

Întrebări frecvente despre semnătura electronică “disposable” (“de unică folosință”)

Q1: Ce sunt certificatele Disposable?

Semnătură “disposable” („de unică folosință”) sau „one-shot” este un certificat de semnătură electronică de unică folosință calificată, are o durată de maximum 60 de minute de la emitere și este valabilă pentru o singură utilizare (semnătură „de unică folosință” sau „one-shot”). Utilizatorul se identifică la momentul respectiv și în mod independent.

Q2. Care este baza legală care reglementează procesul de identificare la distanță prin intermediul video?

Regulamentul eIDAS (UE 910/2014) impune furnizorilor de servicii de încredere (Trust Service Providers) să verifice identitatea persoanei care solicită o semnătură calificată la același nivel de securitate ca identificarea fizică.

În România, acest proces este reglementat suplimentar de acte normative precum Legea 455/2001 privind semnătura electronică, dar și de reglementările ASF, ADR sau ANSPDCP (în cazul protecției datelor).

Q3. Când pot vizualiza documentul transmis de Banca pentru semnare cu semnătură electronică “disposable”?

După aprobarea fluxului de identificare video clientul va putea accesa documentul transmis, îl va putea citi și va putea aplica semnătura electronică calificată.

Q4: De ce voi avea nevoie în timpul procedurii de identificare video?

În timpul sesiunii de identificare video, utilizatorul trebuie să aibă:

- un document de identitate valabil (carte de identitate), fără protecție din plastic, intact, lizibil și cu fotografie.
- telefonul mobil;

Q5. Sunt necesare toate acțiunile impuse pe parcursul procesului de identificare video (ex. filmarea și mișcarea actului de identitate, încadrarea feței într-un chenar, etc)?

Da, toate aceste acțiuni sunt necesare pentru ca procesul de identificare video să fie eficient și sigur, asigurând astfel că documentul de identitate este real, valid și că persoana care îl prezintă este titularul său. Scopul acțiunilor fiind:

- Prevenirea fraudelor
Prin filmarea actului de identitate și solicitarea mișcării acestuia, se verifică dacă documentul este real, tridimensional, nu o simplă fotografie, print sau imagine pe ecran. Astfel se evită cazurile de spoofing (prezentarea unei imagini false în fața camerei).

- Dovada de viață (liveness check)

În multe cazuri, în paralel, utilizatorul este rugat să se miște (ex: să clipească, să rotească capul, să citească un text) pentru a confirma că este o persoană reală și prezentă în acel moment – nu un video sau o poză.

Mișcarea actului de identitate se corelează cu acest proces: confirmă că persoana deține fizic acel act în timp real.

Q6: Identificarea poate fi afectată de calitatea și procesul de încărcare pe parcursul identificării video sau de calitatea conexiunii la internet?

Autentificarea trebuie să fie realizată în loc cu conexiune bună la internet. Rezoluția filmării și pozelor va fi afectată de luminozitate necorespunzătoare, conexiune slabă la internet, folii protectoare atașate - fie documentelor utilizate în procesul de identificare video, fie dispozitivului cu care se realizează procesul de identificare.

Q7: Ce fac în cazul în care procesul de autentificare nu înregistrează progres semnificativ?

În acest caz, se va verifica conexiunea la internet sau alte aspecte care țin de performanța dispozitivului de pe care se face autentificarea (ex. disponibilitate de memorie, aplicații deschise/care rulează în background, versiunea sistemului de operare, etc).

Q8: În cazul unei întreruperi în procesul de autentificare, reiau procesul de autentificare de la început?

În cazul în care procesul a fost deja inițiat la furnizorul de semnătură calificată, în momentul restartării va continua din pasul în care a rămas.

Q9: În ce constă întreaga procedură de identificare video?

Procedura de identificare video, adesea utilizată în contextul verificării identității clienților, constă în mai multe etape esențiale:

1. Pre-înregistrare: Clientul este adăugat de către reprezentantul Băncii în aplicația de semnătură calificată.
2. Notificare client: Clientul este invitat să acceseze linkul inclus în notificare pentru a efectua identificarea video, care include:
 - o Arătarea documentului de identitate (ex: carte de identitate, pașaport).
 - o Verificarea biometriei
 - o Realizarea unor mișcări specifice sau a unor gesturi pentru a verifica autenticitatea documentului.
3. Verificarea documentului: Sistemele automate sau operatorii umani analizează documentul de identitate pentru a verifica:
 - o Valabilitatea acestuia.
 - o Compararea datelor din document cu informațiile furnizate de client.

4. Verificarea biometriei: Utilizează tehnologia de recunoaștere facială pentru a compara fața clientului cu cea din documentul de identitate.
5. Finalizarea procesului:
 - o Dacă toate verificările sunt satisfăcătoare, clientul va fi notificat pentru a urma pașii de semnare a documentului.
 - o Dacă toate verificările sunt nesatisfăcătoare, clientul va fi notificat prin email și va fi contactat de bancă pentru eventuală abordare alternativă.
6. Stocarea datelor: Informațiile colectate sunt stocate conform reglementărilor legale, asigurându-se confidențialitatea și securitatea acestora.

Q10: De ce nu se recomandă utilizarea laptopului pentru procesul de identificare video?

Pentru o experiență mai bună, este indicat să folosiți un telefon mobil. Utilizarea laptopului pentru procesul de identificare video nu este recomandată. Aplicația, atunci când este deschisă pe desktop, va redirecționa utilizatorul către telefon. Acest lucru se datorează faptului că pe laptopuri sau desktopuri camerele au o calitate mai slabă, ceea ce poate reduce semnificativ rata de succes a identificării.

Q11: Cât durează un proces de identificare video?

Un proces standard cu identificare video poate dura până la 5 minute.

