RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

Remote Identity Proofing for EUDI Wallet Onboarding: Strengthening Assurance Against Evolving Threats

INTRODUCTION

The European Digital Identity (EUDI) Wallet is set to transform how EU citizens interact with digital services by providing a secure, user-controlled identity framework. One of the central activities of this initiative is the onboarding process, in which the verified Personal Identification Data (PID) are issued and installed to the user's EUDI-Wallet.

To ensure trust and security, for all existing and upcoming services and applications involving the EUDI-Wallet with their PIDs, onboarding procedures must meet Level of Assurance (LoA) High, as required by eIDAS. As a trustworthy onboarding method to the EUDI-Wallet, national eID systems must always be considered, especially if they are already notified for the LoA High.

However, among the different methods that are under discussion to achieve this assurance, another pathway is through evaluated and certified remote identity proofing processes. While this offers convenience, it also introduces serious technical and security challenges—especially when video-based methods are used for biometric and document verification.

As a follow-up to the BSI-ANSSI Joint Release of December[1] 2023 that presented the general threat models, this document aims at presenting the progress made since the last paper and identify gaps that affect the reliability of video-based remote identity proofing.

[1].https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ANSSI-BSI-joint-releases/ANSSI-BSI_joint-release_2023.pdf

Technical Considerations for EUDI Wallet Onboarding

Remote identity proofing solutions for EUDI Wallets must ensure the validity and trustworthiness of both biometric verification and document authentication, particularly when these are conducted via video.

Essential Verification Goals:

- **Biometric genuineness:** Confirm that the captured face is live and untampered.
- **Document authenticity:** Ensure that the identity document is live, genuine, unaltered and in current possession of the applicant.
- **Face matching:** The captured face and the identity document source data (face picture of the rightful holder) are successfully verified by biometric comparison and the identity document is bound to the applicant.

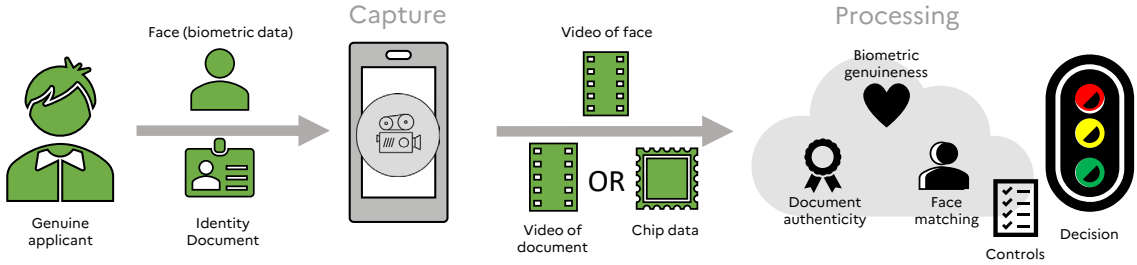

Figure 1: Remote identity proofing general process

Systems using video capture must integrate:

- Presentation Attack Detection (PAD) including liveness detection mechanisms, robust against presentation attacks
- Injection Attack Detection (IAD), such as detecting virtual cameras or other methods altering the intended data communication
- Randomized challenge response mechanisms to detect pre-recorded (replay-attacks) content
- Tamper detection features in the video stream (e.g. glitch detection, motion consistency)

These briefly described counter measures are discussed in more detail in our previous Joint Paper (December 2023).

Identity Data Extraction

Most remote identity verification systems still rely **on optical character recognition (OCR)** to extract data from ID documents. However, OCR is particularly sensitive to lighting, focus, and image distortion. This process introduces a high risk of incorrect data capture and especially the potential usage as an attack vector—compromising the integrity of the Personal Identification Data (PID) that populates the EUDI Wallet. A more secure way to extract the data is to electronically read the integrated chip, but currently in some countries, this is restricted by national laws.

Currently, the "Proposal for a council regulation on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement" is under debate, which clarifies Regulation (EU) 2019/1157 article 11(6) regarding the use of biometric data stored on identity and residence documents.

Threat Landscape: Challenges of Video-Based Identity Verification

In many remote onboarding scenarios, verification relies on video capture to analyse both biometric data (e.g. facial features) and identity documents. This mode of verification, while accessible, is potentially vulnerable to a broad spectrum of attack vectors from unsophisticated up to highly specialised attacks, which are already outlined in the previous BSI-ANSSI joint paper on remote identity proofing.

