CAIET DE SARCINI

SERVICII DE DEZVOLTARE A SOLUȚIEI “MOLDOVA GOV CA”

CONȚINUT

1. TERMENI ȘI ABREVIERI

MoldovaGovCA – soluția (serviciul din SO) de administrare a Autorității de Certificare

CA WEB Panel – panelul de gestionare unificat

LDAP - Lightweight Directory Access Protocol

CA – Autoritate de Certificare

RA – Autoritate de Înregistrare

CRL – Certificate Revocation List

CMP – Certificate Management Protocol

STISC – I.P Serviciul Tehnologia Informatiei și Securitate Cibernetica

CSR – fișier-cerere de certificare

HSM – modulul hardware de securitate

OCSP – Online Certificate Status Protocol

PKI – Public Key Infrastructure

SO – Sistem de Operare

TSA – autoritate de marcare temporală

TSP – Time Stamp Protocol

X.509 – standard ce determină structura certificatului cheii publice

XML - Extensible Markup Language

WSDL - Web Services Description Language

SOAP - Simple Object Access Protocol

Robot – mecanism autonom ce va permite executarea unei sarcini care se declanșează periodic sau ca urmare unei cereri(request) parvenit prin interfața de administrare sau interfața programabila API sau CMP

2. RFC ȘI ALTE STANDARTE

X.509 – RFC 5280

OCSP – RFC 6960

CRL – RFC 5280

CMP – RFC 2510 4210 4211

TSP – RFC 3161

IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
IETF RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP, HTTP;

IETF RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP, HTTP;

IETF RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP, HTTP;

3. SCOP DOCUMENT

Acest document oferă o ilustrare detaliată a cerințelor funcționale și non funcționale ale MoldovaGovCA destinate gestionării autorității de certificare, inclusiv configurarea serviciilor.

4. SFERA DE APLICARE

Acest document este menit folosirii drept resursă informațională detaliată a cerințelor arhitecturii soluției MoldovaGovCA la etapa de proiectare a acestora. Documentul este adresat dezvoltatorilor și arhitecților de sistem.

Cunoștințe necesare: Tehnologii Web, Web Servicii (SOAP), cunoștințe avansate în rețele, UML, criptografie, PKI.

5. ANALIZA DOMENIULUI DE APLICARE

5.1. INTRODUCERE

Soluția MoldovaGovCA urmează a fi aplicată în cadrul infrastructurii cheilor publice, și presupune un spectru de funcționalități care ar acoperi în mare parte acest segment.

Aceasta se solicită a avea la bază o structură arborescentă în cadrul căreia vor fi amplasate componentele. Procesul de setare/interacțiune cu MoldovaGovCA se propune a fi prin intermediul WEB-interfeței și presupune careva etape stabilite, și anume crearea CA, dar și TSA, și specificarea parametrilor nemijlocit pentru acesta, după care, la un nivelul mai jos, doar pentru CA configurarea serviciilor pentru acesta (API, CMP, OCSP, CRL robot) cu parametrii adiacenți acestora, configurarea și management-ul roboților serviciilor și modului în care acestea funcționează. Pentru TSA va fi prezentă paleta de configurări specifice acestuia și robotul care va răspunde la cereri. De menționat că pot exista mai multe asemenea structuri în paralel (multiple CA/TSA). Time Stamp Authority (TSA), din perspectiva specificului acestui component, se presupune că va fi amplasat la același nivel, alături de CA, și nu va fi specific pentru fiecare CA spre deosebire de componentele API, CMP, OCSP, CRL.

Soluția se propune a fi una modulară, scalabilă, formată din mai multe componente de bază ce vor funcționa autonom.

Sistemul va cuprinde obligatoriu câteva componente autonome de bază:

- MoldovaGovCA Core – componenta principală ce realizează nucleul de bază;
- MoldovaGovCA UI – interfața utilizatorului, modul de administrare (CA WebPanel);
- MoldovaGovCA API – componenta ce implementează interfețele programabile API (CMP,Soap/XML) destinate gestionarii certificatelor;
- MoldovaGovCA Public Services – componenta ce implementează interfețele publice(OCSP,TSP,HTTP-CRL)

Toate componente vor lucra într-un regim autonom, care va permite separare fizică și logică. Suplimentar aceste componente vor rula într-un regim de ***Grup*** (Cluster,Farm) pentru asigurarea unui nivel înalt de disponibilitate precum și pentru distribuirea încărcăturii.

Adăugător la acestea care sunt prezente nemijlocit în procesul de setare și configurare inițial, se presupune prezența funcționalului de administrare și management cu posibilitatea modificării oricărui parametru, re-emiterii listei certificatelor revocate manual, semnarea manuala a certificatelor utilizând CSR și altele.

Fiecare interacțiune a utilizatorului fie cu interfața CA Web Panel fie cu API-ul nemijlocit se loghează în strânsă legătură cu certificatul folosit la autentificare în baza căruia a fost primit accesul. Logurile sunt necesare de stocat în baza de date separată, cu asigurarea unui mecanism de integritate a acesteia pentru a preveni careva modificări efectuate în istoric.

Sub formă de fișiere textuale sunt necesare de logat în mai multe nivele setabile (All, Info, Debug, Error, etc) log-urile nemijlocit a aplicațiilor.

Toate operațiunile administrative se propun a fi realizate prin intermediul CA WEB Panel.

5.2. DOMENIUL DE APLICARE

Soluția de administrare a autorității de certificare este destinată pentru crearea și configurarea diferitor CAs, TSAs, inclusiv și configurarea unor servicii pentru acestea.

