Cod de practici de verificare a identității

Verificarea identității de la distanță, prin video

Data:v1.0 – Ian.2026

Notificare importantă

Adresa: bulevardul Tudor Vladimirescu nr. 29,
AFI Tech Park 1, București, România
Telefon: 004-021-31.19.901
Web:www.certsign.ro

Istoricul documentelor

Versiune	Data intrării în vigoare[1]	Motiv	Responsabil
1.0	ianuarie 2026	Publicarea primei versiuni	CISO

Acest document a fost creat și este proprietatea:

Proprietar	Autor	Data creării
certSIGN	CISO	ianuarie 2026

Listă de distribuție

Destinație	Data distribuirii
Internet public	ianuarie 2026

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Organismul de gestionare a politicilor și procedurilor	ianuarie 2026

[1]Ultima zi a lunii, dacă nu este explicită

Conţinut

1 Domeniu de aplicare și scop

Această Declarație de Practici de Verificare a Identității (IPPS) descrie practicile de verificare a identității aplicate în sprijinul serviciilor de încredere furnizate de certSIGN în calitate de QTSP, în conformitate cu ETSI TS 119 461.

Verificarea identității nu este un serviciu de încredere independent în temeiul Regulamentului eIDAS. Este efectuată ca o componentă a unui serviciu de încredere și susține emiterea de certificate de către certSIGN.

Acest IPPS oferă transparență cu privire la practicile de verificare a identității tuturor părților care se bazează pe rezultatul procesului de verificare a identității, inclusiv certSIGN, organismele de evaluare a conformității (OAC) și părțile care au încredere în certificatele emise în urma verificării cu succes a identității.

2 Modelul și responsabilitățile furnizorului de servicii de verificare a identității

Capacitatea de verificare a identității descrisă în acest IPPS este furnizată prin intermediul unui model operațional hibrid.

certSIGN acționează în calitate de Furnizor de Servicii de Verificare a Identității (IPSP) responsabil și efectuează activități manuale de verificare a identității, inclusiv revizuirea manuală și luarea deciziilor finale. certSIGN rămâne pe deplin responsabil pentru rezultatele verificării identității și emiterea certificatelor.

Componentele automate care susțin procesul de verificare a identității sunt furnizate de furnizori externi de soluții care acționează ca subcontractanți sub controlul contractual și guvernanța certSIGN. Responsabilitatea pentru rezultatele verificării identității nu este transferată subcontractanților.

3 Contexte de verificare a identității și revendicare de conformitate

3.1 Contexte de verificare a identității acceptate

Verificarea identității în temeiul prezentului IPPS se aplică exclusiv persoanelor fizice și se efectuează într-un mediu la distanță, cu:

- funcționare nesupravegheată;
- procesare hibridă care combină activități automatizate și manuale;
- Nivel extins de verificare a identității (LoIP extins).

Verificarea identității se efectuează exclusiv folosind documente de identitate fizice, limitându-se la:

- pașapoarte;
- cărți de identitate naționale.

Nu se utilizează registre de încredere, mecanisme de verificare a accesului, documente suplimentare, atestări sau scheme de identificare electronică.

3.2 Declarație de conformitate pentru cazurile de utilizare acceptate

Conformitatea cu ETSI TS 119 461 este declarată pentru următoarele cazuri de utilizare:

- Verificare a identității la distanță, nesupravegheată, cu nivel extins de verificare a identității, așa cum se specifică în clauza 9.2.3.1;
- Verificare hibridă a identității care combină operarea automată și manuală, așa cum se specifică în clauza 9.2.3.3;
- Verificarea identității pentru emiterea certificatelor calificate, așa cum se specifică în anexa C.3.4.

Conformitatea este declarată numai pentru cazurile de utilizare menționate mai sus și numai în domeniul de aplicare definit în acest IPPS.

4 Colecție de atribute și dovezi de identitate

Atributele de identitate sunt colectate exclusiv din documentul de identitate fizic prezentat de solicitant. Documentele de identitate cu cip încorporat sunt tratate exclusiv ca documente fizice.

Mijloacele utilizate pentru colectarea atributelor de identitate includ:

- extragerea automată a atributelor din documentul de identitate fizic (inclusiv OCR și zonele lizibile automat, acolo unde sunt disponibile);
- revizuire și corectare manuală de către operatorii certSIGN, acolo unde este necesar.

Se colectează doar atributele de identitate necesare pentru identificarea unică a solicitantului. Nu se colectează sau se validează atribute suplimentare.

Pentru fiecare context de verificare a identității acceptat, documentele de identitate acceptate sunt limitate la pașapoarte și cărți de identitate naționale.

5 Gestionarea diferențelor de codificare și reprezentare a numelor

În cazul în care atributele de identitate sunt obținute din reprezentări diferite ale aceluiași document de identitate fizică, se aplică reguli predefinite și documentate pentru a rezolva diferențele de codificare, transliterare și reprezentare a numelui într-un mod consecvent și controlat.

Zona lizibilă de mașină (MRZ), acolo unde este prezentă, este utilizată ca sursă autorizată pentru reprezentarea numelor transliterate.

6 Principii generale ale procesului de verificare a identității

Procesul de verificare a identității stabilește identitatea unică a solicitantului și leagă această identitate de persoana care participă la proces.

