Manual de utilizare a semnăturii electronice

European Commission

EU Digital Identity Wallet

Un manual de cazuri de utilizare reprezintă o descriere a unui caz de utilizare specific pentru Portofelul de identitate digitală al UE. Acesta include o introducere în cazul de utilizare și parcursul utilizatorului, stadiul actual al dezvoltării cazului de utilizare, precum și referințe la specificațiile tehnice și infrastructurile relevante, la legislație și la structurile de guvernanță.

Manualul de cazuri de utilizare este conceput pentru implementatorii Portofelului, statele membre și alte părți interesate de dezvoltarea Portofelului și de cazurile sale de utilizare.

Manualul de cazuri de utilizare nu are scopul de a conține specificații tehnice complete și detaliate pentru cazul de utilizare. Cu toate acestea, în cazul în care astfel de specificații sunt disponibile, manualul de cazuri de utilizare conține trimiteri către acestea.

Descriere

O semnătură electronică calificată (QES) este o semnătură electronică avansată creată de un dispozitiv calificat de creare a semnăturilor (QSCD) și bazată pe un certificat calificat pentru semnături electronice. Aceasta poate fi utilizată în diverse situații: la semnarea unui contract de muncă, la deschiderea unui cont bancar online, la depunerea declarației fiscale sau la solicitarea unui certificat de naștere… Acestea au aceeași valoare juridică ca și semnăturile olografe.

Crearea semnăturii electronice calificate prin intermediul Wallet-ului se poate realiza fie printr-un Wallet certificat care acționează ca QSCD și creează semnături la nivel local, fie printr-un QSCD la distanță gestionat de un Furnizor de Servicii de Încredere Calificat (QTSP). QTSP-urile obțin statutul de calificare de la organismul național de supraveghere și sunt incluse în Lista de Încredere națională corespunzătoare.

POTENTIAL LSP a testat integrarea QES cu servicii de semnare la distanță și cu funcțiile unui Furnizor de Servicii de Încredere Calificat (QTSP).

Parcursul (parcursurile) utilizatorului

Scenariul 1

Semnătura electronică calificată bazată pe portofel:

Simplificat

1. Utilizatorul primește un contract de închiriere (de exemplu, prin e-mail) și îl încarcă în portofelul său EUDI.
2. Portofelul afișează contractul și detaliile acestuia pentru verificare și solicită utilizatorului să semneze folosind codul PIN sau datele biometrice.
3. Portofelul se conectează la un furnizor de încredere securizat, care verifică identitatea utilizatorului și sigilează oficial documentul în numele acestuia.
4. Contractul este acum semnat legal și poate fi trimis înapoi proprietarului.

Flux detaliat

1. Proprietarul pregătește contractul în format PDF, îl semnează și îl trimite utilizatorului prin e-mail sau mesagerie instant.
2. Utilizatorul deschide aplicația EUDI Wallet (și se autentifică folosind codul PIN sau datele biometrice).
3. PDF-ul este încărcat în funcția de semnare a aplicației Wallet.
4. Aplicația EUDI Wallet afișează contractul în format PDF (sau îl deschide într-o altă aplicație).

5. Utilizatorul verifică documentul/datele și solicită portofelului să semneze documentul.

6. Opțional: utilizatorul selectează serviciul de semnare (dacă este diferit de cel implicit sau dacă este înscris la mai multe servicii).

7. Portofelul EUDI calculează hash-ul și îl trimite furnizorului de servicii de încredere calificat (QTSP) care gestionează dispozitivul calificat de creare a semnăturii în numele utilizatorului.

8. QTSP solicită portofelului EUDI să aprobe semnarea documentului în numele utilizatorului.

9. Portofelul EUDI notifică utilizatorul cu privire la cererea de aprobare în așteptare.

10. Utilizatorul verifică detaliile tranzacției și aprobă semnarea.

11. Utilizatorul se autentifică folosind date biometrice sau un cod PIN, iar portofelul creează o prezentare către QTSP de exemplu, prezentând PID-ul.

