



# CONSILIUL NAȚIONAL DE SOLUȚIONARE A CONTESTAȚIILOR

C. N. S. C.

Str. Stavropoleos, nr. 6, sector 3, ..., România, CP 030084, CIF 20329980  
Tel. +4 021 3104641 Fax. +4 021 3104642, +40218900745 [www.cnsc.ro](http://www.cnsc.ro)

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

## DECIZIE

**Nr. .../.../...**

**Data: ...**

Prin contestația nr. 586/31.08.2015, înregistrată la CNSC sub nr. 16796/02.09.2015, înaintată de SC ... SRL, cu sediul în ..., ..., ..., înmatriculată la Oficiul Registrului Comerțului sub nr. ..., având CUI ..., reprezentată legal prin ...- Administrator, formulată împotriva rezultatului procedurii aferent lotului 2, ce i-a fost adus la cunoștință prin adresa nr. 538/24.08.2015, emis de ..., cu sediul în ..., ..., ..., în calitate de autoritate contractantă, în cadrul procedurii de atribuire, cerere de oferte, organizată în vederea atribuirii contractului de furnizare având ca obiect „SIC pregătire operații cibernetice (CyberRange), ..., Instrumente computer forensics, Soluție de evaluare securitate rețele”, cu invitație de participare nr. ..., publicată în SEAP la ..., s-a solicitat Consiliului: ...contractante la emiterea unui nou raport de evaluare; obligarea autorității contractante la anularea deciziei de anulare a procedurii pentru lotul 2 - „...”.

În baza legii și a documentelor depuse de părți,  
CONSILIUL NAȚIONAL DE SOLUȚIONARE A CONTESTAȚIILOR

## DECIDE:

Respinge contestația, ca nefondată, și menține măsura anulării procedurii, dispusă de autoritatea contractantă.

Obligatorie.

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

## MOTIVARE

În luarea deciziei, s-au avut în vedere următoarele:

Prin contestația nr. 586/31.08.2015, înregistrată la CNSC sub nr. 16796/02.09.2015, SC ... SRL atacă rezultatul procedurii aferent lotului 2, ce i-a fost adus la cunoștință prin adresa nr. 538/24.08.2015, emis de ..., în calitate de autoritate contractantă, în cadrul procedurii de atribuire mai sus arătate, considerând nelegală decizia acesteia de respingere, ca neconformă, a ofertei sale pentru lotul 2 și de anulare a procedurii pentru acest lot.

Pe de o parte, contestatoarea reclamă modalitatea abuzivă de evaluare a ofertei sale, modalitate de evaluare ce a avut la bază cerințe care nu există în cadrul caietului de sarcini.

Chiar și în aceste condiții, contestatoarea susține că oferta sa îndeplinește și criteriile suplimentare apărute în cadrul procesului de evaluare.

În continuare, contestatoarea prezintă întrebările primite și răspunsurile sale, care demonstrează conformitatea ofertei depuse.

Astfel, potrivit documentației de atribuire, 1.1.2 *Soluția va include toate componentele hardware, de ultimă generație, și licențele software necesare menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice investigate prin prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specific acestora în perioada de viață a soluției ofertate (până la declararea acesteia de producător ca fiind "end of support").*"

Referitor la concluzia autorității contractante potrivit căreia *Soluția ofertată este de un server și un software open-source și nu o platformă dedicată cu suport oferit de un producător*, contestatoarea precizează că documentația de atribuire nu conține, nicăieri, o cerință care să impună ca soluția ofertată să fie „o platformă dedicată cu suport oferit de un producător”. Așadar, concluzia autorității contractante este una subiectivă și nu se raportează la cerințele documentației de atribuire.

Mai mult, contestatoarea precizează că afirmația autorității contractante din adresa nr. A3/6547 din 24.08.2015, potrivit căreia *tabelul transmis, atât în oferta tehnică, cât și în răspunsul la cererile de clarificări nr. A3/3267 din 26.06.2015 și nr. A3/3399 din 03.07.2015, nu conține toate componentele necesare funcționării soluției, așa cum s-a solicitat cu adresa nr. A3/3399 din 03.07.2015 și nici detaliile cerute prin cererea de clarificare este din nou, subiectivă, și nu se raportează la cerința documentației de atribuire.*

De altfel, la întrebarea nr. 1 din adresa nr. A3/3399 din 03.07.2015 (Clarificări cu privire la componentele hardware și software care vor fi integrate de către ofertant, pentru obținerea soluției ... ofertată), contestatoarea susține că a formulat următorul răspuns:

*Precum se poate verifica atât în oferta tehnică, cât și în clarificarea cu nr. 411 (nr. A3/3267 din 26 iunie 2015 transmisă de autoritate) răspunsă și transmisă în data de 01 iulie 2015, elementele solicitate au fost deja transmise, cu producătorul, ediția și versiunea ofertată, atașate în cadrul răspunsului referențiat mai sus - nr. 411 transmisă în data de 01 iulie 2015 autorității. Completăm mai jos tabelul solicitat de dumneavoastră.*

<i>Nr crt</i>	<i>PRODUS/ COMPONENTE</i>	<i>Cantitate</i>
1	LOT 2 - Sisteme operare Windows + Licențe Office si Adobe	1 complet compus din:
	Windows 8.1 Pro x32/ x64 pentru VM	2
	Windows 8.1 x32/ x64 pentru VM	2
	Microsoft VDI GOV	5
	Office Home and Business	4
	Adobe Standard DC 2015 Windows International English AOO License	4
2	2 - Cuckoo Sandbox	1
3	2 - Volatility Foundation	1
4	2 - HP DL380 Gen9	1

De asemenea, contestatoarea prezintă aspectele conținute de oferta tehnică depusă:

Platformă Analiză Malware	Furnizorul soluției va pune la dispoziție licențele sistemelor de operare și aplicațiilor comerciale din cadrul mașinilor virtuale preinstalate/preconfigurate;	Da	Ofertantul pune la dispoziția autorității contractante licențele sistemelor de operare și aplicațiilor comerciale: - una bucata licența Windows 7 SP1 - una bucata licența Windows 7 SP2 - una bucata licența Windows 8 - una bucata licența Windows 8.1 - patru bucăți licențe Microsoft Office - una pentru fiecare mediu simulat cu sistemele de operare de mai sus - patru bucăți licențe Adobe Reader - una pentru fiecare mediu simulat cu sistemele de operare de mai sus Mediile virtuale se vor putea crea și emula sub licența Microsoft VDI pe care ofertantul o pune la dispoziție
---------------------------------	---	----	--

La întrebarea nr. 2 din adresa nr. A3/3267 din 26.06.2015 (Clarificări cu privire la prețul scăzut al propunerii financiare depuse pentru Lotul nr. 2, din care să rezulte modul de formare a prețului, pentru elementele componente ale sistemului, contestatoarea a răspuns, precizând că a luat în considerare următoarele costuri:

- costul total al produselor/componentelor în valoare de 181,622.51 lei fără TVA:

<i>Nr. crt.</i>	<i>PRODUS/ COMPONENTE</i>	<i>Oferta</i>
<i>LOT 2</i>		
1	Sisteme operare Windows + Licențe Office și Adobe	Oferta Maguay Software Client Oferta Maguay Software Adobe
2	Cuckoo Sandbox	Este un Produs complet open source, fără costuri de achiziție, cu drepturi de utilizare incluse: <a href="http://www.cuckoosandbox.org/">http://www.cuckoosandbox.org/</a>
3	Volatility Foundation	Este un produs complet open source, fără costuri de achiziție, cu drepturi de utilizare incluse: <a href="http://www.volatilityfoundation.org/">http://www.volatilityfoundation.org/</a>
4	HP DL380 Gen9	Oferta BitNet Server HP DL380 Gen 9

<i>NR. CRT</i>	<i>PRODUS/ COMPONENTĂ OFERTATĂ</i>	<i>CANTITATE</i>	<i>PREȚ UNITAR (FĂRĂ TVA)</i>	<i>PREȚ TOTAL (FĂRĂ TVA)</i>
1	Windows 8.1 Pro x32/ x64 pentru VM	2	565.19	1,299.94
2	Windows 8.1 x32/ x64 pentru VM	2	395.24	909.05
3	Microsoft VDI GOV, 36 luni	5	129.24	743.15
4	Office Home and Business	4	830.00	3,818.02
5	Adobe Standard DC	4	1,223.86	5,629.75
6	Laptop Maguay P1704x	2	5,908.84	13,590.33
7	Statie GamePower Z97, monitor Asus 23 inch VS229NV	8	3,545.30	32,616.79
8	Server HP DL380 Gen9	1	106,969.98	123,015.48
<i>TOTAL:</i>				<i>181,622.51</i>

- costul total al serviciilor necesare implementării calculat pe baza unor medii ale tarifelor practicate pe piața de profil IT&C, astfel:

<i>NR. CRT.</i>	<i>TIP SERVICIU</i>	<i>CANTITATE (ZILE)</i>	<i>PREȚ/ ZI</i>	<i>PREȚ TOTAL</i>
-----------------	---------------------	-------------------------	-----------------	-------------------

1	Servicii livrare și punere în funcțiune	9	1,100.00	9,900.00
2	Servicii instruire pentru soluțiile oferite Cuckoo Sandbox și Volatility Foundation	1	1,995.00	1,995.00
3	Servicii de management de proiect de baza - gestiune contract, procese verbale	7	1,572.26	11,005.82
<i>TOTAL</i>				<i>22,900.82</i>

- și profitul de 40,637.67 lei (aprox. 17% din valoarea contractului fără TVA).

