraţia de producător pusă la dispoziţia autorităţii.

Contestatoarea face trimitere la acelaşi proces verbal al primei sesiuni demonstrative în legătură cu care s-a stabilit că nu poate fi folosit în cauză, pe de o parte, deoarece nicăieri nu există vreo confirmare că produsul ar fi disponibil în Google Play/App store, cu atât mai mult cu cât produsul oferit nu este comercializat cu un model de versionare. De asemenea, contestatoarea nu a prezentat dovezi în acest sens, ci trimite

la un site. Contestatoarea nu a făcut dovada disponibilităţii facile pentru utilizatori a Aplicaţiei de generare a cheilor criptografice direct pe terminalul mobil, astfel încât cerinţa respectivă nu este îndeplinită. Ca şi în cazul precedentului motiv, contestatoarea nu şi-a valorificat posibilitatea de a-şi dovedi conformitatea ofertei, deşi în două rânduri i s-au solicitat clarificări.

În urma studiului dosarului, contestatoarea a transmis Consiliului un punct de vedere prin care critică raportul expertului tehnic cooptat, arătând că acesta a denaturat adevărul, nicăieri în documentaţia de atribuire nu a fost exprimată vreo cerinţă ca autentificarea să fie făcută atât cu aplicaţii, cât şi cu browser, ci doar să poată fi făcută de pe telefoanele mobile.

Da, Consiliul observă că nu s-a solicitat o asemenea cerinţă, ci s-a solicitat o aplicaţie disponibilă, şi nu autentificarea cu browser, aşa cum a ofertat contestatoarea. Argumentele contestatoarei invocate în concluzii nu fac decât să genereze confuzie, deşi prevederile documentaţiei de atribuire erau clare, solicitându-se o aplicaţie pentru Apple iOS/Google Android disponibilă. Prin urmare, este corectă concluzia de la pag. 19 a raportului de expertiza tehnică revizuit înregistrat cu nr. 4461/02.03.2015, potrivit căreia autentificarea din browser de pe sistemul de operare Android demonstrază că nu există o aplicaţie comercială ofertată care să genereze chei criptografice şi cereri de certificate pentru acest sistem de operare. Folosirea browserului implică faptul că acestea sunt generate pe un server, şi nu pe dispozitivul mobil, aşa cum s-a solicitat prin caietul de sarcini.

Astfel fiind, Consiliul constată că cele două motive de neconformitate a ofertei au fost corect stabilite de autoritatea contractantă.

Având în vedere că motivele analizate mai sus sunt suficiente pentru a stabili neconformitatea ofertei, Consiliul nu va mai analiza şi restul motivelor pentru care autoritatea a respins oferta contestatoarei, fiind lipsit de relevanţă dacă a fost respinsă pentru unul sau mai multe motive, fiind lipsit de relevanţă dacă oferta este respinsă pentru două sau mai multe motive. Astfel, Consiliul reţine că societatea contestatoare nu a respectat documentaţia de atribuire, astfel cum a fost modificată în urma deciziilor anterioare, iar în urma solicitărilor de clarificări, a oferit autorităţii contractante răspunsuri din care rezultă că şi-a modificat propunerea tehnică, fiind aplicabile următoarele dispoziţii legale:

-Art. 170 din OUG nr. 34/2006- ,,Ofertantul elaborează oferta în conformitate cu prevederile din documentaţia de atribuire''

-Art. 36 alin. (2) din HG nr. 925/2006, potrivit căruia ,,Oferta este considerată neconformă, în următoarele situaţii:

a) nu satisface în mod corespunzător cerinţele caietului de sarcini''.

-Art. 79 alin. (1) din HG nr. 925/2006, potrivit căruia ,,În cazul în care ofertantul nu transmite în perioada precizată de comisia de evaluare clarificările/răspunsurile solicitate sau în cazul în care explicaţiile

prezentate de ofertant nu sunt concludente, oferta sa va fi considerată neconformă.

(2) În cazul în care ofertantul modifică prin răspunsurile pe care le prezintă conţinutul propunerii tehnice, oferta sa va fi considerată neconformă''.

În cadrul primei contestaţii depuse, contestatoarea critică şi oferta câştigătoare, respectiv cea depusă de Asocierii ..., considerând că această ofertă este inadmisibilă şi neconformă.

