FORUM OF EUROPEAN SUPERVISORY AUTHORITIES
FOR TRUST SERVICE PROVIDERS

Tallinn, 16 April 2024

# Position Paper
# On remote identity proofing
## FESA's interpretation and minimal requirements for the use of remote identity proofing for trust services

The Forum of European Supervisory Authorities (FESA) for trust service providers, is open to national bodies responsible for supervision and/or trusted lists in accordance with the eIDAS Regulation[1].

Supporting the idea of the Digital Agenda for Europe, FESA sees itself as an experienced and competent body that supports the cooperation, information and assistance among its members and facilitates the exchange of views and agreement on good practices corresponding to Arts.17(4)(a), (c) and Art.18(1) of the eIDAS Regulation.

FESA intends to advance the harmonization of supervisory bodies' activities, to develop common points of view for the dialog with political or technical institutions, in particular the European Commission and standardization institutions, and to establish a levelled European playing field for trust service providers in terms of supervision.

## Review of the eIDAS regulation revised text

On 3 June 2021, the European Commission published a proposal for a revision of the eIDAS Regulation. The proposal represents a major paradigm shift by requiring Member States to provide European digital identity wallets (hereinafter wallets), the specifications for which will be harmonized at European level.

At the end of 2023, under the Spanish Presidency, a compromise was reached with the European Parliament on the regulation on digital identity and trust services repealing Regulation (EU) 910/2014. This compromise includes references to the use of remote identity proofing solutions to verify the identity of users, particularly for the issuance of qualified electronic certificates. In addition, an implementing act is foreseen in article 24, paragraph 1c, to establish a list of reference standards and, where necessary, establish technical specifications and procedures for the verification of identity and attributes in accordance with paragraphs 1 to 1b, which includes the remote identity proofing case.

In this Position Paper FESA presents its interpretation on the legal text and its minimum requirements regarding the use of remote identity proofing for trust services, either by the trust service providers themselves or by their subcontractors.

These minimum requirements are to be considered as part of the conformity assessment of trust service providers (and their subcontractors) aiming to provide a qualified trust service relying on remote identity proofing. In the following, for simplicity, the term remote identity proofing service provider is used to denote either the trust service provider or the subcontractor that performs remote identity proofing.

These requirements do not mean to replace ongoing standardization works by ETSI/ESI (TS 119 461) or CEN TC 224 but may be used as complements.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

FESA is convinced that conformity to these minimum requirements will contribute to achieving the adequate level of security and harmonization for trust services, ensuring a level playing field for trust service providers.

## 1. Article 24.1: Interpretation of “High level of confidence”

In the previous version of the text, four different identification methods could be used to issue a qualified electronic certificate, including remote identity proofing. While this identification method remains in the compromise, changes have been made to exact requirements.

Whereas the previous text referred to "another identification method recognized at national level which offers equivalent assurance in terms of reliability to physical presence", the new text replaces the requirement for equivalence to physical presence with the concept of "high level of confidence".

Considering the entirety of Article 24.1, which now requires the use a wallet or electronic identification means of electronic identification with a high level of assurance (formerly substantial), and based on the assumption that all these identity proofing methods should reach a similar level of reliability, FESA members understand that the methods that have to meet a "high level of confidence" will have to meet similar requirements as those applicable to assurance level high for electronic identification means as defined in Article 8 and detailed in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

In line with this interpretation, FESA members have listed the minimum requirements needed to achieve such a high level of confidence.

## 2. Risk assessment

Remote identity proofing services can be the target of attackers having various skills. Thus, a risk analysis covering risks relating to identity theft and risks relating to information systems security of the remote identity proofing system shall be performed.

Requirements of [ETSI 319 401 – Chapter 5. Risk Assessment] shall apply.

### 2.1. Risk analysis relating to identity theft

The remote identity proofing service provider shall at least explicitly identify the following feared event:

- identity theft.

The remote identity proofing service provider should use:

- standard ISO30107-3 as a guide to identify risk scenarios for biometric presentation attacks
- the ongoing work of CEN TC224 on Digital injection attacks as a guide to identify risk scenarios for the digital injection attacks in biometrics, including the analysis of the attack potential.
- and the ongoing work of CEN TC224 on European Requirements for Biometric Products (ERBP), which will be a multipart standard that covers the evaluation methodology for biometric products (both for performance and for security), the particular tests for each biometric mode (in the case of face recognition this is in part 5 of the ERBP), and Application Profiles for the use of a particular biometric mode (where there is already the definition of the Profile 1 in Annex A, which considers the identity proofing using videoidentification and human intervention).

