Portofel de identitate digitală

Bazat pe tehnologie blockchain

Lansare curentă

Autori **(în ordine alfabetică)**	Augustin Jianu
Proprietar	certME
Nr. versiune	1.2
Data publicării documentului	Ianuarie 2022
Clasificare	Public

Istoric document

Versiune	Autor	Data	Descriere
1.0	*Product Owner*	*2021-03-01*	*Prima publicare*
1.1	*Product Owner*	*2021-08-13*	*Actualizări minore*
1.2	*Product Owner*	*2022-01-04*	*Adăugat verificare video, conectivitate API și alte actualizări minore*

Cuprins

1. Abstract 5
2. Companie 6
   2.1. Despre 6
   2.2. Misiune 6
   2.3. Viziune 6
3. Scop și aplicabilitate 7
   3.1. Scop 7
   3.2. Domeniu de aplicabilitate 7
4. Abordări ale eID 7
   4.1. Context 7
   4.2. Abordarea comercială curentă 7
   4.3. eID-ul național centralizat 8
   4.4. ID auto-suveran 8
5. Serviciu 9
   5.1. Descriere 9
   5.2. Rețea de parteneri 9
   5.3. Model operațional 9
   5.4. Validatori 10
   5.5. Politica datelor 10
   5.6. Politica de reziliere 11
6. Tehnologie 11
   6.1. Mijloace de identificare electronică 11
   6.2. Aplicația mobilă 12
      6.2.1. ID electronic 12
      6.2.2. Emitere eID 12
      6.2.3. Autentificare 13
      6.2.4. Solicitarea și furnizarea datelor de identificare personală 13
      6.2.5. Consimțământul utilizatorului și respectarea GDPR 13
      6.2.6. Suspendare 14
   6.3. Aplicația Validator 14
      6.3.1. Verificarea identității 14
      6.3.2. Colectarea și procesarea datelor utilizatorului 14
      6.3.3. Răspuns la cererile de validare 14

6.3.4. Suspendare 15
6.3.5. Reactivare 15
6.3.6. Revocare 15
6.4. Serviciul autentificator 15
6.4.1. Interacțiunea cu utilizatorul 15
6.4.2. Interacțiunea cu Blockchain 16
6.5. Contracte inteligente 16
7. Concluzii 16
8. Abrevieri 17
9. Glosar 18

1. Abstract

Era digitală a permis noi tipuri de modele de afaceri colaborative - denumite în mod obișnuit „sharing economy”. Aceste modele de afaceri creează valoare adăugată oferind organizațiilor și persoanelor fizice mijloacele tehnologice pentru a pune în comun resursele și procesele, menținând în același timp securitatea operațiunilor, transparența proceselor și confidențialitatea datelor. Modelele de afaceri colaborative permit companiilor să deduplice eforturile și să reducă cheltuielile, stimulând calitatea produselor și a serviciilor prin încurajarea concurenței corecte.

certME oferă un cadru tehnologic și organizațional, prin utilizarea DLT (tehnologie de registru descentralizat), care permite companiilor să partajeze procesele KYC (cunoașteți-vă clientul) utilizând mijloace de identificare electronică comune.

Prin utilizarea DLT și a criptografiei avansate, certME permite organizațiilor partenere să solicite emiterea mijloacelor de identificare electronică și să le utilizeze fără a stoca sau dezvălui datele personale de identificare ale utilizatorului, făcând schema de identificare electronică certME auto-suverană și conformă cu GDPR prin proiectare.

2. Companie

2.1. Despre

certME este un serviciu de identificare electronică furnizat de certSIGN, o companie românească cunoscută, cu o vastă experiență în securitatea IT.

CertSIGN oferă identitatea electronică certME ca serviciu prin operarea unei scheme de identificare electronică ce utilizează tehnologia mobilă și blockchain. Acest serviciu este construit pe principiile unui model de afaceri cu economie partajată care permite organizațiilor să elimine redundanțele, să eficientizeze procesele și să reducă cheltuielile.

certSIGN este un furnizor calificat de servicii de încredere, o companie de software care dezvoltă aplicații de securitate a informațiilor și furnizor de arhivare fizică și electronică. De-a lungul timpului certSIGN și-a dezvoltat propriul portofoliu de soluții și a oferit servicii specializate în domeniul securității IT. certSAFE, shellSAFE, trust4Mobile sunt doar câteva dintre produsele dezvoltate de echipa de cercetare și dezvoltare certSIGN, care inițial erau prototipuri și acum sunt utilizate de utilizatori la scară largă.

2.2. Misiune

Misiunea noastră este de a furniza un serviciu de identificare electronică adaptat nevoilor societății digitale globale.

2.3. Viziune

Credem că identitatea electronică este piesa centrală a societății digitale globale și că oamenii ar trebui să fie în complet control asupra datelor lor personale de identificare.

3. Scop și aplicabilitate

3.1. Scop

Această carte albă își propune să informeze cititorii cu privire la conceptul general de identitate digitală și cu privire la serviciului de identificare electronică certME – principiile și tehnologia pe care se bazează – în contextul reglementărilor existente la nivelul UE și la nivel național.

