



Servicii de mentenanță preventivă, corectivă și adaptivă a aplicației MoldSign Desktop Suite

Clasificare de
securitate

C4

CAIET DE SARCINI

**Pentru Servicii de mentenanță preventivă, corectivă și adaptivă a aplicației
MoldSign Desktop Suite.**



Conținut

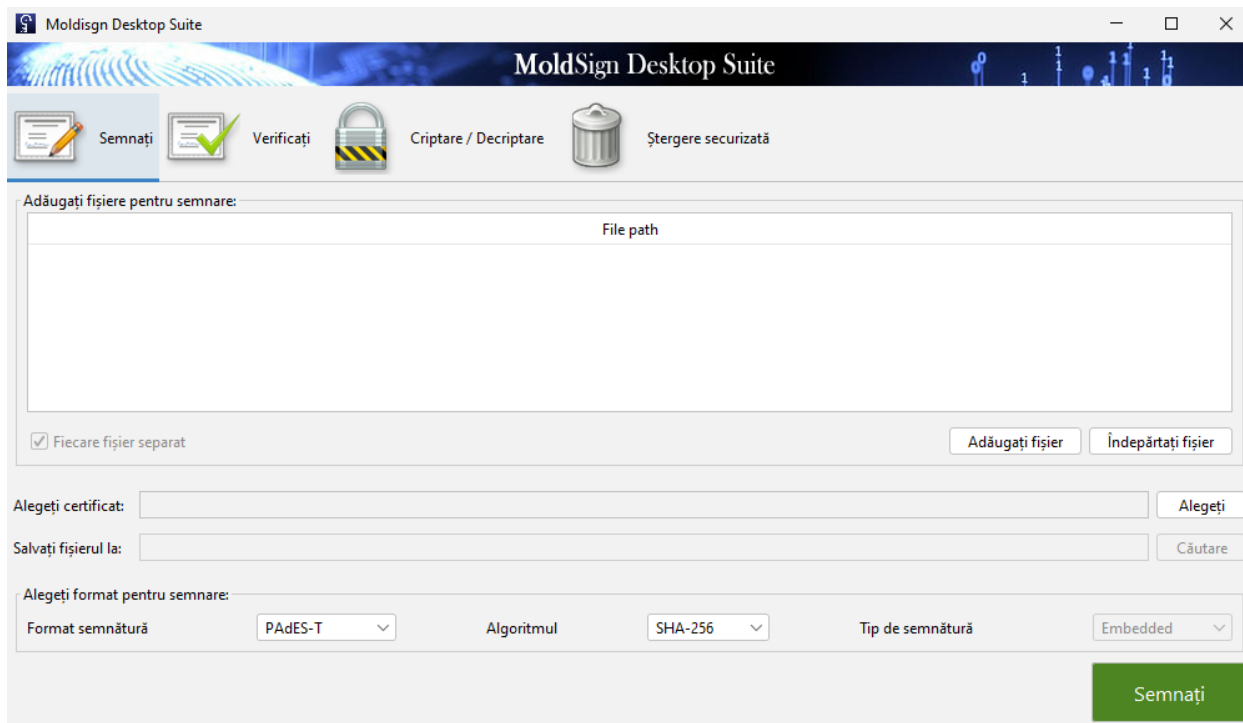
I. Generalități	4
II. Referințe	4
III. Obiectivul documentului	5
IV. Destinația aplicației	Ошибка! Закладка не определена.
V. Integrarea aplicației cu alte sisteme, protocoale și servicii	5
VI. Cerințe față de serviciile de mentenanță	7
VII. Modalitatea de prestare a serviciilor de mentenanță	7



I. Generalități

Aplicația MoldSign Desktop Suite (în continuare *Aplicația MSDS*) este un produs destinat utilizatorilor serviciilor de încredere calificate, ce permite realizarea operațiunilor de creare, verificare și validare a semnăturii electronice calificate, precum și dispune de funcționalități suplimentare menită să asigure un nivel înalt al securității datelor ce se conțin în documentele utilizatorilor.

Caietul de sarcini conține o descriere succintă a scopului utilizării Aplicației MSDS, tehnologiilor utilizate și cerințele pentru mentenanța acesteia.