În plus, contestatoarea arată că toate licențele referențiate în cadrul justificării de preț transmise ca răspuns, includ, cel puțin, numele producătorului, versiunea, ediția, tipul licenței și cantitatea.

De altfel, contestatoarea susține că nu s-au primit solicitări de clarificare referitoare la sistemul de operare pe care va fi instalată soluția *Cuckoo Sandbox* și nici nu există o astfel de cerință în documentația de atribuire. Componentele amintite de autoritatea contractantă: API pentru scanare antivirus de la VirusTotal, tcpdump, cybox, MAEC, DiStorm (utilizat de Volatility) sunt componente/module ale soluției oferite, ele nu sunt module oferite separat, ci sunt parte din Soluția oferită sau utilitare ale sistemului de operare. Soluția oferită include toate elementele listate de ofertant în formularul 14 - Formular Inventar de Complet, elemente cu caracter de produs, care răspund la cerințele documentației de atribuire și care au fost detaliate în urma solicitărilor de clarificare nr. A3/3399 din 03.07.2015 și nr. A3/3267 din 26.06.2015. Răspunsurile ofertantului la cerințele documentației de atribuire referă diverse module ale soluției/ produsului oferit - și au fost scrise la nivelul de detaliu solicitat (fie prin linkuri, fie prin detalieri, fie prin exemplificări) tocmai pentru a arăta că soluția oferită îndeplinește cerința documentației de atribuire.

În acest context, contestatoarea consideră tendențioasă afirmația autorității contractante conform căreia există „componente care necesită a fi integrate în acesta (Cuckoo Sandbox) pentru a răspunde la cerințele din specificația tehnică”.

De asemenea, afirmația autorității contractante potrivit căreia „Componenta Cuckoo Sandbox dispune de licența de tip GNU GPL 3 și, conform acesteia, după instalarea la beneficiar și integrarea cu alte produse, nu se mai garantează nici un fel de suport sau actualizare pentru componenta instalată. Cu alte cuvinte, nu se pot menține toate funcționalitățile solicitate (...)” este, în opinia contestatoarei, falsă și este

extrasă din contextul termenilor de licențiere GNU GPL 3, care se traduc, în mod corect, astfel:

„Un produs recipient (User Product) este fie un produs de consum, care reprezintă orice proprietate personală tangibilă care este normal utilizată în scop personal, de familie, sau de cămin/casă, sau orice proiectat sau vândut pentru incorporarea într-o locuință”.

„Cerința de a oferi informații de instalare nu include cerința de a continua să se ofere servicii de suport, garanție sau actualizări pentru o lucrare care a fost modificată sau instalată de client sau pentru produsul recipient în care s-a modificat sau instalat”.

Astfel, termenii de licențiere referențiați de autoritatea contractantă conțin afirmații de tip disclaimer pentru cazurile în care produsul este instalat sau modificat pentru integrarea într-o locuință sau orice alt produs de consum. Acesta nu este cazul prezentei documentației de atribuire și a ofertei depuse.

Totodată, contestatoarea susține că afirmația autorității contractante, potrivit căreia, „Ofertantul nu a specificat, pentru fiecare component sau, dacă este cazul, pentru toată Soluția oferată, tipul de licență, nerăspunzând cererii de clarificare solicitată (...)”, este falsă.

În acest sens, contestatoarea reiterează răspunsurile la solicitările de clarificări nr. A3/4377 din 14.08.2015, nr. A3/3399 din 03.07.2015 și nr. A3/3267 din 26.06.2015 - din care reies în mod concret și detaliat tipul de licență pentru toate componentele ofertei:

- extras din clarificarea nr. A3/4377/14.08.2015 - „(...) ofertantul a inclus în propunerea tehnică și financiară, după cum se vede atât în formularul inventar de complet, cât și în justificarea de preț transmisă ca răspuns la solicitarea de clarificări nr. A3/3267 din 26.06.2015, licențe pentru sistemele de operare Windows, cu diverse versiuni și variante de aplicații software instalate - așa cum a fost solicitat în cadrul documentației de atribuire”.

În continuare, contestatoarea arată că, potrivit documentației de atribuire - cerința 3.1.1.1, „Soluția conține o serie de mașini virtuale preinstalate, cu versiuni ale sistemelor de operare Microsoft Windows XP, Vista, 7, 8 și Android”.

Legat de această cerință, contestatoarea arată că afirmația autorității contractante potrivit căreia „Nu s-a specificat ce tip de licență au sistemele de operare Microsoft astfel încât nu se poate stabili dacă licența suportă downgrade la Windows XP” este falsă.

Or, prin licența oferată, producătorul Microsoft permite downgrade-ul la versiuni anterioare - precum XP - aceasta fiind unica modalitate de achiziție legală și conformă cu regulamentul Microsoft pentru instalarea sistemului de operare Microsoft Windows XP. Astfel, oferta tehnică depusă este 100% conformă.

Contestatoarea susține că a inclus, precum se vede în centralizatorul de produse, toate licențele solicitate, și tipul de licență oferat (așa cum sunt ele achiziționate - a se vedea și anexele - oferte furnizori transmise ca răspuns la clarificarea nr. A3/3267 din 26.06.2015).

1	Platformă analiză malware	Soluția conține o serie de mașini virtuale, preinstalate cu versiuni ale sistemului de operare Microsoft Windows XP, Vista, 7, 8 și Android	Da	Soluția propusa conține o serie de mașini virtuale, preinstalate cu versiuni ale sistemului de operare Microsoft Windows XP, Vista, 7,8 și Android
---	---------------------------	---	----	--

Referitor la cerința 3.1.1.4 potrivit căreia „Furnizorul soluției va pune la dispoziție licențele sistemelor de operare și aplicațiilor comerciale din cadrul mașinilor virtuale preinstalate/preconfigurate”, precum și la afirmația autorității contractante potrivit căreia „Ofertantul nu a răspuns cererii de clarificare nr. A3/4377/14.08.2015, conform căreia trebuia să se facă un tabel cu mașinile virtuale conținute în soluție din care să reiasă ce sisteme de operare și ce aplicații sunt instalate”, contestatoarea susține că a răspuns clarificării nr. A3/4377/14.08.2015.

Contestatoarea precizează că Windows XP este versiunea de sistem de operare rezultat în urma downgrade-ului, care se poate obține la cererea Beneficiarului, precum și-a asumat prin oferta tehnică și precum permit regulile producătorului Microsoft.

La întrebarea nr. 7 din adresa nr. A3/4377/14.08.2015 (Clarificări cu privire la mașinile virtuale emulate în cadrul soluției oferite prin transmiterea unui tabel centralizat cu mașinile virtuale preinstalate care vor fi furnizate în cadrul soluției oferite, inclusiv licențele pentru sistemele de operare ce vor fi instalate acestora și cele ale aplicațiilor software conform cerinței tehnice), contestatoarea arată că a indicat răspunsul de la întrebarea 1. Oferta include soluția virtualizare Microsoft VDI, cu ajutorul căreia se pot configura mașinile virtuale, așa cum au fost solicitate în caietul de sarcini.

VM1 (virtual machine 1)	Sistem de operare: Windows 7 SP1
VM2	Sistem de operare: Windows 7 SP2
VM3	Sistem de operare: Windows 8
VM4	Sistem de operare: Windows 8.1
VM5 (opțional)	Sistem de operare: Android 5.0

De asemenea, contestatoarea susține că a răspuns solicitării referitoare la cerința 3.1.2.6. (întrebarea nr. 8 din solicitarea nr. A3/4377/14.08.2015), precizând că adresa de Internet furnizată ca exemplu avea rolul unic de a demonstra, pe un studiu de caz real, modul în care *Cuckoo Sandbox* identifică programele malițioase care încearcă să determine incidența instrumentelor de analiză asupra codului lor, mașinile virtuale sau programele de tip debugger. Astfel de studii de caz real nu fac parte din documentația produsului, cel mult - documentația produsului oferă exemple minimaliste. S-a oferit acest studiu de caz



pentru a se verifica capabilitatea soluției oferite de a îndeplini cerința. În plus, dezvoltatorii soluției *Cuckoo Sandbox* pun la dispoziția comunității un exemplu de analiză asupra executabilului pafish.exe.

Astfel, la întrebarea nr. 8 (*Argumentați modul în care soluția realizează analiza malware în cazul unor aplicații malițioase care prezintă mecanisme de detecție și prevenire a rulării în cadrul unor medii virtualizate*), contestatoarea arată că a formulat următorul răspuns: „Menționăm că hyperlink-ul oferit (<https://www.alienvault.com/open-threat-exchange/blog/hardening-cuckoo-sandbox-against-vm-aware-malware>) referă un blog personal al unui dezvoltator *Alien Vault*, nu face referință deloc la produsul *Alien Vault*, și are rolul unic de a exemplifica modul în care *Cuckoo Sandbox* poate fi folosit cu succes în analiza codului malițios care detectează tehnicile de analiză prin identificarea mașinilor virtuale.