6. CERINȚE FUNCȚIONALE

Panoul primar de administrare/configurare se presupune a fi CA WEB Panel, care va rula prin intermediul unui WEB server în legătură cu SGBD, unde se vor stoca configurările făcute, logurile acțiunilor dar și tranzacționale și altă informație relevantă. Se propune ca soluția dezvoltata să înregistreze cate un serviciu pentru fiecare CA, CMP, OCSP, TSA, CRL ce vor asigura funcționalitatea acestora și care vor fi configurate din CA WEB Panel. API prin care vor avea loc prelucrările cererilor similar ca CMP va fi de tip XM SOAP WEB API. Adăugător la API și CA WEB Panel vor mai persista și componente/servicii ce vor rula în background (CMP protocol pentru certificarea/emiterea cheilor, CRL robot, ...), toate rulând pe porturi diferite setabile în interfață.

6.1. TEHNOLOGII ȘI ALGORITMI SUPORTAȚI

Tipuri de HASH-uri suportate:

Toate componentele/serviciile soluției trebuie să suporte următorii algoritmi de hash, cu posibilitatea de a selecta pentru fiecare varianta potrivită:

- SHA-1
- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)

Algoritmi privind lungimea cheilor:

- RSA până la 8192 biți
- DSA până la 1024 biți

În cazul unei soluții MoldovaGovCA compatibile cu SO Windows aceasta trebuie să funcționeze atât folosind certificate stocate în Windows Certificate Store prin intermediul Microsoft CryptoService Provider și/sau certificate stocate pe dispozitive HSM (cu asigurarea compatibilității și posibilitatea de a interacționa cu diverse modele de HSM cu librării PKCS#11). Configurarea locului de stocare a cheilor va avea loc la etapa inițială de creare și setare CA.

6.2. INTERFAȚA CA WEB PANEL

Soluția va dispune de o interfață WEB ce va fi folosită pentru management.

Autentificarea în interfață este necesar de realizat în bază de certificat de autentificare, cu posibilitatea gestionarii drepturilor pentru fiecare utilizator. Au fost identificate câteva roluri de bază și anume: AllReadOnly – se permite accesarea tuturor funcționalităților doar pentru a le vizualiza, fără a putea efectua careva modificări, StatisticsReadOnly – se permite vizualizarea tuturor compartimentelor ce conțin date statistice aferente tranzacțiilor, la fel este permisă căutare în certificate, și Full – care cuprinde întreg spectrul de funcționalități.

Pentru OCSP/CRL roboți sunt necesare funcționalități de sheduller care vor avea ca scop definirea acțiunilor caracteristice acestora. CRL va putea fi programat în raport cu retenția acestuia, cu setarea perioadei de auto-emitere, cu suportul Base CRL dar și Delta CRL, opțional.

Pentru CA/TSA este necesar să fie prezent funcționalul de definire a template-urilor cu anumite configurări, salvarea acestora, și utilizarea opțională ulterioară la crearea CA/TSA.

În continuare sunt descrise succint etapele identificate în procesul de configurare CA/TSA după cum urmează a fi amplasate ierarhic și o imagine cum acestea sunt văzute:

- Nivelul 1, Crearea și setarea nemijlocit a CA/TSA – configurarea unui profil de CA/TSA, folosind un template presetat, sau selectând fiecare parametru în particular după necesități. După care se execută generarea perechii de chei și a certificatului cheii publice, precum și a CSR în cazul când acesta urmează să fie semnat de o autoritate superioară (în cazul CA/TSA de nivel superior – auto certifică cheia publică), instalarea certificatului cheii publice.
  Este necesar funcționalul de utilizare la creare a template-urilor configurabile de administrator, cu selectarea tuturor parametrilor necesari, salvarea acestui template și ulterior utilizarea lui la crearea altui CA, pentru a omite setarea manuală a tuturor parametrilor repetat, la fel pot fi extrași toți parametrii și opțiunile de la un CA care deja este setat și funcționează.

- Nivelul 2, Configurarea serviciilor CA – cu ajutorul CA WEB Panel se configurează următoarele servicii adiacente: prelucrarea cererilor de certificare (requesturilor) și emiterea certificatelor cheilor publice (de către CA) utilizând CSR, XML SOAP API sau Certificate Management Protocol (CMP), serviciul de obținere a informației despre statutul certificatului (OCSP), configurarea sheduler-urilor pentru retenția de actualizare a listei certificatelor revocate (CRL) și reemiteri automate cu posibilitatea folosirii Base CRLs dar și Delta CRLs opțional.
  Configurarea roboților CA – poate fi pornit/oprit/repornit programul-robot aferent autorității căruia îi este atribuit. Acesta se propune să ruleze ca component autonom, fiind gestionat din interfața CA WEB Panel, cu posibilitatea setării parametrilor de autopornire la startul sistemului, monitorizare și auto-repornire în caz de crush/lipsă proces/serviciu.
- Nivelul 3, Configurarea serviciilor TSA – la accesarea unui TSA definit anterior este posibilă setarea configurărilor pentru acesta din perspectiva specificului lui, la fel a roboților ce vor răspunde de funcționalitatea TSA.

În regim normal fiecare parametru setat inițial poate fi accesat și modificat de către administrator.
Prin interfață urmează să fie efectuate toate operațiunile de (re)configurare și mentenanță, în special:

- Crearea și configurarea profilului pentru autoritățile de certificare;
- Crearea și configurarea autorității TSA;