(Interfața Aplicației MSDS)

II. Referințe

Aplicația MSDS corespunde prevederilor cadrului normativ național și standardelor internaționale în domeniul serviciilor de încredere, și anume:

- Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere,
- Normele tehnice în domeniul semnăturii electronice avansate calificate, aprobate prin Ordinul Directorului Serviciului de Informații și Securitate al Republicii Moldova nr.69/2016
- Standardul SMV CWA 14170:2015 *Cerințe de securitate pentru aplicațiile de creare a semnăturilor electronice.*
- Standardul SM CWA 14171:2015 *Ghid general pentru verificarea semnăturii electronice.*
- Recomandarea IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 5816 ESSCertIDv2 Update for RFC 3161.
- Recomandarea IETF RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification.



- Recomandarea IETF RFC 3029 Data Validation and Certification Server Protocols (DVCS).

III. Obiectivul documentului

Aplicația MSDS, descrisă în continuare, face obiectul achiziției serviciilor de mentenanță preventivă, corectivă și adaptivă în scopul asigurării bunei funcționări și extinderii acesteia. În mod concret prezentul document are următoarele componente:

Denumirea aplicației	Activitatea de mentenanță
MoldSign Desktop Suite	Servicii de mentenanță preventivă, corectivă și adaptivă asigurate până la 31.12.2024. Serviciile se referă inclusiv la artefactele dezvoltate asupra funcționalităților existente pe parcursul perioadei de valabilitate a contractului.

În prezenta documentație sunt reflectate informații privind tehnologia folosită și modul în care sunt prelucrate datele. Prestatorul va avea acces la codul sursă al aplicației și își va asuma riscurile ce decurg din modificările acestuia. Asumarea serviciilor implică acordarea garanției asupra aplicației pentru o perioadă de minim 12 luni după semnarea actului de predare primire. De asemenea prestatorul serviciilor va documenta toate operațiunile de modificare a aplicației și le va prezenta Beneficiarului.

IV. Destinația aplicației.

Aplicația (MSDS) este utilizată în scopul:

- aplicării semnăturii electronice calificate pe date în format electronic (*.pdf, *.doc, *.png, *.jpg, *.txt, etc), utilizând dispozitivul de creare a semnăturii electronice calificate;
- verificării valabilității și autenticității semnăturii electronice calificate;
- criptării/decriptării, cu utilizarea parolei, a fișierului și ștergerii securizate (irreversibile) a acestuia de pe calculator..

V. Integrarea aplicației cu alte sisteme, protocoale și servicii

Aplicația MSDS este integrat cu următoarele sisteme și servicii guvernamentale:

- Serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- Serviciul electronic guvernamental integrat de semnătură electronică (MSign).

Tehnologii utilizate

Aplicația MSDS este bazată pe :

- OpenJDK 8.0.412+8 x86
- Java 8 LTS
- IAIK JCE 5.1
- IAIK PKCS#11 Provider 1.3
- IAIK XSECT 1.17
- IAIK XaDES 1.4.2
- IAIK TSP 2.2
- IAIK CMS 4.1



- Grizzly 2.2.16
- Jersey 1.17
- Jettison 1.1
- iText 5.4.3

Aplicația MSDS este compusă din următoarele artefacte:

- CardManager
- ClientCardServer
- PKCS11CardReader
- TransferObjects
- MoldSignClientCardManager

Aplicația MSDS suportă următoarele standarde de semnare

- **PAdES** - semnătura fișierelor pdf;
- **PAdES-T** - semnătura fișierelor pdf ce include și un marcaj temporal din partea unui server autorizat pentru marcare temporală;
- **XAdES-BES** – semnătură de bază în format XML;
- **XAdES-T** – semnătură de bază în format XML cu marcaj temporal adițional din partea unui server autorizat pentru marcare temporală;
- **XAdES-C** – semnătură XAdES-T cu referințe complete privind statutul certificatului cheii publice.

