Anexa 1

Caiet de sarcini

Necesar certificate digitale calificate din cadrul Centrului National pentru Informatii Financiare

1) Mentiune

În cadrul acestei proceduri, MINISTERUL FINANȚELOR îndeplinește rolul de Autoritate Contractantă, respectiv Achizitor în cadrul Contractului.

Pentru scopul prezentei secțiuni a Documentației de atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

Caietul de sarcini face parte integrantă din Documentația de atribuire şi conține specificațiile tehnice, respectiv ansamblul cerințelor minimale și obligatoriu de îndeplinit, pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Ofertele care nu îndeplinesc toate cerințele minimale vor fi declarate neconforme. Nu se acceptă depunerea de oferte alternative. Nu se admit ofertele parțiale din punct de vedere cantitativ şi calitativ, ci numai ofertele integrale, care corespund tuturor cerințelor stabilite prin prezentul caiet de sarcini. Orice ofertă care se abate de la cerințele minimale va fi considerată admisibilă numai în condițiile în care aceasta asigură un nivel calitativ superior cerințelor minimale.

În conformitate cu regulile de elaborare a documentației de atribuire din Legea nr. 98/2016, privind achizițiile publice, cu modificările și completările ulterioare, art. 156, alin (2) și (3), specificaţiile tehnice din prezentul Caiet de sarcini care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează produsele sau serviciile furnizate şi care se referă la mărci, brevete, tipuri, la o origine sau la o producţie specifică se consideră a fi însoțite de cuvintele “sau echivalent”, indiferent dacă aceste cuvinte sunt prevăzute expres sau nu în prezentul document.

2) Informatii despre Autoritatea contractantă

Ministerul Finanțelor este un minister cu rol de sinteză, care se organizează și funcționează ca organ de specialitate al administrației publice centrale, cu personalitate juridică, în subordinea Guvernului, care aplică strategia și Programul de guvernare în domeniul finanțelor publice.

Ministerul Finanțelor aplică Programul de guvernare și contribuie la elaborarea și implementarea strategiei în domeniul finanțelor publice, în exercitarea administrării generale a finanțelor publice, asigurând utilizarea pârghiilor financiare, în concordanță cu cerințele economiei de piață și pentru stimularea inițiativei operatorilor economici.

Ministerul Finanțelor îndeplinește toate atribuțiile și are toate competențele conferite prin legi sau prin alte acte normative în vigoare, monitorizează și coordonează atribuțiile conferite de lege unităților subordonate.

Sediul principal al Ministerului Finanțelor este în municipiul București, Bulevardul Libertății nr. 16, sectorul 5. Ministerul Finanțelor își desfășoară activitatea și în alte sedii deținute potrivit legii.

Informații suplimentare despre Autoritatea Contractantă, Ministerul Finanțelor, se pot regăsi pe site-ul web oficial al instituției: www.mfinante.gov.ro.

3) Scopul achiziției

Asigurarea securitatii site-urilor de aplicatii si accesului la portalurile din serverele sistemului informatic din cadrul Centrului National pentru Informatii Financiare aferente Ministerului Finantelor si Agentiei Nationale de Administrare Fiscala .

4) Obiectul achiziției

Reinnoirea si/sau achizitia de certificate digitale calificate si de securitate, aferente aplicatiilor si accesului securizat la diferitele portale pe care Centrul National pentru Informatii Financiare le are in intretinere, acestea apartinand diversilor utilizatori din cadrul directiilor Ministerului Finantelor.

5) Situaţia existentă

Sistemul informatic al Ministerului Finanțelor (MF) este unic în România atât din punct de vedere al complexității și specificității aplicațiilor, cât și al numărului de entități ale administrației publice și entități private deservite, precum și al întinderii teritoriale. Numărul de aplicații informatice, volumul de date, numărul de entități deservite și numărul de utilizatori interni și externi crește permanent, crescând implicit și volumul de muncă depusă, precum și necesarul de resurse pentru dezvoltarea și administrarea sistemului informatic. Actualmente sistemul informatic al Ministerului Finanțelor este cel mai mare Contractant de date pentru instituțiile publice și instituțiile financiare din România și din străinătate.