În sprijinul acestei afirmaţii, contestatoarea arată că la Secţiunea 2, cap 3.3.8.3 – Componenta de depozitare fizică din caietul de sarcini, autoritatea contractantă a impus un set de cerinţe tehnice obligatorii ce trebuiau respectate de ofertanţi cu privire la Centrul de arhivare fizică a documentelor. Conform secţiunii menţionate din caietul de sarcini, acesta trebuie să întrunească următoarele cerinţe minime:

- *"Va trebui ca aplicatia de gestiune a informatiilor electronice referitoare la arhiva fizica sa poata gestiona la nivel de cod de bare unic si dosarele din interiorul unei cutii, nu doar cutiile cu documente. Aplicatia va trebui sa poate gestiona inclusiv etichete cu coduri de bare RFID pasive";*
- *"Va trebui ca fluxul operational, inclusiv pe perioada transportului, sa fie monitorizat online".*

Aceasta arată că în acest moment niciunul dintre operatorii membri în Asocierea declarată câştigătoare nu îndeplineşte condiţia de gestionare a etichetelor cu coduri de bare RFID Pasive, motivându-şi suspiciunea pe faptul că până în acest moment nu au existat proceduri de achiziţie care să impună acest mod de lucru, tagurile RFID nefiind solicitate şi nici recomandate spre utilizare de către Arhivele Naţionale.

Intervenienta şi autoritatea contractantă consideră nefondată susţinerea contestatoarei.

Faţă de cele susţinute în cuprinsul contestaţiei, intervenienta invocă prevederile art. 270 alin. (1) lit. e) şi f) din O.U.G. nr. 34/2006, şi afirmă că la soluţionarea contestaţiei deduse judecăţii, societatea contestatoare nu a înţeles să evidenţieze în cuprinsul contestaţiei motivele de fapt pentru care consideră că oferta ... trebuia respinsă ca neconformă, și nici mijloacele de probă avute în vedere pentru a face dovada că propunerea tehnică a ... nu îndeplinește cerinţele minime din caietul de sarcini, iar simpla menţiune „din cunoştinţele noastre" nu poate corespunde unei motivări în fapt corespunzătoare.

Altfel spus, intervenienta susţine că societatea contestatoare ar trebui să motiveze în fapt contestaţia, respectiv să indice pagina din ofertă de unde rezultă neîndeplinirea cerinţei respective. Cel mai simplu în combaterea argumentului contestatoarei era ca intervenienta să indice pagina din ofertă care demonstrează contrariul. Cum societatea contestatoare nu a avut acces la oferta tehnică a asocierii câştigătoare, ar fi inechitabilă respingerea contestaţiei fără ca organul de soluţionare să verifice dacă, într-adevăr, specificaţia tehnică este menţionată sau nu în oferta câştigătoare.

Autoritatea contractantă susţine că oferta tehnică înaintată de Asocierea formată din ... demonstrează îndeplinirea cerinţelor cu privire

la gestionarea etichetelor cu coduri de bare RFID pasive şi la monitorizarea on-line a fluxului operațional, apreciind susţinerile contestatoarei drept nefondate, nefiind bazate pe niciun argument concret, fiind simple presupuneri, întreaga contestaţie având ca scop tergiversarea încheierii procedurii de atribuire şi semnarea contractului, putând conduce, astfel, la pierderea fondurilor alocate realizării proiectului. Cu toate că susţine acest lucru, nici ea nu motivează unde, anume, în oferta câştigătoare se regăsesc cerinţele respective, spre a-şi argumenta punctul de vedere şi spre a facilita căutarea în interiorul miilor de pagini din oferta câştigătoare.