12. QTSP verifică aprobarea utilizatorului și utilizează cheile acestuia pentru a semna documentul.

13. QTSP returnează aplicației de semnare a portofelului documentul semnat.

14. Contractul în format PDF este acum semnat de ambele părți.

15. Utilizatorul trimite o copie a documentului semnat înapoi proprietarului, astfel încât ambii să o aibă.

Scenariul 2
Aplicație de semnătură electronică inițiată de partea care se bazează pe semnătura electronică
- Semnarea prin intermediul unui portal web

Simplificat

1. Utilizatorul accesează portalul web al furnizorului de servicii energetice, se înscrie pentru a beneficia de serviciu, parcurge procesul de înregistrare și, în final, ajunge la etapa de semnare a contractului.

2. Portalul afișează contractul pentru revizuire și, la etapa de semnare, oferă serviciul furnizorului său de servicii de încredere calificat (QTSP) pentru crearea semnăturii („Semnează cu DocuSign”).

3. Utilizatorul examinează contractul și scanează codul QR pentru a iniția o semnătură folosind un cod PIN sau date biometrice.

4. Portofelul electronic trimite dovada criptografică către furnizorul de servicii de încredere securizat, care semnează și sigilează documentul și îl trimite înapoi către sistemul furnizorului de servicii.

5. Portalul web confirmă că contractul este semnat și că serviciul este activ.

Flux detaliat

1. Utilizatorul accesează portalul web al furnizorului de servicii energetice, care acționează în calitate de parte de încredere (RP), și se înscrie pentru a beneficia de serviciu.

2. Furnizorul pregătește și pune la dispoziție un contract pentru a fi semnat.

3. Portalul afișează contractul pentru revizuire și, la etapa de semnare, propune furnizorul său QTSP pentru crearea semnăturii („Semnează cu DocuSign”).

4. Utilizatorul examinează contractul și continuă.

5. RP trimite către QTSP hash-ul datelor și informează QTSP cu privire la identitatea semnatarului vizat.

6. QTSP-ul contactează apoi portofelul utilizatorului pentru a confirma aprobarea acestuia (fie direct, fie prin redirecționarea utilizatorului către un site web al QTSP-ului, unde este prezentat un cod QR (sau un link) pentru a iniția sesiunea de semnare).

7. Utilizatorul deschide portofelul și verifică identitatea părții solicitante.

8. Utilizatorul aprobă semnarea folosind portofelul său EUDI (de exemplu, prezintă PID-ul furnizorului de servicii de semnare).

9. QTSP verifică aprobarea utilizatorului și utilizează cheile utilizatorului pentru a semna documentul.

10. QTSP returnează documentul semnat către sistemul RP.

11. RP generează semnătura completă și finalizează crearea documentului semnat.

12. Portalul web confirmă utilizatorului că acordul de servicii a fost semnat atât de utilizator, cât și de furnizorul de servicii energetice și că utilizatorul a fost înscris pentru a beneficia de serviciu.

Impactul cazului de utilizare

Beneficii

Valoarea pentru utilizatorul final/cetățean
Integrarea funcționalităților semnăturii electronice calificate (QES) în portofelul de identitate digitală europeană (EUDI) oferă o valoare substanțială utilizatorilor finali și cetățenilor, sporind atât comoditatea, cât și accesibilitatea. Persoanele fizice pot semna documente oficiale în condiții de siguranță din orice locație și în orice moment, fără a fi nevoie de hardware sau software suplimentar și fără proceduri complexe de înregistrare. Odată înregistrați, cetățenii beneficiază de generarea gratuită a semnăturii electronice calificate (QES), eliminând astfel cheltuielile care apar de obicei în cazul serviciilor de semnătură oferite de terți. Echivalența juridică a QES cu semnăturile olografe în toate statele membre ale UE asigură un grad ridicat de certitudine juridică, consolidând încrederea în tranzacțiile administrative și comerciale complet digitale. În plus, utilizarea protocoalelor de autentificare puternică și a certificatelor de încredere reduce riscurile legate de fraudă, furtul de identitate și contestarea semnăturii. Prin eliminarea necesității de a imprima, scana, trimite prin poștă sau de a se prezenta personal, sistemul accelerează semnificativ finalizarea proceselor, sporind astfel eficiența atât pentru cetățeni, cât și pentru furnizorii de servicii.