In addition, this risk analysis shall contain scenarios relating to counterfeiting and falsification of identity documents by physical or digital means, as well as scenarios relating to the alteration of the user’s appearance by physical or digital means.

Examples of attacks can be found in ENISA report “Remote Identity Proofing – Attacks & Countermeasures[2]”.

[2] *https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures*

The remote identity proofing service provider shall review the risk assessment on a regular basis and in the event of any structural changes to the identity proofing process, either technical or organizational.

### 2.2. Risk analysis relating to information systems security:

In addition to risks specific to remote identity proofing (such as the use of deep fakes), general IT security risks shall be considered.
Any successful attack giving access to the information system of the service could allow an attacker to modify or delete data, including forcing a successful result for a failed identity proofing (or create a successful result from scratch) and forge or delete any record linked to this verification.

Also, personal identifiable information is processed by the service to carry out the service.

The remote identity proofing service provider shall explicitly identify at least the following feared events:

- personal data leak;
- leak of sensitive information relating to fraud detection processes.

The remote identity proofing service provider should identify in its risk assessment the feared events relating to deterioration of the user experience and system downtime.

The remote identity proofing service provider shall review the risk assessment on a regular basis and in the event of any structural changes to the information system of the remote identity proofing service, including changes to its hosting, infrastructure or architecture.

## 3. Policies and practices

### 3.1. Remote identity service policy

The remote identity proofing policy must be public and made available to end-users.

It is a set of rules, which has a unique reference identified by an OID, defining the requirements with which a remote identity proofing service provider complies in setting up and delivering its service.

A remote identity proofing policy may also, if necessary, identify obligations and requirements on other stakeholders, including users and clients.

In particular, the policy shall explicit:

- conditions that need to be met by the user to use the service. Here is a non-exhaustive list:
    - Use a device with video capture capability of sufficient quality
    - Possess a valid identity document
    - Speak a language supported by the service provider (with the list of supported languages in the document)
- Personal data that is processed when using the service and stored as part of records

The remote identity proofing service provider shall also implement the following procedures linked to the provision of the service, including a documented identity proofing procedure including:

- The list identity documents eligible on the service
- the attributes of the identity document that characterize the uniqueness of a natural person's identity

- the remote identity proofing service is "asynchronous[3]", "synchronous with interaction[4]" or "synchronous without interaction[5]".
- identify all reasons for remote identity proofing failure that can be communicated to the user and the business service. These reasons shall not include information on the verifications carried out and the type of fraud suspected, if any.
- Fraud:
  - define indicators for detecting identity theft attempts relating to the risk scenarios identified in the assessment of the risks relating to identity theft
  - for each suspected or proven identity theft, whether detected by the remote identity proofing service provider or reported by the business service, an alert is generated.
  - specify the remedies available to users of the service, including for the purpose of cancelling fraudulent identification or refusing to identify a bona fide user.

### 3.2. Remote identity service practice statement

It is a set of detailed practices (organization, operational procedures, technical and human resources, etc.) that the remote identity proofing service provider applies in the context of the provision of its service and in accordance with the remote identity proofing policy.

The statement of remote identity proofing practices shall be confidential and shall be made available only to those with a need to know to avoid their use by attackers to understand the system and algorithm.

### 3.3. Information security policy

The service provider must define and implement an information systems security policy in compliance with ETSI EN 319 401 and, in particular, based on the information systems security risk assessment identified in chapter 2.2 and the associated risk management plan.

This policy shall be reviewed at least every two years and in the event of a change in the risk assessment or risk management plan.

## 4. Specific requirements[6]

### 4.1. NFC chip reading

When the photograph and identity data of the holder are not directly read from an authoritative source such as a population register, but are directly obtained from an identity document, it is essential to ensure that this identity document is not falsified or counterfeit.