3.2. Domeniu de aplicabilitate

Această carte albă este o prezentare de nivel înalt care cuprinde abordări existente privind identificarea electronică (eID) și detalii despre serviciul de identificare electronică certME furnizat de compania certSIGN, ce acoperă principiile, politicile, fluxurile de lucru, modelul de afaceri și tehnologiile într-un mod accesibil și ușor de înțeles de către publicul larg.

4. Abordări ale eID

4.1. Context

Folosirea identității electronice pentru a furniza servicii online ajută companiile să își crească cota de piață, să intre pe piețe noi și să ofere servicii mai bune la costuri mai mici. Guvernele locale și centrale beneficiază, de asemenea, de utilizarea identității electronice, oferind cetățenilor servicii de e-guvernare disponibile 24/7.

Pentru a furniza servicii online, unele organizații, cum ar fi organismele guvernamentale sau instituțiile financiare, sunt obligate, fie prin regulamente, fie prin politici de gestionarea riscurilor, să efectueze procese costisitoare de verificare a identității (uneori denumite KYC - Know Your Customer / Cunoașteți-vă clientul) înainte de înrolarea digitală a utilizatorilor.

4.2. Abordarea comercială curentă

Instituțiile financiare desfășoară în prezent procese de înrolare digitală care necesită o verificare față în față a identității și a mai multor documente. Acest lucru este costisitor atât pentru organizație, cât și pentru utilizatori. Organizațiile trebuie să asigure suficient personal și birouri. În același timp, utilizatorii trebuie să repete aceste procese pentru fiecare furnizor de servicii cu care interacționează.

Abordarea comercială a identificării electronice presupune de obicei emiterea unor mijloace de identificare, bazate pe unul sau doi factori de autentificare (cum ar fi numele de utilizator și parola și eventual un cod OTP / SMS OTP), care pot fi utilizate numai între emitent și clienții săi.

O problemă cu care se confruntă această abordare este că procesele de înrolare digitală sunt lungi și consumă resurse atât pentru furnizorii de servicii, cât și pentru clienții lor. Când apar modificări în datele de identificare ale unui client, procesele de verificare a identității trebuie repetate fie parțial, fie în unele cazuri în întregime. Acest lucru este și mai dificil pentru clienți, care trebuie să treacă prin aceste procese pentru toți furnizorii lor de servicii.

Deoarece această abordare necesită ca toți furnizorii de servicii să stocheze datele de identificare ale clienților lor în legătură cu mijloacele de identificare electronică emise, organizațiile se confruntă cu costuri suplimentare cu protecția datelor și securitatea cibernetică, care sunt de obicei proporționale cu numărul de clienți. Din perspectiva utilizatorului, riscul de confidențialitate pentru datele sale

personale crește proporțional cu numărul furnizorilor de servicii ai cărui client este. În plus, clienții nu au control efectiv asupra accesării datele lor de către terți. De asemenea, auditorii de securitate și conformitate se confruntă cu numeroase provocări atunci când evaluează astfel de scheme de identificare electronică, deoarece jurnalele și urmele de audit pot fi pierdute, deteriorate sau manipulate.

4.3. eID-ul național centralizat

Cardurile sau pașapoartele electronice naționale și alte scheme naționale de identificare electronică pot fi utilizate cu succes pentru identificarea și autentificarea utilizatorilor, dar prezintă dezavantaje semnificative care necesită soluții costisitoare.

Un astfel de dezavantaj este capacitatea limitată de stocare a cipului din cardul electronic. Cardurile electronice pot fi utilizate doar pentru a stoca informații de bază despre identitate sau sănătate, ceea ce le face utile pentru identificare, dar incapabile de funcționalități mai complexe. Pentru a ocoli această problemă, furnizorii de servicii care folosesc carduri electronice pentru a-și autentifica clienții sunt obligați să stocheze date personale mai complexe pe serverele lor. Acest lucru dă naștere riscurilor de confidențialitate și securitate și limitează controlul pe care oamenii îl au asupra datelor lor. Pentru a-și gestiona datele și accesul la acestea, utilizatorii trebuie să interacționeze cu mai multe panouri de control – câte unul pentru fiecare furnizor de servicii care le stochează datele. În plus, utilizatorii nu pot transfera sau copia aproape niciodată datele personale între depozitarele a două organizații diferite. Chiar dacă ar fi posibil să se transfere fără probleme datele personale, nivelul de asigurare al datelor menționate nu ar fi transferat de la o organizație la alta.

Deoarece cardurile electronice oferă o granularitate foarte mică a accesului la datele personale stocate în acestea, riscurile de confidențialitate sunt ridicate atunci când se utilizează un card electronic în legătură cu furnizorii de servicii care nu sunt pe deplin de încredere. De exemplu, atunci când mecanismul de autentificare al unui furnizor de servicii necesită doar o dată de naștere verificată pentru confirmarea vârstei, utilizatorii sunt obligați să dezvăluie și toate celelalte atribute de identificare personală, inclusiv numele, adresa de reședință etc.