Q12: Poate dura un proces de identificare video mai mult de 5 minute?

Da, un proces de identificare video poate dura mai mult de 5 min. Extinderea intervalului de autentificare video peste intervalul de 5 min. indică o posibilă redirecționare a fluxului în lucru către un operator al furnizorului de semnătură calificată. Este recomandat ca până la obținerea unei rezoluții pentru fluxul aflat în lucru să nu fie inițiat un alt flux de identificare video.

Q13: Clientul va fi notificat în legătură cu rezultatul identificării video?

Clientul va fi notificat în legătură cu rezultatul identificării video pe adresa de email pe care a primit notificarea pentru semnare.

Q14: Care sunt browserele recomandate pentru o optimă identificare video?

Browser recomandat de furnizorul soluției: Chrome, Firefox, Safari, Edge.

Nota: Ultima versiune de Chrome, Firefox, Safari, Edge.

Q15: Nu pot deschide camera pe dispozitivul de pe care fac autentificarea. Ce fac?

Pentru a putea realiza identificarea video, este esențial să vă asigurați că accesul la cameră este permis.

Dacă ați apăsător din greșeală „Nu permit” (sau „Block”) când un site v-a cerut acces la cameră pentru un proces de identificare video, iată cum puteți remedia situația în funcție de browserul pe care îl folosiți:

Google Chrome (desktop)

1. Accesează site-ul unde ai refuzat accesul la cameră.
2. În bara de adrese (sus), apasă pe pictograma lacătului  din stânga adresei.
3. În meniul care se deschide, caută secțiunea „Permisuni”.
4. La „Cameră”, schimbă din „Blocat” în „Permite”.
5. Reîncarcă pagina (F5 sau Ctrl+R).

Mozilla Firefox

1. Accesează site-ul în cauză.
2. Apasă pe pictograma lacătului  din stânga adresei.
3. Mergi la „Mai multe informații” → Permisuni.
4. Găsește „Utilizează camera” și debifează „Blocat” sau selectează „Permite”.
5. Reîncarcă pagina.

Microsoft Edge

1. Accesează site-ul.
2. Apasă pe lacătul  din stânga adresei.
3. Mergi la Permisuni pentru acest site.
4. La „Cameră”, selectează „Permite”.
5. Reîncarcă pagina.

Pe telefon (Android/iOS)

În browserul Chrome:

1. Accesează site-ul.
2. Apasă pe lacătul  din bara de adrese.

3. Alege „Permise” → „Cameră”.

4. Selectează „Permite”.

5. Reîncarcă pagina.

Sau:

- Mergi în Setări > Aplicații > Chrome > Permise și asigură-te că Camera este permisă pentru browser.

Q16: De ce nu primesc codul OTP (one time password) pentru semnarea calificată a documentului?

În cazul în care identificarea video s-a desfășurat cu succes și semnătura a fost emisă, verificați că numărul de telefon este valid și a fost transmis în format internațional cu prefix +4, fără a conține spații sau alte caractere (ex. +407XXXXXXX). În acest caz, contactați Banca.

Motivele cel mai frecvent întâlnite pentru care identificarea video nu se poate finaliza și solicitarea este redirecționată către operator uman:

- **Utilizarea unui document greșit pentru identificare**

- De exemplu, se prezintă pașaportul în locul cărții de identitate (CI), dacă sistemul solicită specific CI.

- **Documentul de identitate este deteriorat sau murdar**

- Anumite elemente de securitate sau informații esențiale nu pot fi citite de sistem din cauza calității documentului.

- **Documentul nu este prezentat corect în fața camerei**

- Este afișat parțial, iese din cadru sau degetele acoperă zone importante

- **Reflexii puternice de lumină pe document**

- Lumina excesivă sau unghiul greșit poate împiedica sistemul să recunoască detaliile documentului.

- **Datele introduse de Banca nu corespund cu cele din document**

- Numele sau prenumele completate în sistem sunt diferite de cele din actul de identitate.

- **Expresie facială neutră sau lipsa mișcării în timpul selfie-ului**

- Dacă clientul rămâne complet nemișcat, sistemul poate interpreta că este o fotografie, nu o persoană reală.

- **Elemente faciale acoperite în timpul selfie-ului**

- De exemplu, purtarea ochelarilor de soare poate împiedica recunoașterea facială.

- **Prezentarea unei copii a documentului în locul originalului**

– Afișarea unei xerocopii, a unei fotografii de pe alt dispozitiv sau a unui print nu este acceptată de sistem.

- **Calitatea imaginii camerei este scăzută**

– Rezoluția camerei este prea mică, iar imaginea devine neclară sau pixelată, ceea ce împiedică sistemul să analizeze corect documentul sau fața utilizatorului.

- **Lipsa stabilității imaginii**

– Mișcarea constantă a camerei sau a documentului în timpul scanării duce la capturi neclare sau deformate.

- **Lumina ambientală insuficientă**

– Încăperea este prea întunecată, iar fața sau documentul nu sunt vizibile suficient pentru sistemul automat.

- **Interferențe vizuale în fundal**

– Alte persoane, obiecte în mișcare sau elemente care pot induce în eroare sistemul apar în fundal.

- **Înregistrarea este efectuată orizontal sau invers**

– Sistemul poate interpreta greșit dacă documentul este rotit, inversat sau filmat din unghiuri neobișnuite.

- **Utilizatorul refuză permisiunile necesare**

– De exemplu, nu acordă acces la cameră sau microfon, caz în care identificarea nu poate fi inițiată.

- **Erori tehnice ale browserului sau aplicației**

– Probleme de compatibilitate cu browserul, lipsa actualizărilor sau blocaje din partea unor extensii (adblock, privacy tools).