EUROPEAN UNION AGENCY
FOR CYBERSECURITY

REMOTE ID PROOFING

Analysis of methods to carry out identity proofing remotely

MARCH 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use trust@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

CONTRIBUTORS

Paolo Campegiani (Bit4id), Marc Norlain (AriadNEXT), Nikolaos Soumelidis (SpearIT), Michał Tabor (Obserwatorium.biz), Andrea Röck (Universign)

EDITORS

Evgenia Nikolouzou (ENISA), Slawomir Gorniak (ENISA), Dorin Bugneac (ENISA), Ioannis Agrafiotis (ENISA)

ACKNOWLEDGEMENTS

Special thanks go to various stakeholders in Europe who provided their response to the survey and/or were interviewed for the purpose of this report.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: XXXXX – DOI: XXX

TABLE OF CONTENTS

ABBREVIATIONS

AI	Artificial Intelligence
CA	Certification Authority
CAB	Conformity Assessment Body
CEN	Centre Européen de Normalisation
CIR	Commission Implementing Rules
DPA	Data Protection Authority
EEA	European Economic Area
eID	electronic identification
eIDAS	electronic IDentification, Authentication and trust Services
EN	European Standard
ERDS	Electronic Registered Delivery Service
ETSI	European Telecommunications Standards Institute
ETSI EN	ETSI European Norm
ETSI TR	ETSI Technical Report
ETSI TS	ETSI Technical Specifications
eSig	electronic Signature
eSeal	electronic Seal
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IdM	Identity Management
IDP	IDentity Provider
IPSP	Identity proofing service provider
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
KYC	Know-your-customer
LCP	Lightweight Certificate Policy
LoA	Level of Assurance
GDPR	General Data Protection Regulation
ISO	International Organization for Standardisation
MS	Member State
NCP	Normalized Certificate Policy
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
PAD	Presentation Attack Detection
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
QSCD	Qualified Signature Creation Device
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QERDS	Qualified Electronic Registered Delivery Service
RP	Relying Party
SB	Supervisory Body
SCD / SCDev	Signature Creation Device
SSCD	Secure Signature Creation Device
SSI	Self-sovereign identity
STF	Special Task Force
TOE	Target Of Evaluation
TS	Trust Service
TSP	Trust Service Provider

EXECUTIVE SUMMARY

The Regulation (EU) Nº910/2014 on electronic identification and trust services for electronic transactions in the internal market, hereafter eIDAS (electronic IDentification, Authentication and trust Services) introduces provisions for electronic identification, as being a key lever for the development of a singly digital market across Member States. Electronic identification under eIDAS constitutes a digital solution which provides proof of identity for citizens or organisations, to access online services or conduct online transactions. Specifically, under article 24(1) (section 1.3), it allows alternatives to physical presence for identity proofing in the context of issuing qualified certificates and paves the way for remote identity proofing. It is stated that other *identifications methods* can be used that are *recognised at national level which provide equivalent assurance in terms of reliability* and the *equivalent assurance shall be confirmed by a Conformity Assessment Body (CAB)*. The ability of remote identify proofing promotes and increases the possibility of electronic transactions while at the same time ensuring the validity of the identities of the involved parties in the transaction.

Identity proofing was generally achieved by an identity proofing operator being physical present at the same place as the applicant, when extracting information and verifying an ID card of the applicant. However, the increase of the digital market rendered the idea of identifying a person remotely more attractive, since remote identification allows customers who are physically far away to access such services. During the COVID-19 pandemic crisis, the possibility of identifying a person without physical presence became even more crucial given that physical presence is not only cumbersome, but can even be dangerous, or just not possible while observing the safety measures to reduce the impact of the pandemic.

This report provides an overview of the most common methods for identity proofing being enriched by some illustrative examples received by the different stakeholders, presents the current legal / regulatory landscape and supporting standards at the international and EU level and provides the current status quo in the European Member States with regards to their remote identity proofing laws, regulations and practices. Moreover, it provides a practical approach to apply risk management on the basis of examples presenting two typical identity proofing processes as also identified by the stakeholders. The report also discusses the input received though questionnaires from different stakeholders which use, offer or evaluate identity proofing solutions. In particular, the contribution of 80 different stakeholders show the importance of this topic which is currently under study also by the European Telecommunications Standards Institute (ETSI) special task force (STF) 588 that is working on a report on survey of technologies and regulatory requirements for identity proofing for trust services. Finally, it presents a preliminary gap analysis on existing standards and regulations, stresses the need for a harmonised adoption and cross-recognition of remote identity proofing and provides a number of legal and technical recommendations.

Recommendations in the Legal Context

- **Cross recognition** is a key element for an extended use of identity proofing methods in digital services and for cross-border business within the internal market. Standards and technical guidelines should be defined at EU level to provide a more or less analogous process for remote identity proofing, fostering the exchange of ideas and cross-fertilization between the different stakeholders, resulting in a more harmonized process.
- **Evaluation criteria and methodology** should cover the policy and security management areas, the process architecture and also the testing of the actual

performance of the service in handling positive and negative cases. It would be useful to have some metrics that allow to compare the efficiency of different methods, e.g. the false acceptance rate and the false rejection rate.

- **Article 24(1) of the [eIDAS] regulation** should be clarified to avoid different interpretations on what is “physical presence” (article 24.1 (a)), what eID means are acceptable (article 24.1 (b)), how to verify that a qualified certificate was issued based on article 24.1 (a) or (b) (article 24.1 (c)), and how evaluate “equivalence assurance in terms of reliability to physical presence” (article 24.1 (d)).
- Member states **should support automatic and online verification of identity documents**, for example based on a validation service of identity documents. This allows a uniform capability of remote identity proofing services to accept or reject identity documents.
- A central, well-maintained repository with reference material (laws, regulations, good practices, guidelines) would also be appreciated, in the same way the “Compilation of Member States notification on Secure Signature Creation Devices (SSCDs) and Qualified Signature Creation Devices (QSCDs)” is maintained.
- General Data Protection Regulation (GDPR) must be fully embraced by the different stakeholders not only fearing the consequences for not compliance, but as a useful tool that conceptualize the need for security-by-design and privacy-by-design as fundamental blocks for each computing system, including the ones used for the remote identity proofing.