Informațiile de mai jos sunt prezentate cu următoarele scopuri:

- *Înțelegerea infrastructurii în care vor fi integrate certificatele digitale livrate;*
- *Înțelegerea conditiilor pe care certificatele digitale ofertate trebuie să le asigure.*

Situatia actuala a certificatelor care sunt in intretinere este urmatoarea:

Nr. crt.	Titular certificat digital sau tip certificat digital	Emitent certificat digital	Reînnoire începând cu data
1	FATCA-IRS, 1 tip server SSL Secure Site, emis de o autoritate de certificare acceptată de către IRS	DigiSign (Symantec)	16.12.2023
2	Fiscnet, 1 tip digital SSL Secure Site OV cu Wildcard	DigiSign (Symantec)	16.12.2023
3	CTS - OECD, 1 certificat SSL Web Server whit EV,	DigiSign (Thawte)	10.12.2023

	emis de o autoritate de certificare acceptată de către CTS		
4	ANAF, 2 tip Server Web SSL cu Wildcard *.anaf.ro, *.anaf.mfinante.gov.ro	DigiSign	16.09.2023
5	HSM, 1 Certificat digital calificat server HSM	DigiSign (DigiSign)	01.12.2023
6	DTICSV, 1 tip serverSSL Geo Trust True Bussiness ID-mail.customs.ro	DigiSign	15.06.2023
7	DTICSV, 1 tip serverSSL Geo Trust True Bussiness ID-sslvpn.customs.ro	DigiSign	02.06.2023
8	DTICSV, 1 tip server Web SSL cu Wildcard- *.customs.ro	DigiSign	12.06.2023
9	MFINANTE, 2 tip server Web SSL cu Wildcard *.mfinante.ro, *.mfinante.gov.ro	DigiSign	16.09.2023
10	DTICSV, 1 tip serverSSL Sistem EORI-RO, siiv-eori.customs.ro	DigiSign	14.12.2023
11	DTICSV, 1 tip server Web SSL cu Wildcard *.swiss-contribution.ro	DigiSign	11.05.2023

La punctul 1 din tabel este specificat un certificat digital de tip SSL Secure Site – 1 bucata, care certifica schimbul de date intre institutiile financiare si autoritatile fiscale in Serviciul de Schimb International de Date (IDES), sistem care accepta numai certificatele aprobate de catre IRS. Certificatul va fi validat în timpul procesului de înscriere pentru a confirma că aderă la IDES, aceasta necesită validarea certificatului prezentat, lista aprobată de autorități de certificare (CA) de catre IRS este publica in pagina IDES (https://www.ides-support.com/KnowledgeBase/InfoCertificateAuthorities) aceasta fiind:

Autoritatea de certificare (CA)	**Certificatul necesar**	**Linkul site-ului extern**
DigiCert	Standard SSL	Standard SSL
DigiCert	EV SSL	EV SSL
GlobalSign	Organization SSL	Organization SSL
GlobalSign	Extended SSL	Extended SSL
Go Daddy	EV-SSL	EV-SSL
Entrust	Standard SSL	Standard SSL
Entrust	EV Multi-Domain SSL	EV Multi-Domain SSL
IdenTrust	Standard Server SSL	Standard Server SSL

IdenTrust	FATCA Organizational Certificate	FATCA Organizational Certificate
Sectigo (formerly Comodo)	EV-SSL	EV-SSL

La punctul 2 din tabel este specificat un certificat digital de tip SSL Secure Site OV cu Wildcard – 1 bucată, folosit pentru portalul Intranet al MFP si ANAF, acesta asigură utilizatorilor și gazdelor web să securizeze, un domeniu și subdomenii nelimitate cu asigurare ridicată, cu cheie de lungime 2048 – 4096bit, cu criptare de până la 256 de biți, cu licențe server nelimitate, având sigiliu DigiCert sau Norton Trust și scanare malware cu validare prioritizată.

La punctul 3 din tabel este specificat un certificat SSL Web Server whit EV, emis de o autoritate de certificare acceptată de către CTS. Acest certificat digital trebuie sa fie emis de una din autoritatile de certificare agreate de catre administratorul portalului CTS, lista care este data de acesta odata cu indicatiile de instalare, administrare si utilizare a respectivului portal.