Avantaje pentru furnizorii de servicii
Pentru furnizorii de servicii, implementarea funcționalității semnăturii electronice calificate (QES) prin intermediul portofelului European Digital Identity (EUDI) oferă beneficii operaționale și strategice semnificative. Automatizarea proceselor permite executarea digitală fără întreruperi a contractelor, înregistrarea clienților și fluxurile de lucru de aprobare în sectoare precum cel bancar, resursele umane, serviciile juridice și telecomunicațiile, reducând astfel durata ciclurilor și sarcinile administrative. Prin minimizarea dependenței de tipărire, expediere prin poștă, stocarea fizică și gestionarea manuală a documentelor, organizațiile pot obține

fluxuri de lucru mai eficiente și costuri operaționale mai mici. Experiența de semnare simplificată și intuitivă nu numai că sporește satisfacția clienților, dar și consolidează încrederea prin reducerea fricțiunilor tranzacționale. Respectarea deplină a Regulamentului-cadru al UE privind identitatea digitală garantează că semnăturile electronice calificate (QES) executate prin intermediul portofelului EUDI beneficiază de valabilitate juridică transfrontalieră, reducând complexitatea operațiunilor care implică mai multe jurisdicții. În plus, integrarea cu furnizorii de servicii de încredere calificați (QTSP) și mecanismele solide de autentificare garantează autenticitatea documentelor și consolidează măsurile de protecție împotriva fraudei și falsificării.

Beneficii pentru autoritățile publice
Pentru autoritățile publice, integrarea capacităților de semnătură electronică calificată (QES) în portofelul de identitate digitală europeană (EUDI) reprezintă un factor cheie al transformării digitale cuprinzătoare. Aceasta facilitează furnizarea de servicii publice complet online – de la declarații fiscale și cereri de autorizații până la solicitări de documente de stare civilă – asigurând în același timp schimburi sigure, autentificate și care nu pot fi contestate între cetățeni și administrații. Interoperabilitatea transfrontalieră inerentă sistemului, aliniată la Cadrul UE privind identitatea digitală 2.0, susține colaborarea administrativă fără sincope între statele membre ale UE și garantează recunoașterea reciprocă a documentelor semnate electronic. Prin reducerea dependenței de procesele bazate pe hârtie, de comunicarea poștală și de prestarea serviciilor în persoană, autoritățile publice pot obține o eficiență operațională mai mare, costuri mai mici și pot aloca resursele mai eficient către servicii publice de mare valoare.

Valoarea economică și dimensiunea potențială a pieței

Această secțiune va fi actualizată odată cu apariția portofelelor operaționale și a modelelor lor de afaceri

Sinergii cu alte cazuri de utilizare

Se pot obține beneficii suplimentare din utilizarea portofelului pentru semnătura electronică prin sinergia cu următoarele cazuri de utilizare:

- *Autorizarea plăților online:*
  Semnăturile electronice pot autoriza tranzacții de valoare mare sau reglementate, îndeplinind cerințele de autentificare puternică a clientului (SCA).

- *Reprezentarea persoanelor fizice sau juridice:*
  Semnăturile electronice pot confirma faptul că o persoană acționează oficial în numele unei organizații sau al unei alte persoane.

- *Deschiderea unui cont bancar:*
  Băncile ar putea utiliza QES pentru a semna contracte de la distanță, cu valabilitate juridică deplină.

- *Diplome de studii:*
  Eliberarea și verificarea diplomelor, certificatelor sau foilor matricole ar putea fi semnate digital pentru a asigura autenticitatea acestora.

- *Rețeta electronică (eP):*
  O QES poate confirma că o rețetă provine de la un medic autorizat, prevenind falsificarea.