Din verificarea matricii de conformitate, Consiliul observă că lipseşte în întregime Modulul 8 al capitolului 3- Modulul de arhivare a documentelor. Deşi paginile sunt numerotate cursiv din momentul imprimării, din matrice lipsesc mai multe părţi, iar o parte dintre cerinţe nu respectă ordinea din caietul de sarcini, astfel încât verificarea conformităţii ofertei câştigătoare este greoaie. Ceea ce este cert, este faptul că NU EXISTĂ Modulul de arhivare a documentelor, deci Consiliul nu a putut identifica cap. 3.3.8.3 – Componenta de depozitare fizică, a cărei nerespectare este invocată de contestatoare, fiind menţionat în conţinutul ofertei la cap. 5.1.2.3. Din lectura întregului document, Consiliul observă că există referiri la coduri de bare RFID Pasive la pagina 1213 a propunerii tehnice prezentate de asocierea câştigătoare, cerinţa caietului de sarcini *"Va trebui ca aplicatia de gestiune a informatiilor electronice referitoare la arhiva fizica sa poata gestiona la nivel de cod de bare unic si dosarele din interiorul unei cutii, nu doar cutiile cu documente. Aplicatia va trebui sa poate gestiona inclusiv etichete cu coduri de bare RFID pasive*". La Specificaţii oferite, ofertantul susţine, la cerinţa RQ 974 la pagina 1213, că aplicaţia UTI Arch poate gestiona inclusiv etichete cu coduri de bare RFID Pasive, menţionând, totodată, că detalii în acest sens, se regăsesc la cap. 4.3.8.3 din propunerea tehnică. Verificând în cadrul propunerii tehnice, Consiliul nu a identificat acel capitol cu numărul indicat în ofertă, ci a fost introdus la cap. 4.**5.**8.3 din propunerea tehnică, intitulat Componenta de depozitare fizică. În cadrul capitolului respectiv, Consiliul nu a identificat informaţii referitoare la coduri de bare RFID Pasive.

Potrivit documentaţiei de atribuire, propunerea tehnică se prezintă după cum urmează:

,,4.1) Modul de prezentare a propunerii tehnice

In cadrul Ofertei Tehnice se va detalia de catre Prestator conformitatea solutiei ofertate cu toate cerintele specificate in Documentatia de Atribuire.

*Furnizorul trebuie **sa raspunda punctual la toate cerintele cuprinse in Documentatia de Atribuire si sa detalieze in propunerea sa tehnica modurile si mijloacele prin care solutia ofertata indeplineste aceste cerinte, astfel incat comisia de evaluare sa aiba posibilitatea evaluarii acesteia in mod cat mai informat**. In cazul in care oferta nu ofera informatii complete prin detalierea raspunsului la cerinte sau nu indeplineste cerintele exprimate*

in Documentatia de Atribuire, ***comisia de evaluare poate sa declare oferta ca fiind inacceptabila/neconforma.***

Nu vor fi luate in considerare componente ale ofertei tehnice cum ar fi: pliante, diverse materiale promotionale ale firmelor producatoare sau furnizoare de servicii, prezentari, brosuri, etc. care nu au legatura directa cu obiectul, structura si cerintele din prezenta Documentatie de Atribuire''.

Având în vedere că:

-în matricea de conformitate răspunsurile ofertantului nu respectă numerotarea din documentaţia de atribuire, deci ofertantul nu a răspuns punctual la toate cerinţele cuprinse în documentaţia de atribuire;

- în cadrul solicitărilor de clarificări nu se regăsesc întrebări referitoare la gestionarea etichetelor cu coduri de bare RFID pasive;

- din procesele verbale ale Comisiei de evaluare nu rezultă dacă s-a realizat corespondenţa dintre prevederile documentaţiei de atribuire şi propunerea tehnică a ofertei câştigătoare;

- în cadrul matricii de conformitate se face trimitere la o serie de capitole ale propunerii tehnice care, ori nu există, ori au altă numerotare, fiind greu de verificat conformitatea ofertei, Consiliul consideră că se impune reverificarea propunerii tehnice a asocierii câştigătoare.

Chiar dacă în Documentaţia de Atribuire, se prevede ca în situaţia neîndeplinirii cerinţelor tehnice din documentaţia de atribuire ,,**comisia de evaluare poate sa declare oferta ca fiind inacceptabila/neconforma''**, aplicabilă este prevederea legală de la art. 81 din HG nr. 925/2006, potrivit căreia ,,Comisia de evaluare **are obligaţia** de a respinge ofertele inacceptabile şi ofertele neconforme''. Prin urmare, autoritatea contractantă, în situaţia în care ar constata, în urma evaluării ofertelor că oferta depusă de asocierea ... ar fi neconformă, ea nu poate aplica prevederea documentaţiei de atribuire, ci preevederea legală care stabileşte obligaţia de a respinge ofertele neconforme.