Lista cu autoritatile de certificare acceptata de catre CTS este urmatoarea:

Following is the list of authorized certificate authorities and certificate types:

Certificate Authority	Authorized Certificate Type
Digicert	EV SSL Plus (Single Name) https://www.digicert.com/ev-ssl-certification.htm
Entrust	EV Multi Domain SSL https://www.entrust.com/ev-multi-domain-ssl-certificates
Thawte	SSL Web Server https://www.thawte.com/ssl/extended-validation-ssl-certificates

La punctul 4 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 2 bucati, folosite pentru site-urile oficiale ANAF respectiv pentru cele 2 domenii, si anume, *.anaf.ro si pentru *.anaf.mfinante.gov.ro, acestea asigurand securitatea accesului la respectivele pagini – inclusiv la zona de portal de aplicatii.

La punctul 5 din tabel este specificat un certificat digital de tip Certificat Digital Calificat Server – 1 bucata, folosit pentru activitatea de semnare si criptare calificata automata de mare volum in portalul Agentiei Nationale de Administrare Fiscala. Acesta va fi instalat in cele 2 Module de Securitate Hardware (HSM).

La punctul 6 din tabel este specificat un certificat digital de tip Standard Server SSL – 1 bucata, folosit pentru serverul de posta electronica al Directiei Vamale, respectiv mail.customs.ro. Acesta asigura securitatea prin criptarea datelor din serverul de posta electronica.

La punctul 7 din tabel este specificat un certificat digital de tip Standard Server SSL – 1 bucata, folosit pentru serverul de retea virtuala privata (VPN), respectiv sslvpn.customs.ro. Acesta asigura securitatea prin criptarea datelor transferate prin acest server, ce asigura conexiunile la reteaua virtuala privata.

La punctul 8 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 1 bucata, si anume, *.customs.ro folosit pentru serverul ce administreaza site-ul si portalul Directiei Vamale. Acesta asigura securitatea accesului la pagina respectiva.

La punctul 9 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 2 bucati, folosite pentru site-urile oficiale ale Ministerului de Finante, respectiv pentru cele 2 domenii, si anume, *.mfinante.ro si pentru *.mfinante.gov.ro, acestea asigurand securitatea accesului la respectivele pagini – inclusiv la zona de portal de aplicatii.

La punctul 10 din tabel este specificat un certificat digital de tip Standard Server SSL – 1 bucata, necesare pentru Sistemul de Înregistrare și Identificare al Operatorilor Economici EORI-RO, component a Sistemului Informatic integrat Vamal.

La punctul 11 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 1 bucată, si anume, *.swiss-contribution.ro folosit pentru serverul ce administrează site-ul și portalul site-ului Swiss-contribution.ro. Acesta asigură securitatea accesului la pagina respectivă.

6) Specificații tehnice

Specificațiile tehnice cuprinse sunt minimale, obligatorii și reprezintă criteriul de acceptare a ofertei. *Lista certificatelor ce urmeaza a fi achizitionate / reinnoite este urmatoarea:*

Nr. crt.	Titular certificat digital sau tip certificat digital	Reînnoire începând cu data	Cantitate bucata
1	FATCA, 1 tip server SSL Secure Site, emis de o autoritate de certificare acceptată de către IRS	16.12.2023	1
2	Fiscnet, 1 tip digital SSL Secure Site OV cu Wildcard	16.12.2023	1
3	CTS, 1 certificat SSL Web Server whit EV, emis de o autoritate de certificare acceptată de către CTS	10.12.2023	1
4	ANAF, 1 tip Server Web SSL cu Wildcard *.anaf.ro	16.09.2023	1
5	ANAF, 1 tip Server Web SSL cu Wildcard * anaf.mfinante.gov.ro	16.09.2023	1
6	HSM, 1 Certificat digital calificat server HSM	01.12.2023	1
7	DTICSV, 1 tip serverSSL Geo Trust True Bussiness ID-mail.customs.ro	15.06.2023	1