When the identity document is presented remotely, it can be subject to both physical modifications (which are harder to detect through a video compared to a physical inspection) and digital modifications (such as deepfakes, which are increasingly easy to create and use with software widely available). It can even be possible to have a full digital generation of an identity document that does not even exist in the physical world. The quality that can be reached with digital modifications or generations and the limited

[3] when the identification data verification phase is carried out at a later time than the identification data acquisition phase

[4] when it is synchronous (does not meet the criteria for asynchronous) and allows interactions between the user and the operator during the identification data acquisition or verification phase

[5] when it is synchronous and does not allow any interaction between the user and the operator during the identification data acquisition and verification phases

[6] *In December 2023, The French National Cybersecurity Agency (ANSSI) and the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) published their 6th joint annual release, which focuses on remote identity proofing and present the main threats and recommendations on the subject. https://cyber.gouv.fr/sites/default/files/document/ANSSI-BSI-Joint-Release_20231220.pdf*

resources available to remote identity proofing service providers make it complex, if not impossible in some cases, to detect these modifications or generations when relying solely on a video stream.

**In this context, FESA members consider that NFC reading of the chip contained in identity documents is the most appropriate method of guaranteeing the authenticity of the document and the origin and integrity of the data it contains, and should be required when the identity proofing relies directly on an identity document.**

In order to perform an identity proofing, the NFC reading shall grant access to two types of data contained in the ID chip, while respecting the minimization principles as defined in the general data protection regulation and national regulations:
- The civil status (surname, first name, date of birth, place of birth, etc.); and
- The photograph of the legitimate holder.

Currently, accessing this data, in particular the facial image of the holder, through NFC reading of this chip is not possible for private entities in several Member States, due to national legislation based in particular on EU regulation 2019/1157.

**Therefore, FESA members consider that it should be clarified whether EU regulation 2019/1157 should indeed be understood as forbidding access to these data for the private sector.**

### 4.2. Checks for lost and stolen documents

In order to guarantee the status of an identity document, and to ensure that its legitimate holder is in possession of it, it is essential for remote identity proofing service providers to check it against a lost and stolen register.

At present, this type of register is only available in certain European Union countries. The European Union should ensure that such a register is kept in every country. In addition, accessibility to such a register, especially for private providers, needs to be enabled through clear guidelines.

### 4.3. Use of video

Liveness detection, facial comparison, and document authenticity check need to be carried out using appropriate and sufficient media material.

For biometrics controls, input data shall be based on a video recording of the applicant’s face.

Where NFC chip reading is unfeasible, a video recording of the document shall be used provided that the document can be authenticated on the basis of this video (with sufficient security elements that can be verified on a video).

Videos shall be recorded in a live stream (so a malicious attacker cannot prepare a fake video in advance), and any photograph used to facilitate comparison with the facial image on the identity document shall be extracted from this video.

The video shall be of sufficient quality and length to enable presentation and injection attack detection.

In addition, random challenges shall be implemented, such as requiring the user to perform a movement or speech, to protect against replay attacks.

Requirements should be defined as mandatory standards by the EU - if necessary with the help of standardization experts (such as ETSI).

### 4.4. Up-to-date Artificial Intelligence (AI) solutions

AI solutions are now widely used in remote identity proofing services to carry out partial or the totality of controls related to liveness detection, facial comparison, and document authenticity.

AI solutions involved in remote identity proofing service shall be able to detect known-attacks, including both presentation and injection attacks, and attacks relying on the use of video replay, deep fakes, virtual masks, physical masks or make-up…

AI solutions shall be trained and maintained at the state of the art[7] against these attacks.

These AI solutions may be developed in-house by the remote identity service provider or purchased from a vendor. Procedures shall be defined and enforced to protect assets specific to AI systems, e.g. datasets, algorithm and model, that are under responsibility of the remote identity service provider.

Some types of attacks target specifically AI systems and must be considered and countered. For example:

- Evasion attacks
- Poisoning attacks
- Backdoor attacks
- Model Extraction attacks
- Data Extraction attacks

In particular, algorithms shall not be trained on untrusted dataset.

More generally, all information security requirements that apply to IT systems also apply to AI solutions (asset management, access control, operation security).

### 4.5. Records

Qualified trust service providers shall retain the associated records in accordance with Article 24(2)(h).