Astfel, se poate consulta codul prin care, soluția utilizată - *Cuckoo* - identifică mediul virtualizat - VirtualBox:

```
[pafish] Start  
[pafish] Windows version: 5.1 build 2600  
[pafish] Sandbox traced using mouse activity
```

.....

```
C:\WINDOWS\system32\driversWBoxMouse.sys
```

```
[pafish] End - See more at: https://www.alienvault.com/open-threat-exchange/blog/hardening-cuckoo-sandbox-against-vm-aware-malware#sthash.rozGPGkQ.dpuf
```

Pentru a monitoriza activitatea malware, Cuckoo execută proba cu cuckoomon, partea responsabilă a sistemului de interceptare apeluri pentru a salva acțiunile malware. Cu acest sistem de interceptare, se pot modifica apelurile să întoarcă răspunsuri false, de exemplu pentru a verifica apelurile fișiere/cheile de registry/procese pentru a detecta VM.

Potrivit analizei asupra acestui fișier, al cărui raport există la adresa <https://malwr.com/analysis/NTIYigyM2IxNzk3NDI3YikvYzNkN2Y3NGEINW FmZjE/>, Cuckoo Sandbox identifică programele care încearcă să identifice mediul virtualizat”.

Contestatoarea reiterează faptul că <https://malwr.com> este o platformă online pusă la dispoziția comunității de către dezvoltatorii soluției *Cuckoo Sandbox*, pentru a facilita analiza mostrelor de malware și pentru a exemplifica livrabilele unei analize cu *Cuckoo Sandbox*.

Referitor la cerința 3.1.4. și la concluzia autorității contractante, potrivit căreia, „Ofertantul nu a răspuns cererii de clarificare (întrebarea nr. 10 din solicitarea nr. A3/4377/14.08.2015) și a furnizat o documentație de exemplificare de pe un blog personal (...)”, contestatoarea învederează că a răspuns solicitării de clarificare.

Astfel, la întrebarea nr. 10 (*Clarificări cu privire la mecanismele de identificare, extragere și analiză în profunzime a fișierelor injectate în memoria fizică a unui SIC, instalate și configurate în cadrul soluției oferite*), a formulat următorul răspuns: „Hyperlinkul oferit ca referință la adresa <http://kromer.pl/malware-analysis/memory-forensics-using-volatility-toolkit-to-extract-malware-samples-from-memory-dump/>, are



rolul de a exemplifica metodologia prin care Volatility poate fi folosit pentru a identifica, extrage și analiza în profunzime cod injectat în memoria unui SIC, începând de la secțiunea „Analyzing memory dump”. Am optat pentru a referi direct hyperlink-ul cu metodologia aferentă din considerente de spațiu, fiind un proces destul de complex. Menționăm că salvarea memoriei într-un fișier este realizată de Cuckoo Sandbox, iar analiza fișierului este realizată prin integrarea cu Volatility”.

Contestatoarea precizează că fișierele nu pot fi injectate în memorie, un fișier nefiind decât un format agreat, în care datele sau codul sunt stocate într-un sistem de fișiere, pe hard-disk. Încărcarea în memorie a unui cod malițios se realizează fie prin încărcarea directă, prin execuția fișierului, care creează un proces în memorie, fie prin injectarea codului malițios în procesul din memorie aferent unui fișier executabil.

În oricare dintre cele două cazuri, *Cuckoo Sandbox*, prin integrarea cu *Volatility*, permite analiza în detaliu a codului malițios injectat în memorie.

În continuare, contestatoarea procedează la descrierea pașilor ce trebuie urmați în vederea analizei unui cod malițios injectat în memorie:

1. Se realizează o captură a memoriei
2. Se pornește Volatility  
\$ emerge -av app-forensics/volatility
3. Se identifica profilul (sistemul de operare) memoriei analizate  
\$ volatility -f/path/to/MEMORY.DMP imageinfo
4. Se setează profilul pentru analiză  
\$ export VOLATILITY\_PROFILE=WinXPSP3x86  
\$ export VOLATILITY\_LOCATION=file:///path/to/MEMORY.DMP
5. Se realizează listarea tuturor proceselor  
\$ volatility psxview
6. Pentru fiecare proces se analizează:
  - parent  
\$ volatility pstree
  - parent lipsă  
\$ volatility psscan
  - conexiuni de rețea  
\$ volatility connscan
  - cod injectat în procesul din memorie, prin intermediul plugin-ului malfînd  
\$ volatility malfmd -D /path/to/dump/dir

Referitor la cerința 3.1.5., potrivit căreia, „deține module de identificare a algoritmilor de criptare sau extragere a cheilor asociate pornind de la încărcarea de pachete criptate, având posibilitatea de a selecta un fișier sau un grup de fișiere criptate cu aceeași metodă”, precum și la concluzia autorității contractante, potrivit căreia, „D/V/ analiza documentației componenteii Cuckoo Sandbox dată ca referință la răspunsul la întrebarea 11 din solicitarea nr. A4/4377/14.08.2015 rezultă că Soluția nu corespunde cerinței”, contestatoarea precizează că aplicarea unor elemente de identificare în cadrul datelor criptate ar

contraveni flagrant cu scopul intrinsec al criptării, și anume, acela de a transforma datele dintr-un format inteligibil, într-unul neinteligibil, fără elemente de identificare, astfel încât conținutul să pară generat aleator.

În ciuda acestui fapt, soluția propusă pune la dispoziția analistului toate instrumentele necesare pentru identificarea cheilor de criptare (ca prim pas în identificarea algoritmului de criptare) și pentru identificarea algoritmilor de criptare, folosiți pentru a cripta un fișier, sau un grup de fișiere, însă această analiză nu poate fi automatizată, fiind un proces ce ține de experiență și intuiția analistului.

În acest sens, contestatoarea reiterează răspunsul său la întrebarea nr. 11 din solicitarea de clarificare nr. A4/4377/14.08.2015 (Clarificări cu privire la modulul integrat în soluția ofertată care poate răspunde cerinței prin furnizarea documentației aferente), potrivit căruia „Criptarea este procesul de conversie a informației obișnuite (text în clar) într-un text neinteligibil, printr-un algoritm, folosind o cheie. Având în vedere că rolul criptării este acela de a disimula informația astfel încât aceasta să pară un text neinteligibil, și să fie accesibilă doar celui care cunoaște algoritmul și se află în posesia cheii de criptare, munca de criptanaliză nu poate fi realizată în mod automat, fiind necesară o metodologie similară cu cea descrisă în hyperlink-ul furnizat, deoarece în special creatorii de programe malițioase preferă să ascundă sau să elimine elementele identificatoare ale algoritmului de criptare folosit, primul pas în identificarea algoritmului de criptare folosit fiind identificarea cheilor de criptare și tipul acestora.

De altfel, activitatea de criptanaliză este un proces îndelungat și senzitiv ce nu poate fi lăsat pe seama unui proces automat, fiind implicate intuiția, experiența și flerul criptanalistului.

De asemenea, pachetele de trafic, dacă la ele face referire autoritatea contractantă, nu conțin cheile folosite în criptarea traficului, acestea găsindu-se doar pe cele două capete ale canalului de comunicație folosit.

*Cuckoo Sandbox* permite identificarea tipului de criptare folosit în cadrul programelor prin interceptarea apelurilor către Crypto API prezent în Windows (<http://cuckoosandbox.org/2015-03-04-cuckoo-sandbox-12.htmrAdded> Microsoft Crypto API hooks).

Raportându-se la cerințele 3.1.6.1.3, 3.1.6.2.2, 3.1.6.2.11, 3.1.6.2.12, 3.1.6.2.15, 3.1.6.3, contestatoarea arată că, deși a prezentat un exemplu de raport de analiză malware asupra unui fișier suspect, pe site-ul dezvoltat de către echipa Cuckoo Sandbox, autoritatea contractantă refuză să ia în considerare acest aspect evident.

Astfel, conform declarației de producător, prezentă la adresa <http://cuckoosandbox.org/2013-03-14-malwr-reloaded.html>, paragraful „(...) We launched Malwr in January 2012 and we got huge response from our users and it steadily grew to be one of the prevalent online malware analysis service. If you're not familiar with it, it basically consist in a live Cuckoo Sandbox instance with a friendly interface that allows you to leverage the collected data and the contributions from the rest of the community. (...)”, în traducere „Am lansat Malwr în Ianuarie 2012 și

am primit un răspuns covârșitor din partea utilizatorilor noștri, iar în timp a devenit unul dintre serviciile prevalente de analiză malware online. Dacă nu ești familiarizat cu acest serviciu, este pur și simplu o instanță live de Cuckoo Sandbox cu o interfață prietenoasă care permite integrarea datelor și contribuțiilor de la restul comunității”.

În lumina acestei traduceri, instanța live de *Cuckoo Sandbox*, care este motorul de analiză al serviciului <https://malwr.com>, nu este o instalare specială sau diferită față de soluția pusă la dispoziția publicului. Sistemul de operare pe care rulează *Cuckoo Sandbox* poate fi orice distribuție recentă de Linux, utilitarul tcpdump, fiind parte integrantă din majoritatea distribuțiilor existente. Or, integrarea dintre cele două se realizează nativ, *Cuckoo Sandbox* preluând rezultate provenind de la tcpdump.

Referitor la cerința 3.2.1, precum și la concluzia autorității contractante, potrivit căreia, „Ofertantul nu a răspuns întrebării nr. 18 din solicitarea de clarificări nr. A3/4377/14.08.2015 și nu a înțeles ce trebuie să facă Soluția, deși autoritatea contractantă a specificat exact că Soluția oferită trebuie să aibă capacitatea de a se integra și a prelua malware, eventual de la alte soluții de Securitate, pe care să-l analizeze automat, fără intervenția utilizatorilor”, contestatoarea susține că nu există în cadrul documentației de atribuire cerința ca „Soluția oferită trebuie să aibă capacitatea de a se integra și a prelua malware, eventual de la alte soluții de Securitate, pe care să-l analizeze automat, fără intervenția utilizatorilor”.