Tipul de semnătură poate fi **Detached (Detașată)** sau **Embedded (Încorporată)**. Semnătura **Detached (Detașată)** presupune existența unui fișier separat ce conține semnătura pentru unul sau mai multe fișiere; în timp ce, semnătura **Embedded (Încorporată)** presupune că atât fișierul semnat, cât și semnătura sunt localizate în cadrul aceluiași fișier.

În cazul semnăturilor fișierelor pdf (**PAdES**, **PAdES-T**) este aplicabil doar tipul **Embedded (Încorporată)**.

Pentru formatul **XAdES** sunt disponibile ambele tipuri, însă, pentru limitarea consumului de resurse, formatul **Embedded (Încorporată)** este disponibil numai pentru fișiere mai mici de 100KB.

Semnătura în formatul **XAdES** și de tip **Detached (Detașată)** permite semnarea a mai multor fișiere cu un singur fișier de semnătură. Această opțiune poate fi realizată dacă opțiunea **Sign each file separately (Semnează fiecare fișier separat)** este debifată. În acest caz, se selectează numele și locația fișierului de semnătură. Fișierele semnate sunt salvate prin adăugarea automată a extensiei **.xades** la sfârșitul numelui fișierului (pentru formatele de semnătură **XAdES**), sau prin adăugarea **.signed** în fața extensiei **.pdf** (pentru formate de semnătură **PAdES**).



VI. Cerințe față de serviciile de mentenanță

Serviciile respective vor fi contractate per abonament lunar. Toate cerințele sunt minime și obligatorii. Serviciul de mentenanță se va asigura de către Prestator până la data de 31.12.2024.

Serviciile de mentenanță preventivă includ următoarele activități din partea Prestatorului:

- Recepționarea incidentelor prin aplicația de tichetare, telefon, e-mail sau skype;
- Actualizarea jurnalului de incidente;
- Monitorizarea activității de mentenanță și suport;
- Raportarea periodică cu privire la statutul incidentelor;
- Soluționarea incidentului;
- Servicii de consultanță.
- Integrarea infrastructurii cheilor publice cu alte entități din sectorul public și organizații din mediul privat pentru prestarea serviciilor de semnătură electronică calificată.
- Mentenanța server-ului pentru aplicația MoldSign Desktop Suite: publicarea versiunilor noi a MoldSign Desktop Suite, mentenanța serverului, monitorizarea fluxurilor de descărcări (download) a aplicației de către utilizatori și optimizarea lor pentru evitarea suprasolicității rețelei, asigurarea securității și integrității aplicației descărcate prin verificarea hash-ului și semnăturii electronice aplicate pe aceasta).

Serviciile de mentenanță corectivă

Serviciile respective intervin drept rezultat al unei *solicitări de corectare* și includ următoarele activități din partea Prestatorului:

- modificarea în procesul de lucru al aplicației pentru corectarea problemelor detectate (neconformități, erori de funcționare) cu un impact minim asupra activității operaționale. Serviciile de mentenanță de corecție vor asigura suportul tuturor modulelor aplicației, create în conformitate cu Cerințele Tehnice prevăzute în Caietul de sarcini și amendamente privind elaborarea aplicației și presupun activitățile de management, logistică și servicii de îndepărtare a erorilor.
- Analiza impactului modificărilor mediului (cadrul normativ, procesele de business, impactul modificării componentelor infrastructurii TIC, etc.) asupra aplicației și formularea recomandărilor de corectare a aplicației;
- Analiza parametrilor de funcționare a aplicației în vederea stabilirii suficienței performanței și formularea sarcinilor de corectare;
- Analiza solicitărilor și definirea cerințelor de corectare;
- Consultarea Beneficiarului în aspecte ce dețin de identificare, analiză și formulare a sarcinilor de corectare;
- Modificarea codului sursă conform noilor cerințe impuse de cadrul normativ sau mediul de producție;
- Managementul schimbărilor:
 - i. Consultarea specialiștilor beneficiarului în vederea elaborării planurilor de implementare a modificărilor și suportul la implementarea acestora;
 - ii. Analiza impactului, testarea și suportul privind aplicarea reînnoirilor pentru aplicație;
 - iii. Testarea de comun cu specialiștii Beneficiarului a impactului modificărilor asupra parametrilor de funcționare și siguranței aplicației.