Cu privire la cea de-a doua contestaţie, Consiliul reţine că societatea contestatoare a intenţionat iniţial să formuleze completări la contestaţie, în urma studiului dosarului. Ca urmare a invocării de către intervenientă a inadmisibilităţii completării contestaţiei dincolo de termenul de depunere a contestaţiei. Drept urmare, contestatoarea a depus la Consiliu o nouă contestaţie, având acelaşi conţinut ca şi completarea la contestaţia iniţială, constituind garanţia de bună conduită.

În legătură cu cea de-a doua contestaţie, Consiliul reţine că şi aceasta vizează raportul procedurii nr. 13739/16.03.2015, faţă de care contestaţia depusă la 20.04.2015 este tardivă. Faptul că societatea contestatoare a luat cunoştinţă de o serie de documente care au concurat la stabilirea rezultatului procedurii odată cu studiul dosarului, nu conduce la apariţia unui nou drept de a contesta raportul procedurii. Raportul procedurii se contestă în termenul legal stabilit de art. 256^2 din OUG nr. 34/2006. A admite că operatorii economici ar avea dreptul să conteste în etape raportul procedurii, de fiecare dată când iau la cunoştinţă de conţinutul unui act întocmit de autoritatea contractantă, echivalează cu

inexistenţa unui termen şi lăsarea termenului de contestare la libera apreciere a ofertanţilor. Legislaţia achiziţiilor este guvernată de principiul celerităţi, acesta fiind şi motivul pentru care termenele de contestare sunt scurte faţă de cele stabilite în alte materii. În cazul procedurii de faţă, termenul de formulare a contestaţiei este cel stabilit la art. 256^2 lit. a) din OUG nr. 34/2006, respectiv ,,10 zile începând cu ziua următoare luării la cunoştinţă, în condiţiile prezentei ordonanţe de urgenţă, despre un act al autorităţii contractante considerat nelegal, în cazul în care valoarea contractului care urmează să fie atribuit, estimată conform prevederilor art. 23 şi ale cap. II secţiunea a 2-a, este egală sau mai mare decât pragurile valorice prevăzute la art. 55 alin. (2)''. Faţă de prevederea imperativă a legii, Consiliul nu poate interpreta dispoziţia legală în sensul în care contestatoarea poate depune contestaţie împotriva raportului procedurii de la data luării la cunoştinţă despre actele din dosar premergătoare raportului procedurii, acte care nu se comunică ofertanţilor pe perioada evaluării ofertelor şi nici ulterior, motiv pentru care va respinge ca tardivă contestaţia nr. T/1179/20.04.2015. Cu toate acestea, Consiliul va analiza criticile formulate de contestatoare cu ocazia completării contestaţiei, practica judiciară recentă fiind în sensul verificării şi a criticilor suplimentare formulate după expirarea termenului prevăzut la art. 256^2 lit. a) din OUG nr. 34/2006.

În acest sens, este de remarcat Decizia civilă nr. 1687 din 6 martie 2014 pronuţată de Curtea de Apel Bucureşti, Secţia a VIII-a contencios administrativ şi fiscal, în care au fost reţinute următoarele aspecte:

,,În ce priveşte considerentele Consiliului privind respingerea ca inadmisibile a criticilor formulate de contestatoare prin concluziile scrise, Curtea reţine următoarele:

Prin decizia Consiliului s-au reţinut prevederile art. 270 din ordonanţă şi s-a concluzionat că, din aceste dispoziţii, rezultă că persoana vătămată sesizează Consiliul, într-un termen anume dat, cu o contestaţie care trebuie să cuprindă obligatoriu motivarea în fapt şi drept. Întrucât contestaţia din 29.11.2013 nu era completă, s-a făcut aplicarea art. 270 alin. (2) teza I, solicitându-se completarea acesteia cu motivarea în fapt şi în drept.

A reţinut Consiliul că „nicăieri în cuprinsul cap. IX din ordonanţă nu se aminteşte că persoana vătămată îşi poate schimba motivarea contestaţiei prin care s-a delimitat cadrul judecăţii, astfel încât Consiliul să analizeze alte critici decât cele cu care a fost învestit în termenul legal de contestare".

Curtea reţine că, la data de 05.12.2013, Consiliul a solicitat petentei comunicarea în termen de 5 zile a motivării susţinerilor cu privire la faptul că ofertele celorlalţi ofertanţi sunt inacceptabile şi neconforme.