Implementarea cazurilor de utilizare

Implementări existente

Cazul de utilizare a fost testat în cadrul proiectului **POTENTIAL**, unde cel de-al cincilea caz de utilizare s-a axat pe integrarea QES cu serviciile de semnare la distanță și cu funcțiile furnizorului de servicii de încredere calificat (QTSP). Cazul de utilizare a fost testat în cadrul proiectului **NOBID** (ca parte a proiectului-pilot principal – integrarea în serviciile financiare prin QES) de către patru state membre (Danemarca, Letonia, Germania, Italia), precum și de Islanda și Norvegia.

În **Estonia**, aplicația Smart-ID permite utilizatorilor să se autentifice și să realizeze semnături electronice calificate (QES) care respectă standardele Cadrului de identitate digitală al UE. Smart-ID Basic este disponibilă și în Letonia și Lituania și poate fi utilizată numai pentru serviciile bancare online.

ID Austria este o platformă de identitate electronică bazată pe o aplicație care include funcționalități de autentificare digitală și semnătură electronică.

Carta d'Identità Elettronica (CIE) este cartea de identitate electronică a **Italiei**, care permite cetățenilor să realizeze semnături electronice avansate (AdES), inclusiv în formatele PAdES și CAdES, utilizând tehnologia NFC și fie un cod PIN, fie verificarea biometrică.

Aplicația itsme oferă cetățenilor din **Belgia** comoditatea unui singur proces de înregistrare, autentificare și semnare pentru numeroase servicii online diferite. Aplicația este certificată conform eIDAS și poate fi utilizată pentru a îndeplini cerințele PSD2 și GDPR.

IDMe.cy este identitatea electronică națională recent introdusă în **Cipru** (parte a platformei „Digital Citizen"), oferind autentificare de înaltă siguranță și semnături electronice echivalente din punct de vedere legal cu cele olografe.

Gov.gr Wallet este aplicația oficială a **Republicii Elene**, care permite cetățenilor să semneze documente digitale rapid și în siguranță prin intermediul docs.gov.gr.

Aplicația mobilă ID.gov.pt din **Portugalia** este un portofel digital care permite cetățenilor să-și stocheze cărțile de identitate și să exporte certificate PDF semnate digital cu o semnătură digitală calificată garantată de stat. **Diia** este aplicația ucraineană open-source pentru servicii publice, care integrează pe scară largă documente digitale, semnături digitale și schimbul securizat de documente.

Legislație

Articolul 22 din Regulamentul-cadru al UE privind identitatea digitală obligă statele membre să publice informații referitoare la furnizorii de servicii de încredere calificați (QTSP) pentru care sunt responsabile, împreună cu informații referitoare la serviciile de încredere calificate furnizate de aceștia. Furnizorul de servicii de încredere obține statutul de „calificat" de la organismul național de supraveghere, a cărui decizie este reflectată și publicată în „listele de încredere" corespunzătoare. Decizia de punere în aplicare (UE) 2015/1505 a Comisiei definește specificațiile tehnice ale acestor liste de încredere.

În conformitate cu articolele 27 și 37 din Regulamentul-cadru al UE privind identitatea digitală, Decizia de punere în aplicare a Comisiei (UE) 2015/1506 specifică formatele minime ale semnăturilor electronice

avansate și ale sigiliilor avansate care trebuie recunoscute de organismele din sectorul public pentru a asigura interoperabilitatea transfrontalieră a serviciilor online oferite de acestea.

Sursă

Regulamentul de punere în aplicare 2024/2981: Stabilește norme pentru aplicarea Regulamentului (UE) nr. 910/2014 privind certificarea portofelelor de identitate digitală europene și asigură că portofelele gestionează certificatele calificate și mecanismele de creare a semnăturilor (cum ar fi QSCD-urile sau rQSCD-urile) într-un mod de încredere, rezultând semnături electronice cu forță juridică obligatorie.

Regulamentul de punere în aplicare 2024/2979: Recunoaște în mod explicit că portofelele trebuie să poată primi sau gestiona certificate calificate legate de dispozitive calificate de creare a semnăturilor electronice (QSCD) și să execute aplicații de creare a semnăturilor (fie integrate, separate sau la distanță), permițând astfel semnăturile electronice calificate.