Capacitatea de analiză		DA		
	În două moduri : Live mode și sandbox;		în două moduri: live mode și sandbox;	
	Mini m 8200 analize/zi		10368 analize/ zi (72 de instante x 6/h x 24h , considerând că o analiză durează max 10 min) Propunem ca suport hardware serverul <b>HP</b>	<a href="http://www8.hp.com/h20195/v2/GetDocument.a?spx?docname=c04375627">http://www8.hp.com/h20195/v2/GetDocument.a?spx?docname=c04375627</a>

			DL380 Gen9, mașină performantă de ultimă generație. Pentru fiecare instanță se va configura o mașină virtuală cu 0,5 vCPU core, 4 GB RAM, 40 GB spațiu de stocare pe disc). Am ales un procesor de ultimă generație Intel E5-2699v3 , 2,3 GHz, 35 MB cache cu 18 core/CP U. Se vor configura 320 GB RAM (mai mult decât 4 GB x 72 instanțe paralele = 288 GB RAM) și 4 discuri SAS de 1 TB configurate RAID 5 (3 TB util) adică mai mult de 72 instanțe x 40 GB disc = 2,88 TB	
--	--	--	--	--

Analiza locală a formatelor consacrate de fișiere malițioase	DA	Analiza locală a formatelor consacrate de fișiere malițioase	<a href="https://malwr.com/analysis/MGUONWE1MzkvZTImNDIIM2ZiZhMWE3MmZiZmJhODE/share/b2ddca548aaa42c6be19fee7fb7c4d72">https://malwr.com/analysis/MGUONWE1MzkvZTImNDIIM2ZiZhMWE3MmZiZmJhODE/share/b2ddca548aaa42c6be19fee7fb7c4d72</a>
--	----	--	---

Astfel, la întrebarea nr. 18 („Prezentați, argumentat, modul în care soluția furnizată realizează analiza malware în mod live, în timp real”), contestatoarea arată că a formulat următorul răspuns: „Autoritatea contractantă face confuzie între tehnologiile de tip „detectare/prevenire intruziuni” și o platformă de analiză malware. Astfel, pentru a clarifica eroarea autorității e necesar să explicăm că tehnologiile de detectare și prevenire a intruziunilor analizează traficul de rețea prin scanarea unor semnături de atacuri cunoscute, în timp ce o platformă de analiză malware presupune un spectru larg de analize ce nu pot fi realizate în timp real, dacă sintagma „în timp real” presupune analiza traficului fără blocarea acestuia. Din acest punct de vedere o platformă de analiză malware este mai asemănătoare cu un program antivirus decât cu un senzor de detecție a intruziunilor.

O platformă de analiză malware realizează interceptarea traficului de rețea generat de un program malițios, asigurată de *Cuckoo Sandbox*, prin intermediul capturilor de trafic realizate de *Tcpdump*, prin intermediul capabilității de sniffer, descrisă la adresa [http://docs.cuckoosandbox.org/en/0.3/installation/host\\_configuration/Secțiunea "Sniffer"](http://docs.cuckoosandbox.org/en/0.3/installation/host_configuration/Secțiunea%20Sniffer). Interceptarea traficului se poate face fie direct, prin intermediul mașinii virtuale, fie prin integrarea cu utilitarul *Tcpdump*.

De asemenea, contestatoarea prezintă și punctul său de vedere din clarificarea înaintată la 14.07.2015.

În referire la cerința 3.5.2 potrivit căreia „Toate serviciile privind mentenanța vor fi efectuate de către persoane autorizate de către proprietarul mărcii produselor pentru care se efectuează serviciile respective”, contestatoarea susține că și-a asumat îndeplinirea cerinței. Software-ul open-source reprezintă un tip de software/aplicații unde reglementarea liberei distribuiri se face de către producătorul acestuia.

Dreptul de licență pentru software open-source există și se transmite, în termeni legali, către Beneficiarul final, așa cum ofertantul a ilustrat în Formularul Inventar de Complet. Software-ul open-source nu implică costuri de achiziție, dar reprezintă o licență software. Autorizarea mărcii produsului solicitată provine din cursurile specializate ale producătorului software-ului open-source la care Ofertantul va participa pentru îndeplinirea obligațiilor contractuale în cazul acceptării ofertei tehnice depuse și semnării unui contract cu Beneficiarul.

De altfel, solicitarea de documente de eligibilitate prin caietul de sarcini, fără ca acestea să fie incluse în fișa de date a achiziției, contravine legislației din domeniu, fiind considerate clauze nescrise.

Totodată, contestatoarea reiterează răspunsul la întrebarea nr. 21 din solicitarea de clarificare nr. A3/3399/ 03.07.2015 (Transmiteți documentele doveditoare existenței a cel puțin unui specialist care are autorizarea necesară pentru realizarea instalării și mentenanței soluției oferite, care să conțină și cursurile de certificare/autorizare specific soluției la care acesta a participat sau este înscris) potrivit căruia „Oferta depusă conține toate informațiile solicitate prin documentația de atribuire, atât din perspectiva eligibilității și a documentelor doveditoare, cât și din perspectiva tehnică, prin propunerea tehnică depusă”.

Indiferent de caracterul open-source al soluțiilor, acestea oferă training specializat, ca și modalitate de certificare/autorizare a personalului - <http://www.memoryanalysis.net/#!memory-forensics-training/clq3n>.

În plus, în cazul în care oferta va fi declarată câștigătoare, expertul va lua parte la trainingul din 31 august din Amsterdam.

De altfel, contestatoarea arată că a prezentat strategia de certificare a personalului pentru produsul *Volatility*, pentru că dezvoltatorii *Cuckoo Sandbox* nu organizează astfel de cursuri.

Strict raportându-ne la cerințele documentației de atribuire, atât privind eligibilitatea - experții solicitați prin fișa de date, cât și caietul de sarcini - contestatoarea menționează că a inclus prin oferta sa toate elementele necesare desfășurării contractului precum a fost solicitat prin documentația de atribuire.

Referitor la cerința 3.5.3, precum și la concluzia autorității contractante potrivit căreia „răspunsul la solicitarea de clarificări nr. A3/4377/14/08/2015 - nu este conform cu cerința, ofertantul nu a luat în considerare cererea de clarificare formulată de autoritatea contractantă. Ofertantul nu înțelege că Soluția oferită trebuie să fie completă, să răspundă cerințelor ca întreg, nu pe componente”, contestatoarea precizează că nu există nicăieri în documentația de atribuire cerința potrivit căreia „Soluția oferită trebuie să fie completă, să răspundă cerințelor ca întreg, nu pe componente”.

Or, soluția oferită este enumerată și detaliată prin Formularul nr. 14 - Inventar de complet. Orice afirmație diferită, cum că Soluția ar conține alte componente precum: *VirusTotal*, *Mitmproxy*, *DiStorm* etc. este falsă.

Contestatoarea susține că a inclus în propunerea sa tehnică servicii de suport tehnic permanent. Având în vedere software-ul open-source oferat, accesul online, permanent, la baza de date a producătorului soluției este gratuit; la fel și actualizările pentru software - acestea fiind disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului de software open-source; accesul la suport on-line permanent, prin intermediul unui portal pus la dispoziție în internet și prin email - este inclus din partea ofertantului și este asigurat de producătorul aplicațiilor open-source, pe site-urile web oficiale; suportul telefonic și on-site la sediul Beneficiarului este asigurat de ofertant.

Faptul că dezvoltatorii aplicațiilor open-source oferă suport doar pentru modulele proprii nu și pentru problemele apărute la integrarea și la comunicarea cu alte module este parțial adevărat și este valabil și pentru producătorii de software comercial. De aceea, ofertantul este cel responsabil de asigurarea suportului, prin relația contractuală cu Beneficiarul. Dezvoltatorii aplicațiilor open-source nu au o relație contractuală cu Beneficiarul.

Referitor la cerința 3.13.1 (Componentele produsului trebuie să fie garantate de furnizor prin certificate de calitate și garanție emise de organul abilitat al acestuia), contestatoarea arată că componentele produselor oferate, care se regăsesc atât în oferta tehnică cât și în formularul Inventar de Complet, sunt garantate de furnizor prin certificate de calitate și garanție emise de organul abilitat al acestuia. Software-ul open source este software COTS (commercial off the shelf) și este garantat de producător. Or, nicăieri în documentația de atribuire nu a fost menționat că sunt inacceptabile oferte ce propun produse open-source.

De altfel, ofertantul, prin relația contractuală cu Beneficiarul, se angajează și garantează produsele oferate prin certificate de calitate și garanție, după caz, și va asigura suportul tehnic pentru acestea, în conformitate cu oferta sa tehnică și cerințele documentației de atribuire.

Disclaimerele dezvoltatorilor de soluții open-source se referă la cazurile în care soluțiile sunt instalate, modificate, integrate și, astfel, devine responsabilitatea integratorului de a asigura funcționarea soluțiilor integrate, întrucât dezvoltatorii nu pot să garanteze funcționarea soluției, deoarece nu cunosc în întregime mediul în care acestea se instalează, integrează sau modifică.