4.4. ID auto-suveran

Într-o schemă de identificare electronică auto-suverană datele sunt stocate, deținute și controlate de utilizator.

O schemă de identificare electronică auto suverană oferă o granularitate ridicată a accesului la datele de identificare personală. Propunerea schemelor de identitate auto-suverane este că o cerere simplă trebuie să primească o confirmare simplă, fără a fi nevoie să se dezvăluie mai multe informații decât este necesar. Utilizatorii pot alege să dezvăluie numai atributele specifice necesare pentru un anumit serviciu. De exemplu, un eID auto-suveran permite utilizatorilor să își împărtășească exclusiv numele atunci când participă la un eveniment bazat pe invitație, fără a-și dezvălui adresa de domiciliu.

Consecințele utilizării schemelor de identitate auto-suverane sunt de mare amploare, deoarece pot oferi o bază pentru alte inovații economice și digitale.

Directivele și reglementările actuale ale UE, cum ar fi PSD2, GDPR, eIDAS și MiFID2, susțin ID-ul auto-suveran, confirmând o perspectivă pozitivă pentru sistemele de identificare electronică auto-suverane.

5. Serviciu

5.1. Descriere

certME este un serviciu digital la cerere livrat de compania certSIGN clienților săi printr-un sistem IT care cuprinde hardware, software, utilizatori și proceduri de utilizare. Componenta software a sistemului certME cuprinde o aplicație mobilă (disponibilă pentru Android), mai multe aplicații web, micro-servicii și API-uri care interacționează între ele prin contracte inteligente pe un blockchain enterprise de tip PoA (Proof of Authority – Dovada Autorității) ancorat în blockchain-ul public Ethereum. Aplicația mobilă certME permite utilizatorilor să se înregistreze și să se autentifice la furnizorii de servicii online care sunt integrați cu certME prin utilizarea API-urilor.

Mijloacele de identificare electronică certME (certME eID) sunt emise la un nivel substanțial de asigurare în conformitate cu Regulamentul (UE) 2014/910 și Regulamentul de punere în aplicare (UE) 2015/1502. eID-ul certME poate fi obținut fie printr-o verificare față în față cu prezență fizică a subiectului de către o organizație parteneră de încredere (i.e., un validator certME), fie printr-o verificare video la distanță efectuată în cadrul aplicației mobile certME de către certSIGN.

Întrucât cererile pentru datele utilizatorilor făcute de furnizorii de servicii sunt gestionate de contracte inteligente, tranzacțiile blockchain creează căi de audit irevocabile care asigură transparența ecosistemului digital tuturor părților implicate.

Mijloacele de identificare electronică cu un nivel substanțial de asigurare pot fi folosite pentru a genera semnături electronice calificate la distanță. Deoarece certME se bazează pe blockchain și permite funcții de portofel criptografic, ar putea fi folosit pentru a asocia semnături electronice calificate activelor criptografice (e.g., token-uri imobiliare) ceea ce ar oferi deținătorilor de token-uri drepturi de proprietate sau de utilizare asupra activului reprezentat de token.

5.2. Rețea de parteneri

Pentru verificarea în persoană, serviciul certME se bazează pe o rețea de organizații partenere – numite validatori – care furnizează servicii de verificarea identității pentru certSIGN. Parteneriatul se bazează pe acorduri contractuale bilaterale între certME și fiecare validator. Acordurile contractuale respectă aceleași principii, model și structură și includ clauze obligatorii nealterabile care sunt comune tuturor acordurilor.

După efectuarea dovedirii și verificări identității unui solicitant, validatorii solicită emiterea mijloacelor de identificare electronică ce este gestionată automat de contractele inteligente certME. Rolul validatorilor include, de asemenea, răspunsul la cererile de validare a credențialelor făcute de furnizorii de servicii prin intermediul contractelor inteligente atunci când deținătorii certME eID se autentifică pentru prima oară sau se înregistrează la serviciul lor. Autentificările ulterioare pot să nu necesite confirmare de la validatori.

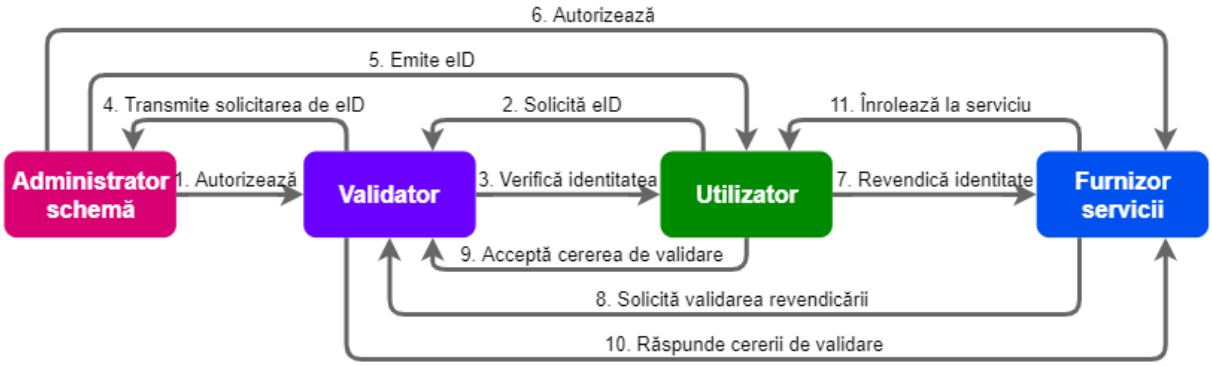
5.3. Model operațional

În cadrul ecosistemului certME, actorii pot avea următoarele roluri neexclusive:

- ***Administrator schemă*** – În calitate de reprezentant legal al schemei eID, compania certSIGN deține rolul de *administrator al schemei*. Prin acordarea sau revocarea de permisiuni specifice prin intermediul contractelor inteligente certME, administratorul schemei (i) autorizează/ dezautorizează *validatorii*, (ii) autorizează/dezautorizează *furnizorii de servicii* și (iii) emite,

suspendă, reactivează și revocă mijloacele de identificare electronică. *Administratorul schemei* poate deține rolurile de *validator* și/sau *furnizor de servicii*. *Administratorul schemei* este, de asemenea, responsabil pentru operarea mecanismului de autentificare.

- ***Validator*** – O organizație parteneră certME autorizată să (i) efectueze dovedirea identității, (ii) să verifice datele de identificare personală ale utilizatorilor, (iii) să solicite emiterea, suspendarea, reactivarea și revocarea mijloacelor de identificare electronică și (iv) să răspundă cererilor de validare a revendicărilor de identitate înregistrate de *furnizorii de servicii* pe contractele inteligente. Un *validator* poate răspunde numai la cererile de validare a revendicărilor de identitate care sunt autorizate de *utilizatori* și care privesc *utilizatorii* verificați de *validatorul* respectiv. Un *validator* ar putea deține de asemenea și rolul de *furnizor de servicii* și interacționa cu utilizatorii înrolați de sine sau de alți *validatori*.
- ***Furnizor servicii*** – Este o organizație client certME autorizată să emită cereri de validare a revendicărilor de identitate în numele *utilizatorilor*. Orice cerere emisă de un *furnizor de servicii* pentru validarea a unei revendicări de identitate trebuie să fie autorizată de *utilizatorul* care emite revendicarea de identitate. Un *furnizor de servicii* ar putea deține și rolul de *validator*.
- ***Utilizator*** – Este o persoană fizică ce a acceptat Termenii și Condițiile Generale certME, a trecut printr-un proces de verificare și dovedire a identității efectuat de un *validator* și a primit un mijloc de identificare electronică certME pe care îl poate utiliza pentru înregistrarea/autentificarea la *furnizorii de servicii*.



Imagine de ansamblu a ecosistemului certME

5.4. Validatori

Validatorii certME actuali sunt:

- CERTSIGN S.A.

5.5. Politica datelor

certME nu stochează datele de identificare personală ale utilizatorilor certME eID pentru a furniza serviciul. Pentru a permite utilizatorilor să se autentifice și să se înregistreze la furnizorii de servicii sunt stocate și procesate numai date non-personale, cum ar fi dovezile de verificare criptate. Datele cu caracter personal, pe care furnizorii de servicii le pot solicita pentru prestarea serviciilor, pot fi trimise de numai de către utilizatori din aplicația mobilă certME după aprobarea și consimțământul acestora, care este exprimat ca o semnătură digitală ce însoțește datele.

certME stochează jurnalele de acces la date în scopul conformității cu cerințele legale și pentru facturare. Astfel de date sunt limitate la: marca temporală, starea, serviciul furnizat (înregistrare / autentificare), domeniul de aplicare și tokenul unic al tranzacției.

Datele de identificare personală sunt colectate de personalul autorizat al validatorilor în timpul dovedirii și verificării identității utilizatorilor certME, în conformitate cu acordul contractual semnat cu certME și cu reglementările aplicabile - eIDAS, GDPR și legislația națională. Datele colectate sunt utilizate pentru a genera dovezi de verificare, după care sunt trimise printr-un canal sigur către aplicația certME a utilizatorului și sunt eliberate din memorie fără a fi stocate. Acest lucru asigură faptul că datele sunt cunoscute și controlate numai de persoana identificată. Dovezile de verificare sunt criptate și stocate pe blockchain din motive de securitate și transparență.

În timpul procesului de dovedire și verificare a identității utilizatorilor certME, în scopuri de conformitate eIDAS, personalul autorizat al validatorilor generează rapoarte de verificare tipărite care sunt semnate fizic de utilizatori și care sunt ulterior arhivate. Rapoartele de verificare sunt complet analogice (adică pe hârtie tipărită) și conțin toate informațiile personale verificate, colectate și transferate pe dispozitivul mobil al utilizatorului, precum și informații privind operatorul și validatorul care a efectuat verificarea, marca temporală, etc. Dacă verificarea identității se realizează prin mijloace video la distanță în cadrul aplicației mobile certME, o înregistrare a verificării video împreună cu datele de identificare personală și alte metadate sunt stocate și arhivate pe un sistem diferit, în conformitate cu legislația națională referitoare la verificarea video la distanță.