8	DTICSV, 1 tip serverSSL Geo Trust True Bussiness ID-sslvpn.customs.ro	02.06.2023	1
9	DTICSV, 1 tip server Web SSL cu Wildcard-*.customs.ro	12.06.2023	1
10	MFINANTE, 1 tip server Web SSL cu Wildcard *. mfinante.gov.ro	16.09.2023	1
11	MFINANTE, 1 tip server Web SSL cu Wildcard *.mfinante.ro	16.09.2023	1
12	DTICSV, 1 tip server SSL Sistem EORI-RO, siiv-eori.customs.ro	14.12.2023	1
13	DTICSV, 1 tip server Web SSL cu Wildcard *.swiss-contribution.ro	11.05.2023	1
14	Certificat tip Server SSL	necesități ulterioare	10
15	Certificat digital calificat Server	necesități ulterioare	2

Specificatiile tehnice pe care certificatele trebuie sa le prezinte este urmatoarea:

1) La punctul 1 din tabel certificatul de tip SSL Secure Site are urmatoarele caracteristici tehnice; Certificatul SSL Secure site asigura utilizatorilor și gazdelor web să securizeze, un domeniu cu asigurare ridicata, cu cheie de lungime 2048 – 4096bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat. La acestea se adauga specificatiile exprese ale autoritatii care administreaza portalul, respectiv de catre IRS. Lista aprobată de autorități de certificare (CA) de catre IRS este publica in pagina IDES (https://www.ides-support.com/KnowledgeBase/InfoCertificateAuthorities) aceasta fiind:

Autoritatea de certificare (CA)	**Certificatul necesar**	**Linkul site-ului extern**
DigiCert	Standard SSL	Standard SSL
DigiCert	EV SSL	EV SSL
GlobalSign	Organization SSL	Organization SSL
GlobalSign	Extended SSL	Extended SSL
Go Daddy	EV-SSL	EV-SSL
Entrust	Standard SSL	Standard SSL
Entrust	EV Multi-Domain SSL	EV Multi-Domain SSL
IdenTrust	Standard Server SSL	Standard Server SSL
IdenTrust	FATCA Organizational Certificate	FATCA Organizational Certificate
Sectigo (formerly Comodo)	EV-SSL	EV-SSL

2) La punctul 2 din tabel certificatul de tip SSL Full Business Validation (OV) cu Wildcard are următoarele caracteristici tehnice; Certificatul SSL OV cu Wildcard este de tip Full Business Validation (OV) și asigură utilizatorilor și gazdelor web să securizeze, un domeniu și subdomenii nelimitate cu asigurare ridicată, cu cheie de lungime 2048 – 4096bit, cu criptare de până la 256 de biți, cu licențe server nelimitate, având sigiliu DigiCert sau Norton Trust și scanare malware cu validare prioritizată. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

3) La punctul 3 din tabel certificatul de tip SSL Web Server cu EV are urmatoarele caracteristici tehnice; Certificatul SSL Web Server cu EV asigura utilizatorilor și gazdelor web să securizeze, intre 3 si 100 domenii cu asigurare foarte ridicata,cu validare extinsa, cu cheie de lungime 2048 – 4096bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat. In plus, acest certificat digital trebuie sa fie emis de una din autoritatile de certificare agreate de catre administratorul portalului CTS, lista care este data de acesta odata cu indicatiile de instalare, administrare si utilizare a respectivului portal.

Lista cu autoritatile de certificare acceptata de catre CTS este urmatoarea:

Following is the list of authorized certificate authorities and certificate types:

Certificate Authority	Authorized Certificate Type
Digicert	EV SSL Plus (Single Name) https://www.digicert.com/ev-ssl-certification.htm
Entrust	EV Multi Domain SSL https://www.entrust.com/ev-multi-domain-ssl-certificates
Thawte	SSL Web Server https://www.thawte.com/ssl/extended-validation-ssl-certificates

4) La punctele 4 și 5 din tabel certificatul de tip SSL cu Wildcard are urmatoarele caracteristici tehnice; Certificatul SSL cu Wildcard asigura utilizatorilor și gazdelor web să securizeze, un domeniu si toate subdomeniile cu asigurare ridicata, cu cheie de lungime 2048 – 4096bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat.