În plus, nicăieri în documentația de atribuire nu s-a solicitat suport direct de la producătorul soluțiilor software.

În ceea ce privește cerința 3.14.1 („Ofertanții vor pune la dispoziție pachete de informații complete ale componentelor produsului. Specificațiile tehnice și de calitate ale componentelor oferite trebuie, obligatoriu, susținute de documentații originale: prospecte, foi de catalog, documentații tehnice descărcate de pe site-urile producătorilor. Declarațiile nesusținute de documentații originale nu vor fi luate în considerare, conducând la eliminarea ofertei”), contestatoarea precizează că oferta sa a inclus pachete de informații complete ale



componentelor produsului. Specificațiile tehnice și de calitate ale componentelor oferite sunt însoțite de documentațiile originale: prospecte, foi de catalog, documentații tehnice descărcate de pe site-urile producătorilor și hyperlink-uri de pe site-urile web oficiale ale producătorilor, după caz.

De altfel, nu există nicăieri în documentația de atribuire cerința potrivit căreia „Soluția oferită trebuie să fie completă, să răspundă cerințelor ca întreg, nu pe componente”.

De asemenea, solicitările de clarificări cu privire la capabilitatea soluției de îndeplinire a anumitor cerințe au avut ca scop clarificarea sau detalierea modalității prin care soluțiile oferite îndeplinesc cerințele documentației de atribuire. Pe lângă documentațiile tehnice originale - descărcate sau referențiate de pe site-urile dezvoltatorilor/producătorilor soluțiilor oferite - au fost utilizate în cadrul răspunsurilor link-uri adiționale terțe, forum-uri de specialitate, blog-uri de specialitate - pentru a ajuta autoritatea contractantă, inclusiv prin studii de caz complexe, imposibil de găsit în orice documentație producător (fie el open-source sau software comercial), acestea fiind disponibile pe bloguri de specialitate.

Oferta tehnică depusă include documentații tehnice originale - descărcate de pe site-urile producătorilor.

Exemple din oferta tehnică:

<http://docs.cuckoosandbox.org/en/latest/>

<http://www.volatilityfoundation.org/>

<http://www8.hp.com>

Pe de altă parte, în ceea ce privește decizia autorității contractante de anulare a procedurii pentru lotul 2, contestatoarea apreciază că, în conformitate cu dispozițiile art. 181. lit. a), art. 64 alin. (2) lit. a), art. 79 alin. (2) lit. a), art. 94 alin. (2) lit. a) și ale art. 114 lit. a) din OUG nr. 114/2011, aceasta este abuzivă și nefundamentată.

Prin adresa nr. 4927/10.09.2015, înregistrată la CNSC sub nr. 17483/10.09.2015, autoritatea contractantă a transmis Consiliului punctul de vedere la contestație, solicitând respingerea acesteia, ca nefondată.

Având în vedere Decizia CNSC nr. 1268/C2/1354 din 06.08.2015, precum și răspunsurile la solicitările de clarificări nr. A3/4377 din 14.08.2015 și nr. A3/4490 din 20.08.2015, autoritatea contractantă arată că membrii comisiei de evaluare au considerat că propunerea tehnică aparținând SC ... SRL nu îndeplinește cerințele nr. 1.1.2, 3.1.1.1., 3.1.1.4, 3.1.2.6, 3.1.4., 3.1.5., 3.1.6.1.3, 3.1.6.2.2, 3.1.6.2.11, 3.1.6.2.12, 3.1.6.2.15, 3.1.6.3, 3.2.1, 3.5.2, 3.5.3, 3.13.1, 3.14.1 din caietul de sarcini.

Astfel, autoritatea contractantă precizează că prin Cerința 1.1.2. a solicitat ofertanților ca „Soluția va include toate componentele hardware, de ultimă generație, și licențele software necesare menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice investigate prin prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora în perioada de

viață a soluției oferite (până la declararea acesteia de producător ca fiind „end of support”).

Analizând răspunsurile furnizate la solicitările de clarificare, autoritatea contractantă apreciază că autoarea contestației refuză să înțeleagă conținutul cerinței prin care se solicită explicit o soluție care va include toate componentele hardware și licențele software utilizabile până la declararea de producător ca fiind „end of support”.

De altfel, autoritatea contractantă arată că afirmația contestatoarei potrivit căreia „documentația de atribuire nu conține nicăieri o cerință care să impună ca soluția oferită trebuie să fie o platformă dedicată cu suport oferit de un producător” este falsă și nu respectă prevederile cerinței sus menționate.

Mai mult, contestatoarea este într-o mare eroare cu privire la componentele minime necesare funcționării soluției oferite astfel că, pentru îndeplinirea funcționalităților solicitate, sunt necesare: o platformă hardware pe care să fie instalat un sistem de operare ce va fi utilizat ca bază pentru integrarea soluțiilor software propuse: Cuckoo Sandbox și Volatility, o astfel de licență (pentru sistemul de operare) nefiind inclusă de ofertant în formularul 14, Formular inventar de complet. Contestatoarea este subiectivă și interpretează abuziv conținutul solicitării de clarificări din partea autorității contractante pentru sistemul de operare utilizat ca bază de soluția oferită. Mai mult, în răspunsul transmis sub nr. 338 din 19.08.2015, la solicitarea de clarificări a autorității contractante (întrebarea nr. 3), pentru serverul HP DL380 GEN9, ofertantul a menționat explicit că tipul de licență este: N/A (Not applicable).

În consecință, autoritatea contractantă susține că, prin ofertă, nu se asigură licențe pentru toate produsele software necesare funcționării produsului, în conformitate cu prevederile cerinței.

Referitor la licențiere, contestatoarea încearcă, în opinia autorității contractante, să dezinformeze cu privire la modul de interpretare a prevederilor licenței de tip GNU GPL 3, unde se prezintă explicit că după instalarea la beneficiar și integrarea Cuckoo Sandbox cu alte produse nu se mai garantează niciun fel de suport sau actualizare pentru componentele instalate. Afirmația contestatoarei potrivit căreia soluția propusă nu se regăsește în condițiile menționate anterior este eronată întrucât *Cuckoo Sandbox* și *Volatility* sunt 2 aplicații diferite care trebuie integrate pentru funcționare cu alte pachete/aplicații furnizate de terțe persoane. Astfel, este evident că în momentul apariției unei noi versiuni de *Cuckoo Sandbox*, terțele aplicații utilizate nu vor mai fi compatibile cu versiunea curentă.

Mai mult, în justificarea prețului pentru componentele lotului 2, contestatoarea nu reușește să facă diferență între produsele/componentele aferente fiecărui lot pentru care a depus oferte, astfel că în prezenta contestație apar informații specifice altor oferte tehnice diferite de oferta prezentului lot.

Referitor la licențele solicitate necesare pentru buna funcționare a aplicațiilor *Cuckoo Sandox* se integrează cu un API (cheie) de Virus Total,

predefinit, pentru a realiza analize statice asupra softului nociv, așa cum se specifică și în cerințele de la punctele 3.1.3, 3.1.4 și 3.1.6.

Pentru analiza statică a unui malware care nu a fost încărcat anterior pe site-ul Virus Total, analiza acestuia nu este posibilă cu varianta de API inclusă în *Cuckoo Sandbox*. Beneficiarul trebuie să încarce manual, pe site-ul acestora, fișierul malware, după care să efectueze analiza din *Cuckoo Sandbox*, ceea ce presupune că folosind API-ul predefinit soluția nu răspunde în totalitate cerinței de a efectua analize statice asupra softului nociv, ci numai în anumite condiții.

Autoritatea contractantă menționează că a pus la dispoziție contestatoarei un extras din fișierele de configurare ale *Cuckoo Sandbox*, solicitând clarificări cu privire la necesitatea existenței unei chei pentru a asigura funcționalitățile din specificație fără restricții:

```
„referință:http://cuckoo.readthedocs.org/en/latest/installation/host  
/configuration/processing.conf [virustotal]
```

```
enabled = yes
```

```
# Add your VirusTotal API key here. The default API key, kindly  
provided
```

```
# by the VirusTotal team, should enable you with a sufficient  
throughput
```

```
# and while being shared with all our users, it shouldn't affect  
your use.
```

```
key =
```

```
a0283a2...d55728300d064874239b5346fb991317e8449fe43c902879d75  
8088
```

VirusTotal (modules/processing/virustotal.py) - searches on VirusTotal.com for antivirus signatures of the analyzed file. Note: the file is not uploaded on VirusTotal.com, if the file was not previously uploaded on the website no results will be retrieved."

Or, contestatoarea a refuzat să răspundă solicitării de clarificări, susținând că solicitarea nu se aplică în cazul ofertei depuse, afirmație falsă și în contradicție cu motivația sa din prima contestație depusă, cu privire la modul de îndeplinire a cerinței 3.1.3 : „(...) după cum se poate vedea (...) se identifică în mod clar modulul de procesare Virus Total”.

