

Caiet de sarcini

Necesar certificate digitale calificate din cadrul Centrului Național pentru Informații Financiare

1) Mențiuni

În cadrul acestei proceduri, MINISTERUL FINANTELOR 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 și 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 și 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), specificațiile tehnice din prezentul Caiet de sarcini care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează produsele sau serviciile furnizate și care se referă la mărci, brevete, tipuri, la o origine sau la o producție specifică se consideră a fi însoțite de cuvintele "sau echivalent", indiferent dacă aceste cuvinte sunt prevăzute expres sau nu în prezentul document.

2) Informații 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 securității site-urilor de aplicații și accesului la portalurile din serverele sistemului informatic din cadrul Centrului Național pentru Informații Financiare aferente Ministerului Finanțelor și Agenției Naționale de Administrare Fiscală .

4) Obiectul achiziției

Reînnoirea și/sau achiziția de certificate digitale calificate și de securitate, aferente aplicațiilor și accesului securizat la diferitele portale pe care Centrul Național pentru Informații Financiare le are în întreținere, acestea aparținând diversilor utilizatori din cadrul direcțiilor Ministerului Finanțelor.

5) Situația 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 condițiilor pe care certificatele digitale oferite trebuie să le asigure.*

Situația actuală a certificatelor care sunt în întreținere este următoarea:

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)	16.12.2025
2	Fiscnet, 1 tip digital SSL Secure Site OV cu Wildcard	DigiSign (Symantec)	16.12.2025
3	CTS - OECD, 1 certificat SSL Web Server whit EV, emis de o autoritate de certificare acceptată de către CTS	DigiSign (Thawte)	11.12.2025

4	ANAF, 1 tip Server Web SSL cu Wildcard *.anaf.ro	DigiSign	16.09.2025
5	ANAF, 1 tip Server Web SSL cu Wildcard *.anaf.mfinante.gov.ro	DigiSign	16.09.2025
6	HSM, 1 Certificat digital calificat server HSM	DigiSign (DigiSign)	21.11.2025
7	DTICSV, 1 tip server Web SSL cu Wildcard-*.customs.ro	DigiSign	11.06.2025
8	MFINANTE, 1 tip server Web SSL cu Wildcard *.mfinante.ro,	DigiSign	16.09.2025
9	MFINANTE, 1 tip server Web SSL cu Wildcard *.mfinante.gov.ro	DigiSign	16.09.2025
10	DTICSV, 1 tip server Web SSL cu Wildcard *.swiss-contribution.ro	DigiSign	22.06.2025
11	Certificat tip Server SSL de tip DV (domain validation)	DigiSign	necesități ulterioare
12	Certificat digital calificat Server stocat pe HSM sau eToken	DigiSign	necesități ulterioare

La punctul 1 din tabel este specificat un certificat digital de tip SSL Secure Site – 1 bucată, care certifică schimbul de date între instituțiile financiare și autoritățile fiscale în Serviciul de Schimb Internațional de Date (IDES), sistem care acceptă numai certificatele aprobate de către 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 către IRS este publică în 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 – 1 bucată, emis de o autoritate de certificare acceptată de către CTS. Acest certificat digital trebuie să fie emis de una din autoritățile de certificare agreeate de către administratorul portalului CTS, lista care este dată de acesta odată cu indicațiile de instalare, administrare și utilizare a respectivului portal.

Lista cu autoritățile de certificare acceptată de către CTS este următoarea:

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 – 1 bucată, folosit pentru site-ul oficial ANAF respectiv pentru domeniul *.anaf.ro , acesta asigurând securitatea accesului la respectiva pagină – inclusiv la zona de portal de aplicații.

La punctul 5 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 1 bucată, folosit pentru site-ul oficial ANAF respectiv pentru domeniul *.anaf.mfinante.gov.ro acesta asigurând securitatea accesului la respectiva pagină – inclusiv la zona de portal de aplicații.

La punctul 6 din tabel este specificat un certificat digital de tip Certificat Digital Calificat Server – 1 bucată, folosit pentru activitatea de semnare și criptare calificată automată de mare volum în portalul Agenției Naționale de Administrare Fiscală. Acesta va fi instalat în cele 2 Module de Securitate Hardware (HSM).

La punctul 7 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 1 bucată, și anume, *.customs.ro folosit pentru serverul ce administrează site-ul și portalul Direcției Vamale. Acesta asigură securitatea accesului la pagina respectivă precum și la alte pagini din același domeniu și ale aplicațiilor din acestea.

La punctul 8 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 1 bucată, folosit pentru site-ul oficial al Ministerului de Finanțe, respectiv pentru domeniul *.mfinante.ro, acesta asigurând securitatea accesului la respectiva pagină – inclusiv la zona de portal de aplicații.