In the context of remote identity proofing, those records shall contain, for each identity proofing (either successful or not), all relevant information for the purpose of providing evidence in legal proceedings, and at least the following elements:

- the video of the identity document (when applicable) OR the facial image of the applicant extracted from the secure component of the identity document;
- the video of the face of the applicant;
- the list of all verifications carried out on the identification data, and the detailed results of these verifications, including the verifications of authenticity of the document, of “liveness” of the applicant and of the face matching between the video of the applicant and the facial image extracted from the identity documents;
- the entity responsible for this verification (i.e. the version and configuration of any automated system, and the identity of any operator);
- all relevant identity data regarding the applicant;
- when the remote identity proofing is performed by a subcontractor, the exact data sent to the qualified trust provider following the verifications.

Those data shall be retained in full compliance with the general data protection regulation or any national legislation. They shall be protected in a way that prevents any unauthorized disclosure (such as full encryption, or storage on dedicated systems separated from the systems in charge of the identity proofing) and guarantees their integrity and authenticity (for example, sealing records with a qualified electronic seal).

### 4.6. Biometric external evaluation

[7] There is a strong need for standards and guidelines in this area.

Biometric technologies are subject to rapid changes of the state-of-the-art, and the assessment of the efficiency of the biometric verifications need to rely on actual testing in order to ensure, in practice, that the services are protected against attacks corresponding to a given attack potential.

This includes, in particular, biometric functionality (following ISO/IEC 19795-1 and -2), presentation attacks (following the guidance in ISO/IEC 30107-3) and digital injection attacks (which is a topic of ongoing works within CEN TC224, the European Committee for Standardization). This shall be done considering the scenarios (both for bona-fide use and for attacks) identified during the system definition and the risk analysis.

In order to assist stakeholders (i.e., trust service providers, administrations, industry and testing laboratories) in carrying out all these evaluation requirements, CEN TC224 is working in the definition of the "European Requirements for Biometric Products", which is expected to be included in the future within the evaluation domain of EUCC. This work also considers the evaluation of those solutions based on Artificial Intelligence.
The results and methodology applied to this test plan shall be shared to the supervisory body and the competent authority in charge of accrediting the competent third-party evaluation entities.

The remote identity proofing service provider should perform every 2 years or in case of a significant change in the biometrics verification process (either technical or organizational), an evaluation by a competent accredited third-party specialized in presentation and injection attacks.

To verify the service's ability to detect biometric fraud, these results should be confirmed by a conformity assessment body recognized as competent in biometrics (e.g. accredited by a national accreditation body and in capacity to perform attacks with a high attack potential), and be realized in a timeframe sufficient for an efficient testing.

### 4.7. Biometric internal testing

In addition, the remote identity proofing service provider shall develop and maintain an internal plan to test the effective ability of the service to detect attempted identity theft.

- For the liveness detection: test the effectiveness of the measures applied to reduce the risks relating to the alteration of the user's appearance by physical or digital means identified in the assessment of risks relating to identity theft;
- For the comparison of the user's face: test the effectiveness of the measures applied to reduce the risks relating to the user's natural resemblance to another person (lookalike, twin, etc.);
- For risks relating to influencing user behavior: test the effectiveness of the measures to reduce the risks relating to influencing user behavior

These tests shall be performed internally by the remote identity proofing service provider at least once a year or in case of a significant change in the biometrics verification process (either technical or organizational).

### 4.8. Identity document external evaluation

[When document authenticity is based on optical verification of identity document authenticity] Depending on national legislation, assessment of the ability of the system to detect fraudulent identity documents using forged documents, for example from a collection of seized documents of law enforcement, in the context of a partnership with law enforcement. In this case, external tests in collaboration with law enforcement should be performed.

[When document authenticity is based on NFC chip reading] NFC chip robustness of identity documents against attacker of high level has been tested and is monitored as part of their CC certification, thus additional evaluation is not required.

## 5. **Management and operation**

In addition to requirements below, see [ETSI EN 319 401 – 7.TSP management and operation] requirements for guidance.

### 5.1. Subcontracting

If the service provider subcontracts part of the activities of the remote identity proofing service, then the subcontractors implementing all or part of the human, technical and organizational means necessary to comply with the requirements of this document must be assessed to verify that they comply with the requirements incumbent upon them.

The qualified trust service provider using a subcontractor for remote identity proofing shall ensure such assessment by a conformity assessment body is possible as part of their service contract.

### 5.2. Human operators

Verifications by human operators are a safeguard against bias or vulnerabilities within the automated systems used for liveness detection or face-matching, that shall be put in place when required according to the results of the corresponding risk assessment, to achieve a high level of confidence. However, this safeguard is efficient only if human operators are adequately trained and possess the necessary knowledge and skills. Training should be performed periodically (for example, annually) and also specifically when new vulnerabilities affecting the identity proofing process appear.