5.6. Politica de reziliere

În cazul încetării serviciului, certSIGN va oferi utilizatorilor certME eID o înștiințare cu cel puțin 6 luni înainte prin notificări și mesaje în aplicația mobilă. Planificăm să asigurăm continuitatea serviciului în conformitate cu Regulamentul (UE) 910/2014 prin Planul nostru de reziliere.

6. Tehnologie

6.1. Mijloace de identificare electronică

Mijloacele de identificare electronică emise unei persoane în cadrul serviciului certME sunt compuse din:

1) **Aplicația mobilă certME și cheia privată** – Aplicația este instalată și operată de persoanele cărora li se eliberează mijloacele de identificare pe un dispozitiv mobil aflat sub controlul lor. Aplicația mobilă certME este protejată prin utilizarea unor chei de criptare puternice generate ca neexportabile în elementul securizat al dispozitivului sau în enclava securizată și sunt accesibile exclusiv prin autentificare biometrică puternică (cum ar fi amprenta digitală sau recunoașterea facială cu percepția adâncimii). O pereche de chei publică-privată pe curbă eliptică este generată de persoana care utilizează aplicația mobilă certME, în conformitate cu specificațiile blockchain-ului Ethereum. Cheia publică este hash-uită pentru a obține o adresă care identifică utilizatorul pe blockchain. Cheia privată este utilizată pentru a semna tranzacții care reprezintă consimțământul utilizatorului și autorizarea cererilor de validare adăugate de furnizorii de servicii sau alte tipuri de interacțiuni.
2) O **tranzacție în blockchain-ul certME** – La finalizarea unui proces de dovedire și verificare a identității, un validator certME semnează și emite o tranzacție către blockchain-ul certME, care conține adresa blockchain a utilizatorului și o listă de dovezi criptate de verificare a

identității. Această tranzacție, împreună cu cheia privată din aplicația mobilă, constituie mijlocul electronic de identificare.

6.2. Aplicația mobilă

Aplicația mobilă certME este o aplicație software disponibilă pentru sistemele de operare Android. Aplicația este disponibilă pentru descărcare atât de pe Google Play și poate fi descărcată și rulată numai pe dispozitivele dotate cu elemente securizate sau enclave securizate și interfețe de autentificare biometrică puternică, cum ar fi amprenta digitală sau recunoașterea facială cu percepția adâncimii. Aplicația mobilă certME nu rulează pe dispozitive jailbroken sau rooted și nici pe dispozitive care nu sunt securizate cu blocarea ecranului. Aplicația mobilă certME poate fi rulată și accesată numai cu autentificare biometrică, iar cheia privată stocată în elementul / enclava securizată este indisolubil legată de biometria utilizată pentru a o crea. Dacă utilizatorii dezactivează blocarea ecranului sau autentificarea biometrică sau își root-ează dispozitivul, cheia privată din elementul securizat, împreună cu întreaga bază de date locală a aplicației mobile sunt șterse definitiv pentru a proteja informațiile personale ale utilizatorului.

6.2.1. ID electronic

Aplicația mobilă certME permite utilizatorului să creeze un identificator electronic sub forma unei perechi de chei publice private cu curbă eliptică secp256k1 (pe baza specificațiilor blockchain-ului Ethereum). Cheia privată este generată de utilizator pe dispozitivul său și se află întotdeauna sub controlul exclusiv al acestora. Adresa publică blockchain este obținută prin aplicarea funcției hash Keccak-256 pe cheia publică.

Aplicația permite utilizatorului să stocheze până la 253 de atribute statice. Toate atributele sunt criptate în baza de date locală a aplicației mobile. Elementul securizat sau enclava securizată este utilizat pentru a crea și stoca două chei neexportabile legate indisolubil de biometria utilizatorului cu care sunt criptate cheia privată de blockchain și baza de date locală a aplicației.

Aplicația mobilă nu rulează pe dispozitive care nu acceptă elemente securizate sau enclave securizate. Ori de câte ori o tranzacție blockchain trebuie să fie semnată de utilizator, este necesară o autentificare biometrică ce permite cheii stocate în elementul securizat / enclavă să decripteze cheia privată de blockchain. Cu alte cuvinte, cheia privată de blockchain este decriptată la cerere în urma unei autentificări biometrice a utilizatorului și este ștearsă complet din memorie (prin suprascriere cu zerouri) după semnarea tranzacției.

6.2.2. Emitere eID

Emiterea certME eID este efectuată de către un contract inteligent fie în urma unei verificări față în față în persoană a utilizatorului de către un Validator autorizat, fie în urma unei verificări video la distanță efectuată de un operator al certSIGN prin intermediul aplicației mobile certME.

În cazul verificării în persoană, aplicația mobilă certME utilizează un sistem bazat pe coduri QR pentru autentificarea și schimbul de date în siguranță cu aplicația validator certME. Procesul este detaliat mai jos în secțiunea de verificare a identității din capitolul aplicației Validator.

