Remote Identity Proofing

ANSSI-BSI Joint Release

Federal Office
for Information Security

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

An overview

The digital transformation affects many areas of citizens' everyday life, including their identity. Today, digital identification technologies allow European citizens to access public and private services (e.g. taxes, banking, health registers or qualified trust services) using a common digital identity.

On a technical level, a growing number of electronic identification (eID) schemes have emerged in Europe in the last few years, notably under the eIDAS EU 2014/910 regulation. This regulation mandates Member States to issue a digital identity wallet to expand the use of digital identity solutions in Europe.

The assessment of an eID scheme, following the requirements laid out in CIR (EU) 2015/1502 covers the whole life cycle of the electronic identification means. This includes the enrolment, which aims to confirm the identity of the user before delivering the electronic identification means. It is the first step and one of the most critical. It can be done during a physical meeting with an authorized agent (such as during the issuance of an identity document) or through the use of an existing electronic identification means. However, providers of electronic identification means are increasingly likely to use video-based remote identity proofing for enrolment purposes.

Although identifying a person may not seem a difficult task at first glance, it implies establishing a reasonable assurance that the identity document is genuine, as well as matching the characteristics (e.g. the face or fingerprints) of the applicant, which becomes a complex topic when carried out remotely. In particular, the digital space and technological advances enable attackers to use a wide variety of skills and materials to carry out identity theft, and attacks are more easily repeatable than during a physical meeting.

Attacks on remote identity proofing aim at performing identity fraud to obtain unauthorized access for espionage, sabotage or financial gain. These attacks may target one or several components of the remote identity proofing service (Fig. 1).

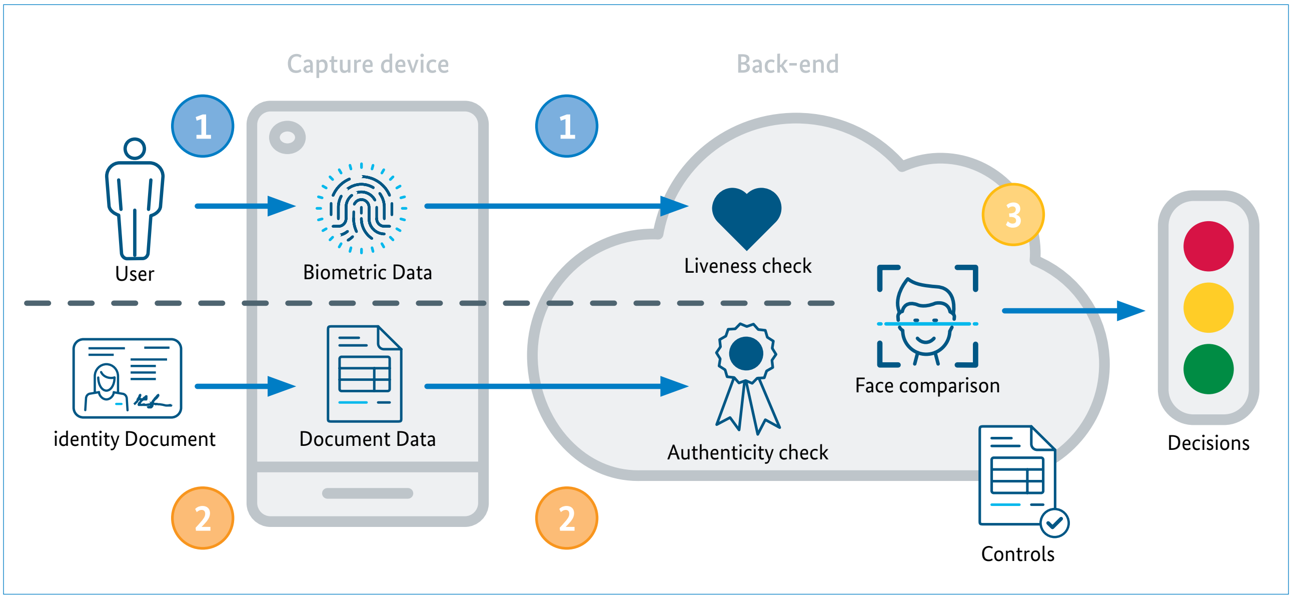

Figure 1: Principles of remote identity proofing

The aim of remote identity proofing is to ensure that the individual behind the screen and the identity document presented match and are authentic. To achieve this, three steps are required:

- The biometric verification, aiming to ensure that the representation of the face of the applicant has not been modified;
- The identity document verification, aiming to ensure that the user has a genuine identity document;
- The matching and results, aiming to ensure that the face of the applicant matches the photography on the document.

This joint release of ANSSI and BSI will focus on relevant attack vectors that need to be considered, and examples of counter-measures currently seen in the industry.

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.

1. Biometric verification

The same threats that apply to face-to-face physical meetings also apply to remote verification of biometric data, albeit with a lower degree of difficulty for the attacker. In both cases, the attacker‘s aim is to impersonate the victim‘s identity. However, when it comes to remote verification, the attacker has a wider range of options and can wear masks of diverse quality and material (e.g paper, silicon, moulded) in addition to make-up. These attacks are commonly known as Presentation Attacks.