Recommendations in the Technical Context

- **Awareness and clear process** - Training (on the operators’ side) and awareness (also for subjects) should be duly pursued, especially considering that the process is based on possibly many different identity documents and, from the point of view of users, is relatively new and all of its security implications could be not entirely clear.
- **Uniformity through risk analysis -** Risk analysis should be done in a systematic way, to provide for a secure remote identity proofing process, align the different implementations and result in more comparable outcomes. A regular review of risks and a sharing of security incidents between the different actors should further strengthen convergence for processes with comparable Levels of Assurance (LoAs).
- **Uniformity through equal access to government data** - Technical support from issuers of those documents is needed to allow identity proofing service providers a secured access to those documents' electronic data. Access to lost/stolen/invalid identity document online service is also needed to be able to verify the validity of the document produced during identity proofing process.
- **Putting the test first -** Testing should have a relevant role in the analysis, implementation and continuous monitoring of these systems, as it is often overlooked while it is a critical security tool.
- A good way to compensate for the weakness of specific remote identity proofing methods, is to **combine several methods of complementary natures**. Another example would be the usage of several identity sources that can be checked and compared against each other.

1. INTRODUCTION

1.1 CONTEXT

Identity proofing is “the process by which a (trust) service provider collects and validates information about an applicant and verifies that collected and validated information actually belongs to the applicant” [ETSI TR 119 460]. For a long time, this was generally achieved by an identity proofing operator (see section 2.1.1) being physical present at the same place as the applicant, when extracting information and verifying an ID card of the applicant. However, the increase of the digital market rendered the idea of identifying a person remotely more attractive, since remote identification allows customers who are physically far away to access such services. During the COVID-19 pandemic crisis, the possibility of identifying a person without physical presence became even more crucial, given that physical presence is not only cumbersome, but can even be dangerous, or just not possible while observing the safety measures to reduce the impact of the pandemic. The ability of remote identify proofing promotes and increases the possibility of electronic transactions while at the same time ensuring the validity of the identities of the involved in the transaction partners.

Regulation (EU) No 910/2014 on electronic identification and trust services, hereafter the [eIDAS] regulation, provides a common foundation for secure electronic transactions between citizens, business and public authorities. Under article 24(1) (section 1.3), it allows for identity proofing in the context of issuance of qualified certificates, alternatives to physical presence and paves the way for remote identity proofing. It is stated that a trust service provider can use electronic identification means or qualified certificates to proof the identity of an applicant as well as other *identifications methods* that are *recognised at national level and which provide equivalent assurance in terms of reliability, where* the *equivalent assurance shall be confirmed by a Conformity Assessment Body (CAB)*.

Remote identity proofing becomes more and more important. When asked, 11 out of 27 European Supervisory Bodies stated that they have already accepted methods for remote identity proofing. In the same way as the [eIDAS] regulation has enabled the use of remote identity proofing for trust service and electronic identification means, the anti-money laundering directive [AMLD5] has introduced this technique in the banking sector (section 1.3). Unfortunately, the existing legal framework can be interpreted differently, resulting in very different implementations.

Remote identity proofing is not only used in the context of trust services and electronic identity means as defined in the [eIDAS] or in the financial sector as covered by the [AMLD5]. It can be used also in a variety of contexts, for example registering new customers or providing access to a specific service. The present report starts from the context of [eIDAS] and [AMLD5] but is not limited to this context.

1.2 PURPOSE OF IDENTITY PROOFING

Identity proofing is important for all cases where trust in the identity of a natural or legal person is essential. It might be used to create another identifying token, such as a qualified certificate or an electronic identification mean, as defined in the [eIDAS] regulation, or to allow the correct person to access a specific service (i.e. banking services or administration services). It is a crucial element in creating trust into digital services. Identity of a person is a set of attributes that uniquely identifies a person. There may be several sets of attributes that uniquely identifies a person.

The classical way of proofing the identity of a person is that the applicant provides evidence of his identity. During a meeting with physical presence it can be checked if the evidence is acceptable and if it identifies the applicant. However, this classical method has several shortcomings. First of all, it requires the applicant and the person proofing the identity to be at the same place, a process which can be complicated, time consuming, and given the recent pandemic crisis even dangerous for health-related reasons. Furthermore, often proof of the evidence validation is not retained and the person proofing the identity might not be well trained to conduct a correct check of the different kinds of evidence or could be psychologically manipulated, like being threaten, bribed or convinced to improperly validate an identity verification operation by appealing to his sensitivity.

Remote identity proofing methods provide the possibility to identify persons without needing an actual physical presence in the same room. It can improve the user experience, help in the development of cross-border services, and avoid unnecessary health risk due to physical presence. This opens a new level of business opportunities, if there is trust that the identity proofing was done in a trustworthy and secure way.

Not all remote identity solutions are fit for all circumstances. Sometimes, it is more crucial to have a higher confidence in the identity of the person, even if the check takes a long time or costs more. In other situations, it is acceptable to have less assurance of the identity, which allows to use faster, cheaper or easier identity proofing processes. What is acceptable, depends for example on the financial consequences of a false identity. Electronic identification (or eID) under [eIDAS] constitutes a digital solution which provides proof of identity for citizens or organisations, to access online services or conduct online transactions. Moreover, article 8, introduces three Levels of Assurances (LoAs) for electronic identification means, as low, substantial, and high. This provides one categorisation of different solutions, which covers not only the identity proofing, but also other aspects of the electronic identification means, such as authentication means and information security management aspects. The LoA of the electronic identification means refers to the degree of confidence that can be put in the claimed identity of a person during an electronic identification using this electronic identification means.

Remote identity proofing can be used by qualified trust services as defined in the [eIDAS] regulation to issue qualified certificates, to identify the sender or receiver in qualified electronic delivery services, or for a qualified trust service managing the key for the user, to make sure that access to the key is provided to the same person that is identified in the corresponding certificate. It can also be used by banks, financial services, insurance companies to identify their customers. In addition, remote identification is used in plenty of other situations, where the identification of a customer is important, like hotel industry, Human Resources, airports, rental companies, temporary work or matching platforms (including delivery and ride-hailing services), public administrations, online gambling, etc.