- Crearea și configurarea serviciului OCSP;
- Gestionarea Certificatelor cheilor publice;
- Gestionarea și vizualizarea logurilor cu aplicarea filtrelor de căutare (logurile presupun să includă toate acțiunile efectuate prin CMP sau XML SOAP API, dar și logurile din cererile spre TSA și OCSP);
- Gestionarea notificărilor ce urmează a fi expediate în cazul expirării certificatelor cheilor publice, dar și a cheilor private (pentru toate certificatele root/subroot separat pentru care destinatari vor fi administratorii, cât și pentru certificatele emise de CA titularilor finali, adresa acestora fiind extrasa din câmpul respectiv conform RFC822), ca funcțional adăugător opțional, cu posibilitatea de a seta retenția expedierii notificărilor, intensității și template-ului textului notificărilor dar și setarea MAIL server-ului prin care va avea loc expedierea acestor mesaje. Adăugător este necesar de elaborat funcțional ce ar permite expedierea notificărilor pentru toate certificatele către o adresă de email adăugătoare paralel cu adresa indicată în certificat nemijlocit.
- Vizualizarea statistică ce ține de certificatele emise, revocate și suspendate, cu posibilitatea aplicării filtrelor după tip cerere(emitere/revocare/suspendare), diapazon de timp, autoritate, persoana juridică (IDNO) sau fizică (IDNP; Nume, Prenume), persoanei care a inițiat acțiunea conform certificatului cu care a fost realizată autentificarea în sistem (Serial Number la certificat) și exportării rapoartelor în CSV;
- Componenta va permite gestionarea parametrilor de autentificare și autorizare în componenta MoldovaGovCA API cel puțin după următoarele criterii:

  .1. GroupName(RaCenter,ClientID);

  .2. IpSource(ClientIP, ProxyIP);

  .3. ClientCertificate;

  .4. HttpAction;

  .5. TypeOfRequest(IssueCertificate,Revocation,etc…);

  .6. AllowedParameterValue (static,wildcard);

  .7. TimeRange restriction(sample: 08:00-17:00).

- Și alte configurări.

6.3. CERINȚE FAȚĂ DE CREAREA ȘI CONFIGURAREA AUTORITĂȚII DE CERTIFICARE

Crearea și configurarea autorității de certificare presupune următoarele:

- Crearea și setarea profilului CA.

1. configurarea unui profil pentru un CA concret presupune câteva etape. Inițial este definita denumirea acestuia și în baza ei este creată în mod automat la final o bază de date cu denumirea corespunzătoare în care urmează a fi stocate toate datele aferente acestui CA, si anume tabela cu logurile tranzacționale, tabela cu câmpurile aferente tuturor certificatelor parvenite spre semnare în care ulterior, după finisarea procedurii de certificare, va fi stocat și certificatul cheii publice semnat de CA sub forma de blob, tabela de sistema în care se vor stoca datele aferente configurărilor acestui CA și alte date aferente. Pentru fiecare CA, opțional, este necesară funcționalitatea de setare a unui director LDAP în care acesta automat, in baza de scheduling setat, va salva certificatele cheilor publice conform schemei oferite, sau le va salva imediat, posibilitate configurabilă de către administrator pentru fiecare CA.

2. generarea perechii de chei și a certificatului cheii publice:

Pentru CA de nivel superior – după crearea profilului CA, aceasta va fi selectată din lista CAs pentru a realiza procesul de generare a perechii de chei în baza cererii de certificare ce va conține următoarele câmpuri: Country, State or Province, City, Organization, Department, CA Name, Email address. Totodată, se vor menționa parametrii criptografici (algoritmul semnăturii electronice, funcțiile hash, tipul criptoprovider-ului, lungimea cheii) și tipul CA – Root CA, parametrii și statutul lor în conformitate cu X.509 (e.g., URL-urile aferente CRL/OCSP, utilizarea cheii, utilizarea extinsă a cheii). În plus, va exista posibilitatea creării copiei certificatului în fișier format PKCS#12 cu specificarea parolei.

Pentru CA subordonat – după crearea CA aceasta va fi selectată din lista CAs pentru a realiza procesul de generare a perechii de chei în baza cererii de certificare ce va conține următoarele câmpuri: Country, State or Province, City, Organization, Department, CA Name, Email address. Totodată, se vor menționa parametrii criptografici (algoritmul semnăturii electronice, funcțiile hash, tipul criptoprovider-ului, lungimea cheii) și tipul CA – SubRoot CA, parametrii și statutul lor în conformitate cu X.509 (e.g., URL-urile aferente CRL/OCSP, utilizarea cheii, utilizarea extinsă a cheii). În plus, se va indica calea și numele CSR-ului și opțiunea de codificare (implicit – formatul DER, dar cu posibilitatea de a selecta și PEM).

3. instalarea certificatului cheii publice:

dacă lanțul de certificare se păstrează în fișierul generat de RootCA pentru instalarea certificatului cheii publice se indică calea completă și numele fișierului. În plus, va exista posibilitatea creării copiei certificatului în fișier format PKCS#12;

dacă lanțul de certificare se păstrează în fișier format PKCS#12 acesta, împreună cu cheia, se impostează.

- Configurarea serviciilor CA

Cu ajutorul funcțiilor CA WEB Panel se configurează următoarele servicii: prelucrarea cererilor de certificare (requesturilor) prin CMP over HTTP sau XML SOAP și emiterea certificatelor cheilor publice (CA), serviciul de obținere a informației despre statutul certificatului (OCSP), actualizarea automată a listei certificatelor revocate (CRL). Fiecare CA va beneficia de serviciile proprii, care nu va avea tangente cu alte CA.

- Configurarea roboților.

1. setarea clientului poștal și a directoriilor active,

2. selectarea serviciului-robot (Certificate Authority, Online Certificate Status Protocol, Certificate Revocation List, Time-Stamp Authority) și înscrierea setărilor aferente acestuia. Programul-robot poate fi pornit/oprit/repornit și acesta aparține doar autorității în cadrul căreia a fost creat. Acesta se propune să ruleze ca service aparte în sistem pentru fiecare serviciu, fiind gestionat din interfața CA WEB Panel, cu posibilitatea setării parametrilor de autopornire la startul sistemului, monitorizare și auto-repornire în caz de crush/lipsa proces/serviciu.

2.1. *Robotul de emitere a certificatelor (CMP / XML SOAP API)*. După selectarea robotului se vor introduce parametrii certificatului în conformitate cu X.509, se va selecta regimul de prelucrare a cererilor de certificare (obișnuit sau în așteptare).

2.2. *Robotul pentru obținerea informației privind statutul certificatului (OCSP)*.