In addition to these pre-existing threats, attackers can also use digital tools to create 3D models or deepfakes of their victims. Before carrying out these frauds of a new kind, attackers need to intercept and replace biometric data either by filming manipulated images on a screen or using vulnerabilities to inject manipulated images in the video flow. This type of attack is called Injection Attacks.

In the typical remote identification scenario, an attacker has additional control about the environmental parameters such as lighting, camera quality, framerate, etc. This may help to cover attacks which under more favourable conditions could be detected. Therefore a minimum set of requirements needs to be set out and enforced.

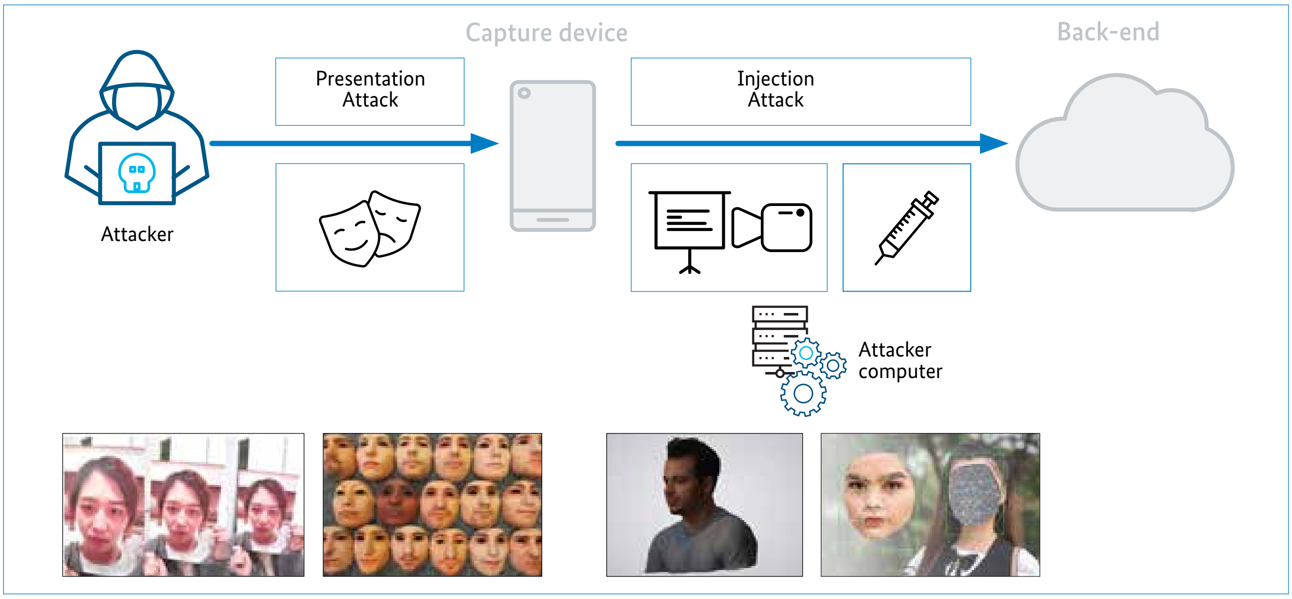

Figure 2: Examples of Presentation and Injection Attacks

Objectives of the remote identity proofing service:

- To capture a video of the applicant’s face with sufficient quality and length – Video fluidity, resolution (e.g. minimum 720p at the time of writing of this document) and duration should be sufficient to enable verification tasks that are performed by AI and human operators;
- To verify that the captured video was not tampered with – Including random challenges to be performed by the applicant during the video capture are a good way to help detect video tampering by making glitches and artefacts appear if the video is digitally tampered;
- To verify that the applicant on the captured video is a genuine person (e.g no mask, no deepfakes).

2. Identity document verification

In the context of remote identity proofing, several technical methods to capture identity documents may be in use: photo, video or chip reading. In a similar way to biometric data, identity document data is exposed to physical counterfeit and forgery, but also to injection of digitally modified data.

Objectives of the remote identity proofing service:

- To verify the authenticity of the presented identity document;
- To verify the integrity of data on the identity document;
- To verify that the user is in possession of this document at the time of the identification.

The success of the attack depends on the level of security that the identity document reaches. As a matter of fact, security features included in the document (e.g. visual securities) or in the chip may differ due to different national legislations.

If an identity document has little to no visual security features, the use of photo or video-based methods to verify its authenticity cannot be effective (e.g. holograms cannot be effectively seen on photos). Furthermore, many security aspects of an identity document are lost in an RGB video stream, such as infrared information or haptic structures on the document. Security research on deep faked video identity manipulation and notably the one conducted by the Chaos Computer Club in 2022, have shown that attacks on the visual representation of the identity document, using computer graphics to change the information on the document, can be performed with quite simple preparations and little effort limiting the assurance level that could be achieved when utilizing such methods.