La punctul 9 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 1 bucată, folosit pentru site-ul oficial al Ministerului de Finanțe, respectiv pentru domeniul *.mfinante.gov.ro, acesta asigurând securitatea accesului la respectiva pagină – inclusiv la zona de portal de aplicații.

La punctul 10 din tabel este specificat un certificat digital de tip Server Web SSL cu Wildcard – 1 bucată, și 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.

La punctul 11 din tabel este specificată o rezervă de Certificate Server SSL de tip DV (domain validation), care se vor asigura pentru necesități ulterioare, utilizate în cazul aplicării securității noilor domenii sau site-uri ale Ministerului Finanțelor.

La punctul 12 din tabel este specificată o rezervă de Certificat digital calificat Server stocat pe HSM sau eToken, care se vor asigura pentru necesități ulterioare, utilizate în cazul aplicării securității prin instalarea în noi Module de Securitate Hardware (HSM) achiziționate de Ministerului Finanțelor.

6) Specificații tehnice

Specificațiile tehnice cuprinse sunt minimale, obligatorii și reprezintă criteriul de acceptare a ofertei. *Lista certificatelor ce urmează a fi achiziționate / reînnoite este următoarea:*

Nr. crt.	Titular 5ertificate 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	16.12.2025	1
2	Fiscnet, 1 tip digital SSL Secure Site OV cu Wildcard	16.12.2025	1
3	CTS, 1 certificat SSL Web Server whit EV, emis de o autoritate de certificare acceptată de către CTS	11.12.2025	1
4	ANAF, 1 tip Server Web SSL cu Wildcard *.anaf.ro	16.09.2025	1
5	ANAF, 1 tip Server Web SSL cu Wildcard *.anaf.mfinante.gov.ro	16.09.2025	1
6	HSM, 1 Certificat digital calificat server HSM	21.11.2025	1
7	DTICSV, 1 tip server Web SSL cu Wildcard-*.customs.ro	11.06.2025	1
8	MFINANTE, 1 tip server Web SSL cu Wildcard *. mfinante.gov.ro	16.09.2025	1

9	MFINANTE, 1 tip server Web SSL cu Wildcard *.mfinante.ro	16.09.2025	1
10	DTICSV, 1 tip server Web SSL cu Wildcard *.swiss-contribution.ro	22.06.2025	1
11	Certificat tip Server SSL de tip DV (domain validation)	necesități ulterioare	6
12	Certificat digital calificat Server stocat pe HSM sau eToken	necesități ulterioare	6

Specificațiile tehnice pe care certificatele trebuie să le prezinte este următoarea:

1) La punctul 1 din tabel certificatul de tip SSL Secure Site are următoarele caracteristici tehnice; Certificatul SSL Secure site asigură utilizatorilor și gazdelor web să securizeze, un domeniu 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. La acestea se adaugă specificațiile exprese ale autorității care administrează portalul, respectiv de către IRS. Lista aprobată de autorități de certificare (CA) de către IRS este publică în 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 securizarea, unui domeniu și subdomenii nelimitate cu nivel de asigurare ridicată, cu cheie de lungime 2048 – 4096 biți, cu criptare de până la 256 de biți, cu licențe server nelimitate, având sigiliu DigiCert sau Norton Trust și scanare malware cu validare prioritară. 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 următoarele caracteristici tehnice; Certificatul SSL Web Server cu EV asigură utilizatorilor și gazdelor web să securizeze, între 3 și 100 domenii cu asigurare foarte ridicată, cu validare extinsă, cu cheie de lungime 2048 – 4096 biți, cu criptare de până la 256 de biți. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat. În plus, acest certificat digital trebuie să fie emis de una din autoritățile de certificare aprobate de către administratorul portalului CTS, lista care este dată de acesta odată cu indicațiile de instalare, administrare și utilizare a respectivului portal.

Lista cu autoritățile de certificare acceptată de către CTS este următoarea:

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 Server Web SSL cu Wildcard are următoarele caracteristici tehnice; Certificatul SSL cu Wildcard asigură utilizatorilor și gazdelor web să securizeze, un domeniu și toate subdomeniile cu asigurare ridicată, cu cheie de lungime 2048 – 4096 biți, cu criptare de până la 256 de biți. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

5) La punctul 6 din tabel certificatul de tip Certificat Digital Calificat Server are următoarele caracteristici tehnice; Certificat Digital Calificat Server asigură cheia de semnare pentru serverele de semnare de mare capacitate, cu cheie de lungime 2048 – 4096 biți, cu criptare de până la 256 de biți, cu valoare extinsă. Același certificat va fi utilizat pentru două servere (module) de semnare de mare capacitate (HSM). Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