2.3. *Robotul de modificare a listei certificatelor revocate (CRL)*. După selectarea robotului se vor introduce parametrii de creare a listei certificatelor revocate. Lunar, adăugător la certificatul CRL generat și înlocuit în mod normal, se vor genera CRLs cu o valabilitate de 24 luni ce urmează a fi păstrate într-un anumit tabel în baza de date, sub forma de blob, cu câmpuri ce reprezintă data emiterii acestuia, data expirării, numărul de înscrieri din el, alta informație relevantă, retenția fiind configurabilă. De asemenea robotul de modificare a listei de certificate revocate trebuia sa conțină careva funcționalități adăugătoare specifice ce ar permite mai flexibil gestionarea lui și listei nemijlocite.

2.4. *Robotul de aplicare a mărcii temporale (TSA)*. După selectarea robotului se vor introduce parametrii pentru crearea mărcii temporale cu indicarea politicii și a canalului de comunicații.

NOTĂ: O politică poate fi adăugată/ștearsă/redenumită în lista politicilor.

NOTĂ: toate procesele se finalizează cu un mesaj (de succes sau cu menționarea erorii).

6.4. CERINȚE FAȚĂ DE EMITEREA CERTIFICATULUI CHEII PUBLICE A UTILIZATORULUI

Emiterea certificatului cheii publice a utilizatorului are loc în baza cererii de certificare (CSR, folosind protocolul CMP prin HTTP sau prin XML SOAP API). Parametrii din certificat și statutul acestora vor fi în conformitate cu X.509. Procesul se finalizează cu un mesaj (de succes în log separat sau cu menționarea erorii în caz că aceasta are loc, în log separat).

Toate certificatele emise/certificate de către CA se păstrează în baza de date în o tabela, opțional cu posibilitatea setării adăugător unui director LDAP în care certificatele să fie stocate în baza de o schema predefinita, acțiunea având loc în bază de scheduler ce defineste timpul de sinhronizare și înscrie toate certificatele din perioada x, dar si cu posibilitatea setării înscrierii momentane a certificatului în LDAP. Structura tabelei presupune prezenta tuturor câmpurilor posibile la emiterea certificatului, cu alte careva câmpuri de sistem necesare după caz, și cu un câmp în care se păstrează certificatul nemijlocit sub forma de blob. În aceasta tabela automat sunt pre completate și salvate absolut toate câmpurile certificatului care parvin spre semnare, și alături certificatul cheii publice integral sub forma de blob, dar și SN al certificatului în baza căruia a fost autentificata tranzacția și a parvenit cererea respectiva.

XML SOAP API (WSDL) presupune o alternativă pentru CMP cu funcțional similar, adresarea spre care are loc prin HTTPS, folosind autentificarea prin certificatul utilizatorului la adresare.

6.5. CERINȚE FAȚĂ DE LISTA CERTIFICATELOR REVOCATE

Fiecărei autorități de certificare îi corespunde o listă a certificatelor revocate. Parametrii aferenți CRL și statutul acestora vor fi în conformitate cu X.509. Fiecărui certificat al cheii publice, ce urmează a fi revocat, îi va corespunde o cauză de revocare din lista predefinită. CRL va fi actualizat la un anumit număr de zile și ori de câte ori în listă se adaugă un nou certificat, iar lunar se vor genera CRLs, cu perioada de valabilitate de 24 luni, ce urmează a fi păstrate într-un anumit tabel în baza de date, sub forma de blob, cu câmpuri ce reprezintă data emiterii acestuia, data expirării, numărul de înscrieri din el, alta informație relevantă, retenția fiind configurabilă.

6.6. LOGAREA EVENIMENTELOR

Soluția va poseda 2 tipuri de loguri:

- Loguri de Aplicație (Error / Debug cu mai multe nivele)

- Loguri Tranzacționale (absolut toate tranzacțiile efectuate cat prin interfața atât și prin API)

6.6.1. LOGURILE DE APLICAȚIE

Logurile de Aplicație vor fi salvate în fișiere local, delimitate zilnic, pentru Error și altul pentru Debug, sau trimise la un server remote de syslog în formatul JSON.
Denumirea fișierului, adresa ip a serverului, portul și protocolul de transport (tcp/udp) vor fi citite din config.
Aplicația trebuie să ofere un șablon customizat de logare a evenimentelor. Acest șablon va permite alegerea acțiunilor ce necesită logate și ordinea lor.
Șablonul va include:

- Hostname-ul serverului pe care a avut loc acțiunea
- Timpul acțiunii
- Acțiunea propriu zisă
- Altă informație relevantă

De asemenea, șablonul va oferi posibilitatea să alegem unul din următoarele nivele de logare p-u fiecare acțiune:

- Error
- Warning
- Info
- Debug

6.6.2. LOGURILE TRANZACȚIONALE

Toate Logurile Tranzacționale vor fi logate în baza de date.
Șablonul va permite alegerea următorilor parametri pentru logare:

- Încercările de transmitere a cererii de certificare către CA
- Timpul consumat pentru îndeplinirea acestei acțiuni
- Încercările de autentificare (ssl client authentication)
- Statutul acțiunii (dacă s-a finisat cu succes ori nu)
- IP unde a avut loc acțiunea
- CN-ul Certificatului
- Serial Number al certificatului

6.7. MODULUL CMP

Modulul CMP va fi folosit pentru emiterea, generarea și revocarea certificatelor conform RFC4210, RFC4211.

7. CERINȚE NEFUNCȚIONALE

Ofertantul va prezenta o data cu oferta de preț și descrierea tehnica a soluție, ce va ilustra arhitectura propusa spre implementare.

7.1. ADMINISTRARE

Administratorul soluției MoldovaGovCA trebuie să dețină cunoștințe de bază legate de X.509, CRL, OCSP, TSP, SOAP.