Documentele de identitate fizice sunt prezentate de către solicitant în timp real printr-o interacțiune video la distanță pentru a demonstra deținerea documentului original.

Procesul combină mecanisme automate și activități de verificare manuală și are ca rezultat unul dintre următoarele:

- acceptarea solicitantului;
- respingerea solicitantului;
- încetarea procesului de verificare a identității în cazul în care nu se poate realiza o identificare fiabilă.

În cazul în care activitățile de verificare automată și manuală dau rezultate contradictorii, procesul de verificare a identității este încheiat.

7 Performanță biometrică și guvernanță pentru detectarea atacurilor de prezentare (PAD)

certSIGN, în calitate de IPSP, aplică un proces de verificare a identității bazat pe risc, în care rezistența la acceptarea falsă și respingerea falsă se realizează prin logică decizională conservatoare și controale operaționale, în conformitate cu ETSI TS 119 461.

La nivel de proces, securitatea este prioritizată prin prevenirea acceptării solicitanților a căror identitate nu poate fi stabilită în mod fiabil. Suspiciunea de uzurpare a identității, frauda documentelor, atacurile de prezentare sau încrederea insuficientă duc la încetarea sau escaladarea procesului de verificare a identității.

Calitatea este abordată prin combinarea mecanismelor automate cu revizuirea manuală, inclusiv gestionarea controlată a diferențelor de codificare și reprezentare, pentru a evita respingerea inutilă a solicitanților legitimi.

7.1 Obiective de performanță biometrică

În ceea ce privește potrivirea facială biometrică, IPSP își propune să obțină performanțe aliniate cu cele mai bune practici din industrie pentru recunoașterea facială unu-la-unu. Acest obiectiv este atins prin utilizarea unor soluții biometrice a căror performanță este demonstrată public prin intermediul unor parametri de referință recunoscuți în industrie, cum ar fi Testul furnizorilor de recunoaștere facială NIST (FRVT).

IPSP nu definește sau măsoară independent valorile ratei de acceptare falsă (FAR) sau ale ratei de respingere falsă (FRR), dar asigură că soluțiile biometrice funcționează în configurația lor standard, recomandată de furnizor, și că pragurile de decizie relevante pentru securitate nu sunt relaxate.

7.2 Obiective de detectare a atacurilor de reprezentare

Capacitățile de detectare a atacurilor de prezentare (PAD) sunt furnizate prin intermediul unei componente PAD certificate ISO/IEC 30107-3. Caracteristicile de performanță ale PAD, inclusiv APCER și BPCER, se bazează pe activități de testare și certificare întreținute de furnizor.

Adecvarea obiectivelor de securitate legate de PAD este revizuită periodic ca parte a procesului de gestionare a informațiilor despre amenințări și a riscurilor IPSP. Tehnicile emergente de atac prin prezentare nu duc la relaxarea criteriilor de acceptare a PAD, dar pot duce la consolidarea controalelor operaționale sau a măsurilor de escaladare.

8 Principii de gestionare a riscurilor și securitate

Procesul de verificare a identității este conceput ținând cont de potențialul ridicat de atac asociat scenariilor de verificare a identității la distanță și nesupravegheată.

certSIGN aplică o abordare bazată pe riscuri, care abordează riscurile, inclusiv:

- frauda de identitate și uzurparea de identitate;
- atacuri de prezentare, reluare și injecție;
- manipularea probelor obținute;
- utilizarea necorespunzătoare sau compromiterea sistemelor de verificare a identității.

Se aplică măsuri pentru a asigura integritatea captării dovezilor și pentru a atenua riscurile legate de redarea, injectarea sau manipularea datelor captate.

Evaluările riscurilor sunt revizuite periodic și ori de câte ori apar modificări semnificative în procesul de verificare a identității sau în mediul de amenințare.

9 Controale organizaționale și operaționale

Activitățile de verificare a identității se desfășoară într-un mediu operațional controlat.

certSIGN garantează că:

- rolurile și responsabilitățile sunt clar definite;
- personalul implicat în activitățile de verificare manuală este instruit și competent;
- Operațiunile de verificare a identității sunt reglementate de proceduri documentate.

Supravegherea componentelor automate subcontractate este menținută prin cerințe contractuale, monitorizarea serviciilor și proceduri de escalare și rezervă.

10 Gestionarea dovezilor și a înregistrărilor

Dovezile legate de procesul de verificare a identității sunt colectate și gestionate în conformitate cu cerințele legale, contractuale și de reglementare aplicabile.

Înregistrările de verificare a identității susțin trasabilitatea și auditabilitatea și sunt protejate în ceea ce privește integritatea și confidențialitatea. Păstrarea și ștergerea dovezilor se efectuează în conformitate cu cerințele de păstrare definite.

11 Limitări și excluderi explicite

Această IPPS exclude în mod explicit:

- registre de încredere;
- mecanisme de verificare a accesului;
- documente suplimentare sau atestări;
- identificarea persoanelor juridice sau reprezentarea persoanelor juridice;
- reutilizarea sau gestionarea ciclului de viață al imaginilor fețelor de referință.

12 Întreținerea IPPS-ului

Acest IPPS este revizuit periodic și actualizat atunci când apar modificări semnificative în practicile de verificare a identității, standardele aplicabile, peisajul amenințărilor sau aranjamentele operaționale.

Prevederile privind rezilierea serviciilor sunt conforme cu procedura generală de reziliere certSIGN.