1.3 NEED OF IDENTITY PROOFING

[eIDAS] Article 24(1) states:

> *When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.*
>
> *The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:*
>
> *a) by the physical presence of the natural person or of an authorized representative of the legal person; or*

> b) *remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or*
>
> c) *by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or*
>
> d) *by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body*

The [eIDAS] regulation allows alternatives to identity proofing with physical presence for issuing qualified certificates, which includes the usage of electronic identification means, qualified certificates and *"methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence*". The issuance of qualified certificates is not the only trust service defined in the [eIDAS] regulation which needs to identify legal or natural persons. This is also an important part for qualified electronic registered delivery services (QERDS) or registered electronic mail (REM) for identifying sender and recipient ([ETSI EN 319 521] and [ETSI EN 319 531]), and for trust services managing the key on behalf of the user ([ETSI TS 119 431-1]). In the latter case, the identification is needed to guarantee that only the right person accesses the key *(i.e. sole control) as identified in the certificate.*

In addition, chapter II of the [eIDAS] regulation introduces the definition, issuance, and management of electronic identification means. This includes the definition of three LoAs in article 8: low, substantial and high. Electronic identification means are linked to remote identity proofing in two ways. On one hand, already existing eID means can be used to remotely proof the identity of a person. On the other hand, when first issuing eID means, the legal or natural person needs to be identified during the enrolment phase ([CIR 2015/1502]). This identification might itself be based on remote identity proofing.

Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [AMLD5] foresees that eIDs or relevant trust services as defined in the [eIDAS] regulation can be used for identifying the customer.

> *[AMLD5] Article 13.1 states :*
>
> e) *identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council (*4) or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities;*

Issuance of qualified certificates as defined in [eIDAS] article 24(1), electronic identification means as defined in [eIDAS] article 8, and identifying a customer as per [AMLD5] article 13.1 are already three legal use cases that allow remote identity proofing. However, they can only work if there is trust in the provided solutions. And to have trust in these solutions, a unified way of evaluating remote identity proofing solutions is needed. This is not only needed for comparing solutions within the same country, but also for having trust in solutions evaluated in another country and allowing cross recognition of these solutions.

1.4 PURPOSE AND STRUCTURE OF THIS DOCUMENT

The present document is not only focused on remote identity proofing for trust service providers but takes a more holistic view on the topics and considers also remote identity proofing methods used for example by banks or by electronic identification means. The purpose is to get an overview of current implementations, standards, regulatory framework on the topic on identity proofing in Europe, and to provide guidance on what to consider when analysing a remote identity proofing method. The report only analyses the current situation and gives some recommendation to improve the current situation. It is not a standard containing requirements for remote identity proofing services, but can be used as input for such a standard.

- **Section 2** provides an overview of the most common identity proofing methods. It first introduces the different actors playing a role in remote identity proofing. Subsequently, it presents the different steps of a remote identity proofing process, which will later allow us to compare the different general identity proofing methods. The section also shows which methods are currently used or planned to be used.
- **Section 3** discusses the legal landscape and standards linked to remote identity proofing. It discusses the legal situation in the different European member states and gives an overview of existing standards on remote identification.
- **Section 4** discusses what needs to be considered when designing or evaluating a remote identity proofing solution. It discusses, by means of two examples, how risk analysis can be used to evaluate specific methods and what needs to be taken into account considering risks, vulnerabilities and security controls.
- **Section 5** provides a gap analysis of existing standards and regulations and shows what is needed to allow harmonized adoption and cross-recognition of remote identity proofing systems, providing also some recommendations.
- **Annex A** gives a more detailed description of the legal situation in the different EU Member States. Annex B provides a (non-exhaustive) inventory of threats and vulnerabilities which completes the examples in section 4. Annex C gives a (non-exhaustive) list of security controls which can be used to counter the threats and vulnerabilities presented in Annex B. It also gives a matrix which shows which security control can be used to avoid which vulnerabilities.

1.5 TARGET AUDIENCE

The present document is useful for a number of different stakeholders.

For Conformity Assessment Bodies (CAB) and Supervisory Bodies (SB) it shows what needs to be taken into account when evaluating (or supervising the evaluation of) a remote identity proofing solution or a Trust Service (TS) using such a solution.

For Trust Service Providers (TSP) and Identity Providers (IDP) it is a valuable source of the relevant standards and legal landscape to be taken into account as well as how to prepare a self-assessment of an identity proofing solution.

For standardisation organisations and regulators, it provides a gap analysis of current standards and legal landscapes.

For anyone wanting to use a remote identity proofing solution, it gives an overview of the existing solutions including the corresponding risks and safeguards.

1.6 METHODOLOGY

The present report analyses the current landscape of remote identity proofing methods. To have a most global overview, several sources were taken into account. Especially the [eIDAS] regulation, [CIR 2015/1502] and [AMLD5] from the legal side, but also [ETSI TR 119 460] were taken into account. In addition, we considered many national and international documents, which are listed in more details in section 3.

The goal was to analyse the current situation not only in the context of [eIDAS] and [AMLD5], but to have a more global overview on where it is needed. Especial emphasis was taken to analyse the national laws and requirements in different European members states, including national documents which are sometime only available in the national language. The aim was to have an overview of what solutions are used, for which purpose and based on which requirements they are evaluated. Currently, literature is scarce on threats and vulnerabilities for remote identity proofing methods, which is essential for a uniform evaluation of these methods. To overcome this gap and to get a good overview of the national situations, specific questionnaires were sent to different stakeholders, which use, offer, or evaluate identity proofing solutions:

1. **Supervisory bodies (SB):** They were asked about national laws and requirements, which types of solutions they allow in their countries, which solutions/technologies are provided by QTSPs, against which standards /criteria the services are audited, how to improve harmonization in identity proofing methods and what are their experiences in qualifying TSPs using remote identity proofing.
2. **Conformity assessment bodies (CAB)** evaluate identity proofing solution in different countries, not only in the context of [eIDAS] but also for other use cases like banks or notified eID means. They were asked about which industries use remote identity proofing, which solutions they have evaluated and against which requirements. They were also asked specifically about threats and risks to be considered when evaluating remote identity proofing methods, and on the kind of security testing to be applied.
3. **Trust service providers (TSP):** They were asked if they use or plan to use remote identity proofing, and if yes, which methods and solutions (e.g. in-house or external). They were also asked against which requirements the solution was audited, which are the main security threats and mitigations measures applied. In addition they were asked about how they handle evidences concerning [GDPR] and on the user perception of the solution.
4. **Banks and financial institutions**: They were asked on their experience with remote identity proofing solutions, against which requirements these solutions were audited, and what are the main threats and good practices according to risk analysis. They were also asked on their point of view on handling evidences based on the [GDPR].
5. **Identity providers (IDP)** are specialized in the provision of identity proofing methods. They were asked to provide details on their implemented remote identity proofing method, against which standards and regulation it is evaluated, and what are the main threats, risks and security controls to be considered. They were also asked on their target market and on their handling of the [GDPR] for evidences.
6. **European data protection authorities (EDPA)**: In the context of remote identity proofing, personal data is stored as evidence and might also be needed for tests. These organizations were asked if they were already consulted in the context of remote identity proofing, and what is their point of view on the handling of evidences and test data, in the context of the [GDPR].

