Digitally signed by Grițcan Dorin
Date: 2024.09.23 23:55:48 EEST
Reason: MoldSign Signature
Location: Moldova

MOLDOVA EUROPEANĂ

Oferta Tehnica Next Generation PKI

Costel

1. Cuprins

1. Introducere

În contextul extinderii cerințelor legate de serviciile de încredere calificate, dezvoltarea unei soluții complexe, capabile să gestioneze crearea, verificarea și validarea certificatelor digitale și a semnăturilor electronice calificate, este o necesitate stringentă. Acest proiect vizează implementarea unei soluții centralizate și integratoare, care să respecte toate standardele și cerințele tehnice impuse de reglementările internaționale și naționale, precum ETSI, FIPS 140-2 și eIDAS.

Serviciile de încredere calificate sunt critice pentru facilitarea tranzacțiilor digitale sigure, fie că este vorba de semnarea electronică a documentelor de către persoane fizice sau juridice, fie de implementarea unor procese guvernamentale sau comerciale ce implică autentificarea electronică. Soluția propusă răspunde acestor provocări prin integrarea unui set de componente de înaltă performanță și securitate, fiecare respectând cele mai stricte standarde din domeniu.

1.1. Scopul Soluției

Obiectivul principal al soluției propuse este de a dezvolta o infrastructură tehnică solidă, bazată pe cele mai recente tehnologii pentru crearea și gestionarea cheilor publice și private, precum și crearea semnăturilor electronice calificate. Sistemul va fi capabil să funcționeze în cadrul infrastructurii existente, permițând utilizarea dispozitivelor și componentelor hardware certificate (de exemplu, HSM-uri) și oferind servicii de semnătură electronică atât pentru entități publice, cât și private.

1.2. Componentele Soluției

Oferta tehnică include o combinație de soluții certificate și dezvoltări personalizate, adaptate cerințelor proiectului, pentru a crea o infrastructură integrată și robustă. Printre componentele cheie se numără:

1. **Infrastructura de Autoritate de Certificare (CA)** – se va implementa soluția **EJBCA** (Enterprise Java Beans Certificate Authority) ca sistem central de emitere și gestionare a certificatelor digitale. EJBCA oferă un mediu scalabil, capabil să emită certificate pentru semnături electronice și să asigure integrarea cu alte soluții PKI (Public Key Infrastructure) existente.
2. **Modul de Semnare Certificat (QSCD)** – **Cryptomatic Signer 6**, un dispozitiv certificat de creare a semnăturilor electronice calificate, va fi utilizat pentru crearea și stocarea în siguranță a cheilor private în conformitate cu standardele EN 419 241-1 și EN 419 241-2. Signer 6 asigură respectarea cerințelor de conformitate eIDAS și oferă o soluție certificată pentru protejarea integrității datelor semnate electronic.
3. **Componente personalizate dezvoltate** – Vor fi dezvoltate mai multe subcomponente specifice nevoilor utilizatorilor, care includ, fără a se limita la:
    1. **Portalul Utilizatorului** – care va oferi o interfață web și mobilă pentru gestionarea documentelor și semnăturilor electronice, permițând utilizatorilor să genereze, să verifice și să valideze semnături electronice într-un mod securizat.

2. **Portalul Organizației** – care va permite managementul utilizatorilor și al certificatelor la nivel de organizație, oferind capabilități avansate de configurare a autentificării și gestionarea rolurilor.
3. **Serviciul de Integrare API** – se vor dezvolta API-uri dedicate pentru interconectarea soluției cu sisteme externe, permițând interoperabilitatea soluției cu alte platforme IT, folosind standarde cum ar fi CSC (Cloud Signature Consortium) și PKCS#11.
4. **Componente de securitate și autentificare** – inclusiv sisteme de autentificare multi-factor (MFA), token-uri securizate și module de criptare care asigură protecția datelor și conformitatea cu standardele de securitate cibernetică

1.3. Contextul Proiectului și Necesitatea Soluției

Proiectul se desfășoară în cadrul extinderii infrastructurii de încredere calificate a I.P. „STISC" (Serviciul Tehnologia Informației și Securitate Cibernetică), organizația responsabilă pentru furnizarea de servicii de încredere calificate în Republica Moldova. În cadrul acestui proiect, este necesară integrarea unei soluții care să asigure păstrarea și gestionarea cheilor publice și private, precum și crearea de semnături electronice la distanță. Aceasta va permite utilizatorilor fizici și juridici din sectorul public și privat să acceseze servicii digitale sigure și conforme cu normele europene și internaționale.

1.4. Beneficii Cheie ale Soluției

- **Conformitate cu standardele internaționale** – Soluția este proiectată pentru a respecta cerințele tehnice impuse de standardele ETSI, CEN și eIDAS. De asemenea, utilizează module criptografice certificate FIPS 140-2 și dispozitive QSCD conforme cu EN 419 241-1 și 419 241-2, asigurând astfel cel mai înalt nivel de securitate pentru semnăturile electronice.
- **Securitate avansată** – Toate componentele soluției sunt construite pe o infrastructură criptografică de înaltă securitate, asigurată prin utilizarea de HSM-uri certificate și module de semnare conform cu eIDAS și alte reglementări internaționale. Soluția oferă criptare în tranzit și la repaus, protejând atât datele utilizatorilor, cât și documentele semnate.
- **Scalabilitate și flexibilitate** – Soluția este capabilă să gestioneze un număr mare de tranzacții și utilizatori. Arhitectura modulară permite extinderea rapidă a capacităților în funcție de nevoile proiectului, fie pentru extinderea numărului de utilizatori, fie pentru integrarea de noi funcționalități.
- **Interoperabilitate și integrare** – Soluția permite integrarea ușoară cu alte sisteme PKI și de semnătură electronică, prin API-uri standardizate. Aceasta asigură interoperabilitatea cu diverse platforme IT existente în organizații publice și private, facilitând migrarea și utilizarea soluției la scară largă.
- **Suport și administrare extinsă** – Componentele dezvoltate oferă capabilități avansate de administrare, monitorizare și raportare. Portalurile personalizate pentru utilizatori și organizații oferă funcționalități de management detaliat, precum și control al fluxurilor de lucru și a semnăturilor electronice generate.

2. Descrierea generală a soluției

Soluția propusă reprezintă o platformă integrată destinată creării, verificării și validării semnăturilor electronice calificate, utilizând infrastructuri sigure și conforme cu standardele europene și internaționale. Soluția are la bază un set de componente certificate și dezvoltări personalizate care asigură nu doar respectarea cerințelor de conformitate, dar și o interoperabilitate extinsă cu alte sisteme IT utilizate în diverse domenii, fie că este vorba de sectorul public sau privat.

Componente principale ale soluției

Soluția include următoarele componente esențiale, fiecare având un rol bine definit în cadrul arhitecturii sistemului:

2.1. Sistemul de Autoritate de Certificare (CA) - EJBCA

EJBCA (Enterprise Java Beans Certificate Authority) este o platformă de Autoritate de Certificare robustă, capabilă să emită și să gestioneze certificatele digitale utilizate pentru semnăturile electronice calificate. EJBCA asigură:

- Emiterea și gestionarea certificatelor X.509 pentru persoane fizice și juridice.
- Implementarea serviciilor de revocare a certificatelor (CRL și OCSP) pentru verificarea statutului certificatelor în timp real.
- Integrabilitate cu Hardware Security Modules (HSM-uri) certificate pentru stocarea sigură a cheilor private.
- O arhitectură flexibilă, care suportă implementări cu înaltă disponibilitate (HA) și funcții de recuperare în caz de dezastru (DR).

EJBCA este conform cu standardele ETSI EN 319 411-1 și 319 411-2, garantând conformitatea soluției cu legislația europeană eIDAS pentru prestatorii de servicii de încredere calificate

2.2. Dispozitiv de Semnătură Calificată (QSCD) - Cryptomatic Signer 6

Cryptomatic Signer 6 este un dispozitiv certificat de creare a semnăturilor electronice calificate (QSCD), care asigură crearea și stocarea cheilor private într-un mediu securizat. Acesta îndeplinește cerințele stricte ale reglementărilor EN 419 241-1 și EN 419 241-2, asigurând:

- Generarea și stocarea cheilor private în dispozitive securizate (HSM-uri).
- Integrarea cu API-uri pentru realizarea semnăturilor la distanță.
- Suport pentru algoritmi criptografici avansați, precum RSA și ECDSA, și standarde de securitate FIPS 140-2.
- Ofera suport pentru API-uri conform Cloud Signature Consortium (CSC) v2.

Pentru mai multe detalii a se analiza documentația atașată specifică Signer 6.

2.3. Componente personalizate dezvoltate

Soluția include o serie de componente personalizate dezvoltate, menite să răspundă cerințelor specifice ale proiectului și să faciliteze utilizarea și administrarea soluției. Aceste componente includ:

- **Portalul Utilizatorului** – Oferă utilizatorilor acces securizat la funcțiile de semnare, verificare și gestionare a documentelor digitale. Portalul permite:
    - Generarea și gestionarea semnăturilor electronice.
    - Verificarea validității semnăturilor existente.
    - Stocarea și descărcarea documentelor semnate în format sigur.
    - Suport pentru multiple fluxuri de lucru pentru semnarea documentelor în serie sau în paralel.
- **Portalul Organizației** – Permite organizațiilor să gestioneze utilizatorii, rolurile și certificarea semnăturilor la nivel centralizat. Portalul oferă capabilități de administrare avansate, inclusiv gestionarea autentificării și a politicilor de securitate pentru fiecare utilizator sau grup de utilizatori.
- **API-uri de Integrare** – Oferă un set de API-uri standardizate pentru integrarea soluției cu alte sisteme IT externe. Aceste API-uri respectă standardele Cloud Signature Consortium (CSC) și PKCS#11, asigurând interoperabilitatea cu alte soluții PKI și de semnătură electronică. API-urile permit interacțiunea cu portalurile utilizatorilor și organizațiilor pentru automatizarea proceselor de semnare, verificare și stocare a documentelor.
- **Servicii de autentificare și securitate** – Integrarea soluțiilor de autentificare multi-factor (MFA) și a mecanismelor de criptare asigură protecția datelor în tranzit și la repaus. Soluția oferă suport pentru token-uri hardware și software, precum și pentru autentificare prin OAuth și OpenID Connect (OIDC).

2.4. Interoperabilitate și Integrabilitate

Unul dintre principalele avantaje ale soluției este interoperabilitatea sa extinsă cu infrastructurile existente de semnătură electronică și certificate. Prin utilizarea API-urilor conforme cu standardele internaționale, soluția propusă poate fi ușor integrată în infrastructurile IT deja existente în organizații sau instituții publice, fără a necesita modificări majore ale acestora.