Aplicația va poseda o interfață WEB simplă, intuitivă și confortabilă.
La proiectarea și implementarea interfeței de administrare se va implementa în baza tehnologiilor:

- MVC
- bootstrap version 4.
- jQuery verion 3

~~7.3.~~7.2. FIABILITATE

Fiabilitatea sistemului este un aspect foarte important. Măsuri de control al excepțiilor trebuie să fie implementate la fiecare nivel de logică al soluției, de exemplu, validarea datelor primite, gestionarea erorilor de comunicare de date.

~~7.4.~~7.3. Disponibilitate

Disponibilitatea sistemului este un aspect foarte important. Sistemul trebuie sa ofere mecanisme de clustering (High Availability) pentru fiecare component, fapt ce va permite extinderea pe orizontala prin adăugarea resurselor de procesare.

~~7.5.~~7.4. PERFORMANȚĂ

Soluția trebuie să fie receptivă, să fie capabilă să funcționeze concomitent, fără degradarea semnificativă a calității, cu cel puțin **100** interpelări pe secundă.

Răspunsul în timpul operațiunilor ce folosesc date de intrare nu trebuie să depășească **3** secunde.

~~7.6.~~7.5. LIVRABILE

Va fi transmisă documentația specifică ce va descrie fiecare componentă a soluției, în scopul eficientizării întreținerii și efectuării viitoarelor modificări.

Va fi transmis către beneficiar codul sursă și drepturi de autor al soluției dezvoltate.

Va fi transmis către beneficiar instrucțiunea de instalare, ghidul de administrare și depănare a aplicației.

Va fi transmisă către beneficiar o licență perpetuă, nelimitată, transmisibilă și fără limitări.

~~7.7.~~7.6. GARANȚII

Garanția pentru soluția MoldovaGovCA trebuie să constituie cel puțin 12 luni calendaristice.

~~7.8.~~7.7. INTERFAȚĂ

Interfața va fi simplă și convenabilă pentru a oferi administratorului un mediu confortabil și intuitiv.

~~7.9.~~7.8. PACKAGING

Echipa de dezvoltatori va instala și configura soluția în mod corespunzător. Adițional, va fi oferită documentația de instalare și configurare.

~~7.10.~~7.9. INTERACȚIUNEA CU SOLUȚIA

Interacțiunea cu soluția MoldovaGovCA și setarea tuturor serviciilor incluse în aceasta se va efectua prin CA WEB Panel.

8. REGULI PRIVIND ORGANIZAREA ȘI PRESTAREA SERVICIILOR DE MENTENANȚĂ

8.1. Scopul regulilor privind organizarea și prestarea serviciilor de mentenanța

Scopul acestor Reguli este de a stabili modalitatea și procesele de interacțiune între Prestator și Beneficiar în vederea prestării și utilizării Serviciilor de mentenanță aferente soluției MoldovaGovCA, nivelul agreat de Servicii, precum și responsabilitățile individuale ale Prestatorului și Beneficiarului în cadrul acestor procese, numite în continuare Servicii.

Prezentele Reguli vor fi anexe la Contract și vor asigură cadrul funcțional pentru prestarea Serviciilor de către Prestator și utilizarea acestora de către Beneficiar.

8.2. Organizarea procesului de prestare a serviciilor

i. Interacțiunea între Părți

Aspectele administrative ce dețin de interacțiunea dintre Prestator și Beneficiar se va efectua prin intermediul Persoanelor responsabile desemnate de Părți.

Fiecare Parte va desemna câte o persoană responsabilă de relația cu cealaltă (Manager Suport Client). Părțile se vor informa reciproc, despre persoana desemnată și informația de contact a acesteia (numele, prenumele, funcția, nr. telefon, e-mail, etc.).

Suportul operațional la utilizarea Serviciilor este asigurat de către Prestator prin intermediul unui singur punct de acces - Serviciul Suport Clienți (SSC).

SSC al Prestatorului va fi disponibil 24x24x365 pentru recepționarea solicitărilor. Disponibilitatea pentru soluționarea acestora este determinată de nivelul agreat de servicii.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități (enumerate în ordinea descreșterii preferinței) :

1. utilizarea sistemului de gestiune a solicitărilor (Service Desk) al Prestatorului.
2. expedierea de e-mail la adresa SSC;
3. apel telefonic la numărul corporativ al SSC.

8.3. Reguli de înregistrare a solicitărilor

Solicitare este orice interpelare formulată de un utilizator al Beneficiarului aferentă sistemului informatic deservit. În funcție de natura evenimentului care a generat solicitarea și rezultatul așteptat, interpelarea poate fi clasificată drept:

a) **Solicitare de suport** – reprezintă o solicitare a unui serviciu privind funcționarea SIF sau/și mediului conex. În rezultatul solicitării de suport Beneficiarul așteaptă prestarea serviciului solicitat conform nivelului de calitate prestabilit. Solicitare de suport nu include și nu prevede dezvoltarea sistemului informatic.

b) **Incident** – reprezintă orice solicitare care are la bază un **incident** de funcționare a sistemului informatic. În rezultatul solicitării de suport Beneficiarul așteaptă o soluție privind înlăturarea sau ocolirea incidentului / problemei enunțate. În cazul când soluția optimă determină necesitatea de dezvoltare a sistemului informatic și există o soluție de ocolire a erorii care asigură funcționarea sistemului informatic la un nivel de performanță acceptabil, atunci va fi aplicată soluția de ocolire, iar soluția optimă va fi recalificată în solicitare de dezvoltare.

c) **Solicitare de dezvoltare** – orice solicitare care necesită dezvoltarea sistemului informatic și presupune realizarea de noi funcționalități prin elaborarea de cod program sau modificare conținut informațional a BD (bazei de date). Serviciile de dezvoltare oferite de Prestator nu includ dezvoltare de funcțional care dețin de alte produse program utilizate de sistemul informatic sau licențele pentru acestea.

Orice solicitare din partea Beneficiarului este adresată Prestatorului prin intermediul SSC al acestuia.