The high number of answers on the questionnaire, 80 in total, shows the importance of this topic for the different stakeholders (Figure 1). The distribution of answers per country is depicted in Figure 2.

Parallel to the work of ENISA on the present document, the European Telecommunications Standards Institute (ETSI) special task force (STF) 588[1] is working on two documents:

[1] Specialist Task Force 588: https://portal.etsi.org/STF/STFs/STF-HomePages/STF588

- [ETSI TR 119 460] “Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects”, which was started before the present report; and
- Future [ETSI TS 119 461] “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects” which will be published after the present report.

The ETSI technical report [ETSI TR 119 460] provides results of a survey on the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing and compares them through a common set of properties. During the writing of this report, a collaboration with ETSI STF 588 was established concerning the use of ETSI TR 119 460 as input to this report as well as how this report can be used as input to the technical specification ETSI TS 119 461. This technical specification ETSI TS 119 461 will provide policy and security requirements for trust service components and will take into account the risk analysis and management described in the present report. It is based on [ETSI EN 319 401] for general security requirement for trust services and is planned to be published end of July 2021.

Figure 1: Number of answers per type of stakeholder

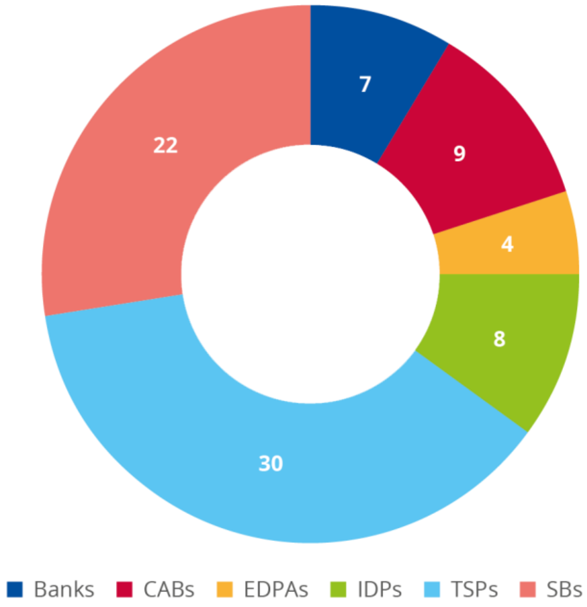
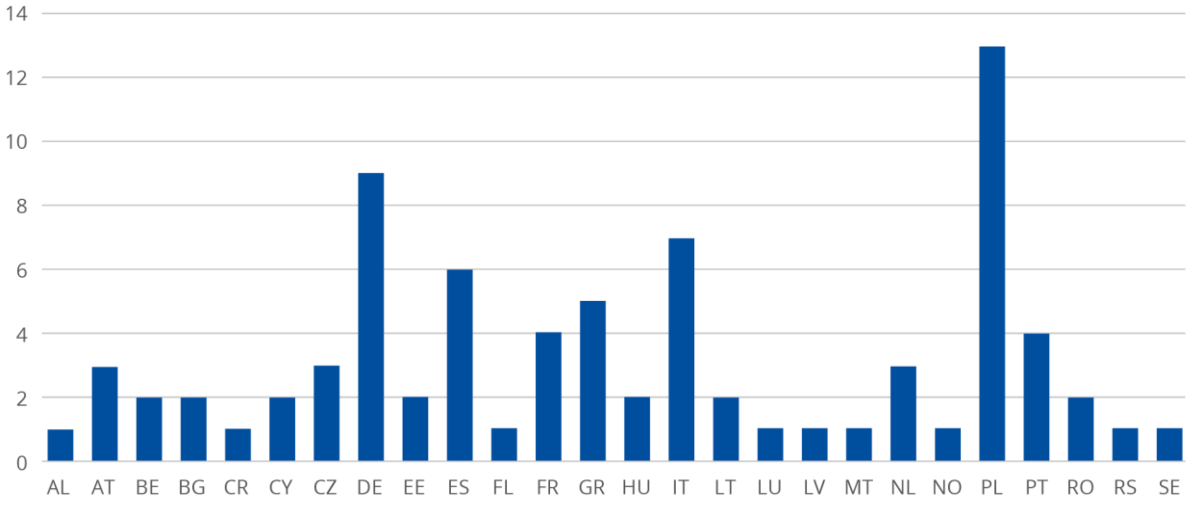