Soluția este compatibilă cu o gamă variată de sisteme și platforme, incluzând:

- Sisteme de identitate și autentificare, precum Active Directory, Azure AD, Okta și Auth0.
- Servicii cloud, precum Google Drive, OneDrive și Dropbox, pentru stocarea securizată a documentelor.
- Sisteme PKI externe, cu suport pentru standardele ETSI și IETF privind semnăturile electronice (PAdES, XAdES, CAdES).

3. Cerințe tehnice și standarde

Pentru a garanta siguranța și conformitatea soluției propuse cu cerințele pieței și legislației aplicabile, aceasta respectă cele mai stricte standarde internaționale și naționale în domeniul semnăturilor electronice, securității cibernetice și criptografiei. Implementarea soluției este fundamentată pe asigurarea unei infrastructuri robuste, în conformitate cu următoarele standarde, dar fără a se limita.

3.1. Standardele tehnice și de conformitate aplicabile

Soluția propusă este construită conform normelor europene și internaționale în vigoare pentru furnizorii de servicii de încredere și infrastructurile de semnături electronice. Aceasta îndeplinește toate cerințele impuse de următoarele standarde cheie:

1. **ETSI EN 319 411-1 & 319 411-2** – Cerințe de politică și securitate pentru furnizorii de servicii de încredere care emit certificate. Partea 1 descrie cerințele generale, iar partea 2 detaliază cerințele pentru certificatele calificate. Acestea sunt esențiale pentru certificarea autorităților de încredere (CA) și pentru garantarea securității infrastructurilor de chei publice (PKI).
2. **CEN EN 419 241-1 & 419 241-2** – Sistemele de semnătură server securizate (Trustworthy Systems Supporting Server Signing). Partea 1 definește cerințele generale de securitate pentru sistemele care susțin semnătura serverului, iar partea 2 specifică profilul de protecție pentru dispozitivele calificate de creare a semnăturii (QSCD).
3. **ETSI TS 119 432** – Protocoale pentru crearea semnăturilor digitale la distanță, care asigură că soluția de semnătură electronică la distanță respectă cerințele specifice de securitate și funcționalitate pentru semnăturile digitale calificate.
4. **SM ETSI EN 319 142** – Reguli pentru semnături digitale PAdES (PDF Advanced Electronic Signatures), care asigură că semnăturile aplicate documentelor PDF sunt conforme cu specificațiile internaționale și sunt recunoscute la nivel global.
5. **FIPS 140-2** – Standardul pentru module criptografice definit de National Institute of Standards and Technology (NIST), asigurând securitatea modulelor de criptografie utilizate pentru stocarea și gestionarea cheilor private
6. **SM EN ISO/IEC 15408 (Common Criteria)** – Criterii comune pentru evaluarea securității IT. Soluția respectă cerințele Common Criteria EAL4+ pentru dispozitivele de creare și păstrare a semnăturilor electronice (QSCD), garantând protecția datelor criptografice și conformitatea cu reglementările europene.
7. **RFC 5280 și RFC 6960** – Standarde pentru infrastructura de chei publice (X.509) și protocolul de verificare a statutului certificatului online (OCSP), utilizate pentru verificarea stării certificatelor emise.
8. **PKCS#11** – Interfață pentru Tokenuri Criptografice, utilizată pentru interacțiunea dintre soluțiile software și dispozitivele criptografice hardware (de exemplu, HSM-uri și tokenuri USB).

3.2. Cerințe generale de securitate

Soluția propusă asigură implementarea celor mai bune practici de securitate, garantând protecția datelor și a semnăturilor electronice împotriva accesului neautorizat, compromiterii și manipulării. Principalele cerințe de securitate respectate de soluție includ:

1. **Păstrarea cheilor private și publice într-un mediu securizat** – Cheile private ale utilizatorilor sunt stocate exclusiv în HSM-uri conforme cu FIPS 140-2 și Common Criteria EAL4+, asigurând astfel protecția maximă a datelor critice.
2. **Criptarea datelor în tranzit și la repaus** – Soluția utilizează protocoale de criptare avansate (TLS 1.2/1.3) pentru a proteja comunicațiile între utilizatori și serverele soluției, precum și

stocarea datelor pe servere securizate. De asemenea, toate datele criptografice, inclusiv cheile private și semnăturile electronice, sunt criptate în repaus.

3. **Autentificare multi-factor (MFA)** – Pentru a asigura protecția accesului la soluție, sunt implementate mecanisme de autentificare multi-factor (MFA), inclusiv utilizarea token-urilor hardware sau software, OTP (One-Time Password) și autentificare prin OAuth sau OpenID Connect.
4. **Mecanisme de control al accesului** – Soluția permite implementarea unui control strict al accesului la nivelul fiecărui utilizator sau grup de utilizatori, asigurând că doar persoanele autorizate au acces la funcțiile critice, cum ar fi semnarea documentelor sau gestionarea cheilor publice și private.
5. **Suport pentru certificarea conformității eIDAS** – Soluția respectă toate cerințele Regulamentului eIDAS pentru furnizorii de servicii de încredere, inclusiv cerințele pentru semnături electronice calificate și sigilii electronice.

3.3. Cerințe tehnice specifice componentelor

Pentru fiecare componentă principală a soluției, sunt stabilite cerințe tehnice clare, care asigură funcționarea corectă și securizată a soluției:

- EJBCA (Enterprise Java Beans Certificate Authority):
  - Suportă generarea de certificate X.509 conforme cu ETSI EN 319 411.
  - Integrează OCSP pentru verificarea în timp real a statutului certificatelor.
  - Permite stocarea certificatelor și a cheilor private în HSM-uri certificate.
  - Oferă suport pentru revocarea certificatelor și generarea CRL-uri conform RFC 5280 și 6960
- Cryptomatic Signer 6:
  - Dispozitiv de semnătură calificată (QSCD), conform cu EN 419 241-1 & 2.
  - Suport pentru algoritmi avansați de criptare: RSA 2048/3072/4096 și ECDSA 256/384/521.
  - Integrare cu Signature Activation Module (SAM) pentru activarea semnăturii la distanță
- Portaluri personalizate (Portalul Utilizatorului și Portalul Organizației):
  - Suportă autentificare multi-factor și roluri de utilizator diferențiate.
  - Asigură managementul semnăturilor electronice și a certificatelor digitale la nivel de organizație.
  - Oferă capabilități de integrare cu API-uri și alte sisteme externe (PKI, IdP)

3.4. Cerințe privind disponibilitatea și redundanța

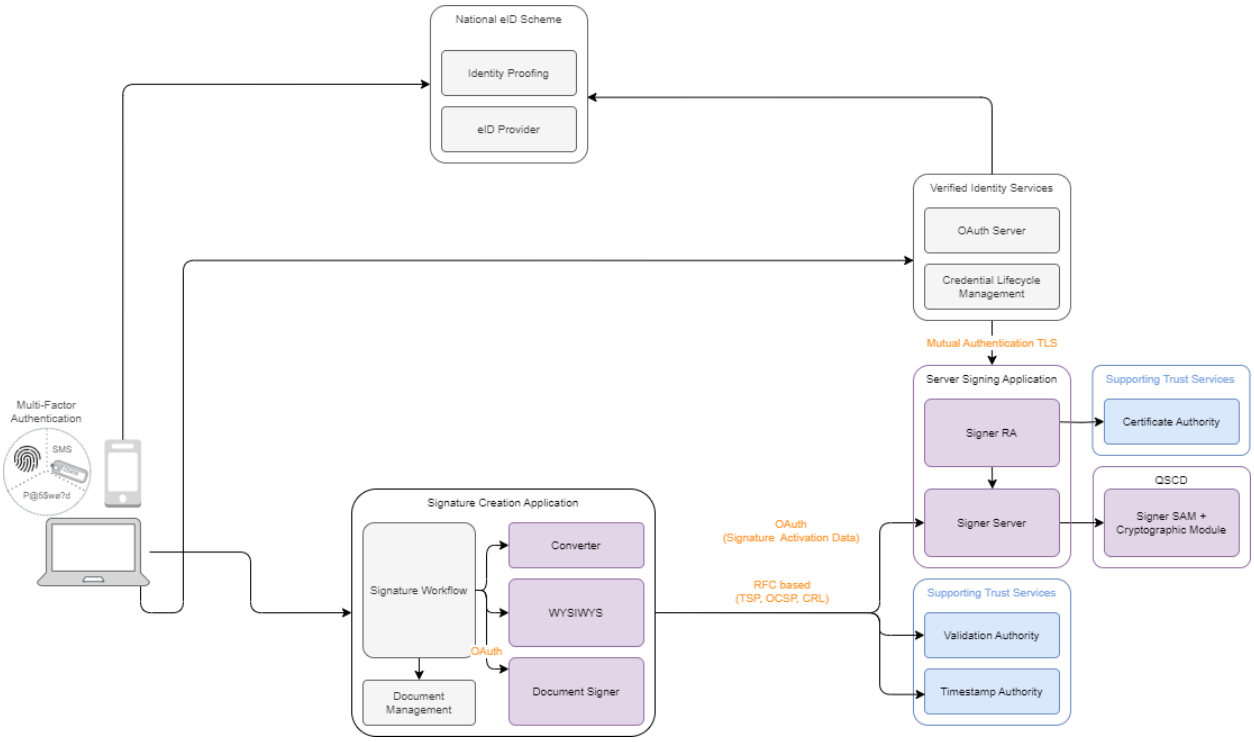
Pentru a asigura continuitatea serviciilor oferite și disponibilitatea constantă a soluției, următoarele cerințe de disponibilitate și redundanță sunt respectate:

1. **Înaltă Disponibilitate (HA)** – Soluția implementează o arhitectură de înaltă disponibilitate, asigurând funcționarea continuă a tuturor componentelor critice (Portaluri, HSM-uri, EJBCA) prin configurări active/active sau active/pasive.

2. **Recuperare în caz de dezastru (DR)** – Soluția include un plan detaliat de recuperare în caz de dezastru, cu proceduri bine definite pentru restaurarea cheilor și certificatelor, utilizând replicare securizată și backup-uri criptate stocate în locații separate.
3. **Mediu de testare și producție** – Soluția va include atât un mediu de producție complet funcțional, cât și un mediu de testare (pre-producție) care permite testarea extensivă a noilor funcționalități și actualizări înainte de implementarea în mediul de producție

4. Arhitectura sistemului

Arhitectura soluției propuse este concepută pentru a oferi un mediu robust, securizat și scalabil, care să permită gestionarea eficientă a cheilor publice și private, crearea semnăturilor electronice calificate și integrarea cu infrastructurile IT existente. Soluția include atât un mediu de producție, cât și un mediu de testare (pre-producție), fiecare fiind configurat pentru a asigura înaltă disponibilitate (HA) și recuperare rapidă în caz de dezastru (DR).