În scopul enunțului solicitării către SSC al Prestatorului, Beneficiarul va întreprinde în ordinea indicată, următoarele:

1. Va consulta ghidurile utilizatorului în vederea asigurării corectitudinii acțiunilor sale și identificării eventualelor soluții;

2. Va consulta prin intermediul persoanei responsabile a Beneficiarului ”Baza de Cunoștințe” pusă la dispoziție de Prestator prin intermediul portalului intern al SSC;

3. Va contacta Serviciul Suport Clienți.

Beneficiarul trebuie să poată justifica modalitatea de contact selectată (ex. de ce apel telefonic și nu interfața web). Prestatorul poate solicita Beneficiarului să utilizeze altă modalitate de contactare a SSC, în cazul în care acest fapt corespunde Regulilor.

În scopul prestării serviciilor de mentenanță în care se încadrează solicitarea SSC:

1. SSC efectuează expertiza preventivă a fiecărei solicitări:
    - identifică tipul acestuia: solicitare de suport, incident sau solicitare de dezvoltare:
    - clasifică solicitările din punct de vedere al impactului și al urgenței declarată de Beneficiar.
    - determinată prioritatea de soluționare considerând regulile privind managementul solicitărilor conform tipului acesteia.
2. Înregistrează informația necesară pentru acordarea suportului:
    - *în cazul incidentelor*, identifică și înregistrează parametrii de mediu: componenta sistemului informatic la care se referă, consecutivitatea de acțiuni care au dus la apariția incidentului, conținutul incidentului, rezultatul așteptat, și alți parametri prevăzuți de reglementarea internă cu privire la gestiunea incidentelor.
    - *în cazul solicitării de suport* identifică serviciul solicitat conform acordului;

- *în cazul solicitărilor de dezvoltare* înregistrează: conținutul solicitării, baza normativă pentru dezvoltare, descrierea succintă a business procesului necesar de dezvoltat și rezultatul așteptat.

3. Orice solicitare parvenită în adresa Prestatorului va fi analizată de acesta și raportată decizia. În funcție de complexitatea solicitării decizia poate să conțină:
   - soluția – în cazul unor incidente/ probleme prezente în baza de cunoștințe sau repetitive.
   - timpul necesar de prezentare a soluției – în cazul lipsei necesității investigării subiectului
   - planul de analiză – în cazul necesității unor analize suplimentare
   - refuzul sau redirecționarea sarcinii în cazul când aceasta nu deține de competența Prestatorului. În cazul refuzului Prestatorul va argumenta decizia și va comunica Beneficiarului în competența cui este soluționarea acesteia.

4. În cazul acceptării solicitării, Prestatorul va comunica soluția sau planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului, iar în cazul solicitărilor de dezvoltare și a costului estimativ conform tarifelor.

   Planul de soluționare poate fi schimbat în funcție de evoluția soluției acesteia doar cu acordul ambelor părți.

5. Modul de realizare a activităților și prezentarea rezultatelor este determinat de tipul solicitării (incident / solicitare de suport / dezvoltare) și se va desfășura conform criteriilor descrise în continuare.

Orice solicitare și istoria prestării serviciului aferent este înregistrată de către SSC într-un sistem de gestiune a solicitărilor (sistemul Service Desk).

8.4. Reguli privind Managementul incidentelor

Serviciile de suport sunt orientate soluționării incidentelor și problemelor de utilizare a sistemului informatic. Solicitările de consultanță sunt considerate de asemenea incidente în cazul dacă determină incapacitatea utilizatorului de a utiliza funcționalul sistemelor informatice supuse mentenanței.

ii. Clasificarea incidentelor

Prestatorul și Beneficiarul vor conlucra strâns în vederea prevenirii incidentelor și în vederea soluționării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul și prioritatea acordată pentru soluționarea unui incident va ține cont de regulile stabilite la acest capitol.

Impactul incidentului caracterizează consecințele acestuia asupra disponibilității și performanței aplicației supuse mentenanței. Urgența incidentului caracterizează operativitatea cu care acesta trebuie soluționat, pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare și soluționare a incidentelor va fi în funcție de impactul și urgența incidentului. Algoritmul aplicat pentru stabilirea priorității unui incident este definit în continuare.

Tabelul 1. Stabilirea priorității de soluționare a incidentelor

		Impact		
		Înalt	*Mediu*	*Jos*
Urgență	*Înalt*	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenței incidentului

URGENȚĂ	Descriere
Înaltă	Un incident este estimat ca având nivelul urgenței ”Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activități și operațiuni critice pentru afacerea Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea imediată poate preveni riscuri legale majore și de securitate (protecție) a informației.
Medie	Un incident este estimat ca având nivelul urgenței „Mediu” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc considerabil în timp; - există activități și operațiuni importante pentru afacerea Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea operativă poate preveni riscuri legale moderate și de securitate a informației.
Joasă	Un incident este estimat ca având nivelul urgenței ”Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puțin în timp; - activitățile și operațiunile afectate nu trebuie continuate imediat; - nu există riscuri legale și de securitate a informației semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	Descriere

Înalt	Un incident este estimat ca având nivelul impactului ”Înalt” în una sau mai multe din următoarele cazuri: - activitățile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizației Beneficiarului și afectează utilizatori externi, reputația și imaginea Beneficiarului; - există riscuri legale și financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca având nivelul impactului ”Major” în una sau mai multe din următoarele cazuri: - activitățile importante ale Beneficiarului sunt întrerupte sau activitățile cheie sunt desfășurate cu dificultate; - incidentul a afectat utilizatori interni și un număr nesemnificativ de utilizatori externi; - există riscuri legale și financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca având nivelul impactului ”Jos” în una sau mai multe din următoarele cazuri: - activitățile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activitățile importante sunt desfășurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

iii. Raportarea și soluționarea incidentelor

Orice incident aferent Serviciilor este raportat de Beneficiar către SSC, conform procedurilor stabilite la capitolul 8.3 ”Reguli de înregistrare a solicitărilor”.