Regulamentul de punere în aplicare 2025/1567: Stabilește norme și definește modul în care trebuie gestionate și reglementate dispozitivele la distanță de creare a semnăturilor electronice calificate (rQSCD).

Specificații tehnice, biblioteci software și infrastructură

Modelul de date, formatul și mecanismele de dovadă
QSCD nu se află neapărat în posesia fizică a semnatarului, ci poate fi gestionat și de la distanță de către QTSP. Conform secțiunii 3.9 din Cadrul de referință al arhitecturii (ARF), crearea unei QES folosind portofelul EUDI se poate realiza în mai multe moduri:

- fie EUDI Wallet în sine ar putea fi certificat ca QSCD, fie
- portofelul poate interacționa cu dispozitive calificate de creare a semnăturilor electronice la distanță (rQSCD) gestionate de furnizori calificați de servicii de încredere (QTSP) pentru a emite semnături. Aceste conexiuni trebuie să respecte standardele de referință din actele de punere în aplicare privind gestionarea la distanță a dispozitivelor de semnătură.

Modelul de date al semnăturii electronice include:

- **Conținut semnat și metadate**, cum ar fi:
  - identitatea și atributele semnatarului
  - Tipul semnăturii (AdES sau QES)
  - Marca temporală și metoda de marcare temporală
  - Profilul semnăturii (de exemplu, PAdES, XAdES)
  - Informații despre certificat, starea revocării și lanțul de încredere

Mecanismele de dovadă variază în funcție de format.

Emitere
Portofelul poate servi drept interfață de utilizator pentru inițierea semnării, transmiterea datelor către rQSCD și recuperarea rezultatelor semnate.

Ca parte a ecosistemului, utilizarea unor interfețe și protocoale comune pentru furnizarea de semnături și sigilii electronice calificate va crea o piață europeană unificată pentru QTSP-uri care oferă servicii de semnare la distanță.

Verificare
Verificarea are loc, de obicei, în cadrul portofelului sau al sistemelor părților de încredere, utilizând protocoale standardizate de validare a semnăturilor electronice integrate cu listele de încredere ale UE și căile de certificate. Acestea trebuie să suporte validarea semnăturilor AdES/QES utilizând profiluri ETSI stabilite, precum PAdES, XAdES, CAdES sau containerele ASiC.

Vedeți un exemplu de flux al procesului de verificare pentru QES la distanță.

Cadrul de încredere
Serviciile de încredere sunt utilizate împreună cu semnătura electronică pentru a asigura validitatea, inclusiv:

- *Marcarea temporală:*
  data și ora indicate pe un document electronic, care dovedesc că documentul a existat la un moment dat și că nu a suferit modificări de atunci.

- *Sigiliul electronic:*
  echivalentul electronic al unui sigiliu sau al unei ștampile care se aplică pe un document pentru a garanta originea și integritatea acestuia.

- *Transmiterea electronică:*
  un serviciu care, într-o anumită măsură, este echivalentul în lumea digitală al scrisorii recomandate din lumea fizică.

- *Admisibilitatea juridică a documentelor electronice*
  pentru a asigura autenticitatea și integritatea acestora.

- *Autentificarea site-ului web:*
  informații de încredere de pe un site web (de exemplu, un certificat) care permit utilizatorilor să verifice autenticitatea site-ului web și legătura acestuia cu entitatea/persoana care deține site-ul web.

Fără certitudinea privind valabilitatea juridică a tuturor acestor servicii conexe, întreprinderile și cetățenii vor rămâne reticenți în a utiliza interacțiunile digitale ca mod natural de interacțiune, deoarece vor fi nesiguri în privința unui eventual litigiu.

Aceasta este intenția care stă la baza Regulamentului-cadru al UE privind identitatea digitală, referitor la identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.

Dispozițiile aplicabile serviciilor de încredere prevăzute de Regulamentul-cadru al UE privind identitatea digitală se aplică direct în toate cele 27 de țări ale UE.

European Commission

EU Digital Identity Wallet