Figură 1High Level Architecture

4.1. Mediul de producție

Pentru a garanta un nivel ridicat de disponibilitate și securitate, arhitectura mediului de producție include componente redundante și mecanisme de protecție împotriva întreruperilor. Componentele critice ale soluției sunt replicate pentru a asigura funcționarea continuă, chiar și în cazul unor incidente care afectează una dintre instanțele sistemului.

Componentele principale ale mediului de producție:

1. Portalul de Semnare:
   - Oferă accesul utilizatorilor la interfața de semnare electronică.
   - O interfață securizată și intuitivă, disponibilă pe platforme web și mobile.
   - Suportă funcționalități de generare, verificare și gestionare a semnăturilor electronice pentru utilizatorii finali.
   - Portalul este integrat cu sistemul de gestiune a certificatelor și cu HSM-uri, asigurând securitatea cheilor private în procesul de semnare.
2. Serverul de Semnare:

- Servește drept componentă centrală pentru procesul de semnătură electronică la distanță.
- Integrare cu Signature Application Server (SSA) pentru gestionarea semnăturilor în mod securizat, utilizând HSM-uri certificate.
- Redundanță la nivelul serverului pentru a garanta continuitatea procesului de semnare.

3. Modulul de Activare a Semnăturii (SAM):
   - Certificat conform EN 419 241-1 & 2 și integrat cu dispozitivele HSM pentru activarea semnăturilor calificate la distanță.
   - Oferă funcționalități avansate de autentificare a utilizatorilor și protejarea datelor de semnătură prin algoritmi criptografici avansați (RSA și ECDSA).
4. Dispozitiv de creare a semnăturii electronice (HSM):
   - HSM-ul este responsabil pentru stocarea cheilor private și asigurarea unui mediu sigur pentru operațiile de semnare.
   - Soluția integrează HSM-uri certificate FIPS 140-2 și Common Criteria EAL4+, care asigură protecția completă a datelor criptografice în timpul procesului de semnătură.
   - Redundanță la nivel de HSM pentru a asigura funcționalitatea în caz de defecțiuni.
5. Autoritatea de Certificare (EJBCA):
   - Autoritatea de certificare este componenta centrală a infrastructurii de chei publice (PKI) și este responsabilă de emiterea și gestionarea certificatelor X.509.
   - EJBCA funcționează în mod redundant, asigurând disponibilitatea certificatelor pentru semnături și validări în timp real, prin servicii precum OCSP și CRL.
6. Serviciul de Marcare Temporală (TSA):
   - Serviciul de marcare temporală este integrat pentru a asigura conformitatea semnăturilor cu cerințele eIDAS privind semnăturile electronice calificate.
   - Marcare temporală pentru fiecare semnătură electronică creată, oferind o dovadă de existență a documentului la un moment determinat.
7. Protocol de verificare online a statutului certificatului (OCSP):
   - Permite verificarea în timp real a statutului certificatului digital, asigurând că certificatul utilizat pentru semnare este valid și nu a fost revocat.
8. Mecanisme de Securitate și Autentificare:
   - Soluția implementează autentificare multi-factor (MFA) și politici stricte de control al accesului pentru a garanta că doar utilizatorii autorizați pot accesa funcțiile critice ale sistemului.
   - Sunt utilizate tehnologii avansate de criptare pentru protejarea datelor în tranzit și la repaus.

4.2. Mediul de testare (pre-producție)

Mediul de testare este configurat astfel încât să reflecte complet mediul de producție, permițând testarea riguroasă a noilor funcționalități și verificarea integrării acestora în infrastructura existentă. Acest mediu este esențial pentru a asigura o tranziție lină a actualizărilor și a noilor componente în mediul de producție.

Componentele mediului de testare:

1. Replica componentelor din mediul de producție:
   - Mediul de testare conține instanțe de testare ale portalurilor, serverelor și componentelor critice, oferind o platformă complet funcțională pentru testare.
   - Permite testarea integrării noilor funcționalități cu HSM-uri, portaluri și alte componente critice înainte de lansarea în producție.
2. Testarea în condiții reale:
   - Toate funcționalitățile și serviciile sunt testate în mediul de testare pentru a asigura funcționarea corectă în condiții reale.
   - Simularea proceselor de semnare, revocare, și verificare a semnăturilor electronice, precum și a certificatelor utilizatorilor.

4.3. Redundanță și recuperare în caz de dezastru

O caracteristică esențială a arhitecturii propuse este capacitatea de a asigura redundanță și recuperare rapidă în caz de dezastru. Fiecare componentă critică este replicată pentru a minimiza timpul de nefuncționare și pentru a permite continuarea serviciilor fără întreruperi.

Redundanță la nivel de hardware și software:

- Toate componentele hardware (inclusiv HSM-uri, servere, și portaluri) sunt configurate în mod redundant, fie în configurație active/active, fie active/pasive, asigurând continuitatea serviciului în caz de eșec a unei componente.
- Replicarea datelor și a certificatelor între instanțele sistemului asigură protecția continuă a datelor critice și a cheilor private.

Recuperare în caz de dezastru (Disaster Recovery):

- Soluția include un plan detaliat de recuperare în caz de dezastru, cu backup-uri criptate și replicare automată a datelor în locații externe securizate.
- Timpul de recuperare este minimizat datorită arhitecturii distribuite și a componentelor redundant configurate.

4.4. Securitatea arhitecturii

Securitatea este un element central al arhitecturii soluției propuse, fiind implementată la toate nivelurile sistemului:

- Protecția datelor: Cheile private și semnăturile electronice sunt stocate și gestionate exclusiv în HSM-uri certificate, protejate împotriva accesului neautorizat și a pierderii de date.
- Autentificare multi-factor (MFA): Toate componentele sistemului sunt protejate prin mecanisme MFA, asigurând acces controlat și protejat la resursele critice.
- Monitorizare și audit: Sistemul oferă capabilități avansate de monitorizare și audit, înregistrând fiecare acțiune legată de procesul de semnătură electronică pentru a asigura conformitatea cu cerințele legale și standardele de securitate.

5. Specificații tehnice ale componentelor

Soluția propusă include o soluție complexă integrată care asigură realizarea în condiții de maximă securitate a serviciilor de creare, verificare și validare a semnăturilor electronice calificate. Fiecare componentă a soluției a fost selectată și configurată pentru a îndeplini cerințele tehnice și funcționale specifice proiectului. Mai jos este prezentată descrierea detaliată a fiecărei componente, ce realizează toate cerințele tehnice solicitate în caietul de sarcini, chiar dacă nu sunt expres menționate, astfel confirmam ca soluția propusa este una completă și conformă. Orice clarificare privind funcționalitățile oferite pot fi clarificate in procedura de evaluare sau de negociere semnării contractului.

5.1. Sistem de Autoritate de Certificare (CA) - EJBCA

EJBCA este nucleul infrastructurii PKI (Public Key Infrastructure) și servește drept Autoritate de Certificare (CA) pentru emiterea și gestionarea certificatelor digitale X.509. EJBCA este utilizat pentru a asigura emiterea certificatelor necesare semnăturilor electronice calificate și pentru a gestiona revocările certificatelor prin listele CRL și OCSP.

Specificații tehnice:

- **Compatibilitate standard**: ETSI EN 319 411-1 și ETSI EN 319 411-2 (pentru certificarea furnizorilor de servicii de încredere calificate).
- **Suport pentru OCSP și CRL**: Verificare în timp real a statutului certificatelor prin protocolul OCSP și generarea de CRL-uri (Certificate Revocation List) conform RFC 5280 și RFC 6960.
- **Integrare cu HSM**: EJBCA suportă integrarea cu Hardware Security Modules (HSM) pentru protejarea cheilor private utilizate la emiterea certificatelor.
- **Redundanță**: Funcționează în mod activ/activ sau activ/pasiv pentru a garanta disponibilitatea serviciului.
- **Algoritmi criptografici**: Suportă o gamă largă de algoritmi, inclusiv RSA (2048, 3072, 4096) și ECDSA (256, 384, 521).
- **Funcții de management**: Oferă management detaliat al certificatelor, al ciclului de viață al certificatelor și posibilitatea revocării automate a certificatelor expirate.

5.2. Dispozitiv de Semnătură Calificată (QSCD) - Cryptomatic Signer 6

Cryptomatic Signer 6 este un modul certificat pentru generarea și stocarea cheilor private și pentru realizarea semnăturilor electronice calificate (QSCD). Acest modul respectă cele mai stricte standarde de securitate și este compatibil cu Regulamentul eIDAS, oferind un mediu sigur pentru operarea semnăturilor electronice la distanță.

Specificații tehnice:

- **Certificare**: Conform cu EN 419 241-1 și EN 419 241-2, conform reglementărilor pentru dispozitivele de creare a semnăturilor calificate (QSCD).
- **Algoritmi criptografici**: RSA 2048/3072/4096 și ECDSA 256/384/521, suport pentru SHA-256, SHA-384 și SHA-512.

- **Suport pentru semnături multiple**: Poate gestiona semnături multiple pe același document, semnături în bloc și sigilii electronice.
- **Integrare cu Signature Application Server (SSA)**: Asigură funcționalități avansate pentru semnarea la distanță și stocarea sigură a cheilor private.
- **Metode de autentificare**: Integrare cu metode de autentificare multi-factor (MFA) și suport pentru OAuth și OIDC (OpenID Connect).
- **Protecția cheilor private**: Cheile private sunt stocate în mod securizat în HSM-uri, iar Signer 6 oferă funcții de management avansat al cheilor pentru a preveni accesul neautorizat.

5.3. Portaluri personalizate pentru utilizatori și organizații

Soluția include dezvoltarea unor portaluri personalizate pentru utilizatori și organizații, care permit gestionarea eficientă a proceselor de semnătură electronică și certificare digitală. Aceste portaluri sunt intuitive, securizate și accesibile prin web și dispozitive mobile, oferind multiple funcționalități pentru gestionarea certificatelor și semnăturilor.

Specificații tehnice:

- Portalul Utilizatorului:
  - Suportă gestionarea documentelor și semnăturilor electronice calificate.
  - Funcții avansate de încărcare, semnare, verificare și descărcare a documentelor digitale.
  - Suport pentru multiple roluri de utilizator: semnatar, verificator, editor de documente.
  - Integrare cu HSM-uri pentru gestionarea cheilor private și siguranța semnăturilor electronice.
  - Autentificare multi-factor și suport pentru diverse metode de autentificare (OAuth, OIDC, tokenuri hardware/software).
- Portalul Organizației:
  - Permite administrarea utilizatorilor și a certificatelor la nivel de organizație.
  - Gestionarea drepturilor de acces, a rolurilor și a metodelor de autentificare autorizate.
  - Suport pentru integrări cu IdP (Identity Providers) externe, cum ar fi Azure AD, Active Directory, Okta, și Auth0.
  - Funcții avansate de raportare și monitorizare a activităților legate de semnăturile electronice.