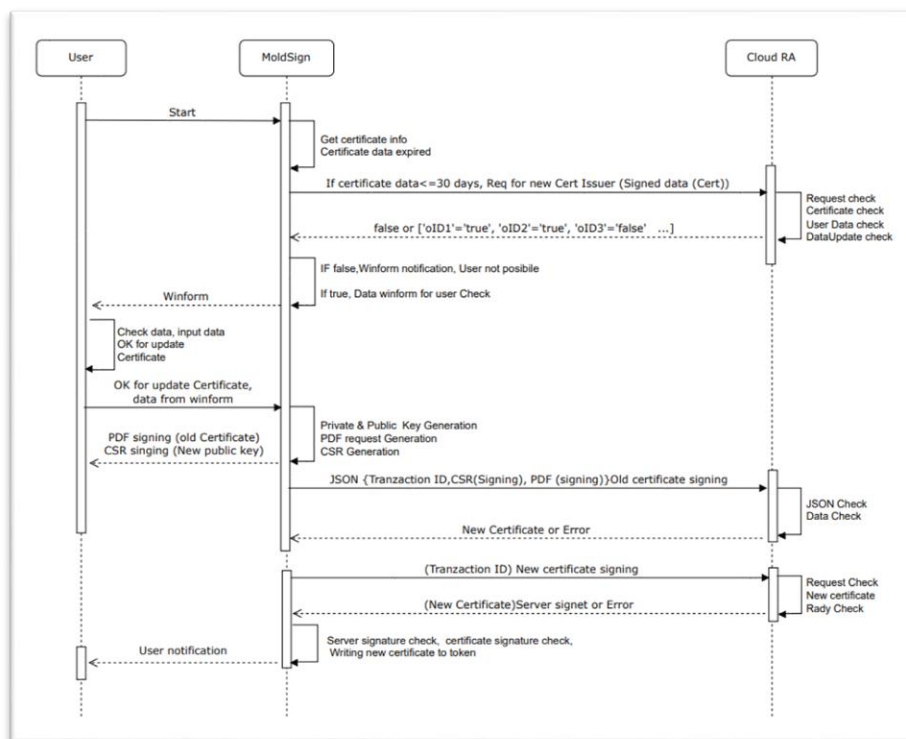
Serviciile de mentenanță adaptivă includ următoarele activități din partea Prestatorului:

- Integrarea infrastructurii cheilor publice cu alte entități din sectorul public și organizații din MSDS - Servicii de mentenanță preventivă, corectivă și adaptivă a aplicației V.002



mediul privat pentru prestarea serviciilor de semnătură electronică calificată;

- micșorarea dimensiunii fișierului cu extensia .pdf, semnat, prin excluderea metodei CRL sau înlocuirea ei prin metoda OCSP;
- adăugarea mai multor tipuri de documente și fișiere semnate;
- asigurarea posibilității de verificare a integrității aplicațiilor terțe descărcate de către utilizator din rețeaua internet, prin verificarea hash-ului și semnăturii electronice a acestora (PGP etc.);
- asigurarea suportului de către aplicația MoldSign Desktop Suite a mai multor tipuri de tokene de la diferiți producători;
- Dezvoltarea unui business proces (modul) nou care va permite reînnoirea certificatelor publice pentru categoria de utilizatori “Subiect al Declarației”, după logica ilustrată mai jos:



Conform cerințelor beneficiarului, certificatele trebuie împărțite în 2 grupuri pe baza OID-ului pentru parametrul Politică de certificate. Grupurile sunt afișate în file separate. Definiția certificatului (OID) în care filă se află în această configurație. Sunt acceptate următoarele:

- „mainframe.secure_profile” - Toate certificatele cu OID-uri pentru profilul securizat. Numele este tradus în funcție de limba pe care utilizatorul a ales-o pentru aplicație;
- "mainframe.generaljorofile" - Toate certificatele care au OID care ar trebui să fie în profilul general. Numele fișierului este tradus pentru fiecare limbă disponibilă în aplicație.