Figure 2: Distribution of answers per country



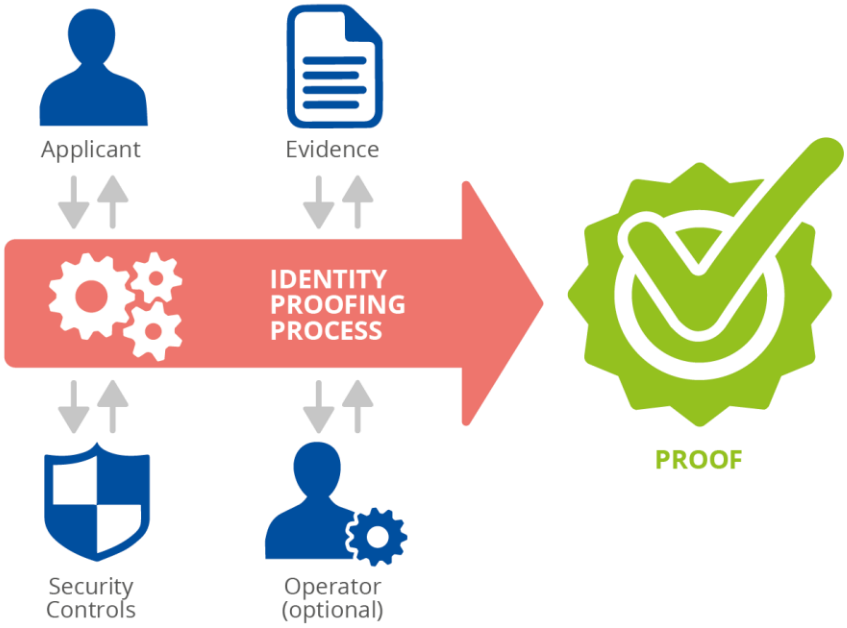
2. IDENTITY PROOFING METHODS

This section gives an overview of the most common methods for identity proofing and describes the different steps of an identity proofing process. Subsequently, it introduces the principles of the most used methods, including for each of them, a process description based on the identified steps. Finally, it presents some illustrative examples identified in the answers we received when the different stakeholders were asked "*Which type of remote identification solution are you using (or planning to use)? (artificial intelligence (AI) based / human based / both, using videos / pictures, eID / traditional ID documents, synchronous / asynchronous".* The purpose of the section is to provide a snapshot of the current situation based on [ETSI TR 119 460], the answers of different stakeholders to the survey and the current practice followed, rather than an exhaustive list of methods.

2.1 IDENTITY PROOFING PROCESS

The identity proofing actors are shown in Figure 3. The identity proofing process is used to confirm personal identity attributes of the applicant. It is generally based on the collection, validation, and verification of evidence. Its components mitigate the risk of false identity verification; at the same time collection of unnecessary data should be avoided and the process should not be too difficult and complex for the applicant.

Figure 3: Identity proofing entities



2.1.1 Actors

The identity proofing process engages the following actors:

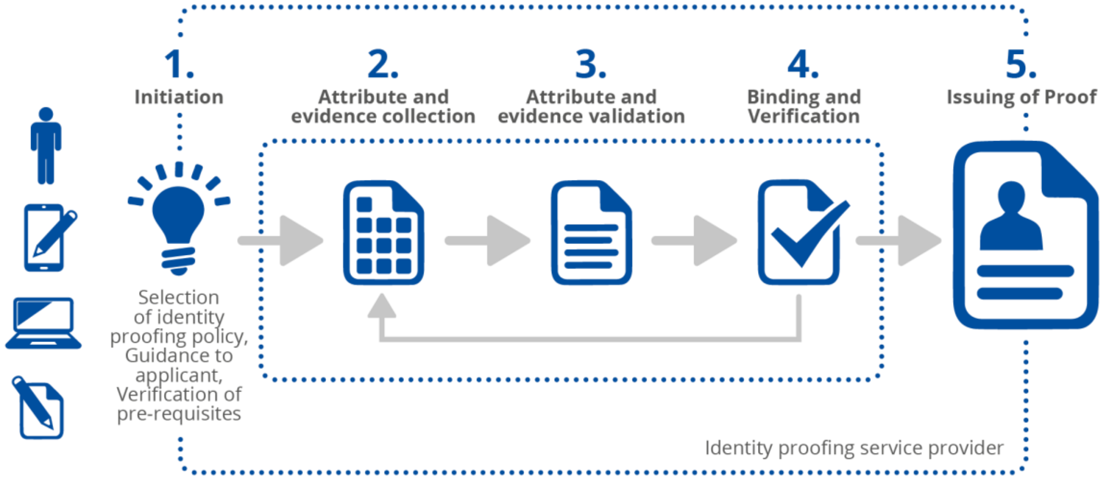
- **Applicant** - person (legal or natural) whose identity is to be proofed in order to become subject or subscriber (of a trust service) [ETSI TR 119 460].
- **Attacker** – a person that is interested in being proofed as an applicant while being a different physical or legal person, through the means of an attack that could combine physical or logical elements.[2]
- **Identity proofing service provider** (IPSP) – a provider offering a service for identity proofing, like TSPs, banks, Identity Providers, etc.
- **Operator** - a natural person, representing the identity proofing service provider, who confirms the applicant's identity directly or indirectly.
- **Relying party** - means a natural or legal person that relies upon an electronic identification or a trust service [NIST SP 800-63-3].

2.1.2 Steps of the process

The technical report [ETSI TR 119 460] presents a methodology based on three (3) steps of the identity proofing process: **attribute and evidence collection**, **attribute and evidence validation** and **binding identity attributes with applicant**. The report states that the process is finalized by issuance of the proof or assertion.

Our analysis of the data received from TSPs and Identity Providers showed that, due to lack of regulation and standardization, there are many diverse remote identity proofing processes. Some are based on just one interaction with the operator, while others are based on many interactions with the operator in many steps. Based on [ETSI TR 119 460], [NIST 800-63A], and [ISO/IEC TS 29003], this report presents a generalized five (5) steps diagram: initiation, attribute and evidence collection, attribute and evidence validation, binding and verification, issuing of proof, in order to capture variance between remote identification approaches.

Figure 4: General identity proofing process


1. Initiation
2. Attribute and evidence collection
3. Attribute and evidence validation
4. Binding and Verification
5. Issuing of Proof
Selection of identity proofing policy, Guidance to applicant, Verification of pre-requisites
Identity proofing service provider

Initiation is a preparatory phase that determines the identity proofing policy, all steps, and the goal of the whole process. Additionally, it allows to deliver to the applicant all necessary information and tools to perform the identity proofing process. Data collection, evidence validation, and binding and verification are the main components of the process, but the order

[2] Other types of attackers are overed by more general documents on IT systems.

and the flow of them can be different between systems and policies. The final step of the process is the issuance of the identity proof.

Note, in this context, “validation” means “the part of identity proofing process that involves determining that an evidence is genuine (not counterfeit or misappropriated) and the information the evidence contains is accurate” [ETSI TR 119 460] and “verification” means the verification of the identity of the person (with regards to the validated identity and any validated attributes).

2.1.3 Initiation

The purpose of this step is to initiate the process, inform the applicant, request acceptance of the context and the steps of the process, the data to be collected, the data protection policy and the applicable identity proofing policy. The initiation step includes:

- Selection of the applicable identity proofing policy
- Provision of initial information and guidance to the applicant
- Verification of any pre-requisites of the identity proofing process.

The use of an identity proofing policy in this process is foreseen by [ISO/IEC TS 29003]. Its purpose is to determine all other components of the identity proofing process which answer the main question “*Who is the applicant?*”. An organization may adopt multiple identity proofing policies for different contexts and use cases.

An identity proofing policy describes the promised level of assurance, the jurisdiction and the applicable legislation, the intended usage, a description of the process, the attributes which are confirmed, eligible evidence, records retention period, etc. One may refer to [ISO/IEC TS 29003] for a complete list of information of this policy.