5.4. Servicii de Integrare API

Soluția propusă include un set complet de API-uri pentru integrarea cu sisteme externe și pentru automatizarea proceselor de semnătură electronică și gestionare a certificatelor digitale. Aceste API-uri sunt conforme cu standardele internaționale și asigură interoperabilitatea cu alte soluții IT.

Specificații tehnice:

- **Standarde suportate**: API-urile sunt conforme cu Cloud Signature Consortium v2 (CSC) și PKCS#11, permițând integrarea cu infrastructuri PKI existente și soluții externe de semnătură electronică.

- Funcții disponibile prin API:
    - Generare perechi de chei și emitere certificate.
    - Semnare și verificare a semnăturilor electronice calificate.
    - Gestionare a utilizatorilor și a drepturilor de acces.
    - Gestionarea semnăturilor în bloc pentru documente multiple.
    - Compatibilitate platforme: API-urile sunt compatibile cu o gamă largă de platforme, inclusiv Microsoft, Linux și sistemele cloud (Azure, AWS, Google Cloud).

5.5. Dispozitivul de crearea semnăturii electronice (HSM)

Soluția se integrează cu Hardware Security Modules (HSM-uri), puse la dispoziție de către autoritatea contractantă, certificate pentru a asigura protecția cheilor private și pentru a permite realizarea semnăturilor electronice într-un mediu sigur.

Specificații tehnice:

- **Certificare**: FIPS 140-2 nivel 3 și Common Criteria EAL4+.
- **Algoritmi de criptare**: Suport pentru algoritmi criptografici avansați (RSA, ECDSA) și funcții de protecție a cheilor private.
- **Redundanță**: Configurație de înaltă disponibilitate pentru a asigura continuitatea funcțiilor de semnare și stocare a cheilor.
- **Suport pentru API-uri**: Integrare cu API-uri pentru semnarea la distanță și gestionarea securizată a cheilor.

6. Cazuri de utilizare a complexului

Cazurile de utilizare descriu situații practice în care soluția propusă va fi implementată pentru a oferi servicii de semnătură electronică calificată, verificare și validare a documentelor digitale. Aceste scenarii acoperă nevoile diferite ale utilizatorilor soluției, inclusiv semnătura la distanță, gestionarea certificatelor digitale și integrarea cu infrastructurile IT existente. Aceste cazuri sunt de referință și pot fi clarificate, ajustate, îmbunătățite în funcție de preferințele autorității contractante.

6.1. Cazul 1: Semnătura electronică prin suport criptografic local

Acest caz de utilizare vizează generarea de semnături electronice utilizând suporturi criptografice locale, cum ar fi token-uri USB sau smartcard-uri.

Fluxul de lucru:

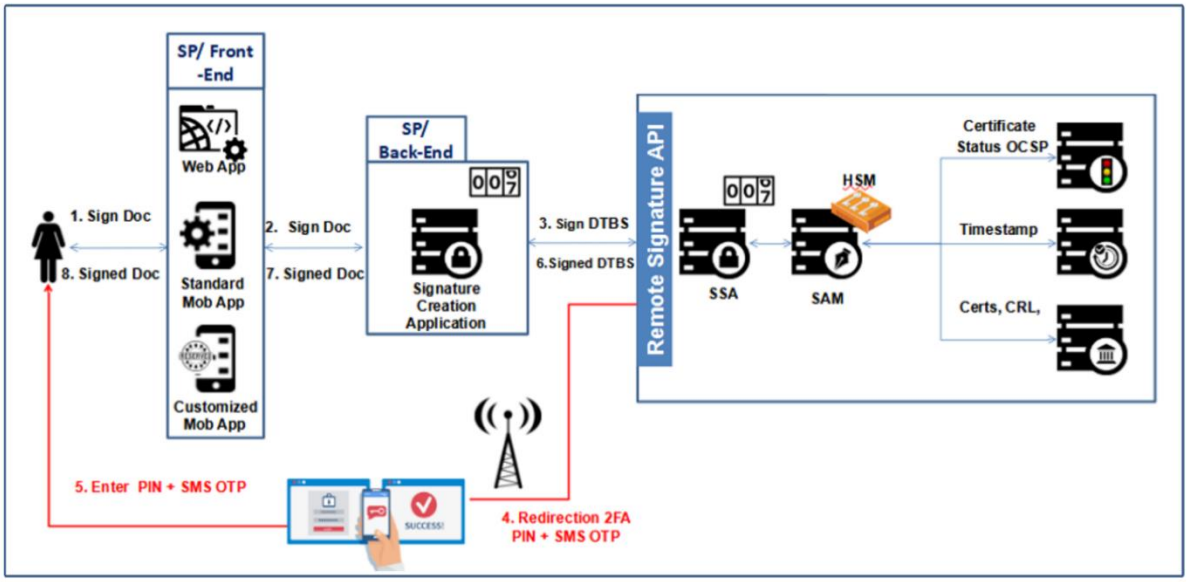
1. Utilizatorul accesează Portalul Utilizatorului pentru a încărca un document care urmează să fie semnat.
2. Sistemul cere utilizatorului să selecteze dispozitivul criptografic local (de exemplu, un token USB) pentru generarea semnăturii electronice.
3. Utilizatorul introduce token-ul USB sau smartcard-ul în dispozitivul său și se autentifică utilizând PIN-ul asociat.
4. Cheia privată de pe dispozitivul criptografic este utilizată pentru a genera semnătura electronică.
5. Semnătura electronică este aplicată documentului, iar documentul semnat este stocat în Portalul Utilizatorului sau descărcat de utilizator.

Caracteristici tehnice:

- **Autentificare**: Suportă autentificarea prin dispozitive criptografice locale, utilizând PKCS#11 pentru integrarea cu token-uri și smartcard-uri.
- **Algoritmi de semnătură**: RSA (2048, 3072, 4096), ECDSA (256, 384, 521).
- **Stocare securizată a cheilor**: Cheile private rămân stocate în mod securizat pe dispozitivul criptografic al utilizatorului.
- **Integrabilitate**: Semnătura este conformă cu standardele ETSI (PAdES, XAdES, CAdES) și poate fi verificată de orice aplicație compatibilă.

6.2. Cazul 2: Semnătura electronică la distanță SCAL 2

Acest scenariu ilustrează semnătura electronică la distanță, unde cheile private sunt stocate într-un HSM, iar utilizatorul accesează serviciul de semnare electronică de la distanță.



Figură 2 Semnătura electronică la distanță - SCAL 2

Fluxul de lucru:

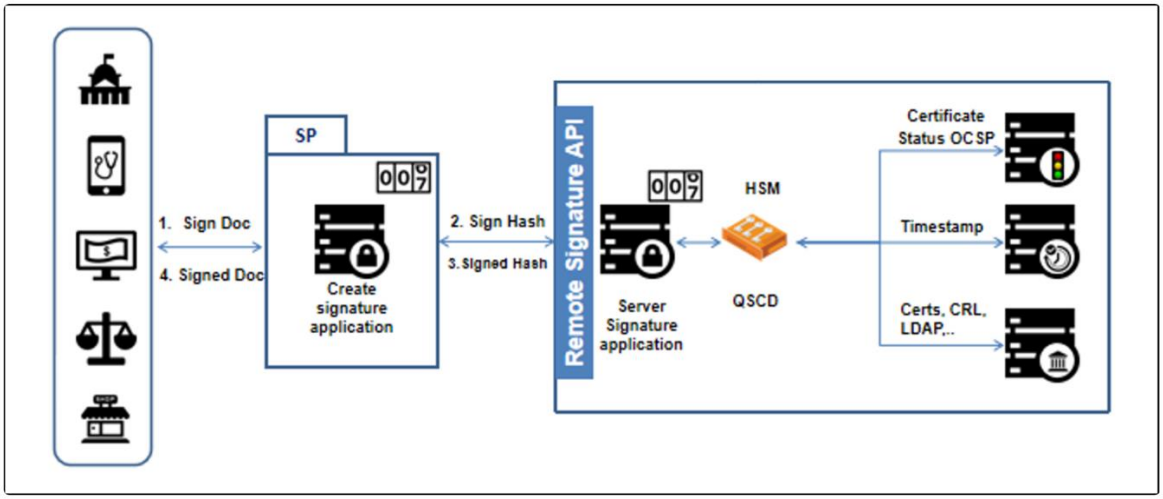
1. Utilizatorul se autentifică în Portalul Utilizatorului folosind un mecanism de autentificare multi-factor (MFA).
2. Utilizatorul încarcă documentul care urmează să fie semnat electronic.
3. Signature Application Server (SSA) primește solicitarea de semnătură și interacționează cu HSM-ul pentru a accesa cheia privată a utilizatorului.
4. Utilizatorul autorizează semnătura printr-un modul de activare a semnăturii (SAM), utilizând un dispozitiv mobil sau un alt mijloc de autentificare sigur.
5. Semnătura electronică este generată și aplicată documentului.
6. Documentul semnat este stocat în Portalul Utilizatorului și poate fi descărcat sau verificat ulterior.

Caracteristici tehnice:

- **Autentificare la distanță**: Soluția utilizează mecanisme MFA pentru autentificarea utilizatorului la distanță (OAuth, OpenID Connect).
- **Protecția cheilor private**: Cheile private sunt stocate într-un HSM certificat, iar accesul la ele este controlat prin intermediul modulului de activare a semnăturii (SAM).
- **Suport pentru semnături multiple**: Acest scenariu suportă semnarea simultană de către mai mulți utilizatori sau semnarea în serie, în funcție de fluxul de lucru stabilit.

6.3. Cazul 3: Semnătura electronică la distanță SCAL 1

Acest scenariu este similar cu SCAL 2, dar se aplică pentru semnăturile electronice unde nivelul de control și securitate este mai ridicat, cu utilizarea de token-uri suplimentare sau elemente hardware pentru activarea semnăturii.



Figură 3 Semnătura electronică la distanță - SCAL 1

Fluxul de lucru:

1. Utilizatorul se autentifică în Portalul Utilizatorului și accesează documentul care urmează să fie semnat.
2. Documentul este trimis către Signature Creation Application (SCA), care solicită activarea semnăturii din partea utilizatorului.
3. Utilizatorul utilizează un token hardware sau alt dispozitiv aprobat pentru a autoriza semnătura electronică.
4. Modulul de activare a semnăturii (SAM) verifică autentificarea utilizatorului și autorizează utilizarea cheii private din HSM.
5. Semnătura este generată, documentul semnat este returnat utilizatorului și stocat pentru verificare ulterioară.