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru. În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort”.

Prioritate incident	**Timpul de reacție**	**Timpul de soluționare**	**Timp max. pentru corectare a cauzei***	**Raportare primară**
Critică	Timpul de reacție al Prestatorului – imediat;	până la 4 oră	8 ore	Telefon.
Înaltă	Timpul de reacție al Prestatorului – 120	6 ore	ora 12 a zilei următoare	Telefon; Sistem Service

	minute;			Desk
Medie	Timpul de reacție al Prestatorului – 4 ore;	24 ore	5 zile	Sistem Service Desk
Joasă	Timpul de reacție al Prestatorului – 24 ore;	3 zile	10 zile	Sistem Service Desk
Neglijabilă	Timpul de reacție al Prestatorului – 72 ore;	Cel mai bun efort.	-	Sistem Service Desk

*Notă: se aplică pentru situația când soluționarea incidentului se face prin aplicarea unor măsuri de ocolire.

Prestatorului poate contacta persoana ce a raportat incidentul, pentru a preciza informația oferită de Beneficiar. De comun acord cu aceasta, Prestatorul poate revizui nivelul impactului și nivelul urgenței soluționării incidentului. Beneficiarul are de asemenea posibilitatea ca ulterior să revizuiască clasificarea stabilită inițial. Revizuirea poate fi necesară în funcție de progresele soluționării incidentului.

Prestatorul va diagnostica cauza incidentului și va identifica măsurile necesare a fi întreprinse pentru soluționarea incidentului. Pe tot parcursul soluționării incidentului, Prestatorul va oferi informația Beneficiarului privind progresele făcute în vederea soluționării incidentului.

Prestatorul pate solicita implicarea la gestiunea incidentului, a persoanelor responsabile ale Beneficiarului. Conlucrarea este necesară în vederea diminuării impactului incidentului și soluționării operative a acestuia.

Un incident se consideră soluționat atunci când funcționalitatea este restabilită pentru Beneficiar, la nivelul stabilit conform prezentelor Reguli. În cazul în care Beneficiarul nu este de acord cu nivelul de soluționare a incidentului, poate solicita deschiderea repetată a incidentului. În caz contrar, incidentul se consideră închis.

Toate incidentele raportate de Beneficiar sunt înregistrate în cadrul SSC. Prestatorul încurajează Beneficiarul să raporteze orice incident sau suspiciune de incident. Acest fapt va permite îmbunătățirea continuă a nivelului Serviciilor prestate.

Îndată ce problema depistată va fi rezolvată, instalarea aplicației modificate pe serverul de producție va avea loc cu acordul Beneficiarului și în baza unui plan de livrare coordonat.

iv. Escaladarea incidentelor

În cazul în care un incident nu poate fi soluționat în timpul agreat, Părțile pot escalada incidentul la un nivel mai înalt de autoritate - către Managerul Suport Clienți. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului și Beneficiarului, pentru a gestiona orice aspect ivit în relațiile dintre aceștia.

8.5. Reguli privind prestare a serviciilor de suport predefinite

i. Reguli de organizare a lucrărilor conform planului-grafic

Planul-program de efectuare a lucrărilor de mentenanță este propus de Prestator și aprobat de Beneficiar.

Planul-program este elaborat în așa mod, încât pe parcursul perioadei de executare a contractului, analizei să fie supus întreg sistemul informatic.

ii. Reguli de asigurare a planului de restabilire

Procedurile de continuitate menite să asigure posibilitatea restabilirii disponibilității Sistemelor informatice în situații de incident vor fi implementate conform cerințelor din tabelul de mai jos.

Nr.	Categorie incident	Planul de restabilire	Timpul Obiectiv pentru Restabilire (TOR)	Momentul în Timp pentru Restabilirii (MTR) (pierderea de date admisă la momentul restabilirii)
1.	Căderea componentelor hard aferente Sistemului Informatic.	Suport în ridicarea sistemului pe echipamentul din rezerva activă Sdandby.	TOR = 15 minute.	MTR = ultima tranzacție confirmată.
2.	Coruperea integrității datelor din bazele de date ale Sistemului Informatic.	Suport în configurarea politicii a copii de rezervă incrementale la un interval de 15 minute.	TOR = 30 minute.	MTR = 15 minute.
3.	Alte incidente ce pot afecta disponibilitatea Sistemului Informatic.	Suport în configurarea politicii a copii de rezervă conform punctelor 1 și 2 mai sus.	TOR = 2 ore.	MTR = 15 minute.
4.	Situații excepționale ce pot afecta disponibilitatea data centrului ce găzduiește infrastructura hard a Sistemului Informatic.	Suport în configurarea politicii a copii de rezervă depline efectuate zilnic, stocate în afara data centrului de bază.	TOR = 3 zile.	MTR = 15 minute

Timpul Obiectiv pentru Restabilire specificat în tabelul de mai sus este valabil în perioada orelor de lucru. În cazul apariției situațiilor de incident ce au dus la pierderea datelor, Beneficiarul va restabili integral datele pierdute de la sursele din copiile de rezervă proprii.

Beneficiarul este responsabil pentru alocarea resurselor necesare organizării planului de restabilire.