În cazul verificării video la distanță, aplicația mobilă certME utilizează un flux audio-video securizat pentru realizarea verificării identității la un nivel de asigurare echivalent cu verificarea în persoană. Pentru acest scop, certME utilizează serviciul VideoID (furnizat de compania Electronic IDentification) prin integrarea SDK-ului aferent acestui serviciu.

În situația în care emiterea se realizează pentru o persoană ce are deja un eID certME activ sau suspendat, acesta se revocă automat înainte de emiterea noului eID certME.

6.2.3. Autentificare

Utilizatorul se poate autentifica la orice furnizor de servicii care integrează serviciul certME astfel:

- folosind aplicația sa mobilă certME utilizatorul scanează un cod QR afișat de furnizorul de servicii pe o interfață web desktop; sau
- utilizatorul atinge un buton afișat de furnizorul de servicii într-o aplicație mobilă ce lansează aplicația mobilă certME pe același dispozitiv.

Acțiunea utilizatorului este confirmată de acesta printr-o autentificare biometrică în aplicația mobilă certME, ce declanșează un apel API, securizat prin TLS, prin care se trimite către furnizorul de servicii un cod unic semnat de către utilizator.

6.2.4. Solicitarea și furnizarea datelor de identificare personală

Un serviciu online, ce integrează serviciul certME, poate oricând să solicite unui utilizator autentificat cu certME oricare dintre datele personale în vederea prestării serviciului. Când o asemenea solicitare de date este efectuată, utilizatorul certME primește o notificare pe dispozitivul său mobil și poate vedea cererea de date în aplicația sa certME. Utilizatorul vede cine face solicitarea și ce date sunt solicitate și poate alege să permită accesul la datele sale (i.e., să trimită datele sale către serviciul care le-a solicitat) sau să refuze accesul.

Aprobarea cererii de date de către utilizator determină aplicația mobilă să trimită automat datele solicitate către serviciul online solicitant printr-un canal securizat creat utilizând ECDH prin TLS.

Serviciul online solicitant generează și înregistrează o cerere de validare în contractului inteligent de pe blockchain. Aprobarea utilizatorului este, de asemenea, înregistrată pe blockchain, semnalând serviciului de validare că utilizatorul consimte ca datele sale să fie validate. Cererea este finalizată atunci când contractul inteligent conține o dovadă de la validator care poate fi folosită de către serviciul online în conjuncție cu datele primite de la utilizator pentru a confirma autenticitatea și nivelul de asigurare a datelor furnizate de utilizator.

Serviciile online care integrează serviciul de identificare electronică certME pot alege să nu stocheze date personale ale utilizatorului într-un cont de utilizator, ci pot alege să ceară datele de care au nevoie doar atunci când au nevoie de ele pentru prestarea serviciului (e.g., solicitarea tuturor datelor din cartea de identitate la semnarea unui contract, solicitarea adresei la livrarea unui colet etc.), minimizând astfel riscurile aferente gestionării datelor personale și având garanția că datele sunt mereu actualizate.

Însă, având în vedere că în prezent majoritatea serviciilor online funcționează pe baza unor sisteme ce necesită conturi cu datele de identificare ale clientului, în majoritatea cazurilor solicitarea de date către utilizatorii certME este trimisă după prima autentificare a utilizatorului la un serviciu, iar datele acestuia furnizate prin intermediul sistemul certME sunt stocate la nivelul serviciului online accesat, în contul utilizatorului, în conformitate cu politica serviciului privind gestionarea datelor personale.

6.2.5. Consimțământul utilizatorului și respectarea GDPR

Aprobarea unei solicitări de date și livrarea ulterioară a acestor date pot fi făcute numai de către utilizator folosind datele stocate în aplicația sa mobilă certME. Tranzacțiile blockchain necesare pentru validarea cererilor de date nu sunt acceptate de contractul inteligent dacă consimțământul semnat al utilizatorului nu este prezent. Orice validare a nivelului de asigurare a datelor utilizatorului solicitată

de un furnizor de servicii către contractul inteligent trebuie să fie aprobată și semnată de utilizator cu cheia privată prin intermediul aplicației mobile certME. Contractul inteligent care intermediază verificarea acreditărilor între utilizatori, furnizori de servicii și validatori nu permite validatorilor să trimită dovezi ale autenticității datelor și ale nivelului de asigurare, dacă lipsește consimțământul semnat al utilizatorului.

6.2.6. Suspendare

Utilizatorii care au acces la dispozitivele lor mobile și doresc să-și suspende eID-ul certME pot face acest lucru atingând un buton în aplicația mobilă certME și autentificându-se biometric, ceea ce generează automat o tranzacție blockchain care este acceptată de contractul inteligent pentru a suspenda eID-ul a cărui adresă corespunde cu semnatarul tranzacției.

6.3. Aplicația Validator

Partenerii certME utilizează o aplicație software denumită în continuare aplicația validator certME care cuprinde o aplicație web compatibilă cu toate browserele majore și niște micro-servicii (accesibile prin REST API) care facilitează interacțiunea cu blockchain-ul certME și aplicația mobilă a utilizatorului.