6) La punctul 7 din tabel Certificatul server Web SSL cu Wildcard are următoarele caracteristici tehnice; Certificatul SSL Server cu Wildcard asigură în acest caz securitatea unui server gazdă, respective a unui site cu următoarele caracteristici, autentificare validată pentru organizație / afaceri, să asigure mai multe domenii și toate subdomeniile cu asigurare ridicată, cu cheie de lungime 2048 – 4096 biți, cu criptare de până la 256 de biți. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

7) La punctele 8 și 9 din tabel certificatul de tip SSL cu Wildcard are următoarele caracteristici tehnice; Certificatul SSL cu Wildcard asigură utilizatorilor și gazdelor web securizarea, unui domeniu și toate subdomeniile cu asigurare ridicată, cu cheie de lungime 2048 – 4096 biți, cu criptare de până la 256 de biți. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

8) La punctul 10 din tabel certificatul de tip SSL Server are următoarele caracteristici tehnice; Certificatul SSL Server cu Wildcard asigură în acest caz securitatea unui server gazdă, a unui site cu următoarele caracteristici, autentificare validată pentru organizație / afaceri, să asigure mai multe domenii și toate subdomeniile cu asigurare ridicată, cu cheie de lungime 2048 – 4096 biți, cu criptare de până la 256 de biți. Acesta are valabilitatea de 2 ani calendaristici de la momentul în care a fost generat.

9) Certificatele de la punctele 11 și 12 din tabel se vor solicita, pentru necesități ulterioare, valabilitatea fiind de maxim 2 ani din momentul emiterii sau după caz.

7) Activități specifice

- Toate documentele și informațiile primite de la Ofertant precum și rezultatele tuturor activităților 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 informații confidențiale, iar Ofertantul câștigător va asigura respectarea confidențialității lor, urmând să semneze o declarație în acest sens.

- Ofertantul și personalul său au obligația de a respecta confidențialitatea documentelor și informațiilor menționate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia și după încetarea contractului. În acest sens, Ofertantul precum și toți experții implicați în activitățile contractului sunt obligați să semneze Acorduri de Confidențialitate cu Autoritatea Contractantă.

- Toate documentele, rapoartele și datele, inclusiv diagrame, desene, specificații, planuri, formule, baze de date, software (cod sursă, cod obiect, biblioteci, librării etc.) și orice alte materiale obținute, compilate sau realizate de către Ofertant în cadrul contractului (chiar dacă sunt module sau pachete program deja construite în alte proiecte sau în cadrul unor pachete disponibile comercial), sunt în proprietatea /proprietatea intelectuală a Autorității Contractante, aceasta având dreptul să le utilizeze, modifice, transfere fără acceptul Ofertantului sau al unei terțe părți. Ofertantul le va furniza Autorității Contractante, la finalizarea contractului, fără a păstra copii și fără a le utiliza în alte scopuri care nu au legătura cu contractul fără acordul scris al Autorității Contractante.

- Ofertantul nu va publica articole sau informații legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terți și nu va divulga informațiile obținute 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 iniția pentru fiecare certificat în parte înainte cu minim 5 zile înainte de expirare, procedura de înlocuire / prelungire a certificatului care expiră.

2. Se vor efectua actele tipice necesare procedurii de achiziție 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 și trimiterea certificatului de revocare pe baza căruia se va livra noul certificat.

5. Se va proceda la instalarea noului certificat emis.

6. Se va testa funcționarea aplicațiilor, nivelelor de securitate și compatibilitatea noului certificat emis.

8) Obligațiile prestatorului de servicii de certificare

Prestatorul de servicii de certificare se va obliga:

1. Să furnizeze produsele și serviciile de certificare aferente certificatelor digitale prezentate, conform unei proceduri propuse de prestator și agreată cu beneficiarul, la prețurile unitare oferite.

2. Să notifice beneficiarul după efectuarea oricărei modificări a Politicii de Certificare, Codului de Practici și Proceduri sau a altei proceduri care stau la baza furnizării produselor și serviciilor.

3. Să respecte prevederile legislației române în vigoare, în legătura cu produsele și serviciile furnizate.

4. Să asigure, în mod gratuit accesul la toate informațiile necesare utilizării corecte și în condiții de siguranță a produselor și serviciilor aferente.

5. Să nu colecteze date cu caracter personal decât în măsura în care aceste informații sunt necesare în vederea eliberării și conservării certificatelor emise.