Caracteristici tehnice:

- **Nivel ridicat de securitate**: Utilizarea unui token hardware sau a unui alt element securizat pentru activarea semnăturii.
- **Protecția datelor**: Semnătura este generată și validată în conformitate cu standardele de securitate impuse de EN 419 241-1 & 2.
- **Autentificare în două etape**: Autentificarea și semnarea implică două etape distincte, crescând nivelul de securitate pentru utilizator.

6.4. Cazul 4: Validarea documentelor semnate electronic

Acest caz de utilizare acoperă procesul de validare a unui document semnat electronic, pentru a verifica autenticitatea semnăturii și statutul certificatului utilizat.

Fluxul de lucru:

1. Utilizatorul accesează Portalul Utilizatorului sau utilizează un API extern pentru a încărca documentul semnat.
2. Sistemul verifică semnătura electronică și generează un raport care indică dacă semnătura este validă sau nu.
3. Sistemul OCSP este utilizat pentru a verifica statutul certificatului folosit la semnătură, asigurând că certificatul este valid și nu a fost revocat.
4. Utilizatorul primește raportul de validare, care poate fi stocat sau descărcat pentru utilizare ulterioară.

Caracteristici tehnice:

- **Suport pentru OCSP și CRL**: Sistemul verifică statutul certificatelor în timp real, utilizând OCSP și CRL conform RFC 6960.
- **Compatibilitate cu standardele ETSI**: Semnăturile sunt verificate conform standardelor ETSI pentru formate precum PAdES, XAdES și CAdES.
- **Raport de validare detaliat**: Utilizatorii primesc un raport complet care include toate informațiile relevante despre semnătură și certificatul asociat.

6.5. Cazul 5: Integrarea semnăturilor electronice în aplicații externe

Acest caz de utilizare descrie integrarea semnăturilor electronice calificate într-o aplicație externă, utilizând API-urile furnizate de soluție.

Fluxul de lucru:

1. Aplicația externă interacționează cu API-ul soluției pentru a transmite documentele care urmează să fie semnate.
2. API-ul CSC gestionează procesul de semnare, generând semnătura electronică calificată și returnând documentul semnat către aplicația externă.
3. Aplicația externă verifică validitatea semnăturii și stochează documentul semnat în sistemul propriu.

Caracteristici tehnice:

- **API standardizat**: API-ul CSC suportă semnături la distanță și integrarea cu diverse aplicații externe.
- **Compatibilitate multiplă**: API-ul este compatibil cu diverse formate de documente și standarde de semnătură electronică (PAdES, XAdES, CAdES).
- **Interoperabilitate**: Soluția permite integrarea cu alte infrastructuri IT, permițând fluxuri de lucru automate pentru semnarea documentelor.

7. Plan de implementare

Implementarea soluției propuse va urma un proces bine definit, împărțit în mai multe etape esențiale. Fiecare etapă va fi atent coordonată pentru a asigura succesul și eficiența procesului de implementare, astfel încât soluția să fie pusă în funcțiune la termen, cu toate componentele configurate și testate în mod corespunzător. Planul de implementare ia în considerare toate cerințele de hardware, software, resurse umane și timpul necesar pentru fiecare activitate.

7.1. Etapele principale ale implementării

1. Faza de proiectare și planificare (Săptămâna 1 - 3)

Această fază este esențială pentru a asigura o înțelegere completă a cerințelor proiectului și pentru a defini toate aspectele tehnice ale soluției. În cadrul acestei etape se va finaliza documentația tehnică, arhitectura sistemului și toate specificațiile funcționale și nefuncționale.

- **Definirea arhitecturii**: Se va elabora un plan detaliat de arhitectură pentru soluția PKI, HSM-uri, portaluri și toate componentele software și hardware.
- **Alocarea resurselor**: Se va desemna echipa de proiect, incluzând dezvoltatori software, arhitecți de sistem, ingineri de rețea și administratori de securitate.
- **Planificarea calendarului de implementare**: Stabilirea etapelor detaliate de implementare, cu termene precise pentru fiecare livrabil.

2. Configurarea și pregătirea mediului (Săptămâna 4 - 5)

În această etapă se vor instala și configura toate componentele necesare pentru funcționarea soluției în mediu de testare. Se va asigura că mediul de testare reflectă complet mediul de producție.

- **Instalarea HSM-urilor**: Configurarea HSM-urilor în mediul de testare, asigurând redundanța și protecția cheilor private.
- **Configurarea EJBCA**: Implementarea sistemului de autoritate de certificare (CA) și integrarea cu HSM-urile.
- **Configurarea portalurilor**: Instalarea și configurarea Portalului Utilizatorului și a Portalului Organizației, precum și integrarea acestora cu sistemul de gestionare a certificatelor și semnăturilor.
- **Configurarea API-urilor**: Integrarea și testarea API-urilor pentru semnătura electronică calificată și validarea semnăturilor electronice.
- **Mediul de testare**: Configurarea mediului de testare, pregătit pentru testarea funcțională și de securitate.

3. Faza de dezvoltare (Săptămâna 4 - 15)

Această fază este dedicată dezvoltării componentelor personalizate incluse în soluție, cum ar fi portalurile utilizatorilor și organizațiilor, integrarea API-urilor și implementarea serviciilor de semnătură la distanță. Dezvoltarea acestor componente se va face în strânsă colaborare cu echipa de arhitectură și inginerie, pentru a asigura conformitatea cu cerințele tehnice și de securitate.

- **Dezvoltarea portalului utilizatorului și organizației**: Crearea și implementarea interfețelor web securizate pentru utilizatori și organizații, permițând gestionarea semnăturilor electronice și a certificatelor digitale.
- **Dezvoltarea și integrarea API-urilor**: Dezvoltarea API-urilor conform standardelor internaționale (CSC, PKCS#11) pentru a permite integrarea semnăturilor electronice în alte sisteme IT.
- **Implementarea fluxurilor de lucru**: Configurarea fluxurilor de lucru pentru semnături multiple, verificarea și validarea documentelor.
- **Testarea inițială**: Testarea funcționalităților dezvoltate în medii izolate, înainte de a le integra în infrastructura principală

4. Faza de testare și validare (Săptămâna 8 - 16)

În această fază vor fi efectuate teste extensive pentru a asigura funcționarea corectă a soluției și pentru a valida conformitatea acesteia cu cerințele de securitate și performanță.

- **Testarea funcționalităților**: Se vor testa toate componentele soluției pentru a confirma că funcțiile de semnare, verificare și gestionare a certificatelor sunt implementate corect.
- **Testarea securității**: Verificarea conformității cu cerințele de securitate, inclusiv criptarea datelor în tranzit și la repaus, autentificarea multi-factor și protecția cheilor private în HSM-uri.
- **Testarea integrării**: Testarea integrării API-urilor cu sisteme terțe și validarea interoperabilității soluției cu alte platforme.
- **Testarea performanței**: Evaluarea performanței soluției pentru a asigura că poate gestiona numărul de utilizatori și tranzacții specificate fără întreruperi.

5. Implementarea în mediul de producție (Săptămâna 14 - 16)

După finalizarea cu succes a testelor, soluția va fi implementată în mediul de producție. Această fază implică replicarea configurațiilor și funcțiilor testate în mediul de producție.

- **Instalarea în producție**: Implementarea și configurarea completă a soluției în mediul de producție, inclusiv HSM-urile, sistemele PKI, portalurile și API-urile.
- **Transferul datelor**: Importarea certificatelor și cheilor private din mediul de testare, după caz, cu protecția deplină a datelor și conformitatea cu cerințele de securitate.
- **Activarea semnăturii electronice**: Activarea funcțiilor de semnătură electronică calificată pentru utilizatori și configurarea modulului de activare a semnăturii (SAM).

6. Instruirea utilizatorilor și administratorilor (Săptămâna 16 - 18)

După implementarea soluției, va fi efectuată instruirea utilizatorilor și a administratorilor pentru a asigura că soluția este utilizată în mod corespunzător și eficient.

- **Instruirea administratorilor**: Administratorii sistemului vor fi instruiți în gestionarea și configurarea soluției, inclusiv gestionarea HSM-urilor, EJBCA și API-urile.
- **Instruirea utilizatorilor finali**: Utilizatorii finali vor primi instrucțiuni privind utilizarea portalurilor, generarea semnăturilor electronice și gestionarea documentelor digitale.
- **Suport tehnic**: Se va oferi suport tehnic post-implementare pentru a răspunde la orice probleme legate de utilizarea soluției.

7.2. Resurse necesare

Implementarea soluției va necesita resurse specifice pentru a asigura succesul fiecărei etape. Resursele includ echipa tehnică, echipamentele hardware și licențele software necesare pentru configurarea și funcționarea soluției.

Resurse umane:

- **Dezvoltatori software**: Responsabili pentru configurarea și dezvoltarea portalurilor și API-urilor.
- **Ingineri de rețea și securitate**: Responsabili pentru configurarea HSM-urilor, infrastructurii de rețea și asigurarea securității soluției.
- **Arhitecți de sistem**: Coordonatori ai proiectului, responsabili pentru designul și integrarea soluției în infrastructura existentă.
- **Traineri**: Responsabili pentru instruirea utilizatorilor și administratorilor.

Resurse hardware și software:

- **Hardware Security Modules (HSM)**: HSM-uri certificate pentru stocarea și gestionarea cheilor private.
- **Servere pentru EJBCA și portaluri**: Servere dedicate pentru sistemul de certificare și portalurile utilizatorilor.
- **Licențe software**: Licențe și alte componente software necesare.

8. Concluzii și avantaje

Soluția propusă reprezintă o platformă complexă, integrată, concepută special pentru a răspunde cerințelor tehnice și legale din Republica Moldova. Aceasta integrează tehnologii certificate și conforme cu standardele europene și internaționale, inclusiv cu regulamentul eIDAS, garantând atât securitatea cât și interoperabilitatea cu soluțiile guvernamentale existente. Proiectată pentru a asigura flexibilitate maximă și independență tehnologică, soluția oferă o infrastructură robustă, fără a impune dependențe tehnologice pe termen lung, comparativ cu alte soluții comerciale similare care creează blocaje și costuri continue pentru stat.

8.1. Avantajele cheie ale soluției

Soluție complexă și adaptată cerințelor Republicii Moldova

Soluția a fost concepută ținând cont de specificitățile legislative și tehnologice ale Republicii Moldova. Aceasta se bazează pe componente certificate și conforme cu regulamentul eIDAS, ceea ce asigură că soluția respectă toate cerințele legale aplicabile serviciilor de încredere și semnăturilor electronice calificate. Astfel, soluția va fi compatibilă cu cadrul normativ existent, inclusiv cu directivele naționale privind semnăturile electronice și protecția datelor.