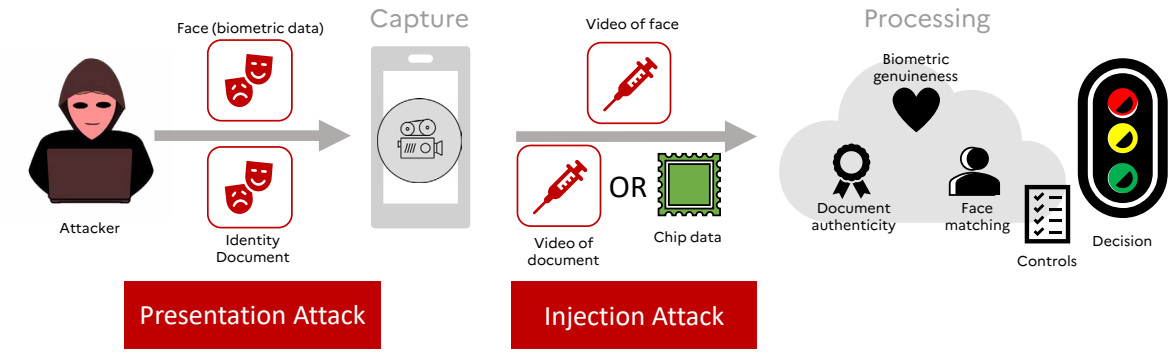

Figure 2: Presentation and injection attacks in a remote identity proofing process

While this joint release mainly discusses risks related to biometrics and identity documents, threats on the remote identity proofing service provider's information system (including web and mobile applications used in the identity verification process) remain an important hazard.

To cover general IT-security requirements ISO[2] , ANSSI[3] and BSI[4] published several standards and recommendations regarding securing IT-systems.

[2].ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements
[3]. ANSSI PVID rule set for remote identity verification service providers (April 2021), https://cyber.gouv.fr/en/actualites/publication-requirement-rule-set-remote-identity-verification-service-providers
[4].BSI IT-Grundschutz Compendium (2022) https://www.bsi.bund.de/dok/it-grundschutz-en

1. Presentation Attacks

Attackers present biometric presentation attack instruments in front of sensors —such as printed photos, masks, or 3D models—that mimic a genuine applicant. In particular:

- **On biometric data:** Printed Photos, use of silicon masks, or manipulated video streams presented on screens or by projectors.
- **On documents:** Presentation of forged, altered, or screen-replayed ID document under real-time capture.

These attacks are increasingly realistic and automated, taking advantage of attackers' control over the capture environment (lighting, device angle, resolution).

2. Injection Attacks

Attackers bypass the camera entirely by injecting pre-recorded or synthetically generated or modified data into the verification stream. In particular:

- **On biometric data:** Deepfakes and AI-generated biometric characteristics can be streamed in place of real-time video.
- **On documents:** Documents can be digitally created or altered using computer graphics before injection into the capture pipeline.

These techniques may elude both human and automated verification, in particular when systems lack robust challenge-response mechanisms or tamper detection.

Key Insight:
Identity documents are mainly designed to be physically verified in a face to face situation. Many of the implemented security features (e.g. tactile, UV- and IR-response, micro print) cannot be sufficiently validated in a remote identity document proofing. Unlike in-person verification, video-based identity proofing therefore exposes the system to easily replicable and remotely deployable attacks, which scale with minimal risk to the attacker who can easily conceal his true identity.

Standardisation: Moving Towards Uniformity

Norms and standards lay important foundations and have met notable accomplishments towards harmonization in the last two years. Standardisation efforts have intensified, yet several issues remain unresolved.

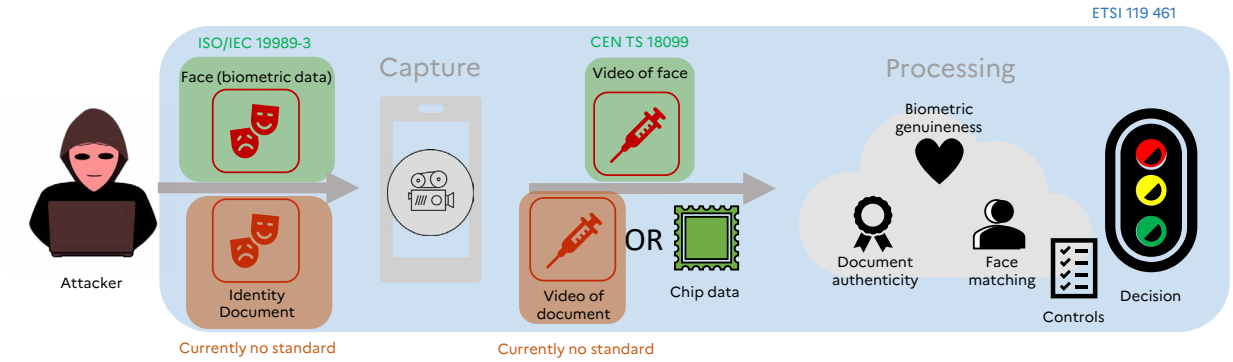

Figure 3: Standardisation mapping

Furthermore, current phrasings of requirements leave room for interpretation during audits or evaluations, which hinders trust comparability, and mapping them to LoA levels remains incomplete.