5) La punctul 6 din tabel certificatul de tip Certificat Digital Calificat Server are urmatoarele caracteristici tehnice; Certificat Digital Calificat Server asigura cheia de semnare pentru serverele de semnare de mare capacitate, cu cheie de lungime 2048 – 4096bit, cu criptare de pana la 256 de biti, cu valoare extinsa.Acelasi certificat va fi utilizat pentru doua servere (module) de semnare de mare capacitate (HSM). Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat.

6) La punctul 7 din tabel certificatul de tip SSL Server are urmatoarele caracteristici tehnice; Certificatul SSL Server asigura in acest caz securitatea unui server de posta electronica cu urmatoarele caracteristici, autentificare validata pentru oragnizatie / afaceri, sa asigure mai multe domenii si toate subdomeniile cu asigurare ridicata, cu cheie de lungime 2048bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat.

7) La punctul 8 din tabel certificatul de tip SSL Server are urmatoarele caracteristici tehnice; Certificatul SSL Server asigura in acest caz securitatea unui server VPN cu urmatoarele caracteristici, autentificare validata pentru oragnizatie / afaceri, sa asigure mai multe domenii si toate subdomeniile cu asigurare ridicata, cu cheie de lungime 2048bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat.

8) La punctul 9 din tabel certificatul de tip SSL Server are urmatoarele caracteristici tehnice; Certificatul SSL Server cu Wildcard asigura in acest caz securitatea unui server gazda site cu urmatoarele caracteristici, autentificare validata pentru oragnizatie / afaceri, sa asigure mai multe domenii si toate subdomeniile cu asigurare ridicata, cu cheie de lungime 2048 – 4096bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat.

9) La punctele 10 și 11 din tabel certificatul de tip SSL cu Wildcard are urmatoarele caracteristici tehnice; Certificatul SSL cu Wildcard asigura utilizatorilor și gazdelor web să

securizeze, un domeniu si toate subdomeniile cu asigurare ridicata, cu cheie de lungime 2048 – 4096bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul in care a fost generat.

10) Certificatul tip Server SSL de la pcunctul 12 din tabel garantează identitatea unui site web şi permite utilizarea protocolului securizat https în vederea protejării transmiterii informaţiilor în mediul on-line, asigurând astfel securitatea comunicației cu utilizatorii săi. Protejează prin criptare informația transmisă între client și server, fiind astfel protejate împotriva vizualizării neautorizate sau modificării. Asigurarea autenticității site-ului web prin verificarea informațiilor referitoare la posesorul acestuia înainte de emiterea certificatului. Confirmarea identității site-ului web pe Internet. Transmiterea în siguranță a datelor cu caracter personal. Controlul accesului utilizatorilor in conformitate cu politicile şi cerinţele de Securitate. Trebuie sa asigure mai multe domenii si toate subdomeniile cu asigurare ridicata, cu cheie de lungime 2048bit, cu criptare de pana la 256 de biti. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

11) La punctul 13 din tabel certificatul de tip SSL Server are următoarele caracteristici tehnice; Certificatul SSL Server cu Wildcard asigură în acest caz securitatea unui server gazdă site cu următoarele caracteristici, autentificare validată pentru oragnizație / afaceri, să asigure mai multe domenii și toate subdomeniile cu asigurare ridicată, cu cheie de lungime 2048 – 4096bit, cu criptare de pana la 256 de biți. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

12) Certificatele de la punctele 14 și 15 din tabel se vor solicita, pentru necesități ulterioare, valabilitatea fiind de maxim 2 ani, după caz.

7) Activitati specifice

• Toate documentele şi informaţiile primite de la Ofertant precum şi rezultatele tuturor activităţilor din cadrul acestui contract (cum ar fi: cod sursă, cod obiect, biblioteci, librării, manuale, documente de analiză, arhitecturi de sisteme, adrese, etc., fără a se limita la acestea) reprezintă informaţii confidenţiale, iar Ofertantul câştigător va asigura respectarea confidenţialităţii lor, urmând să semneze o declaraţie în acest sens.