Due to the fact that the process is performed remotely using computer systems, during the initiation step, all necessary software components need to be delivered to the applicant and / or checked. For example, if the process is using a camera video or picture quality can be verified and low quality can result in negative attribute validation.

2.1.4 Attribute and evidence collection

Evidence collection depends on the identity proofing subject who could be one of the following:

- natural person
- natural person identified in association with a legal person
- legal person.

Evidence may be obtained from several different sources, such as paper and electronic documents, live information, third-party databases including official registers, external electronic identification providers. Collected data may have different reliability according to the source and method of obtaining it. Its authenticity and integrity need to be validated against other collected evidence and known security controls.

Responders to the survey, mainly identity providers and TSPs, indicated the following evidence collected in their processes: pictures of identity documents, video captures, Optical Character Recognition (OCR) data from documents, machine-readable travel documents data (MRTD), machine-readable zone (MRZ), data retrieved from documents through Near Field Communication (NFC), proofs of possession of phone or email, secure mobile applications, digital certificates for identification and registry lookups. Respondents who work in financial institutions indicated that banks further use evidence from bank transfers or PSD2 Account Information Service allowing proof of bank account possession.

2.1.5 Attribute and evidence validation

The goal of the attribute and evidence validation step is to ensure that each piece of collected data is authentic and its information is accurate. Validation confirms the authenticity and validity of attributes and evidence.

In the case of paper documents, this step checks security features which can confirm the authenticity and level of assurance of the provided data. In most cases, the paper document in the remote verification process is shown to the camera, thus the data captured on photos or videos is checked against security features of the paper document. Of course, this requires knowledge of the security features of different documents and their origins. In the case of electronic data collected through a remote connection, validation focuses on source reliability, confirmation of authenticity, and integrity and quality of collected data.

When asked "*How do you assure that the process and its results are faithful and trustworthy*", the majority of identity providers and TSPs mentioned the usage of different validation methods including the participation of human operators in the process, data integrity checks, verification against known security features, AI based methods, mechanisms to detect injection and repetition.

2.1.6 Binding and verification

The binding and verification process step is focused on two goals: confirmation that identity attributes and evidence relate to a unique person and determination whether the applicant is, in fact, the one that declares to be. The binding depends on the type of the collected evidence and how this evidence was validated. For example, in the case of remote biometric verification, this step links the applicant to the identity using biometric facial recognition and liveness detection. The binding and verification step may use the data acquired from different sources and compare them to confirm their relevance. Additionally, this step can be supported by a human operator who confirms data in live video conference or by asynchronously checking video captured in the process. This step can also use authentication means issued internally or from a third party.

Based on the analysis of stakeholders answers, in the most common case when using remote identity proofing with the goal of issuing qualified certificates, the initial identification binding and verification is performed by a human operator who follows documented instructions (i.e. script). In the context of issuing qualified certificates, in most countries, automatic AI systems are only used to support the process, rather than replacing the human operator. In the context of [AMLD5], in some countries, automatic AI solutions without an operator are eligible.

2.1.7 Issuing of proof

The final decision is taken after one or more cycles of interactive steps of data collection, evidence validation and verification. The outcome of this process is the issuance of an identity proof or a corresponding identity assertion. Depending on the type of identity proofing, proof can take three different forms:

- Confirmation of the identity attributes. This confirmation may be absolute (YES or NO) or it may provide a score or a percentage as an indication of the confidence level.
- Delivery of the requested dataset which identifies the subject. A confidence level can accompany the entire dataset or each attribute of the dataset.
- Assignment of credentials. In this case no identification data is released, but the credentials allow reuse of identification data in other processes.

2.2 GENERAL METHODS DESCRIPTION

Taking into account all models described in the [ETSI TR 119 460] "Survey of technologies and regulatory requirements for identity proofing for trust service subjects" and the input we received in our survey, the following types of methods can be distinguished: onsite with the operator, video with the operator, remote automatic, electronic identification means, certificate based and combined.

2.2.1 Onsite with the operator

This method is described here as it is commonly mentioned as a benchmark for remote identity proofing methods. It is based on a face to face meeting in a common physical location where the applicant presents the necessary evidence e.g. identification documents, and the operator confirms the identity based on that evidence.

The awareness of the operator in the secure validation of identity documents is crucial for the reliability of the identity proofing process. The Public Register of Authentic Travel and Identity Documents Online [PRADO], which is shared by the Council of the European Union, is very useful for this purpose. The register contains a list of issued identity documents by EU members and other countries with detailed descriptions of security features, numbering, and position of elements on the document. The [PRADO GLOSSARY] presents general information about security features and methods of validation which are necessary to properly document recognition by operators performing this process.

The "onsite with operator" method refers to [eIDAS] requirements for qualified trust service providers issuing qualified certificate, in particular article 24.1(a) *by the physical presence of the natural person or of an authorised representative of the legal person.*

The process does not exclude the possibility of obtaining electronic evidence both from the applicant, but also from other trusted sources. The standard process includes the steps described in Section 2.1; these steps influence each other and are executed in accordance with the applicable policy.

2.2.2 Video with operator

This method is similar to the method "onsite with the operator", but the presence of the physical person (applicant) is realized by means of a remote internet connection or other type of telecommunications. The operator takes part in the live process of identification by conducting with the applicant a dialog based on documented instructions. The process is supported by a computer or a mobile device containing a digital camera and a microphone which are used to collect and record evidence. Additional controls may be utilised and additional attributes can be collected from relevant trusted sources. Software, including AI, may be used to assist or streamline the collection of information, but it is the human operator who conducts the process and takes the decisions.

[TR-03147] outlines requirements for the identity checks which have to be defined and implemented for identity proofing. For the validation step, this technical guideline requires that ID attributes are up to date; a check is made for lost, stolen, or revoked reports; the set of admitted ID documents is periodically reviewed; authoritative source is validated, ID attributes are determined to be sufficient; security features are checked.

2.2.3 Remote automatic

This method is used to proof the identity of the applicant without real time interaction between the applicant and a human operator. All data in the process is collected automatically by software systems. In the normal case, which is sometimes described informally as "selfie-id", AI software conducts the validation and verification steps. These steps can also be supported by a human operator; this is a case which can be better classified as a combined method (see next sections).