În ceea ce privește cerința 3.1.1 potrivit căreia „Soluția să fie flexibilă și să emuleze, în medii sterile, cel puțin următoarele sisteme de operare: Windows 7 SP1/2, Windows 8/8.1, cu diverse versiuni și variante de aplicații software instalate, în vederea desfășurării de analize informatice a mostrelor de malware”, detaliată prin cerința 3.1.1.1 potrivit căreia „soluția conține o serie de mașini virtuale, preinstalate cu versiuni ale sistemului de operare Microsoft Windows XP, Vista, 7, 8 și Android”, precum și cerința 3.1.1.4 potrivit căreia „Furnizorul soluției va pune la dispoziție licențele sistemelor de operare și aplicațiilor comerciale din cadrul mașinilor virtuale preinstalate/preconfigurate”, autoritatea contractantă precizează că, în oferta tehnică și răspunsul la solicitarea de clarificări nr. A3/4377 din 14.08.2015, sunt ofertate doar 4 licențe Windows (Windows 7 SP1, Windows 7 SP2, Windows 8 și Windows 8.1).

Astfel, nu sunt respectate cerințele din caietul de sarcini privind licențele aferente mașinilor virtuale cu sistem de operare Windows (7 mașini, pentru care sunt necesare 6 licențe Windows), care să corespundă Windows XP, Vista, 7 SP1 și 7 SP 2, 8 și 8.1. Mai mult, prin cerința 3.1.1, s-a solicitat utilizarea mai multor mașini virtuale, cu diverse variante și versiuni, pentru îndeplinirea acestei cerințe numărul de licențe furnizate fiind semnificativ mai mare de 7.

Având în vedere cerința 3.1.2.6, potrivit căreia, „Are capacitatea de a identifica și rula aplicații malware ce prezintă cod executabil pentru identificarea mediilor virtualizate/emulate”, autoritatea contractantă susține că, prin solicitarea de clarificare, a dorit să se asigure că produsul oferit asigură furnizarea de către ofertant a unor medii de lucru deținute, pentru care se cunoaște arhitectura și componentele utilizate și nu să se facă referințe către un produs prezentat la adresa <http://www.alienvault.com>, care este cu totul alt tip de soluție de securitate, dezvoltată de către o terță parte și care nu are legătură cu soluția oferită.

Autoritatea contractantă menționează că există în administrare o soluție *Cuckoo Sandbox*, în cadrul căreia, fără integrări cu alte soluții sau diverse programe, nu se pot analiza aplicații malware, ce prezintă cod executabil pentru identificarea mediilor virtualizate/emulate.

Astfel, afirmația contestatoarei potrivit căreia „exemplul avea rolul unic de a demonstra pe un studiu de caz real (...)” este falsă și încearcă din nou să avantajeze ofertantul prin selecția de diverse publicații neoficiale. Mai mult, documentația atașată ofertei tehnice trebuie să fie furnizată/elaborată de dezvoltatorii soluției oferite (a se vedea și cerința 3.14.1).

În referire la cerința 3.1.4, potrivit căreia, „Dispune de mecanisme pentru identificarea, extragerea și analiza în profunzime a fișierelor injectate în memoria fizică a unui SIC”, autoritatea contractantă arată că autoarea contestației insistă să afirme că soluția corespunde cerinței, în ciuda faptului că aceasta nu dispune de mecanisme pentru analiza în profunzime a fișierelor (noțiunea de fișier a fost utilizată pentru buna înțelegere a cerinței de către ofertanți și prin care este referit un cod binar) injectate în memoria unui SIC. Ofertantul încearcă să o dezinformeze, prin prezentarea unei variante manuale de realizare a analizei asupra fișierelor și nu înțelege faptul că soluția trebuie să aibă integrat un mecanism care să ofere un raport de analiză a fișierelor/codului binar, fără intervenția operatorului. Din modul de răspuns al contestatoarei se poate deduce că sistemul poate face orice, atât timp cât există un analist cu competențe tehnice ridicate, fapt ce contravine specificației tehnice.

De asemenea, contestatoarea continuă să utilizeze hyperlink-uri, care nu pot fi luate în considerare, întrucât nu aparțin producătorului, și din nou, încearcă să demonstreze că soluția ar dispune de respectivele capacități, dar care nu sunt native și nu pot fi probate prin existența unei configurații de test administrate de ofertant. Procedura indicată de contestatoare presupune descărcarea, instalarea și configurarea de către

beneficiar a unui plugin netestat, pentru care nu există garanția de funcționare și menținere a compatibilității cu soluția oferită sau cu versiuni ulterioare ale acesteia. Mai mult, informațiile oferite în cadrul hyperlink-ului devin incompatibile cu versiunile actualizate ale *Cuckoo Sandbox* și *Volatility*, ca software oferit de o terță parte, sau dezvoltatorul aplicației poate modifica drepturile de utilizare, limitate de impunerea unei licențe, ceea ce din nou contravine specificației tehnice.

Totodată, acest plugin nu a fost inclus în Formularul 14 - Inventarul de Complet al soluției.

Raportat la cerința 3.1.5, potrivit căreia, „Deține module de identificare a algoritmilor de criptare sau extragere a cheilor asociate pornind de la încărcarea de pachete criptate, având posibilitatea de a selecta un fișier sau un grup de fișiere criptate cu aceeași metodă”, autoritatea contractantă apreciază că autoarea contestației încearcă să influențeze decizia Consiliului, prin combaterea nivelului de expertiză și înțelegere al autorității contractante, făcând apel la elemente de bază ale utilizării criptografiei în asigurarea datelor și comunicațiilor, și nu caută să înțeleagă tehnicile uzuale utilizate în analiza de malware și să asigure transpunerea acestora în modul de acțiune al platformei. Mai mult, prin faptul că autoarea contestației propune ca soluție o metodologie de identificare a algoritmilor de criptare sau extragere a cheilor asociate pe care să o realizeze analistul, denotă faptul că acesta nu a înțeles cerința tehnică.

Exprimarea contestatoarei cum că „această analiză nu poate fi automatizată, fiind un proces ce ține de experiența și intuiția analistului” nu îndeplinește cerința, ci confirmă recunoașterea de ofertant că prin soluția propusă nu se poate îndeplini această cerință.

În ceea ce privește cerința 3.1.6.1.3, potrivit căreia, „Aplicații de împachetare utilizate identificate și tipul acestora”, autoritatea contractantă reiterează analiza referințelor menționate și a tuturor aspectelor care oferă siguranță ofertantului de a face referire la o platformă despre care nu se cunoaște modalitatea de instalare și modulele software integrate. Deși contestatoarea afirmă că în cadrul [www.malwr.com](http://www.malwr.com) este instalată o instanță live de Cuckoo, a cărei funcționalitate optimă depinde foarte mult de modul de instalare și de alte plugin-uri necesare, autoritatea contractantă apreciază că, referințele la care se face trimitere, nu dovedesc faptul că soluția îndeplinește cerința sus menționată.

Mai mult, contestatoarea preferă traducerea unor declarații de reclamă ale comunității de dezvoltare a Cuckoo Sandbox în loc să furnizeze informații relevante despre cum este îndeplinită cerința.

Referitor la cerința 3.1.6.2.2: „Modificări aduse la nivelul aplicațiilor instalate pe sistemul de analiză”, autoritatea contractantă susține că ofertantul face declarații despre un pretins abuz al său de a lua în considerare un raport de analiză prezentat. Or, autoritatea contractantă precizează că a luat la cunoștință de existența și conținutul raportului de analiză prezentat însă, având în vedere capacitățile implicite ale platformei *Cuckoo Sandbox*, ce o are la dispoziție, fiind instalată la



nivelul autorității contractante, a solicitat clarificări pentru a se asigura de prezența unor eventuale modificări la nivelul integrării de soluții.

Mai mult, răspunsul oferit nu prezintă modificările aduse la nivelul aplicației și, astfel, la modul de îndeplinire a cerinței, ci face referire la o traducere a unei informații prezentă în spațiul public.

În referire la cerința 3.1.6.2.11: „Detalii despre protocoale de comunicații folosite de malware”, cerința 3.1.6.2.12: „Captură trafic de rețea (fișier PCAP) generat de sistemul de analiză”, precum și la cerința 3.1.6.2.15: „Captură memorie procese suspecte de comportament malițios”, autoritatea contractantă arată că autoarea contestației face referire la capabilități incontestabile ale sistemelor de operare *Linux*, dar uită să menționeze unde este instalat acest sistem de operare *Linux*.

Sistemul de operare *Linux*, sus-menționat, nu face parte din oferta tehnică, nefiind inclus în formularul 14 - Inventarul de complet. Mai mult, pe SERVERUL HP DL380 GEN9, unde ar fi putut fi instalat sistemul de operare *Linux*, contestatoarea a menționat explicit că tipul de licență este N/A (a se vedea cerința 1.1.2).

În acest context, autoritatea contractantă învederează că cerințele nu sunt îndeplinite.

În privința cerinței 3.1.6.3: „Tipul de exploit folosit”, autoritatea contractantă susține că autoarea contestației face declarații despre abuzul autorității contractante de a nu lua în considerare un raport de analiză prezentat.

Or, autoritatea contractantă arată că a luat la cunoștință de existența și conținutul raportului de analiză prezentat însă, având în vedere capacitățile implicite ale platformei Cuckoo Sandbox instalată la nivelul autorității contractante, a solicitat clarificări pentru a se asigura că soluția ofertată prezintă detalii despre tipul de exploit folosit.

Mai mult, răspunsul oferit nu prezintă tipul de exploit folosit și, implicit, modul de îndeplinire a cerinței, ci face referire la o traducere a unei informații prezente în spațiul public.