- **Respectarea cerințelor legale**: Soluția este complet conformă cu legislația națională și europeană (eIDAS), garantând că autoritatea contractantă va beneficia de o infrastructură de încredere pentru gestionarea semnăturilor electronice calificate.
- **Integrarea cu soluții guvernamentale**: Soluția oferă flexibilitate pentru integrarea cu alte soluții IT guvernamentale existente, conform cadrului normativ (MPass, MSign), asigurând o interoperabilitate eficientă fără necesitatea unor modificări majore.

Componente certificate și conforme cu eIDAS

Soluția se bazează pe componente certificate (inclusiv EJBCA, Cryptomatic Signer 6 și HSM-uri), toate conforme cu regulamentul eIDAS și alte standarde internaționale de securitate, cum ar fi FIPS 140-2 și Common Criteria EAL4+. Această certificare asigură faptul că soluția îndeplinește cele mai stricte cerințe de securitate și protecție a datelor, garantând integritatea și confidențialitatea proceselor de semnătură electronică calificată.

- Componente certificate: Fiecare componentă critică este certificată conform celor mai stricte standarde de securitate (eIDAS, FIPS 140-2), ceea ce oferă o garanție suplimentară privind protecția datelor sensibile și siguranța operațiunilor criptografice.
- Reducerea riscului de dependență: Prin utilizarea componentelor certificate și a integrărilor flexibile, soluția reduce riscul de dependență de furnizori specifici, oferind statului controlul asupra tehnologiilor esențiale.

Componente personalizate dezvoltate – flexibilitate și independență

Soluția propune dezvoltarea unor componente personalizate care să ofere fiabilitate și să minimizeze dependența completă de soluțiile QSCD (Qualified Signature Creation Device) și HSM-uri certificate. Această abordare va asigura o flexibilitate sporită pentru stat, permițând autorităților să evite blocajele tehnologice impuse de soluții comerciale, cum ar fi **Ascertia**, care ar putea genera dependență totală de un singur furnizor și costuri considerabile pe termen lung.

- **Reducerea dependenței tehnologice**: Spre deosebire de alte soluții care creează blocaje tehnologice, soluția propusă permite statului să mențină un control mai mare asupra infrastructurii tehnice și să evite dependențele de furnizori specifici.
- **Costuri optimizate pe termen lung**: Soluția elimină nevoia de plăți continue și ridicate pentru licențe și extinderi, care ar fi inevitabile în cazul soluțiilor care impun blocaje tehnologice. Această flexibilitate va permite statului să reducă considerabil costurile de operare și extindere.

Flexibilitate de integrare cu soluțiile guvernamentale

Soluția a fost proiectată pentru a fi complet compatibilă cu sistemele IT guvernamentale existente, conform cadrului normativ. Prin intermediul API-urilor standardizate, soluția poate fi integrată cu alte infrastructuri IT deja implementate, facilitând interoperabilitatea și reducând costurile asociate integrării.

- **API-uri standardizate și interoperabilitate**: Soluția oferă un set complet de API-uri conforme cu standardele internaționale, permițând integrarea rapidă și flexibilă cu alte soluții IT guvernamentale și neimpunând dependențe tehnologice pe termen lung.
- **Suport pentru extindere**: Arhitectura modulară permite extinderea soluției pe măsură ce apar noi cerințe legislative sau tehnologice, fără a afecta funcționarea infrastructurii existente.

Implementarea unei soluții complete în 60 de zile – nefezabil

Datorită complexității soluției propuse, implementarea unei platforme complete și integrate în termen de 60 de zile este nerealistă. Un termen de implementare minim realist pentru o astfel de soluție este de cel puțin 5 luni, având în vedere următorii factori esențiali:

- **Complexitatea tehnică**: Soluția implică integrarea unor componente certificate (PKI, HSM, portaluri personalizate), dezvoltarea unor funcționalități custom și asigurarea interoperabilității cu infrastructura IT guvernamentală. Testarea și configurarea acestor componente necesită timp pentru a asigura funcționarea corectă și conformitatea cu cerințele legale și de securitate.
- **Dezvoltare și testare**: Dezvoltarea componentelor custom, precum portalurile utilizatorilor și API-urile de integrare, necesită o perioadă extinsă de testare și validare pentru a evita erori și vulnerabilități. Fără o fază adecvată de testare, implementarea ar putea introduce riscuri de securitate și funcționare defectuoasă.
- **Instruirea și tranziția**: O altă fază esențială a proiectului este instruirea utilizatorilor și administratorilor, care trebuie realizată corect pentru a asigura adoptarea și utilizarea

eficientă a soluției. Aceasta nu poate fi comprimată în termene scurte fără a compromite succesul proiectului.

Termen minim realist: Un termen de 5 luni este mai realist pentru implementarea completă a soluției, permițând dezvoltarea, testarea, configurarea și integrarea componentelor personalizate, asigurând în același timp conformitatea și securitatea la cele mai înalte standarde.

8.2. Beneficiile pentru autoritatea contractantă

Prin adoptarea soluției propuse, autoritatea contractantă va beneficia de o serie de avantaje care se reflectă atât în reducerea costurilor pe termen lung, cât și în îmbunătățirea securității și a eficienței operaționale. Acestea includ:

- **Flexibilitate și independență tehnologică**: Organizarea nu va fi dependentă de furnizori specifici și va putea să gestioneze soluția în mod independent, ceea ce va reduce costurile asociate mentenanței și extinderii soluției.
- **Costuri optimizate**: Comparativ cu alte soluții comerciale, soluția propusă va elimina costurile ridicate asociate licențelor și extinderilor tehnologice forțate de dependența de furnizori specifici.
- **Conformitate și securitate**: Soluția respectă standardele eIDAS și asigură protecția datelor critice printr-o arhitectură certificată și auditabilă, reducând riscurile de neconformitate și vulnerabilități de securitate.

9. Tabel de conformitate cu cerințele tehnice ale proiectului

CERINȚE	CONFIRMARE
IV. CERINȚE GENERALE Cerințele stabilite în acest caiet de sarcini sunt considerate cerințe minime pe care ofertanții trebuie să le respecte. Titularului contractului trebuie să oferă mecanismele care asigură următoarele:	
- Posibilitatea integrării în infrastructura cheilor publice și servicii de marcare temporală existente;	DA
- Posibilitatea interconectării și integrării cu componentele hardware existente (HSM) (inclusiv Utimaco CryptoServer CP5);	DA
- Posibilitatea extinderii capacităților prin crearea și păstrarea cheilor publice și private a utilizatorilor semnăturii electronice în HSM/ cloud protejat;	DA
- Existența posibilității de utilizare a tehnologiilor prin intermediul telefonului mobil;	DA
- Deținerea controlului asupra repozitorului unde sunt păstrate cheile prestatorului și utilizatorului;	DA
- Componentele și soluția în general trebuie să fie în conformitate cu standardelor internaționale inclusiv cu FIPS 140-2 sau de CommonCriteria, precum și la nivel UE;	DA
- Oferirea mediului de testare (pre-producție) și mediului de producție și mediul de recuperare în caz de dezastru;	DA
- Posibilitatea personalizării complexului/dispozitivului sub stilul autentic, cu integrarea denumirii convenționale propuse de I.P. „STISC” și după caz a logo-ului.	DA

CERINȚE		CONFIRMARE
V. ARHITECTURA NECESARĂ		
MEDIUL DE PRODUCȚIE		
Pentru garantarea ridică a disponibilității a serviciilor prestate, este necesară existența componentelor platformei, câte două de fiecare, după cum urmează:		
Portal de semnare,		DA
Serverul de semnare,		DA
Marcare Temporală,		DA
Protocol de verificare online a statutului certificatului,		DA
Autoritatea de certificare,		DA
Modulul de activare a semnăturii,		DA
Dispozitiv de creare a semnăturii electronice.		DA
VI. SPECIFICAȚII TEHNICE		
Descriere	Caracteristici	
Cerințe generale	Această componentă este o soluție care se integrează cu aplicații web și desktop pentru a realiza crearea semnăturii electronice.	DA
	Permite persoanelor juridice și fizice să genereze în siguranță semnături electronice și să le verifice	DA
	Această componentă trebuie să accepte semnarea folosind o cheie privată găzduită:	
	· De la distanță pe un HSM	DA
	· Local pe un mediu criptografic	DA
	Trebuie remarcat faptul că toate mediile criptografice utilizate de STISC sunt compatibile cu protocolul PKCS#11	
	Componentă trebuie să permită partenerilor STISC accesarea/utilizarea API de creare a semnăturii electronice și de verificare a semnăturii electronice	DA
	Soluția de semnătură trebuie să realizeze criptarea în transit și separat	DA
	Această componentă acceptă mai multe limbi:	
	· Engleză	DA
	· Română	DA
Arhitectură	Arhitectura soluției de semnătură electronică trebuie să respecte arhitectura definită în prezentul caiet de sarcini	DA
	Soluția trebuie să fie disponibilă ca interfață web și aplicație mobilă	DA
	Soluția de semnătură trebuie să fie multi-tenant care să sprijine mai multe organizații	DA
Portalul utilizatorului	Managementul și semnarea documentelor	
	Soluția trebuie să oferă:	
	· un vizualizator de documente	DA

CERINȚE		CONFIRMARE
	· posibilitatea de a descărca și semna electronic documentul	DA
	· posibilitatea de a alege suportul pentru semnătură (suport criptografic sau HSM la distanță)	DA
	· posibilitatea de a verifica un document semnat	DA
	· posibilitatea de a insera o imagine a semnăturii lor vizibilă în documentul semnat și de a configura aspectul semnăturii	DA
	posibilitatea de a încărca documente, de a adăuga destinatari, de a alege un Suport pentru mai mulți semnatari per document	DA
	În timpul unui flux de lucru de semnare, posibilitatea acceptării mai multor roluri pentru destinatari: semnatar, editor de documente, o persoană în copie	DA
	· asocierea semnăturii electronice cu imaginea a semnăturii de mână (semnătură olografă) aplicată pe document	DA
	posibilitatea autentificarii semnatarul și obținerea consimțământul acestuia înainte de a emite o semnătură electronică	DA
	posibilitatea încărcării unei varietăți de tipuri de fișiere: PDF, Word, Excel, PowerPoint, text, imagini grafice	DA
	posibilitatea convertării automat fișierele non-PDF în format PDF/A pentru semnare	DA
	Urmărirea fluxului de lucru și a proceselor	
	Soluția trebuie să:	
	Acceptă mai multe tipuri de flux de lucru hibrid, în serie de semnături (de exemplu, un flux de lucru care definește o ordine de secvență pentru semnatarii unui document, un flux de lucru în care fiecare semnatar semnează „copia sa” a documentului sau o combinație a ambelor)	DA
	· Oferă posibilitatea de a urmări starea unui document (de exemplu, document trimis/vizionat/semnat/finalizat)	DA
	· Furnizeze un tablou de bord pentru a vedea starea tuturor fluxurilor de lucru (de exemplu, în curs, finalizat, în așteptare)	DA
	· Trimiterea notificări când un document este în așteptarea semnării	DA
	· Oferirea posibilității de a trimite documentul unui examinator înainte de a putea fi semnat	DA
	· Furnizeze un raport sigilat de dovezi ale fluxului de lucru care curprinde fiecare detaliu al procesului de semnătură	DA
	Securitatea și controlul documentelor	
	Soluția trebuie să:	