The process is conducted on the applicant's side by using a computer or a mobile device containing a digital camera and if needed a microphone. On the backend site, many technologies are utilised: machine-readable zone (MRZ) recognition, OCR of all parts of a document, biometric checks, automatic liveness validation, and reading of chip data on identity documents. Backend systems may also perform additional checks to databases like a register of issued and restricted documents.

The different methods or combinations of methods used are:

1. Fully automated methods without any operator intervention. Identity document is captured through picture(s) or video and authenticated automatically by algorithms. Facial recognition with presentation attack detection (a.k.a. liveness detection) is performed automatically.
2. The method in 1. is completed by a back-office enabling an operator to intervene on demand (when algorithms can't make a decision, when the applicant can't go through the process, etc.)
3. The method in 1. is completed by a back-office with an operator systematically intervening to detect attacks that are not correctly detected by algorithms.

The Machine Readable Travel Document (MRTD) according to [ICAO 9303] provides several security features for the remote recognition process. Documents compliant to this standard contain a Machine Readable Zone (MRZ), which provides name, date of birth, document validity, and document number. The MRZ may also be used to provide search characters for a database inquiry. MRTD can also be biometrically-enabled (eMRTD) and allows automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits. eMRTD enables facial recognition and optionally can contain fingerprint recognition and iris recognition. Information for this purpose is stored on the electronic chip and can be accessed through a contactless interface after the reader authentication process. An electronic travel document provides a "Passive Authentication" or "Active Authentication" feature[3], which supports the verification of the authenticity and integrity of all data stored on the chip.

Biometric face recognition based on identity documents is possible due to capture and digitization requirements for face images [ISO/IEC 19794-5:2005]. It is designed to allow for the specification of visible information discernible by an observer pertaining to the face, such as gender, pose and eye colour.

The rise of facial recognition systems based on deep learning has radically changed the performance of facial recognition systems[4]. Their operation allows them to be trained with data reflecting the characteristics of the problem (altered photo extracted from the identity document, old photo, etc.). The performance of the facial recognition engines can be evaluated using [ISO 19795 Biometric performance testing and reporting]. The challenge is to provide a sufficient learning and evaluation dataset while respecting the [GDPR]. The performance of facial recognition software does not take into account attempts to mislead the system. These must be evaluated by another method [ISO 30107 Biometric presentation attack detection]. Attacks are classified according to different levels. They can be a photo, a video, a more or less elaborate

[3] Both refers to EMRTD. Passive authentication (of a passport) means getting information from the passport without using the chip to verify the information; active authentication means using the chip to verify its legitimacy (this is to avoid chip/passport cloning)
4 See for example the following paper about FaceNet achieving a 99.6% accuracy: F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering", 2015.

mask or a DeepFake[5] type attack. According to the standard, presentation attack detection (PAD) methods detect "*the presentation of a biometric spoof (e.g. a facial image or video of a person on a tablet or a fake silicone or gelatin fingerprint) to a biometric sensor*". PAD is a very active field of research and the state of the art[6] is evolving rapidly.

2.2.4 Electronic identification means

This method is based on an internal or third-party electronic identification process which releases the data identifying the person based on the assigned authentication method.

ENISA Report [eIDAS COMPLIANT eID SOLUTIONS] provides an overview of electronic identification means and the legislative framework; it also presents the landscape of eID schemes. The report includes a description of technologies used for electronic identification, and an overview of the security of eID means management and authentication. The technological landscape covers various technologies based on hardware, mobile, biometrics, and prospective technologies.

A protocol used by several electronic identity means providers is OpenID connect[7]. It is an authentication layer on top of OAuth 2.0 and is specified by the OpenID foundation. This protocol allows to verify the identity of the applicant based on the authentication performed by an Authorization Server, and by obtaining basic information about the applicant. Another technology that can be used in eID solutions is FIDO2. The Fido alliance explains in a white paper[8] how FIDO2 can be used for eID means corresponding to [eIDAS] article 8.

Apart from the usage of notified electronic identification means as defined in the [eIDAS] regulation, eID means proposed by banks or other identity providers is also utilised in the identity proofing process.

Note that for the level of assurance of remote identity proofing solutions based on eID means, the level of assurance of the primary eID means is crucial.

2.2.5 Certificate based

This method is based on an internal or third-party trust service and evidence provided by this service e.g. certificates for electronic signatures and seals. The person's identification data is retrieved from the certificate. Interaction between the identity verification system and the trust service provider is limited to certificate revocation checks. This is often done by using a qualified electronic signature or seal, or an advanced electronic signature based on a qualified certificate.

Qualified TSPs are allowed to issue a qualified certificate based on other qualified certificate which is stated in [eIDAS] article 24.1(c) *by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b);* This requirement is practically impossible to follow if the other qualified certificate was issued by another QTSP. Thus, most QTSPs use this method only if they are the issuers of the previous certificate or the previous certificate is only one factor in the identity proofing process.

2.2.6 Combined methods

Many remote identity proofing solutions combine the methods presented above into one identity proofing process, in order to increase security and the level of assurance.

[5] It is becoming easier and easier to replace a face in a video by using tools such as pre-trained generative adversarial network (GAN). See for instance Pavel Korshunov and Sébastien Marcel "Vulnerability assessment and detection of Deepfake videos"

[6] Marcel, S., Nixon, M.S., Fierrez, J., Evans, N. (Eds), Handbook of Biometric Anti-Spoofing - Presentation Attack Detection, 2019

[7] https://openid.net/connect/

[8] https://media.fidoalliance.org/wp-content/uploads/2020/06/FIDO_Using-FIDO-with-eIDAS-Services-White-Paper.pdf

A combination of methods and components may be done by using one method after the other: the proof is issued if the process from both methods give the same result. In other cases, a combination of methods refers to mixing modalities of each method for the same step.

For security reasons, automatic methods can be supported by a human operator who supervises the automatic process and gives final consent to issue the proof. Automatic methods can also be a security control to human operator-based methods supporting collection of evidence, biometric checks and authenticity validation.

2.2.7 Steps of the process for each method

The 5-step identity proofing process applies to all methods described above. Table 1 summarizes the implications of each step for all these methods. It can be read row by row to gain an understanding of the process of any given method, or column by column to allow a side-by-side comparison between methods.