În referire la cerința 3.2.1: „Capacitatea de analiză”

- a) în două moduri: live mode și sandbox;
- b) Minim 8200 analize/zi;
- c) Analiza locală a formatelor consacrate de fișiere malițioase;
- d) include protocolul SSL,

autoritatea contractantă menționează că cerința nu este abuzivă și face referire la modurile de instalare solicitate la punctul a), live mode și sandbox. Prin definiție, „live mode” reprezintă acea caracteristică ce permite integrarea soluției la nivel de rețea și analiza automată a datelor/fișierelor extrase din traficul de rețea. Pentru buna înțelegere, autoritatea contractantă a prezentat contestatoarei un model similar de funcționare, cel al soluțiilor de tip *Intrusion Detection Systems*, care realizează inspectarea în timp real a traficului de rețea, paralelă pe care aceasta nu a avut capacitatea tehnică de a o înțelege.

Contestatoarea nu a răspuns cererii de clarificare și nu a înțeles ce trebuie să facă soluția, deși beneficiarul a specificat, fără echivoc, că soluția oferită trebuie să aibă capacitatea de a se integra și a prelua



malware, eventual de la alte soluții de securitate, pe care să-l analizeze automat, fără intervenția utilizatorilor, capacitate disponibilă la toate soluțiile de analiză malware dedicate. Mai mult, contestatoarea insistă în capacitățile platformei de *Sandbox* și evită răspunsul concret la modul de instalare „live mode” (datorită limitărilor impuse de integrarea de soluții ofertate).

Mai mult, autoritatea contractantă a solicitat modul de calcul utilizat pentru dovada efectuării numărului de analize/zi, pe baza unui studiu realizat în urma unor teste efectuate pe platforma oferită. Acest studiu nefiind furnizat, cerința nu a fost neîndeplinită.

În ceea ce privește cerința 3.5.2, potrivit căreia, „Toate serviciile privind mentenanța vor fi efectuate de către persoane autorizate de către proprietarul mărcii produselor pentru care se efectuează serviciile respective”, autoritatea contractantă precizează că ofertantul nu a făcut dovada faptului că dispune de personal autorizat, conform cerinței tehnice, pentru a asigura serviciile de mentenanță, considerând că în cazul acceptării ofertei tehnice depuse va participa la cursuri specializate ale producătorului software-ului open-source. Totodată, ofertantul menționează în contestația depusă faptul că „(...) dezvoltatorii *Cuckoo Sandbox* nu organizează astfel de cursuri”.

Afirmațiile contestatoarei, privind lipsa de personal specializat, contravin cerinței 3.3.1, prin care ofertantul trebuie să realizeze servicii de instalare și configurare pentru soluția ofertată.

În continuare, autoritatea contractantă arată că, prin cerința 3.5.3., a solicitat ca „Furnizorul să ofere servicii de suport tehnic permanent, pe toată durata de viață a produsului, care vor include următoarele:

- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției;

- actualizări pentru software-ul de bază și pentru firmware. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ului de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;

- acces la suport on-line permanent prin intermediul unui portal pus la dispoziție în Internet și prin e-mail, precum și suport telefonic și on-site la sediul beneficiarului”.

Accesul online permanent la baza de date cu cunoștințe a producătorului soluției nu este posibil, atât timp cât soluția ofertată reprezintă o integrare de componente open-source, pentru care există baze de date cu cunoștințe la dezvoltatori, dar nu neapărat despre modalitățile de instalare, configurare și utilizare în mod integrat a componentelor. În consecință, pentru soluția ofertată, așa cum va fi ea instalată la beneficiar, nu va exista o bază de date cu cunoștințe. De asemenea, baza de date cu cunoștințe, portalul și site-urile web ale producătorilor componentelor din componența soluției, nu pot fi garantate de către firma ofertantă, accesul la acestea putând fi oricând restricționat. Prin baza de date cu cunoștințe, în accepțiunea cerinței tehnice, nu se înțelege documentație de instalare, configurare și

exploatare a soluției, ci o exemplificare a modului de realizare a unor analize malware complexe ce conține elemente concrete, specifice unor tipuri de malware. Spre exemplu, o astfel de bază de date poate să conțină metodele de abordare a analizelor malware în cazul utilizării unor moduri de împachetare malware folosind instrumente (packers) care nu sunt cunoscute public.

De asemenea, conform prevederilor stipulate în fișierele de licență ale produselor open-source produsele sunt distribuite ca atare, în speranța că vor fi utile, dar fără nicio garanție, fie cea care presupune că produsul vândut va funcționa corect atunci când este folosit în scopul pentru care a fost creat (implied merchantability) sau că se potrivește pentru un anumit scop, ceea ce înseamnă că dacă apar probleme de funcționare/integrare dezvoltatorii nu sunt obligați să ofere suport.

În referire la cerința 3.13.1 potrivit căreia „Componentele produsului trebuie să fie garantate de furnizor prin certificate de calitate și garanție emise de organul abilitat al acestuia”, autoritatea contractantă menționează că, prin soluția oferită, componentele open-source integrate nu pot fi garantate și certificate atâta timp cât licența soluției furnizate este de tip open-source. Toate licențele de tip open-source stipulează clar că nu garantează funcționarea.

În continuare, autoritatea contractantă prezintă câteva exemple din cadrul componentelor soluției furnizate:

- <http://docs.cuckoosandbox.org/en/latest/introduction/license/> „Cuckoo is distributed as it is, in the hope that it will be useful, but without any warranty neither the implied merchantability or fitness for a particular purpose. Whatever you do with this tool is uniquely your own responsibility”.

- <https://github.com/volatilityfoundation/volatility/blob/master/LICENSE.txt> „(...) because the program is licensed free of charge, there is no warranty for the program, to the extent permitted by applicable law”.

În ceea ce privește cerința 3.14.1 potrivit căreia „Ofertanții vor pune la dispoziție pachete de informații complete ale componentelor produsului. Specificațiile tehnice și de calitate ale componentelor oferite trebuie, obligatoriu, susținute de documentații originale: prospecte, foi de catalog, documentații tehnice descărcate de pe site-urile producătorilor. Declarațiile nesusținute de documentații originale nu vor fi luate în considerare, conducând la eliminarea ofertei”, autoritatea contractantă arată că ofertantul a prezentat o mare parte din documentația soluției oferite sub formă de hyperlink și aceasta nu aparține site-ului producătorului/dezvoltatorului (ex. referințe la documente stocate pe portalul malwr.com).

De altfel, autoritatea contractantă arată că, în cadrul contestației, sunt prezentate elemente de analiză, rapoarte etc. extrase din cadrul portalului malwr.com, fără a se preciza și demonstra care este conexiunea dintre acest portal și componentele din soluția oferită: *Cuckoo Sandbox* și *Volatility*.

Concluzionând, autoritatea contractantă precizează că își menține și își asumă decizia privind anularea procedurii de atribuire pentru lotul 2 ca urmare a depunerii numai de oferte neconforme, decizie adoptată în temeiul dispozițiilor art. 181 alin. (1) lit. a) din OUG nr. 114/2011.

În replică, prin adresa nr. 634/15.09.2015, înregistrată la CNSC sub nr. 17807/16.09.2015, SC ... SRL a transmis Consiliului concluzii scrise, prin care reiterează aspectele precizate în contestație, referitoare la conformitatea ofertei sale cu cerințele documentației de atribuire.

Față de susținerile părților și de documentele depuse la dosarul cauzei, Consiliul reține cele ce urmează:

..., în calitate de autoritate contractantă, a organizat, conform prevederilor OUG nr. 114/2011 (*Achiziții în domeniul apărării și securității*), procedura de atribuire, prin cerere de oferte, a contractului de achiziție publică de furnizare având ca obiect „SIC pregătire operații cibernetice (CyberRange), ..., Instrumente computer forensics, Soluție de evaluare securitate rețele”, cod CPV 30211400-5 – *Configurații informatice (Rev. 2)*, publicând în SEAP invitația de participare nr. ... din

....

Împotriva deciziei autorității contractante de anulare a procedurii pentru lotul 2 (măsură ce i-a fost comunicată prin adresa nr. 538/24.08.2015), SC ... SRL a înaintat Consiliului contestația de față (însoțită de garanția de bună conduită în valoare de 3.064,51 lei), solicitând revizuirea ei.

Consiliul reține că, anterior prezentei cauze, a fost admisă în parte o contestație aparținând SC ... SRL, formulată împotriva rezultatului procedurii, CNSC obligând autoritatea contractantă la reevaluarea ofertei depuse de către contestatoarele pentru lotul 2 (Decizia nr. 1268/C2/1354 din 06.08.2015).

În concordanță cu noua decizie de respingere a ofertei acesteia, comunicată prin adresa nr. A3/4547 din 24.08.2015, neconformitatea cu cerințele caietului de sarcini se datorează neîndeplinirii mai multor caracteristici tehnice, indicate explicit în anexa adresei amintite.

În referire la cerința 1.1.2, a caietului de sarcini, ca soluția să includă „toate componentele hardware de ultimă generație, și licențe software...”, Consiliul constată că autoarea criticilor pretinde eronat că nu exista obligația ofertării unei „platforme dedicate cu suport oferit de un producător”.

În fapt, autoritatea contractantă nu achiziționează produse ofertate distinct, cu funcții individuale, ci o platformă informatică integrată, iar soluția de integrare a componentelor trebuie garantată pe durata ei de viață. Din cerință, rezultă nevoia ca funcționalitatea soluției informatice să fie asigurată de producătorul ei, fără a se face distincție între fabricantul componentelor hard și cel al componentelor soft ori integratorul lor.