SC D. SRL a comunicat răspunsul la 09.12.2013, prin care a arătat că, prin clarificările solicitate de autoritatea contractantă în etapa de reevaluare a ofertelor, s-au încălcat decizia Consiliului anterioară şi principiile tratamentului egal, nediscriminării şi transparenţei, acceptându-se completarea ofertei depuse, nu clarificarea acesteia.

Curtea constată că petenta avea obligaţia de a arăta prin acest răspuns toate criticile cu privire la aspectul neconformităţii şi inacceptabilităţii celorlalte oferte, susţinut prin contestaţia din 29.11.2013.

Însă, totodată, constată că, prin contestaţie, petenta solicitase, în temeiul art. 274 din ordonanţă, accesul la dosarul achiziţiei publice. De asemenea, prin completarea motivelor contestaţiei depusă la 09.12.2013, petenta a solicitat accesul la dosarul achiziţiei publice.

Acceptul Consiliului a fost comunicat petentei la data de 12.12.2013, iar dosarul a fost consultat de reprezentantul petentei la 13.12.2013.

În condiţiile în care motivele invocate de petentă în notele scrise au fost determinate de elementele noi de care a luat cunoştinţă cu ocazia studierii dosarului, accesul fiindu-i aprobat după expirarea termenului de motivare a contestaţiei, Curtea apreciază că nu este justificată respingerea acestora ca inadmisibile. Criticile respective au fost comunicate şi autorităţii contractante, care a răspuns prin punctul de vedere înregistrat la Consiliu la 23.12.2013".

Drept urmare, Consiliul va analiza motivele invocate de contestatoare în adresa nr. T/1171/17.04.2015, aceasta cu atât mai mult cu cât atât intervenienta, cât şi autoritatea contractantă au luat cunoştinţă de completările respective, formulând apărări.

Cu privire la primul motiv invocat în completarea la contestaţie, respectiv nedovedirea de către asocierea câştigătoare a inexistenţei datoriilor către finanţele publice locale, motivat de faptul că certificatele pentru impozite şi taxe locale depuse de ..., ... şi ... sunt emise în luna septembrie 2014, or, potrivit documentaţiei de atribuire, certificatele trebuie să reflecte faptul că asociaţii nu aveau obligaţii de plată către bugetele locale exigibile la nivelul lunii anterioare depunerii ofertelor (la nivelul iulie 2014). Din documentele depuse ataşat răspunsului la solicitarea de clarificări nr. 12408/18.09.2014, la pag. 12-29 (Vol II din dosarul achiziţiei publice). Contrar opiniei contestatoarei, depunerea certificatelor emise în luna septembrie nu conduce la respingerea ofertei asocierii câştigătoare, ci ar fi trebuit să conducă la solicitarea de noi clarificări, respectiv dovezi de plată, balanţă, orice document care să lămurească asupra inexistenţei datoriilor la data prevăzută în documentaţia de atribuire. Cu toate acestea, comisia de evaluare a acceptat răspunsul primit la cererea de clarificare comunicată prin adresa nr. 3149/12.09.2014. Întrucât plata impozitelor şi taxelor locale se face până la data de 30.06, autoritatea contractantă trebuia să verifice dacă la data de 31.07.2014, dată menţionată în documentaţie, impozitele şi taxele locale erau achitate. Intervenienta invocă dispoziţiile art. 9 alin. (3) din Ordinul ANRMAP nr. 509/2011, susţinând că pot fi primite şi certificate emise ulterior, care atestă lipsa lipsa datoriilor ulterior acestei date. Articolul 9 din Ordinul respectiv are următorul conţinut:

,, (1) Cerinţele referitoare la obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale către bugetele componente ale bugetului general consolidat sunt considerate ca fiind îndeplinite în măsura în care operatorii economici prezintă înlesniri la plată de genul eşalonărilor sau compensărilor, aprobate de către organele competente în domeniu.

(2) Raportarea se va face la inexistenţa datoriilor faţă de bugetul general consolidat, la o dată corelată cu termenul legal al scadenţei de plată şi nu la termenul de valabilitate al documentului la data depunerii sau deschiderii ofertelor.