• Ofertantul şi personalul său au obligaţia de a respecta confidenţialitatea documentelor şi informaţiilor menţionate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia şi după încetarea contractului. În acest sens, Ofertantul precum şi toţi experţii implicaţi în activităţile contractului sunt obligaţi să semneze Acorduri de Confidențialitate cu Autoritatea Contractantă.
• Toate documentele, rapoartele şi datele, inclusiv diagrame, desene, specificaţii, planuri, formule, baze de date, software (cod sursă, cod obiect, biblioteci, librării etc.) şi orice alte materiale obţinute, compilate sau realizate de către Ofertant în cadrul contractului (chiar daca sunt module sau pachete program deja construite in alte proiecte sau in cadrul unor pachete disponibile comercial), sunt în proprietatea /proprietatea intelectuala a Autorității Contractante, aceasta având dreptul să le utilizeze, modifice, transfere fără acceptul Ofertantului sau al unei terţe părţi. Ofertantul le va furniza Autorităţii Contractante, la finalizarea contractului, fără a păstra copii şi fără a le utiliza în alte scopuri care nu au legătura cu contractul fără acordul scris al Autorităţii Contractante.
• Ofertantul nu va publica articole sau informaţii legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terţi şi nu va divulga informaţiile obţinute de la Autoritatea Contractantă, fără acordul scris al acesteia.

• Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de proprietate intelectuală sau industrială, obținute în cadrul contractului, sunt proprietatea Autorității Contractante, care poate dispune de ele după cum consideră.

1. Se va initia pentru fiecare in certificat in parte inainte cu 15 zile de expirare procedura de inlocuire / prelungire a certificatului care expira.

2. Se vor efectua actele tipice necesare procedurii de achizitie a noului certificat.

3. Se vor efectua procedurile de identificare a solicitantului / beneficiarului conform standardului de acordare a noului certificat.

4. Se va proceda la formarea si trimiterea certificatului de revocare pe baza caruia se va livra noul certificat.

5. Se va proceda la instalarea noului certificat emis.

6. Se va testa functionarea aplicatiilor, nivelelor de securitate si compatibilitatea noului certificat emis.

8) Obligatiile prestatorului de servicii de certificare

Prestatorul de servicii de certificare se va obliga:

1. Să furnizeze produsele si serviciile de certificare aferente certificatelor digitale prezentate, conform unei proceduri propuse de prestator si agreată cu beneficiarul, la preturile unitare ofertate.
2. Să notifice beneficiarul dupa efectuarea oricarei modificări a Politicii de Certificare, Codului de Practici si Proceduri sau a altei proceduri care stau la baza furnizării produselor si serviciilor.
3. Să respecte prevederile legislatiei romane in vigoare, in legătura cu produsele si serviciile furnizate.
4. Să asigure, in mod gratuit accesul la toate informatiile necesare utilizării corecte si in conditii de sigurantă a produselor si serviciilor aferente.
5. Să nu colecteze date cu caracter personal decat in măsura in care aceste informatii sunt necesare in vederea eliberării si conservării certificatelor emise.
6. Să asigure asistenta beneficiarului in implementarea serviciilor de certificare.
7. Să pastreze confidentialitatea informatiilor incredintate, conform legislatiei romane in vigoare.
8. Să tina un registru electronic de evidentă a certificatelor eliberate, suspendate sau revocate, accesibil on-line.
9. Să asigure accesul beneficiarului pentru toate certificatele emise.
10. Să asigure telefonic servicii de Help Desk, pentru beneficiar de luni pană vineri in intervalul orar 08:00 – 19:00.
11. Să notifice beneficiarul in termen de 24 de ore de la orice modificare, in cazul in care informatiile cuprinse in contract, inclusiv adresa, numărul de telefon, numărul de fax si adresa de e-mail, nu mai corespund realitătii.
12. Să notifice beneficiarul asupra deciziei de revocare a unui certificat in cel mai scurt interval de timp de la momentul la care a luat la cunostintă cauza de revocare/suspendare, dar nu mai tarziu de o oră de la decizia de revocare/suspendare a certificatului.
13. Să notifice beneficiarul cu privire la orice modificare care apare in statutul său, situatia sa care se actualizează in Registrul Autoritătii de Reglementare si Supraveghere (conform prevederilor legale in vigoare), precum si orice altă situatie care ar putea afecta derularea in bune conditii a contractului.