CERINȚE		CONFIRMARE
	· Oferă posibilitatea de a bloca documente PDF	DA
	· Implementeze controlul accesului asupra documentelor trimise utilizatorilor invitați (de exemplu, autentificați-vă folosind OTP trimis prin e-mail înainte de a deschide documentul)	DA
	· Creeze câmpuri de formular în documentele PDF și controlați dreptul de a le edita	DA
	Caracteristici suplimentare de semnare	
	Soluția trebuie să:	
	· Suporte posibilitatea semnării mai multor documente în același pachet/plic	DA
	· Suporte capacitatea de a adăuga un substituent într-un flux de lucru de semnătură care să fie completat de următorul semnatar într-un flux de lucru serial	DA
	· Suportă delegarea semnării	DA
	· Ofere posibilitatea unui semnatar de a semna folosind acreditările CSC	DA
	Interfață de utilizator și experiență	
	Soluția trebuie să:	
	· Ofere posibilitatea unui utilizator de a schimba locația și de a enumera limbile acceptate	DA
	· Ofere posibilitatea de a seta întrebări de securitate și de a reseta parolele	DA
Portal de organizare	Managementul utilizatorilor și al rolurilor	
	· Administratorul organizației trebuie să poată gestiona conturile de utilizator la nivel de organizație	DA
	· Administratorul organizației trebuie să fie capabil să gestioneze rolurile la nivel de organizație	DA
	· Administratorul organizației trebuie să fie capabil să definească metodele de autentificare autorizate	DA
	· Administratorul organizației trebuie să poată seta nivelul de asigurare a semnăturii alocat pentru un anumit rol	DA
	Gestionarea notificărilor și șabloanelor	
	Soluția trebuie să ofere acces pentru a configura setările de notificare și șabloanele de e-mail	DA
	Soluția trebuie să ofere capabilități de gestionare a șabloanelor cu fluxuri de lucru standard	DA
	Managementul cotelor și al resurselor	
	Soluția trebuie să ofere capacitatea de a gestiona cota și de a atribui o perioadă de valabilitate (de exemplu, numărul maxim de semnături pentru un utilizator, dimensiunea depozitului pentru un utilizator)	DA

CERINȚE		CONFIRMARE
	Integrare și conectivitate	
	Soluția trebuie să ofere capacitatea de integrare cu IdP-urile organizației (de exemplu, Azure AD, Active Directory, Okta, Auth0)	DA
	Soluția trebuie să ofere capacitatea de a configura webhook-uri	DA
	Soluția trebuie să ofere posibilitatea de a trimite documente finalizate și rapoarte de dovezi ale fluxului de lucru către un server de la distanță	DA
	Cloud și managementul stocării	
	Administratorul organizației trebuie să poată activa/dezactiva unitățile cloud permise (de exemplu, Google Drive, OneDrive, Dropbox)	DA
	Branding	
	· Soluția trebuie să ofere capacitatea de a configura branding la nivel de organizație	DA
Portalul administratorului	Raportare și monitorizare	
	Soluția trebuie să:	
	· Oferere capabilități avansate de raportare	DA
	Managementul configurației	
	Soluția trebuie să:	
	· Aplicați 2FA pentru autentificarea administratorilor	DA
	· Oferere posibilitatea de a configura limita operațiunilor în bloc	DA
	· Ofere posiblitatea configurării dimensiunii permise a atașamentului de e-mail	DA
	· Ofere posibilitatea de a configura politica de securitate a conținutului în interfața de utilizare	DA
	· Ofere capacitatea de a configura nivelul de asigurare al semnăturilor, inclusiv:	DA
	Semnătură electronică avansată/calificată (locală/la distanță)	DA
	Sigiliu electronic avansat/calificat	DA
	Semnătură avansată de mare încredere (AATL)	DA
	Managementul conectărilor și integrării:	
	Soluția trebuie să:	
	Ofere posibilitatea de a configura SMS Gateway	DA
	Ofere posibilitatea de a configura serviciul SMTP	DA
	Ofere posibilitatea de a configura conectorul CSC	DA
	Ofere capacitatea de a configura Cloud Drives	DA
	Ofere posibilitatea de a configura integrarea IdP	DA
	Ofere posibilitatea de a configura Firebase pentru notificarea push	DA

CERINȚE		CONFIRMARE
	Ofere posibilitatea de a configura gateway-uri de plată	DA
	Managementul stocării	
	Soluția trebuie să:	
	· Ofere posibilitatea de a stoca documente în baza de date, Azure Blob sau stocare locală	DA
Serviciul de înregistrare	Interfețe pentru aplicații de afaceri ar trebui să suporte următoarele funcții:	
	Înregistrarea utilizator	DA
	Actualizarea utilizatorul	DA
	Ștergerea utilizator	DA
	Obținerea utilizator	DA
	Obținerea utilizatori	DA
	Schimbarea parolei	DA
	Recuperarea parolei	DA
	Confirmați Recuperarea parolei	DA
	Schimbarea adresei de e-mail a utilizatorului	DA
	Confirmarea modificării e-mailului utilizatorului	DA
	Schimbarea utilizatorul mobil	DA
	Confirmarea schimbării utilizatorului mobil	DA
	Obținerea dispozitivelor înregistrate	DA
	Ștergerea dispozitivului	DA
	Generarea perechii de chei	DA
	Ștergerea perechii de chei	DA
	Obțineți CSR	DA
	Importarea certificatului	DA
	Obțineți certificatelor utilizatorilor	DA
	Autentificare/Logare fără parolă	DA
	API-ul Cloud Signature Consortium (CSC) ar trebui să accepte următoarele funcții:	
	Authentication/Login	DA
	Authentication/Revoke	DA
	Credentials/List	DA
	Credentials/Info	DA
	Credentials/Authorize	DA
	Credentials/extendTransaction	DA
	Credentials/sendOTP (SMS, Email)	DA
	Signatures/signHash	DA
	OAuth2/Authorize	DA
	OAuth2/Token – Authorization Code Flow	DA
	OAuth2/Token – Client Credentials Flow	DA

CERINȚE		CONFIRMARE
	OAuth2/Token – Refresh Token Flow	DA
	OAuth2/Revoke	DA
	API-ul Mobile Application Interfaces ar trebui să accepte următoarele funcții	
	Autentificare client / Authenticate Client	DA
	Autentificare utilizator / Authenticate User	DA
	Verificați OTP-urile / Verify OTPs	DA
	Reînnoiți tokenul de acces / Renew Access Token	DA
	Înregistrarea dispozitivului / Device Registration	DA
	Listați dispozitivele înregistrate / List Registered Devices	DA
	Ștergeți dispozitivul / Delete Device	DA
	Obținerea cererii de autorizare în așteptare / Get a Pending Authorisation Request	DA
	Obținerea solicitării de autorizare în așteptare / Get Pending Authorisation Requests	DA
	Autorizarea solicitării în așteptare / Authorise a Pending Request	DA
	Anularea cererii de autorizare în așteptare / Cancel a Pending Authorisation Request	DA
	Profilul utilizatorilor / Users Profile	DA
	Obțineți setări de înregistrare a dispozitivului / Get Device Registration Settings	DA
	Generați codul QR / Generate QR Code	DA
	Verificați codul QR / Verify QR Code	DA
	Înregistrarea dispozitivului pentru notificarea push / Register Device for Push Notification	DA
	Ștergerea dispozitivului pentru notificare push / Delete Device for Push Notification	DA
Aplicație de creare a semnăturilor (SCA)	Integrare și compatibilitate	
	Soluția trebuie să:	
	Integreze cu serviciul de marcare temporală STISC pentru a încorpora marca temporală atunci când este creată semnătura electronică (pe baza RFC 61)	DA
	Integreze cu serviciul OCSP al STISC pentru a verifica răspunsul OCSP în timpul creării semnăturii electronice (pe baza RFC 6960)	DA
	Încorporeze datele de verificare a certificatului electronic (răspunsul CRL, OCSP) în timpul creării semnăturii electronice pentru valabilitate pe termen lung	DA
	Caracteristici de semnătură	
	Soluția trebuie să:	
	Permită reprezentarea vizuală a unei semnături PAdES	DA

CERINȚE		CONFIRMARE
	Ofere posibilitatea activării inserarea unei semnături imagine vizibile pe documentul semnat	DA
	Aplice o sigila electronică pe un document semnat	DA
	Aplicarea semnăturii electronice pe mai multe pagini ale unui document	DA
	Aplicarea mai multor semnături pe mai multe părți pe același document	DA
	Gestionarea semnăturii electronice unui document și amprenta sa (hash)	DA
	Verificați documentele încărcate înainte de a le semna	DA
	Suporte crearea și verificarea semnăturii electronice pentru diferite tipuri de documente	DA
	Oferă posibilitatea semnării în bloc a documentelor prin diverse interfețe și API-uri	DA
	Ofere suport pentru profiluri de semnătură și politici de securitate pentru diferite aplicații	DA
	Managementul conectorilor și integrării	
	Soluția trebuie să:	
	ofere semnarea în bloc a documentelor, cum ar fi facturi, rapoarte și extrase de cont	DA
	Ofere suport pentru procesarea cu mai multe fire și echilibrarea/balansarea sarcinii pe mai multe servere	DA
	asigure compatibilitatea cu tokene USB, cardurile inteligente și serviciile de semnare de la distanță	DA
	Faciliteze configurarea și utilizarea cheilor/certificatelor de semnare corporative (bulk/în vrac).	DA
	Conformitatea cu standardele și suport pentru documente	
	Soluția trebuie să:	
	Suportă mai multe sisteme de operare, inclusiv Microsoft Server și diverse distribuții Linux	DA
	Ofere compatibilitate cu o gamă largă de baze de date, inclusiv Microsoft SQL Server, Oracle, PostgreSQL, MySQL și Percona-XtraDB-Cluster	DA
	Asigure securitatea datelor cu modulele de securitate hardware (HSM) precum Utimaco CP5, Thales Luna și Entrust nShield	DA
	Conformitatea cu standardele și suport pentru documente	
	Soluția trebuie să:	
	Respecte standarde precum IETF, ETSI, ISO, W3C, OASIS și CSC	DA
	Accepte semnarea și verificarea pentru PDF, documente Office și date XML	DA