6.3.1. Verificarea identității

În cadrul schemei de identificare electronică certME, verificarea identității poate fi efectuată fie prin mijloace video la distanță de către certSIGN prin operatorii săi, fie prin verificare în persoană de către un validator certME. Altfel spus, verificarea video la distanță poate fi efectuată numai de către certSIGN, în timp ce validatorii certME pot efectua numai verificări în persoană.

În consecință, aplicația de validare este concepută pentru a impune verificarea în persoană a utilizatorilor. Acest lucru se face printr-un handshake ce utilizează coduri QR. În primul rând, utilizatorul scanează un cod QR (cu aplicația mobilă certME) generat de aplicația validator certME. Această scanare permite utilizatorului să primească în siguranță pe dispozitivul său mobil atributele colectate și verificate de operatorul validatorului. Apoi, aplicația de validare certME scanează un cod QR generat de aplicația mobilă certME a utilizatorului ca răspuns la QR-ul inițial. Acest lucru permite aplicației de validare să primească în siguranță adresa blockchain-ului utilizatorului și ID-ul dispozitivului mobil, care este necesar pentru a trimite notificări push către aplicația mobilă (cum ar fi cererile de date de la furnizorii de servicii).

6.3.2. Colectarea și procesarea datelor utilizatorului

Aplicația validator include un formular web care este utilizat de personalul autorizat al validatorului pentru a colecta datele de identificare personală ale utilizatorului în timpul procesului de verificare și dovedire a identității. Aplicația de validare nu stochează atributele de date furnizate de utilizatori. În schimb, aplicația de validare creează dovezi pentru fiecare atribut individual de date și le criptează înainte de a le transmite micro serviciului pentru a fi stocate pe blockchain-ul certME. Dovezile nu pot fi utilizate pentru inginerie inversă, deducerea sau determinarea în orice mod a datelor personale de identificare, iar criptarea este necesară doar pentru modelul de afaceri al serviciului certME. Un utilizator este considerat înrolat în certME atunci când o anumită tranzacție ce include adresa blockchain a utilizatorului, poate fi confirmată independent că există pe blockchain-ul certME și a fost acceptată de contractele inteligente certME.

6.3.3. Răspuns la cererile de validare

Un micro-serviciu al aplicației validator certME monitorizează constant blockchain-ul certME pentru cereri noi de validare transmise de furnizorii de servicii. În cazul în care o cerere de validare este legată de un utilizator înscris de proprietarul micro-serviciului (i.e., validatorul care rulează micro-serviciul),

micro-serviciul răspunde automat la cererea de validare prin trimiterea către blockchain-ul certME a dovezii necesare pe care furnizorul de servicii o poate folosi pentru a determina autenticitatea și nivelul de asigurare al datelor primite de la un utilizator al aplicației mobile certME.

6.3.4. Suspendare

Aplicația validator certME include un formular web care este utilizat de personalul autorizat al validatorului pentru a căuta adresa blockchain a unui utilizator pe baza numelui, prenumelui, datei nașterii și a codului numeric personal al utilizatorului care sunt parte din seul minim de date al certME (MDS). Acest lucru este posibil prin stocarea pe blockchain a unei dovezi a atributelor MDS în raport cu adresa blockchain a utilizatorului. Dovada MDS nu poate fi utilizată pentru inginerie inversă, deducerea sau determinarea în orice mod a atributelor MDS care au fost folosite pentru a o crea.

Aplicația de validare certME include, de asemenea, un formular web care este utilizat de personalul autorizat al validatorului pentru a suspenda un eID certME pe baza adresei blockchain a utilizatorului. Utilizatorii pot solicita suspendarea eID-ului personal fie la certSIGN, fie la orice validator. Suspendarea este efectuată în urma unei verificări a identității cu același nivel de asigurare care a fost utilizat pentru emiterea ID-ului.

6.3.5. Reactivare

Aplicația de validare certME include un formular web care este utilizat de personalul autorizat al validatorului pentru a reactiva un eID certME suspendat pe baza adresei blockchain a utilizatorului în urma unui proces de dovedire și verificare a identității cu același nivel de asigurare care a fost utilizat pentru emiterea ID-ului.

6.3.6. Revocare

Aplicația validator certME include un formular web care este utilizat de personalul autorizat al validatorului pentru a revoca un eID certME activ sau suspendat pe baza adresei blockchain a utilizatorului în urma unui proces de verificare și dovedire a identității cu același nivel de asigurare care a fost utilizat pentru emiterea ID-ului.

6.4. Serviciul autentificator

Furnizorii de servicii care utilizează schema de identitate electronică certME trebuie să ruleze un micro serviciu certME (denumit în continuare serviciul autentificator certME) pentru a autentifica utilizatorii certME la serviciile lor și pentru a efectua cereri de date și cereri de validarea datelor.

Alternativ, serviciul autentificator certME poate fi găzduită și gestionată de către certSIGN pentru furnizorii de servicii, aceștia interacționând cu serviciul autentificator prin intermediul unor apeluri API.