6. Să asigure asistența beneficiarului în implementarea serviciilor de certificare.
7. Să pastreze confidențialitatea informațiilor încredințate, conform legislației române în vigoare.
8. Să țină un registru electronic de evidență 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 până vineri în intervalul orar 08:00 – 19:00.
11. Să notifice beneficiarul în termen de 24 de ore de la orice modificare, în cazul în care informațiile cuprinse în contract, inclusiv adresa, numărul de telefon, numărul de fax și adresa de e-mail, nu mai corespund realității.
12. Să notifice beneficiarul asupra deciziei de revocare a unui certificat în cel mai scurt interval de timp de la momentul la care a luat la cunostință cauza de revocare/suspendare, dar nu mai târziu de o oră de la decizia de revocare/suspendare a certificatului.
13. Să notifice beneficiarul cu privire la orice modificare care apare în statutul său, situația sa care se actualizează în Registrul Autorității de Reglementare și Supraveghere (conform prevederilor legale în vigoare), precum și orice altă situație care ar putea afecta derularea în bune condiții a contractului.
14. Să notifice beneficiarul cu privire la apariția oricărei condiții care pot avea ca efect imposibilitatea emiterii de certificate cum ar fi derularea unei acțiuni de investigație a autorităților competente în domeniu.
15. Să notifice beneficiarul cu privire la încetarea calității de furnizor de servicii de certificare și din acel moment, să nu mai emită certificate, returnând către acesta actele de solicitare cărora urma să le dea curs.

9) Calitatea serviciilor

1. Prestatorul de servicii de certificare trebuie să îndeplinească condițiile prevăzute de legislația română, în vederea emiterii certificatelor digitale.
2. Prestatorul de servicii de securitate va confirma că certificatele digitale eliberate sunt în conformitate cu prevederile legale în vigoare specifice domeniului.
3. Nivelul de securitate asigurat de prestatorul de servicii va fi în conformitate cu standardele minime recunoscute: ISO/IEC 15408-1, 2, 3; ISO 27001 și 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 și cu respectarea recomandărilor ITU-T X. 509.

10) Condiții de livrare și recepție

- 1) Prestatorul de servicii de certificare va elibera certificatele digitale solicitate prin comenzile beneficiarului, cu respectarea procedurii stabilite de comun acord cu acesta.

2) Recepția produselor se va efectua prin procese verbale de recepție, semnate de reprezentanții ambelor părți. Facturile vor fi însoțite obligatoriu de procesele verbale de recepție, întocmite în urma verificării conformității acestora cu comanda primită, în copie.

3) Produsele și serviciile din prezentul caiet de sarcini (Anexa 1), reprezintă cantitatea maximă contractuală, prețurile/tarifele oferite fiind ferme și valabile pe toată durata contractului.

11) Garanție și cerințe specific

Certificatele nou emise, sunt, în momentul în care devin funcționale acoperite de garanție, pe toată durata de valabilitate pe care acestea o prezintă în momentul instalării, respectiv 2 ani.

Prestatorul de servicii de certificare va înlocui produsele fără nici un cost suplimentar în perioada de garanție.

Mentenanța pe perioada de garanție este gratuită.

12) Procedura de eliberare a certificatelor digitale tip server

Procedura va fi propusă de prestatorul de servicii de certificare și agreată cu beneficiarul și va conține cel puțin următoarele informații:

1) Procedura de emitere a certificatelor digitale.

2) Procedura de reînnoire a certificatelor digitale.

3) Procedura de revocare a certificatelor digitale:

3.1 Revocare inițiată de prestatorul de servicii de certificare,

3.2 Revocare inițiată de beneficiar.

13) Rezultate așteptate

În urma efectuării acestei achiziții se preconizează atingerea următoarelor obiective:

- asigurarea securității datelor care se vor semna cu aceste certificate,
- ridicarea gradului de încredere a utilizatorilor la accesarea paginilor oficiale prezentate public de cele trei instituții, Ministerul Finanțelor, Agenția Națională de Administrare Fiscală și a Direcției Vamale,
- ridicarea gradului de încredere a utilizatorilor la accesarea portalelor de aplicații oficiale aferente celor trei instituții, Ministerul Finanțelor, Agenția Națională de Administrare Fiscală și a Direcției Vamale,
- ridicarea gradului de securitate a datelor transferate în 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 în ofertă.
- Se va menționa autoritatea de certificare emitentă, după caz în funcție de tipul de certificat digital oferat.
- Se va menționa clar perioada de valabilitate a certificatului oferat, perioadă care va trebui să se regasească în partea de prezentare a acestuia.
- Va trebui să respecte lungimea cheii și nivelul de criptare solicitat.
- Va trebui respectat nivelul și acoperirea asigurată de certificatul anterior la înlocuire / prelungire acolo unde este necesară această caracteristică a certificatului digital oferat.