VII. Modalitatea de prestare a serviciilor de mentenanță

Serviciile de mentenanță presupun acoperirea tuturor lucrărilor de mentenanță solicitate și necesare asigurării bunei funcționări a aplicației.

Apelurile referitoare la problemele de utilizare a aplicației vor fi preluate de specialiștii Beneficiarului care, după examinarea și prioritizarea lor, vor decide care din problemele sesizate de utilizatori necesită a fi



redirecționate către echipa de mentenanță a Prestatorului. Persoanele de contact ale beneficiarului și prestatorului vor fi indicate în contract.

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

În baza unei priorități setate de Beneficiar, problema va fi investigată și va fi oferită o soluție la aceasta într-un termen prestabilit.

În cazul în care este posibil, problema va fi rezolvată în limita timpului de răspuns prestabilit, fie va fi oferită o estimare pentru fixarea și lichidarea acesteia ulterior reieșind din prioritatea acesteia cât și a altor sarcini în derulare.

Termenii de reacție pe care Prestatorul trebuie să-i asigure în cazul incidentelor raportate de Beneficiar se prezintă în tabelul de mai jos.

Neconcordanță/ Incident	Descriere	Timpul maxim de reacție	Timp maxim de restabilire a funcționalității sau soluționare a problemei (ore de lucru, zile)
Critică	Problemă care afectează funcționalitatea întregului sistem.	1 oră	4 ore
Înaltă	Probleme care au o influență înaltă asupra funcționalității aplicației, care pot conduce la limitarea utilizării aplicației.	2 ore	8 ore
Medie	Probleme ce țin de dereglările funcționalității aplicației, care pot fi soluționate fără riscul pierderii de date sau prejudicierea funcționalității aplicației.	4 ore	40 ore
Redusă	Probleme cu impact redus sau foarte redus asupra funcționalității aplicației.	8 ore	72 ore

Prestatorul, prealabil predării către Beneficiar a soluțiilor de corectare, va asigura testarea funcționalităților suplimentare, conform cerințelor și condițiilor înaintate de Beneficiar, care se vor consemna prin proces-verbal. Pentru a testa funcționalitatea suplimentară solicitată de Beneficiar, acesta din urmă va asigura mediul software și hardware, care va corespunde exact cu sistemul real (cu date de test) și va asigura acces liber Prestatorului, precum și va oferi instrumente de testare necesare.

Prestatorul va prezenta, în luna decembrie al anului de gestiune, următoarele livrabile (versionate) care vor corespunde cerințelor Reglementării tehnice "Procesele ciclului de viață al software-ului" RT 38370656 - 002:2006, aprobată prin Ordinul Ministerul Dezvoltării Informaționale nr. 78/2006, inclusiv:

- Ghid de instalare (în limba română);
- Proiectul tehnic al aplicației actualizat (în limba română);
- Ghidul administratorului actualizat (în limba română);
- Ghidul utilizatorului actualizat (în limba română);



- Codul sursă actualizat cu toate bibliotecile și instrumentele necesare compilării componentelor aplicației;

- Actul de predare - primire (în limba română).

Beneficiarul este în drept să verifice (testeze) funcționalitățile suplimentare ale aplicației, predate de către Prestator.

Pe mediul de producție, actualizările/modificările aplicației vor fi aplicate/plasate de către Beneficiar.

Beneficiarul și Prestatorul se vor obliga să se informeze reciproc despre orice modificări aduse aplicației atât prin funcționalitățile suplimentare integrate, cât și prin alte modificări dar fără a se limita la cele de administrare a aplicației (găzduire pe servere, resurse hardware alocate etc.). Informarea se va face în scopul excluderii unor lacune în comunicare ce va putea periclita buna funcționare a aplicației.

În baza nevoilor operaționale, Beneficiarul poate solicita Prestatorului consultanță în formă de răspunsuri scrise la întrebările cu privire la Aplicația MSDS sau consultanță în formă de prezentări la oficiul Beneficiarului cu privire la întrebări specifice legate de aceasta.

Beneficiarul își păstrează dreptul de proprietate asupra Aplicației MSDS indiferent de îmbunătățirile aduse acesteia pe parcursul desfășurării contractului cu Prestatorul.