(3) În situaţiile de la art. 11 alin. (4) şi (5) din Hotărârea Guvernului nr. 925/2006 pentru aprobarea normelor de aplicare a prevederilor referitoare la atribuirea contractelor de achiziţie publică din Ordonanţa de urgenţă a Guvernului nr. 34/2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, cu modificările şi completările

ulterioare, autoritatea contractantă va lua în considerare, la verificarea îndeplinirii cerinţei de calificare privind plata de către ofertant a impozitelor, taxelor şi contribuţiilor de asigurări sociale, atât declaraţia pe propria răspundere prin care se confirmă îndeplinirea cerinţei, cât şi acele certificate de atestare fiscală prezentate de ofertant în urma solicitării primite din partea autorităţii contractante, chiar dacă acestea sunt emise de autorităţile competente ulterior datei de deschidere a ofertelor şi, eventual, atestă lipsa datoriilor ulterior respectivei date''.

Prevederea citată de intervenientă nu este interpretată în contextul întregului artiol, astfel încât să fie respectată şi scadenţa obligaţiei. Tot ceea ce trebuia să facă autoritatea contractantă era să solicite dovezi privind plata la scadenţă a obligaţiilor (31.06.2014) sau cel mai târziu până în data de 31.07.2014, dată menţionată expres în documentaţia de atribuire.

Referitor la cea de-a doua critică, respectiv neîndeplinirea de către ofertanta câştigătoare a cerinţei enunţată la cap. 3.3.7 din caietul de sarcini, respectiv: „Soluţia care implementează funcţionalităţile privind utilizarea certificatelor digitale pe staţiile de lucru (semnare, criptare/decriptare, ştergere sigură) trebuie să fie certificată din punct de vedere al securităţii informatice de către un organism abilitat la nivel naţional, european sau internaţional", aceeaşi cerinţă pentru a cărei neîndeplinire a fost respinsă oferta contestatoarei, Consiliul observă că în oferta asocierii câştigătoare, pentru îndeplinirea acestei cerinţe, acesta a ofertat soluţia compusă din suita shellSafe, produsă de Uti Grup, care include clikSign şi sendSafe, menţionate drept componente chiar de către producător, după cum chiar contestatoarea menţionează. Asocierea câştigătoare a prezentat certificare pentru suita shellSafe, dar nu a prezentat pentru componentele sale. Contrar opiniei contestatoarei, situaţia nu este identică cu a ofertei sale, deoarece cele două componente sunt părţi ale aceleiaşi soluţii, şi nu soluţii independente, cum a prezentat contestatoarea, astfel încât este nefondată critica respectivă. Detalii cu privire la semnare, criptare/decriptare, ştergere sigură se regăsesc în oferta câştigătoare la paginile 321 -345.

Având în vedere cele constatate, Consiliul constată că autoritatea contractantă nu a evaluat riguros oferta asocierii câştigătoare, astfel încât se impune reevaluarea acesteia.

Faţă de cele de mai sus, în temeiul art. 278 alin. (2) şi (4) din OUG nr. 34/2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, cu modificările şi completările ulterioare, Consiliul va admite în parte contestaţia formulată de ..., în contradictoriu cu ... şi va dispune reevaluarea ofertei asocierii ...

În temeiul art. 278 alin. (5) din OUG nr. 34/2006, va respinge ca nefondată contestaţia în partea dedicată reevaluării ofertei proprii.

În temeiul art. 65 alin. (1) şi art. 67 din Codul de procedură civilă, va admite cererea de intervenţie accesorie formulată de ... în calitate de lider al asocierii ..., în partea privitoare la neconformitatea ofertei contestatoarei. În temeiul art. 278 alin. (5) din ordonanţa de urgenţă

menţionată, va respinge ca nefondată cererea respectivă în partea referitoare la solicitarea contestatoarei de reevaluarea ofertei sale.

În temeiul art. 278 alin. (5) din OUG nr. 34/2006, va respinge ca tardiv introdusă contestaţia nr. T/1179/20.04.2015, înregistrată la Consiliul Naţional de Soluţionare a Contestaţiilor sub nr. 6190/20.04.2015, depusă de către ....

În temeiul art. 65 alin. (1) şi art. 67 din Codul de procedură civilă, va admite cererea de intervenţie nr. 311/24.04.2015, înregistrată la Consiliu sub nr. 6625/24.04.2015, formulată de către ... în calitate de lider al asocierii ...

Măsurile dispuse vor fi aduse la îndeplinire într-un termen de maximum 15 zile de la comunicarea prezentei.

Redactată în 5 exemplare, cuprinde 181 pagini.

PREŞEDINTE COMPLET,
...

MEMBRU, **MEMBRU,**
.... **....**