When human operators perform remote identity proofing, they shall possess and demonstrate the following skills and knowledge:

- knowledge of any remote identity proofing policy and/or information systems security policy relevant for their activities;
- knowledge of the threat assessment relating to identity theft, and of the modus operandi of attackers leading to the risk scenarios identified in the assessment of the risks relating to identity theft;
- knowledge of legislation and regulations in force relating to the protection of personal data, and in particular the [GDPR], and eIDAS and national provisions on trust services;
- aptitude at remembering faces, recognize and compare faces accurately from photos and videos;

knowledge of security features of identity documents and the verifications to be carried out to identify falsified or altered identity documents (at least for the information as provided in the PRADO registry);
In addition, where a human operator would validate a verification which has been rejected by any automated verification, controls shall be in place in order to minimize the risks of bribery, blackmailing or negligence, such as an additional verification by another operator.

### 5.3. Software development

Software developed by the remote identity service provider shall be included in a secure development program involving: regular code reviews, non-regression tests, documented acceptance test suite, generation of log records, obligation of discretion for developers, logging and audit of development activities, and change management.

## 6. **Supervision requirements**

### 6.1. Detection of fraud attempts

Interrupting the remote identification process prematurely when detecting a fraud attempt may provide useful information to the attacker regarding the verifications performed by the remote identification proofing service, and may prevent the effective recording of proof.

Therefore, in the event of a suspected attempt to manipulate the application process, use of forged identity documents or other indications of a criminal offense, the remote identity proofing service provider shall carry out the identification process to the end in order to enable effective detection of fraud, as long as the integrity or availability of the productive environment is not compromised.

In case of massive and repeated manipulation attempts from a recognizable attacker, the provider shall inform the national supervisory authority immediately.

### 6.2. Third-party software

The list of third-party software taking part (directly or indirectly) in the identity proofing verdict (success or fail) shall be subject to specific monitoring shall be accessible on demand to the supervisory body. This includes but is not limited to AI solutions performing liveness detection, facial comparison, and document authenticity controls.

This knowledge will help supervisory bodies to have a better cartography of the industrial ecosystem.

Third-party software suppliers shall be required by contract to inform the service providers of any internal fraud or attack aiming at altering the software supplied, as well as any known vulnerability of the software. Service providers shall inform the supervisory body of these events.

### 6.3. Incident report

Significant incident shall be reported to the supervisory body accordingly to the Incident Reporting Framework published by ENISA : Article 19 Incident reporting — ENISA (europa.eu).

### 6.4. Change report

Significant changes in the provision of the remote identity proofing service shall be communicated to the supervisory body.
Eg: any structural changes to the information system of the remote identity proofing service, including changes to its hosting, infrastructure or architecture (see 3.5.2), changes to the methodology (verification algorithms, operator interface), addition of new identity documents, etc.

### 6.5. Quarterly report

Every three months, the remote identity proofing service provider shall consolidate a report over the last 3 months including:

- General usage metrics of the remote identity proofing service
- Volume of failed identifications (by types of error: image quality, suspicion of biometric fraud, suspicion of document fraud)
- Volume of identifications subject to internal quality reviews
- Results of internal quality reviews (aligned results or mismatch)
- Volume of complaints based on an identity proofing verdict being challenged
- Results of complaints processing
- Evolution of staff (human operators with their level of seniority) over the period
- Volume of identifications performed per identity document

For the latter metric, it is crucial to keep track that initial sampling is correct when testing identity documents from a list of eligible documents (can reach 650).

As part of requirement 3.6, the service provider must also define a procedure to test internally the effectiveness of biometrics verifications.
To this end, internal test campaigns results shall also be included in the report.

This report shall be sent to the supervisory body if asked and shared on demand to the conformity assessment body.

### 6.6. Annual threats report

Given the rapid changes of the state-of-the-art in the context of biometrics and identity proofing, for example with the widespread availability of deepfake tools, it is essential that supervisory bodies remain aware of the capabilities of attackers, as they are observed by the service providers.

Every year, the remote identity proofing service provider shall communicate a threat report on frauds and attacks observed on the system (biometrics, identity documents and system security).