CERINȚE		CONFIRMARE
	Furnizeze formatele de semnătură electronică, cum ar fi PAdES, XAdES și CAdES	DA
	Asigure compatibilitatea cu centrele de date cu mai multe niveluri și cu mai multe servere CA, CRL, OCSP și TSA	DA
Server de aplicare a semnăturii (SSA)	SSA trebuie să expună API-urile pentru aplicație de creare a semnăturii folosind interfețe standard, cum ar fi CSCv1	DA
	SSA ar trebui să aibă o componentă gateway care să servească drept proxy frontend	DA
	SSA trebuie să sprijine două mecanisme pentru a semna SAD:	
	· Aplicatie de mobil	DA
	· IdP	DA
	În cazul utilizării aplicației mobile pentru a semna SAD, aplicația mobilă trebuie să genereze/păstreze cheia în elementul securizat al dispozitivului mobil	DA
	SSA trebuie să ofere capacitatea de a impune utilizarea sau nu a datelor biometrice către SAD	DA
	Soluția trebuie să vină cu sau să se integreze cu MobileCA pentru a genera Certificat pentru dispozitive mobile pentru a semna SAD	DA
	SSA trebuie să ofere posibilitatea de a efectua activarea semnăturii folosind OIDC sau Dispozitiv mobil	DA
	SSA ar trebui să accepte autorizarea serviciului folosind OAuth	DA
	SSA trebuie să ofere opțiuni pentru a configura autentificarea inițială a dispozitivului mobil folosind:	
	· OTP prin SMS și/sau EMAIL	DA
	· Cod QR	DA
	· Fără autentificare	DA
Modul de activare a semnăturii (SAM)	Modulul SAM trebuie să fie certificat în Common Criteria EAL4+ și EN 419 241 1 & 2	DA
	Modulul SAM trebuie să fie un aparat fizic inviolabil care să se integreze cu un HSM extern certificat EN 419 221-5	DA
	Modulul SAM trebuie să îndeplinească cerințele:	
	· Dispozitiv compatibil cu FIPS 140-2 Nivel 3	DA
	· Regulamentul eIDAS	DA
	· EN 419 241-1 & 2	DA
	· TS 119 4-1	DA
	· TS 119 4-2	DA
	· TS 119 432	DA
	Modulul SAM trebuie să realizeze următorii algoritmi:	
	· RSA 2048, 3072, 4096, 8192	DA

CERINȚE		CONFIRMARE
	· ECDSA 256, 384, 521	DA
	· SHA-256, SHA-384, SHA-512	DA
	Modulul SAM trebuie să accepte:	
	· Nivelul SCAL 1	DA
	· Nivelul SCAL 2	DA
	Se integrează cu Signature Application Server (SSA) pentru a oferi funcționalitate de semnătură/sigilare la distanță aplicațiilor client prin intermediul API-urilor	DA
	Modulul SAM trebuie să accepte metode de autentificare/autorizare:	
	· Autentificare cu doi factori folosind aplicația mobilă	DA
	· OAuth folosind OIDC pentru SAML	DA
	Dispozitivul SAM trebuie să vină cu propria bază de date încorporată, cu suport pentru configurarea activă/activă	DA
	Modulul SAM trebuie să expună API-ul REST pentru	
	· Înscriere (crearea utilizatorilor, generarea cheilor, importul certificatelor,...)	DA
	· Semnare	DA
	Toate acțiunile de semnare efectuate de un utilizator sunt înregistrate	DA
Formate de semnătură	Componentă trebuie să suporte:	
	· PAdES, XAdES semnături	DA
	· Niveluri de semnătură B- B, B-T, B-LT, B-LTA,	DA
	Pentru semnăturile pe termen lung, această componentă ar trebui să fie integrată cu autoritatea/serviciul existent de marcare temporală STISC	DA
Verificarea semnăturii	Această componentă trebuie să asigure verificarea acestor tipuri de semnături:	
	· CMS/PKCS#7	DA
	· Semnături PDF	DA
	· XML	DA
	· ETSI PAdES, CADES, XAdES (B, T, LT, LTA)	DA
	· S/MIME	DA
	· MS Office	DA
	Această componentă trebuie să ofere ancore de încredere (Trust Anchors) configurabile	DA
	Această componentă trebuie să aibă capacitatea de a impune o listă de algoritmi de semnătură aprobați	DA
	Aceste componente trebuie să aibă capabilități avansate de descoperire a căilor:	
	· Construirea căilii folosind Turst Anchors înregistrate în soluție	DA

CERINȚE		CONFIRMARE
	· Crearea căliі utilizând certificatele furnizate în cerere	DA
	· Crearea căliі utilizând extensia AIA a certificatului de subiect	DA
	· Crearea căliі utilizând certificate în directoarele LDAP	DA
	Această componentă trebuie să aibă capacitatea de a impune validarea căii pe baza:	
	· lista de OID a politicii de certificate acceptabile și/sau	DA
	· Extensii Specific Key Usage sau Extended Key Usage	DA
	Această componentă trebuie să ofere validarea istorică a semnăturii pe baza informațiilor furnizate în semnătură	DA
	Această componentă trebuie să ofere capacitatea de a îmbunătăți semnătura de la *AdES-B la *AdES-T/LT/LTA	DA
	Această componentă ar trebui să ofere clientului OCSP parametri configurabili de solicitare OCSP	DA
Validarea certificatului	Această componentă trebuie să asigure validarea certificatului în timpul semnării prin:	
	· Liste de revocare a certificatelor (CRL)	DA
	· OCSP	DA
Înregistrare evenimente	Toți pașii procesului de semnare/verificare trebuie să fie documentați în jurnalele securizate	DA
	Toate modificările de configurare ar trebui să fie înregistrate	DA
	Asigurarea integrității jurnalelor de evenimente pentru orice tip de investigație (forensics)	DA
	Generarea datelor de audit / Audit data generation	DA
	evenimente de management cheie (generare, utilizare și distrugere);	DA
	evenimente de semnare a utilizatorilor ;	DA
	autentificarea utilizatorului în timpul SAP;	DA
	managementul TW4S al semnatarului SAD;	DA
	pornirea și oprirea funcției de generare a datelor de audit;	DA
	modificări ale parametrilor de audit.	DA
	Parametrii datelor de audit	DA
	Toate înregistrările de audit (inclusiv înregistrările de audit specifice serviciului) TREBUIE să conțină următorii parametri:	DA
	Data și ora evenimentului;	DA
	Tipul evenimentului;	DA
	Identitatea entității (de exemplu, utilizator, administrator, proces) responsabilă pentru acțiune;	DA
	Succesul sau eșecul evenimentului auditat.	DA
Cerințe de securitate	Soluția ar trebui să respecte următoarele cerințe de securitate:	

CERINȚE		CONFIRMARE
	Toate componentele sistemului ar trebui să fie actualizate și fără vulnerabilități cunoscute	DA
	Toate componentele sistemului ar trebui să fie întărite conform celor mai bune practici din industrie	DA
	Pentru dezvoltarea de aplicații, furnizorul ar trebui să urmeze cele mai bune practici OWASP.	DA
	Soluția ar trebui să accepte roluri cu privilegii diferite (ofițeri de securitate , administratori de sistem , operatori de sistem , auditori de sistem)	DA
	Mecanism de identificare și autentificare și aplicare a politicii	DA
	Suport SCAL 2 cu element securizat și SCAL1	DA
Branding	Bradingul acestei componente trebuie adaptat la cartea grafică STISC, cu personalizarea logoului și denumirii soluției/complexului.	DA
Documentație	Ofertantul trebuie să furnizeze toate documentele necesare, și anume:	
	· Manuale de instalare, configurare, administrare, utilizare;	DA
	· Documentația API pentru această componentă;	DA
Licență	Licența perpetuă	DA
	Număr de utilizatori: 2 milioane	DA
	Număr de tranzacții: nelimitat	DA
Medii	Soluția furnizată trebuie să fie disponibilă în medii de preproducție, producție în înaltă disponibilitate și recuperare în caz de dezastru	DA
VII. CAZURI DE UTILIZARE A COMPLEXULUI		
Următoarele cazuri de utilizare reprezintă o descriere simplă a cazurilor/scenariilor de utilizare pe care STISC dorește să le implementeze în procesul prestării serviciilor de încredere. Titularul contractului va defini cazurile de utilizare care urmează să fie implementate cu STISC, în conformitate cu cele mai recente versiuni ale standardelor enumerate în prezentul caiet de sarcini.		DA
CAZUL 1		
Semnătură electronică prin suport criptografic		
În acest caz, STISC pune la dispoziție clienților/utilizatorilor săi un middleware pentru a efectua semnătura electronică prin intermediul suportului criptografic (Token/SC) disponibil, dispozitiv de creare a semnăturii electronice sau a sigiliului electronic. Utilizatorul este liber să aleagă tehnologia și dispozitivele care le convin.		DA
CAZUL 2		
Semnătură electronică la distanță SCAL 2		
STISC va oferi serviciul de semnare de la distanță SCAL 2, așa cum se arată în figura de mai jos. STISC va permite accesul de la distanță la serverul său de semnături prin intermediul API-urilor furnizate (SCAL 2) Furnizorul de servicii (SP) are o aplicație de creare a semnăturii care creează și transmite datele care urmează să fie semnat (Hash) către STISC SP		DA

CERINȚE		CONFIRMARE
construiește documentul semnat din datele semnate furnizate de serverul de semnături STISC		
CAZUL 3		
Semnătură electronică la distanță SCAL 1		
STISC are ca scop prestarea serviciul de creare a semnăturii electronice la distanță SCAL 1, așa cum se arată în figura de mai jos. STISC va permite accesul la SSA de la distanță prin intermediul API-urilor furnizate (SCAL 1). Prestaror /furnizor de servicii are o aplicație de creare a semnăturii (Signature Creation Application) care creează și transmite datele care urmează să fie semnate (Hash) către STISC. Prestator/furnizor de servicii construiește documentul semnat din datele semnate furnizate de STISC SSA		DA
VIII. SPECIFICAȚII TEHNICE PENTRU INSTRUIRE		
Descriere	Caracteristici	
Cicluri de antrenament	1 ciclu de instruire de cel puțin 5 zile care acoperă instalarea, configurarea, administrarea și integrarea API a tuturor componentelor platformei implementate	DA
Participanții	1. Administratori: 2	DA
	2. Operatori: 3	DA
Subiecte de formare	· Instalarea tuturor componentelor propuse,	DA
	· Administrarea, configurarea si productia tuturor componentelor oferite,	DA
	· Troubleshooting,	DA
	· Integrarea API-urilor precum API-urile de înregistrare, semnătura electronică etc	DA

Prenume Nume: Dorin Grițcan

Funcția în cadrul firmei: Administrator

Denumirea firmei și sigiliu: „ESEMPLA Systems” S.R.L.