6.4.1. Interacțiunea cu utilizatorul

Pentru a primi date personale de la utilizatorii eID-ului certME, serviciul autentificator certME este accesibil aplicației mobile certME prin REST API. Răspunsul la o solicitare de date venită de la un furnizor de servicii, implică trimiterea datelor printr-un apel API din aplicația mobilă către serviciul autentificator certME. Comunicațiile sunt protejate de două niveluri de autentificare și criptare (ECDH prin TLS).

Autentificarea unui utilizator certME implică trimiterea unui cod unic (challenge) către aplicația mobilă certME a acestuia fie printr-un cod QR fie prin application intent și primirea codului semnat printr-un apel API securizat prin TLS efectuat de aplicația mobilă.

6.4.2. Interacțiunea cu Blockchain

Serviciul autentificator certME facilitează comunicarea cu blockchain-ul certME pentru furnizorul de servicii. Serviciul autentificator certME este integrat cu infrastructura software a furnizorului de servicii prin REST API. La primirea datelor dintr-o aplicație mobilă certME, serviciul autentificator generează o cerere de validarea a datelor și o trimite contractului inteligent din blockchain-ul certME. Serviciul autentificator certME monitorizează constant contractul inteligent pentru răspunsuri șa cererile de validare. Dovezile de validare sunt extrase din contractul inteligent și utilizate pentru a determina autenticitatea și nivelul de asigurare al datelor de identitate primite de la aplicația mobilă certME.

6.5. Contracte inteligente

Securitatea sistemului este asigurată prin contracte inteligente aflate pe blockchain-ul certME, care este securizat prin consens Proof-of-Authority (IBFT) și legat la rețeaua principală Ethereum (main net) prin tranzacții periodice care înregistrează starea blockchainului certME pentru a asigura imuabilitatea. Contractele inteligente administrează autorizarea/dezautorizarea validatorilor, a furnizorilor de servicii și a utilizatorilor. Autentificarea utilizatorilor este de asemenea administrată printr-un contract inteligent care intermediază interacționa dintre validatori, furnizori de servicii și utilizatori. Contractele inteligente garantează că doar părțile autorizate pot interacționa și că există consimțământului utilizatorului pentru orice tranzacție care implică datele acestuia.

7. Concluzii

Prin folosirea DLT și a criptografiei avansate, certME permite organizațiilor să își partajeze rezultatele proceselor KYC fără a stoca sau divulga datele de identificare personală ale utilizatorilor lor cu ajutorul unei scheme auto-suverane de identificare electronică ce este conformă cu GDPR prin proiectare.

Acest lucru face posibil un nou model de afaceri colaborativ în care se creează valoare adăugată prin faptul că permite companiilor să partajeze resursele și procesele păstrând în același timp securitatea operațiunilor, trasabilitatea proceselor și confidențialitatea datelor.

8. Abrevieri

Termen	Definiție
API	Application Programming Interface (Interfață de programare a aplicației)
DLT	Decentralized Ledger Technology(Tehnologia registrului distribuit)
ECDH	Elliptic-Curve Diffie–Hellman(Curbă eliptică Diffie–Hellman)
eID	Electronic Identity (Identitate electronică)
eIDAS	electronic IDentification, Authentication and trust Services (Identificare, autentificare și servicii de încredere electronice)
EU	Uniunea Europeană
GDPR	Regulamentul General de Protecția Datelor
ID	Identitate
IT	Tehnologia informației
KYC	Know Your Customer (Cunoaște-ți clientul)
MDS	Set minim de date
OTP	Parolă unică
PSD2	Directiva2 privind serviciile de plată
QR code	Cod QR
REST	Representational state transfer
SMS	Short Message Service
TLS	Transport Layer Security
MDS	Minimum Data Set

9. Glosar

Termen	Definiție
Blockchain	Blockchain este un registru partajat, imuabil, ce facilitează procesul de înregistrare a tranzacțiilor.
Jailbreak	Jailbreaking se refera la escaladarea privilegiilor pe un dispozitiv Apple pentru a elimina restricțiile software impuse de Apple.
Keccak-256	Funcție Hash folosită de Ethereum.
MiFID	Este un cadru legislativ instituit de Uniunea Europeană (UE) pentru reglementarea pieților financiare din bloc și îmbunătățirea protecției investitorilor.
Root / rooting	Rooting este procesul prin care utilizatorii de telefoane inteligente, tablete, și alte dispozitive cu sistem de operare Android să ajungă la un control privilegiat (cunoscut ca root access) asupra subsistemelor Android.
secp256k1	secp256k1 se referă la parametrii curbei eliptice utilizată în criptografia cheii publice Ethereum.
Self-soverign ID	Self-sovereign identity (SSI) este un termen utilizat pentru a descrie mișcarea digitală care recunoaște că o persoană ar trebui să aibă control asupra identității fără intervenția autorităților administrative..
Smart contract	Un contract inteligent este un program informatic sau un protocol de tranzacție care este menit să execute automat, să controleze sau să documenteze legal evenimente și acțiuni relevante in conformitate cu termenii unui contract sau acord.