Thus, chip reading is the most secure way which should be used to acquire the information from an identity document. In that regard, although personal information and biometric data are stored based on separate sets of authorization, access to both data groups on the chip is legally restricted in some countries of the European Union, generally on the grounds of privacy protection. As an example, in Germany, it is only granted to government services, once the officer previously verified that the holder of the document matches the printed pictures as an identity verification, to ensure the holders consent.

In case the document to be read is a passport, it is important to keep in mind that not all passports support the same security mechanisms for chip reading. Some passports may still only use passive authentication, without any chip- or active authentication mechanism, as specified in ICAO Doc 9303. While this can still ensure the integrity of the data, it enables attackers to record the data from such a passport at any time, and re-use this data for all subsequent identifications. To ensure that the user is actually in possession of the passport during the identification, active authentication or chip authentication are required.

3. Matching and Results

The purpose of attacks on biometrics and identity documents is to ultimately commit fraud on the last stage of the matching process.

Objectives of the remote identity proofing service:

- The face and the photo – presented by the applicant on the captured video and contained in the identity document, respectively – guarantee that it is the same genuine person;
- Liveness checks on biometric data and identity document data guarantee the applicant was the genuine person performing identity verification.

Aside from edge cases, such as twins or look-alikes, additional considerations have to be given on the performance on biometric matching algorithms that are used.

If automated matching is performed, AI specific attacks need to be considered, such as backdoor attacks or robustness to adversarial attacks. Especially insider attacks, where the attacker has access to the model or training data, can subvert the identification process. Furthermore, matching algorithms in general have to balance their performance to distinguish a group of people with their robustness to factors of aging, varying lighting conditions, etc. The performance can vary for different ethnicities depending on the balance of the training data.

Also, due to continuous training of these models, a firm evaluation of their performance and vulnerability to certain kinds of attacks may not be widely applicable across versions even of the same system. Therefore extensive auditing and vulnerability testing needs to be performed after every update.

Those systems therefore warrant not just one initial evaluation, but continuous assessment, considering not just the biometric performance, but also the whole development cycle, the hosting and the selection and sourcing of any assets used for training.

To complement AI verification, having trained operators performing verifications on liveness and likeness checks on both biometric data and identity document data, adds additional security with a global coherence of the verification material, for example by checking behaviour of the applicant.

Standardisation

Remote identity proofing has been exposed to constant technological advances, due to the topic's technicality and novelty in the standardisation and certification fields. However, standardisation bodies are increasingly paying attention to this technology. ISO/IEC 30107-3 covers biometric presentation attacks, ETSI ESI TS 119 461 discusses identity verification to be used by trust services, while CEN TC 224 works on a standard covering injection attacks and requirement for biometric products. Besides the acceleration in standardization, there is still a lack of certification schemes regarding this topic. Currently, only a few Member States, including France with the PVID certification scheme, have elaborated an evaluation methodology and a certification scheme for remote identity proofing solutions. With the emergence of European digital identity wallets, where remote identity proofing is forseen by the regulation, it has become necessary to guarantee at the European level that identity proofing solutions used for these wallets are secured, and effectively reduce the risk of identity theft. Such guarantees can be reached through the development of a cybersecurity certification scheme including the remote identity proofing process to obtain a digital identity.

Summary

Remote identity proofing may be more convenient and faster than face-to-face physical verification. However, this method is exposed to new risks and challenges, with attacks that can be repeated and industrialized while exposing the attackers less. The evaluation of remote identity proofing methods requires to take into consideration information system security, organizational measures and specific risks: presentation attacks and injection attacks. The large scope of these methods, and the constant evolution of the technologies, make it a challenge to certify them. Plus, by taking into consideration the mutual recognition granted to notified electronic identity schemes within the eIDAS regulation, it does become a European challenge that requires harmonised methodologies and testing. The objective is to guarantee a homogenous level of security all across Europe. Such harmonization could be reached through the use of standards currently in elaboration, and the use of harmonized certification schemes under the Cybersecurity Act.

Bibliography

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

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

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

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

ETSI, TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects, https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

ICAO, Doc 9303: Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, https://www.icao.int/publications/documents/9303_p11_cons_en.pdf

Chaos Computer Club hacks video-based identification, https://www.ccc.de/en/updates/2022/chaos-computer-club-hackt-video-ident

Deep Faked Video Identity Manipulations research paper by R. Herpers, D. Scherfgen, O. Jato, J. Millberg, and A. Hinkenjann: https://www.enisa.europa.eu/events/enisa-etsi-joint-workshop-on-remote-identity-proofing/workshop-presentations/1-1-rainer-herpers-deep-fake-video-identity-manipulations.pdf

Imprint

Published by
Bundesamt für Sicherheit in der Informationstechnik
53133 Bonn, Germany
Tel.: +49 22899 9582- 0

Source:
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

Agence nationale de la sécurité des systèmes d‘information
Secrétariat général de la défense et de la sécurité nationale
51, boulevard de La Tour-Maubourg
75700 Paris 07 SP, France
Phone: +33 (0)1 71 76 85 85
E-Mail: communication@ssi.gouv.fr

Last updated: December 2023

Item number: BSI-LaB23/003

Image credits: Front page and page 3 and 7:
AdobeStock © AddMeshCube

The publication is provided free of charge and is not intended for sale.