8.6. Reguli privind prestare a serviciilor de dezvoltare

i. Solicitarea Serviciilor de dezvoltare

Solicitarea Serviciilor de dezvoltare se efectuează doar de Persoana autorizată din partea Beneficiari în baza unei solicitări conform regulilor descrise în capitolul ”Reguli de înregistrare a solicitărilor”

În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului și a costului estimativ conform tarifelor.

ii. Prestarea Serviciilor de dezvoltare

Prestarea serviciilor de dezvoltare se va efectua cu aplicarea următoarelor reguli:

a) Prestarea Serviciilor se efectuează exclusiv în baza planului aprobat de Beneficiar privind prestarea Serviciilor de dezvoltare. În caz de necesitate planul poate fi modificat, cu acordul Părților, fapt menționat în noul plan, care va conține referința la planul inițial.
b) Un Serviciu de dezvoltare se consideră prestat în momentul confirmării acceptării soluției de către Persoana responsabilă din partea Beneficiarului.
c) Termenul de prestare a Serviciului de dezvoltare include doar timpul necesar Prestatorului colectării informației, documentării, analizei și prestării nemijlocite a serviciului și poate fi diferit de intervalul de timp total dintre momentul enunțului acestuia și acceptării rezultatului.
d) Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea problemei și rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.
e) În cazul nealocări în termenii agreați a resurselor necesare din partea Beneficiarului termenul de soluționare se majorează cu timpul respectiv, aplicându-se după caz penalitățile prevăzute de contract.
f) Prestatorul va asigura executarea lucrărilor de elaborare a funcționalităților suplimentare doar la solicitare Beneficiarului, în baza unor proceduri general recunoscute și acceptate și a standardelor agreate de Beneficiar, ținând cont și de ultimele cerințe în materie de elaborare, și calculate în baza tarifelor convenite de părți.
g) Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcționalităților suplimentare (pe serverul de testare), conform cerințelor și condițiilor înaintate de Beneficiar, care se vor consemna prin proces-verbal (Act de testare). Pentru a testa funcționalitatea suplimentară solicitată de Beneficiar, acesta din urmă va asigura mediul software și hardware, care va corespunde exact cu sistemul real și va asigura acces liber Prestatorului, precum și va oferi instrumente de testare necesare.
h) Beneficiarul este în drept să verifice (testeze) funcționalitățile suplimentare ale sistemului, predate de către Prestator, în conformitate cu procedurile statuate în contract.
i) Integrarea funcționalităților suplimentare în sistemul real se va face de către specialiștii Beneficiarului, sau de către Prestator doar cu aprobarea Beneficiarului. Responsabilitatea pentru funcționarea sistemului real o va purta Beneficiarul.
j) Beneficiarul și Prestatorul se vor obliga să se informeze reciproc despre orice modificări aduse sistemului atât prin funcționalitățile suplimentare integrate, cât și prin alte modificări cum ar fi dar fără a se limita la cele de administrare a sistemului (găzduire pe servere, adrese IP, resurse hardware alocate etc.). Informarea se va face în scopul excluderii unor lacune în comunicare ce va putea periclita buna funcționare a sistemului.

8.7. Alte cerințe și reguli privind prestarea serviciilor

i. Reguli față de procesul de aplicare a modificărilor

Prestatorul poate, la necesitate, implementa modificări de infrastructură sau funcționale aferente aplicației supuse mentenanței.

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea Serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul..

Pentru fiecare lucrare de modificare va fi elaborat planul de aplicare a modificărilor.
Aceste modificări pot necesita testarea prealabilă implementării în mediul de producție. Prestatorul va notifica cu 5 zile în avans despre necesitatea efectuării testelor în mediul de testare și va comunica Planul de testare Beneficiarului

Beneficiarul este responsabil să participe la testele inițiate de Prestator, conform Planului de testare.

În cazul apariției neconcordanței specificației funcționale, Prestatorul se obligă să notifice în scris cu prezentarea descrierii detaliate a soluțiilor pentru înlăturarea neconcordanței.

8.8. Documentația tehnică

Prestatorul menține în stare actuală documentația tehnică aferentă sistemelor informatice. Documentația conține suficientă informație pentru ca orice echipa de dezvoltatori soft /administratori terți să poată prelua serviciile de mentenanță.

Prestatorul va notifica Beneficiarul despre noile versiuni și modificările importante, la documentația tehnică aferentă sistemelor informatice destinată Beneficiarului.

8.9. Mediul de test

Pentru efectuarea testărilor funcționale a Sistemului Informatic supus mentenanței, Prestatorul pune la dispoziția Beneficiarului un mediu de test. Mediul de test va putea fi utilizat de Beneficiar în următoarele cazuri:

- La apariția unor probleme semnificative în mediul de producție. În aceste situații, utilizarea mediului de testare poate fi solicitată atât de Beneficiar, cât și de Prestator;
- La implementarea modificărilor importante pentru sistemele informatice supuse mentenanței și testarea lor prealabilă pe mediul de test

Accesarea sistemelor informatice în mediul de testare se face în bază de canale securizate prin autentificarea similară cu mediul de producție.

8.10. Soluționarea divergențelor

Orice divergențe ivite între Părți vor fi soluționate cu efort comun și prin strânsă conlucrare între Părți. În acest scop, vor fi aplicate următoarele reguli:

1) Părțile vor forma un grup comun de lucru în scopul soluționării divergențelor. De comun acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv: experți independenți.

2) La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.

3) Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite. În acest scop, pot fi ascultate, sau obținute în scris, opiniile membrilor externi, convocați în grupul de lucru, precum și rezultatele de expertiză ale probelor electronice existente.

4) Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru din partea ambelor părți.

Identificarea unei soluții echitabile pentru ambele Părți, în limite angajamentelor asumate ale Părților, este preferabilă în toate situațiile de divergență. În cazul în care o asemenea soluție nu poate fi identificată, părțile vor aplica prevederile Contractului pentru soluționarea litigiilor.

8.11. Securitatea informației

Părțile agreează de comun acord să conlucreze și să coopereze în vederea gestiunii pro active a riscurilor de securitate a informației ce pot afecta serviciile Prestatorului și sistemele Beneficiarului, dependente de serviciile Prestatorului.

Prestatorul este responsabil pentru securitatea tehnologică și funcțională a sistemelor informatice supuse mentenanței, în limitele sarcinilor de mentenanță îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informației, partea ce a constatat incidentul va notifica imediat și cealaltă parte, dacă aceasta poate fi de asemenea afectată de incident. Părțile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului și soluționării acestuia.