14. Să notifice beneficiarul cu privire la aparitia oricărei conditii care pot avea ca efect imposibilitatea emiterii de certificate cum ar fi derularea unei actiuni de investigatie a autoritătilor competente in domeniu.
15. Să notifice beneficiarul cu privire la incetarea calitătii de furnizor de servicii de certificare si din acel moment, să nu mai emită certificate, returnand către acesta actele de solicitare cărora urma să le dea curs.

9) Calitatea serviciilor

1. Prestatorul de servicii de certificare trebuie sa indeplineasca conditiile prevazute de legislatia romana, in vederea emiterii certificatelor digitale.
2. Prestatorul de servicii de securitate va confirma ca certificatele digitale eliberate sunt in conformitate cu prevederile legale in vigoarespecifice domeniului.
3. Nivelul de securitate asigurat de prestatorul de serviciide servicii va fi in conformitate cu standardele minime recunoscute: ISO/IEC 15408-1, 2, 3; ISO 27001 si ISO 17799; ETSI TS 101 456 v.1.1.1.(2000-12); ITSEC-E3, fiind structurat potrivit ETSI TS 101 862 v.1.2.1.(2001-06), RFC 3280 si cu respectarea recomandarilor ITU-T X. 509.

10) Conditii de livrare si receptie

1) Prestatorul de servicii de cartificare va elibera certificatele digitale solicitateprin comenzile beneficiarului, cu respectarea procedurii stabilite de comun acord cu acesta.

2) Receptia produselor se va efectua prin procese verbale de receptie, semnate de reprezentantii ambelor parti. Facturile vor fi insotite obligatoriu de procesele verbale de receptie, intocmite in urma verificarii conformitatii acestora cu comanda primita, in copie.
3) Produsele si serviciile din prezentul caiet de sarcini (Anexa 1), reprezinta cantitatea maxima contractuala, preturile/tarifele ofertate fiind ferme si valabile pe toata durata contractului.

11) Garanție și cerințe specifice

Certificatele nou emise, sunt, in momentul in care devin functionale acoperite de garantie, pe toata durata de valabilitate pe care acestea o prezinta in momentul instalarii, respectiv 2 ani.
Prestatorul de servicii de certificare va inlocui produsele fara nici un cost suplimentar in perioada de garantie.
Mentenanta pe perioada de garantie este gratuita.

12) Procedura de eliberare a certificatelor digitale tip server

Procedura va fi propusa de prestatorul de servicii de certificare si agreata cu beneficiarul si va contine cel putin urmatoarele informatii:
1) Procedura de emitere a certificatelor digitale.
2) Procedura de reinnoire a certificatelor digitale.
3) Procedura de revocare a certificatelor digitale:
    3.1 Revocare initiata de prestatorul de servicii de certificare,
    3.2 Revocare initiata de beneficiar.

13) Rezultate așteptate

În urma efectuării acestei achiziții se preconizează atingerea următoarelor obiective:

- asigurarea securitatii datelor care se vor semna cu aceste certificate,
- ridicarea gradului de incredere a utilizatorilor la accesarea paginilor oficiale prezentate public de cele trei institutii, Ministerul Finantelor Publice, Agentia Nationala de Administrare Fiscala si a Directiei Vamale,
- ridicarea gradului de incredere a utilizatorilor la accesarea portalelor de aplicatii oficiale aferente celor trei institutii, Ministerul Finantelor Publice, Agentia Nationala de Administrare Fiscala si a Directiei Vamale,
- ridicarea gradului de securitate transferate in mediul online prin asigurarea unui nivel ridicat de criptare a acestora.

14) Modul de întocmire a Propunerii tehnice

- Propunerea tehnică constă în descrierea certificatului digital prezentat in oferta.
- Se va mentiona autoritatea de certificare emitenta, dupa caz in functie de tipul de certificat digital ofertat.
- Se va mentiona clar perioada de valabilitate a certificatului ofertat, perioada care va trebui sa se regaseasca in partea de prezentare a acestuia.
- Va trebui sa respecte lungimea cheii si nivelul de criptare solicitat.
- Va trebui respectat nivelul si acoperirea asigurata de certificatul anterior la inlocuire / prelungire acolo unde este necesara aceasta caracteristica a certificatului digital ofertat.