Domain	Ongoing Activity	Gaps
Remote Identity Proofing	ETSI TS 119 461	Abstract; requires clearer mapping to LoA High
Injection-Specific Threats	CEN TS 18099	Technical specificity needed for implementation validation
Security Testing & Evaluation	ETSI TS 119 461 mentions both CEN TS 18099 and ISO/IEC 19989-3	Test specifications neither widely available nor harmonised across Europe
EUDI Wallet Onboarding	CEN TS 18098 (CEN TC 224 WG20)	Still evolving; lacks detailed conformance guidance
Biometric Security	CEN TC 224 WG18 – TS on biometric product requirements	Still under development

In an ideal world the identified gaps would be filled by harmonised EU-wide standards, but in the meantime temporary approaches are necessary.
To ensure secure and trustworthy onboarding into the EUDI Wallet, the following measures are proposed:

1. Harmonise Evaluation and Test Criteria

- Develop uniform conformance tests that are directly mapped to LoA High requirements, to minimize divergence in requirement interpretation between Member States.
- Mandate testing against biometrics injection and presentation attacks during solution evaluation as soon as possible (ETSI TS 119 461 mandates testing according with CEN TS 18099 and ISO/IEC 19989-3 starting end of 2026).

2. Bridge the gap on identity document verification

- Establish test criteria to testing remote identity solution controls on identity documents, similar to standards that were established for biometrics.
- Reach a regulatory context where Member States enable the conformity assessment bodies (CAB) have the legal possibility to execute sufficient tests.
- Prioritize chip reading, where possible, as the primary method for data extraction from identity documents to tackle OCR limitations and reinforce resistance to document tampering.

CONCLUSION

The evolution of digital identity across Europe, spearheaded by the EUDI Wallet, requires robust, secure, and harmonized onboarding mechanisms, in particular remote identity proofing processes. Video-based identity verification, while user-friendly, is inherently vulnerable to repeatable, scalable, and invisible attacks such as presentation and injection threats.

A comprehensive and pan-European approach to testing, certification, and standardization is required to ensure:

- High assurance in onboarding processes,
- Interoperability across national systems,
- Sustained trust from both users and supervisory bodies.

By addressing these threats head-on and advancing coordinated standardization efforts, Europe can lay the groundwork for a resilient and secure digital identity infrastructure.

BIBLIOGRAPHY

EUROPEAN PARLIAMENT AND AND THE COUNCIL OF THE EUROPEAN UNION, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, https://eur-lex.europa.eu/eli/reg/2014/910/

EUROPEAN PARLIAMENT AND AND THE COUNCIL OF THE EUROPEAN UNION, Proposal for a COUNCIL REGULATION on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024PC0316

ETSI, TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects (February 2025),
https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/02.01.01_60/ts_119461v020101p.pdf

CEN/TS 18099: Biometric data injection attack detection (February 2025), https://norminfo.afnor.org/norme/xp-cents-18099/detection-dattaques-par-injection-de-donnees-biometriques/205225

ISO/IEC 19989-3:2020: Information security — Criteria and methodology for security evaluation of biometric systems, Part 3: Presentation attack detection (September 2020), https://www.iso.org/standard/73721.html

BSI-ANSSI, Joint Release on Remote Identity Proofing, December 2023,
https://cyber.gouv.fr/sites/default/files/document/ANSSI-BSI-Joint-Release_20231220.pdf
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ANSSI-BSI-joint-releases/ANSSI-BSI_joint-release_2023.pdf

ENISA, Remote Identity Proofing - Attacks & Countermeasures (January 2022),
https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures

ENISA, Remote ID Proofing (March 2021),
https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing

BSI, TR-03107-1: Technical Guideline Electronic Identities and Trust Services in E-Government Version 1.0 (informative only)
https://www.bsi.bund.de/dok/TR-03107-en

BSI, TR-03147: Technical Guideline Assurance Level Assessment of Procedures for Identity Verification of Natural Persons (December 2021),
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03147/tr03147_node.html

BSI, TR-03166: Technical Guideline for Biometric Authentication Components in Devices for Authentication Version 1.1 (September 2024),
https://www.bsi.bund.de/dok/TR-03166-en

ANSSI, PVID rule set for remote identity verification service providers (April 2021),
https://cyber.gouv.fr/en/actualites/publication-requirement-rule-set-remote-identity-verification-service-providers

ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems – Requirements

BSI, IT-Grundschutz Compendium (2022)
https://www.bsi.bund.de/dok/it-grundschutz-en

VERSION 1.0 – JULY 2025
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, BOULEVARD DE LA TOUR-MAUBOURG — 75 700 PARIS 07 SP
https//www.cyber.gouv.fr

FEDERAL OFFICE FOR INFORMATION SECURITY (BSI)
SECTION WG24 – PUBLIC RELATIONS GODESBERGER
ALLEE 185 - 189 53175 BONN, GERMANY
PHONE: +49 (0) 228 99 9582-0
E-MAIL: BSI@BSI.BUND.DE