Astfel, critica contestatoarei se bazează, exclusiv, pe pretinsa absență din textul cerinței a formei de exprimare explicite privitor la

suportul din partea „unui producător”. Or, din context, se înțelege obligația invocată de autoritatea contractantă.

De altfel, contestatoarea nici nu pretinde că ar putea să probeze posibilitatea existenței unui astfel de suport.

În mod similar, susținerea că nu a primit solicitări de clarificare asupra sistemului de operare propus este întemeiată formal, însă contextul în care face observația nu este întărit și de proba că afirmația autorității contractante ar fi tendențioasă, privitor la: „componente care necesită a fi integrate...”.

De asemenea, pretinsa interpretare eronată a clauzelor referitoare la termenii de licențiere *GNU GPL3* nu este probată fără echivoc de către contestatoare. Dimpotrivă, este notoriu că utilizarea unui produs, așa cum este comercializat, se face cu asigurarea garanției producătorului, în timp ce modificările asupra lui pot conduce la pierderea acestei garanții.

Or, contestatoarea nu a confirmat autorității contractante, dar nici prin contestație nu a probat că, după instalarea Componentei *Cuckoo Sandbox*, licența *GNU GPL3* este în continuare cu suport asigurat de către producător (*perioada de viață*).

În privința modalității alternative de probare a licențierii, se reține că autoarea criticilor a precizat, în formă tabelară, tipurile de licențe oferite, pe fiecare componentă, însă întrebarea de clarificare nu a primit un răspuns punctual și motivat, de ce nu ar fi utilă achiziția unor *licențe corporate/comerciale*, nici după formularea contestației.

De altfel, deși întrebarea autorității contractante (nr. 3, din adresa nr. A3/4377) nu a avut un conținut explicit, privitor la imposibilitatea ca varianta API inclusă în *Cuckoo Sandbox* să asigure analiza statică a unui malware, contestatoarea nu aduce argumente contrare acestui motiv explicit de respingere a ofertei, indicat în adresa de comunicare a rezultatului. În fapt, aceasta se limitează a pretinde că a indicat toate licențele avute în vedere, iar nu să demonteze aprecierea autorității contractante că soluția propusă ar conține și o astfel de incompatibilitate.

În consecință, acest prim motiv (cerința 1.1.2 a caietului de sarcini) de respingere a ofertei ca neconformă a fost corect reținut de către autoritatea contractantă.

În mod similar, disputa părților în privința ne/îndeplinirii cerinței 3.14.1 („Ofertanții vor pune la dispoziție pachete de informații complete ale componentelor produsului...”), argumentată de contestatoare prin invocarea faptului că nu ar exista în documentația de atribuire cerința: „Soluția oferită trebuie să fie completă, să răspundă cerințelor ca întreg, nu pe componente”, este considerată de Consiliu artificial creată. Criticile contestatoarei se bazează, exclusiv, pe interpretări fracționate ale specificațiilor caietului de sarcini și nu pe conținutul integral al acestuia, care privește o platformă informatică funcțională, nu componente achiziționate distinct.

Văzând motivele de respingere a ofertei asociate cerinței tehnice individualizate prin indicativul 3.1.1.1., Consiliul constată că autoritatea

contractantă a reținut lipsa unor precizări explicite privitoare la tipul de licență aferentă sistemelor de operare Microsoft „astfel încât nu se poate stabili dacă licența suportă downgrade la Windows XP”.

Or, în situația dată, Consiliul consideră că această ambiguitate putea fi înlăturată ușor, printr-o întrebare formulată punctual, respectiv confirmarea faptului că se/nu se poate downgrade, demers ce ar fi fost conform cu prevederile art. 176 alin. (1) din OUG nr. 114/2011.

Același raționament juridic apare ca fiind aplicabil și situației privind ambiguitatea asupra existenței sau nu a *Windows XP*, ca mașină virtuală.

În privința neconcordanței între informațiile din propunerea tehnică și din răspunsul de clarificare, privitor la conținutul tabelar al tipurilor de mașini virtuale (întrebările 6 și 7), respectiv lipsa certitudinii că Windows XP, ca mașină virtuală, va fi integrată în soluție, reținute ca motiv de nerespectare a cerinței tehnice nr. 3.1.1.4., Consiliul consideră că autoritatea contractantă trebuia, de asemenea, să solicite informații de certitudine, înainte de a lua măsura excluderii din competiție.

Văzând aprecierea autorității contractante privitoare la neîndeplinirea specificației tehnice de la punctul 3.1.2.6 (capacitatea de identificare și rulare aplicații malware), Consiliul constată că aceasta se bazează pe un considerent nereal. Întrebarea de clarificare la care se referă adresa de comunicare a rezultatului (nr. 8) făcea referire la argumentarea modului în care se face analiza malware, nu trimitea la necesitatea ca această funcție să rezulte dintr-un document furnizat de producător.

În consecință, autoritatea contractantă nu trebuia să considere, implicit, că informațiile cu titlu exemplificativ, numite ca atare chiar de către ofertant, rezultând de la un terț, reprezintă un mod de ocolire a obligației de a furniza și respectivul document. Dimpotrivă, răspunsul de clarificare în cauză are menirea de a întări convingerea autorității contractante că analiza malware poate fi făcută, cu un astfel de produs, informația provenind de la un terț față de disputa în cauză.

Totodată, lipsa sau nu a unui document de tipul celui pretins putea face obiectul unei alte corespondențe de clarificare.

Văzând disputa părților în referire la existența/inexistența funcțiilor de „identificare, extragere și analiză în profunzime a fișierelor injectate în memoria fizică a unui SIC, instalate și configurate în cadrul soluției ofertate”, Consiliul constată că nu sunt combătute ambele motive reținute de autoritatea contractantă (specificația 3.1.4). Astfel, deși aceasta a considerat că trimiterile la un blog terț față de ofertant nu asigură informații de certitudine, dar se puteau solicita documente de natura celor reținute mai sus, în fapt, lipsa din soluția propusă (bazată pe *Cuckoo Sandbox* și *Volatility*) a mecanismelor automate nu este combătută de contestatoare. Astfel, aprecierea autorității contractante apare ca fiind definitivă, ceea ce dă caracter de neconformitate ofertei contestatoarei, sub acest aspect.

În privința modalității de îndeplinire a specificației tehnice nr. 3.1.5. - „deține module de identificare a algoritmilor de criptare sau extragere a cheilor asociate pornind de la încărcarea de pachete criptate, având



posibilitatea de a selecta un fișier sau un grup de fișiere criptate cu aceeași metodă”, Consiliul constată că autoritatea contractantă a reținut corect lipsa funcției din soluția ofertată de contestatoare.

Pe de o parte, răspunsul de clarificare indicat de părți (nr. 11) nu aduce elemente de informare concludente, ceea ce dădea dreptul autorității contractante de a respinge oferta, ca neconformă.

Pe de altă parte, prin contestație, reluându-se conținutul răspunsului de clarificare, se aduc argumente contrare modului de stabilire a specificației tehnice din caietul de sarcini.

Conform contestatoarei, funcția nici nu poate fi automatizată, dar cea propusă de ea nici nu ar avea etapele indicate în caietul de sarcini/întrebarea de clarificare.

Prin urmare, contestația recunoaște, explicit, neconcordanța ofertei cu cerințele autorității contractante. Consiliul consideră că eventuale observații la adresa caietului de sarcini, chiar posibilități alternative la specificațiile acestuia, puteau face obiectul unor corespondențe anterioare ofertării.

Or, depunerea ofertei implică acceptarea în tot și întocmai a documentației de atribuire, conform dispozițiilor art. 32 alin. (1) din OUG nr. 114/2011, iar o ofertă cu caracter alternativ nu ar putea fi depusă fără acceptarea ei în mod explicit, prin indicarea acestei posibilități, chiar în documentație, conform art. 34 alin. (1) din același act normativ.

În consecință, văzând motivele întemeiate de respingere a ofertei, ca neconformă, mai sus amintite, Consiliul consideră de prisos a mai face analiza celorlalte critici aduse de contestatoare, întrucât finalitatea procedurii față de oferta sa nu ar putea fi schimbată pe calea unei reevaluări.

În mod implicit, solicitarea de anulare a deciziei de anulare a procedurii, pentru Lotul 2, aparținând contestatoarei, apare ca nefondată, în condițiile în care nu există oferte conforme, iar art. 181 alin. (1) lit. a) din OUG nr. 114/2011 indică obligativitatea anulării procedurii, pentru acest motiv.

De altfel, aceasta a invocat eronat, în sprijinul cererii sale, alte dispoziții ale OUG nr. 114/2011, decât cele indicate de autoritatea contractantă drept temei de drept al măsurii – art. 181 alin. (1) lit. a).

Pentru cele ce preced, în temeiul dispozițiilor art. 278 alin. (5) și (6) din OUG nr. 34/2006, cu modificările la zi, aplicabile conform art. 188 din OUG nr. 114/2011, Consiliul respinge contestația, ca nefondată și menține măsura anulării procedurii, dispusă de autoritatea contractantă din oficiu.

La punerea în aplicare a deciziei, părțile vor avea în vedere că este obligatorie, dar și că o pot ataca cu plângere, conform dispozițiilor de la art. 280 alin. (1) și art. 281 din OUG nr. 34/2006.

**PREȘEDINTE COMPLET**

...

2  
ε



**MEMBRU COMPLET**

...

...

**MEMBRU COMPLET**

...