Table 1: Steps of the identity proofing process for each method

Process	Initiation	Attribute and evidence collection	Attribute and evidence validation	Binding and verification	Issuing of proof
Onsite with the operator	Information about the process Context establishment Confirmation of the evidence to be used	Transcription of data from the ID document by the operator ID document scanning or photocopying	ID document physical security checks Other relevant data is acquired or checked Validation against internal and external databases	Visual comparison of the applicant to the photo presented on the ID document Binding other evidence based on identification data	Operator issues and possibly signs the attestation of the identity
Video with operator	Information about the process Presentation of the policy, and terms and conditions Internet connection quality checks Internet camera and microphone quality test	Filling in the forms by the applicant Transcription of data from the ID document by the operator Document photo capture and OCR Video recording	ID document physical security checks Script based checks Data consistency checks, data fields comparison Validation against internal and external databases Other relevant data acquired/checked	Visual comparison of the applicant to the photo presented on the ID document Additional verifications based on the script If supported verification and binding based on AI and biometric algorithms	Electronic assertion authorised or electronically signed by the operator
Remote automatic	Information about the process Presentation of the policy, and terms and conditions Download and installation of required software Internet camera and microphone quality test	Filling in the forms Automatic scanning of the ID document, OCR based on data fields and MRZ zone, NFC reading (eMRTD) Additional retrieve of data from internal /external data sources Photo and video recording Interaction for liveness detection	Automatic security features of the ID document and other evidence validation Data consistency checks, data fields comparison Validation against internal and external databases Additional validation supported by an operator	Verification and binding based on AI and biometric algorithms Liveness verified basing on nondeterministic script or movement of face muscles	Automatic proof or if necessary supported by operator Electronic assertion authorised or electronically sealed by the service
Electronic identification means	Redirection to identity provider Information about the process	Credentials input and collection Additional retrieve of data from internal and external data sources	Authentication based on credentials or identification means in possession of the applicant Validation of digital signatures if used	Validity and revocation checks Identification data and attributes binding	Automatic proof In some processes data confirmed additionally by applicant before issuance
Certificate based	Information about the process Presentation of the policy, and terms and conditions Signature creation application download and initialization	Random, one-time data presentation, and its signing Data signing Signing certificate collection Additional retrieve of data from internal and external data sources	Signature validation Certificate validity and revocation verification Validation against internal and external databases	Trust anchors checks Data completeness confirmation Identification data and attributes binding	Automatic proof

2.3 CURRENT PRACTICE

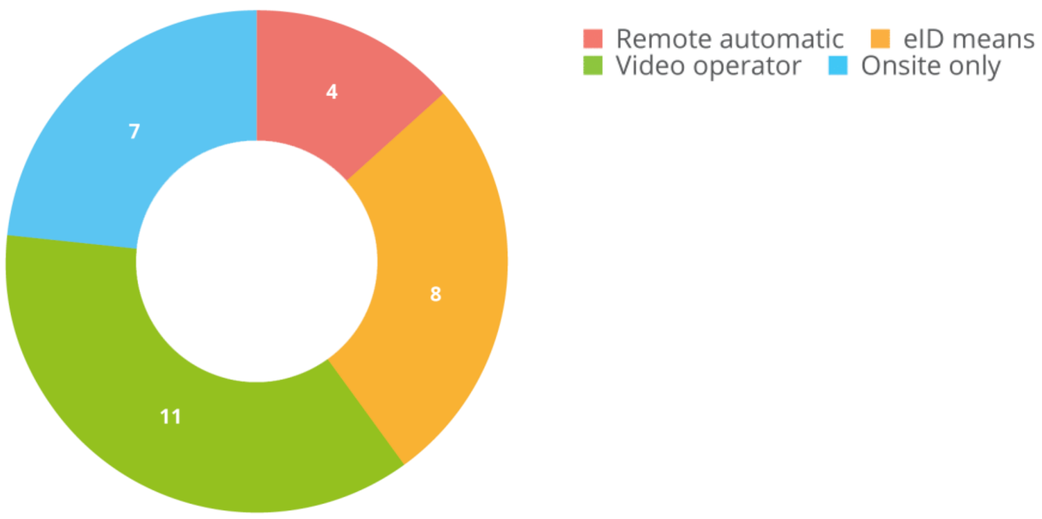
This section provides a series of indicative real-world examples of the above methods which are based on the answers to the questionnaires.

Although the same classification as in the previous section is used, several examples may fit in more than one category. Indeed, reality shows that the spectrum of solutions is somewhat less distinct, with some overlap between approaches. Given the lack of full details for each solution, it is normal that the classification of the solutions referenced here is not absolute.

For our study, we asked identity providers, TSPs and banks a similar question: *"which methods of remote identification do you offer now and which methods do you see in the future*". Their responses are presented in an aggregated way in this section.

23 out of the 30 TSPs who responded to the survey already use remote identity proofing methods for their services including the issuance of Qualified Certificates. The most popular method, cited by 11 TSPs, is the remote with operator, usually conducted with the use of synchronous audio-video call. The second most popular method is based on electronic identification means, including notified electronic identification schemes. Remote automatic process based on AI processing of picture of the applicant (selfie) and a picture of ID, is cited by 4 TSPs. A total of 7 TPSs do not use remote identity proofing for the moment (Figure 5)).

Figure 5: Different identity proofing methods employed by TSPs



Several TSPs reported that they plan to extend the number of remote identity proofing methods or introduce new ones. Video with the operator is planned by 9 providers, use of identity identification means is in preparation by 6; another 6 TSPs plan to offer remote automatic identification based on AI.

Identity providers often support more than one method. From the received answers, 63% of the IDPs apply combined methods, 50% support eIDs, 63% use remote automatic and 25% use video with operator.

2.3.1 Video with operator

The following examples present indicative variations of this method, as utilised by TSPs, banks or other sectors.

2.3.1.1 Plain video call method

This is the simplest “video with operator” method one can find in the market. The applicant submits personal information and is then interviewed by a human operator through a dedicated video conferencing system. The operator follows a precise scenario during this interview and asks the applicant to show the identity document. The operator asks about the reason for the request and can check a code sent separately, for example by SMS. Additional evidence can be collected during that interview. Each step is validated by the operator in the interview log in order to keep a trace. This includes a screenshot of the identity document and the applicant.

2.3.1.2 Usage of assisting/automation software

One of the TSPs reported using video with operator assisted by software for document validation, data extraction and biometric comparison. According to the TSP: “An in-house Video-identification solution is used that is based on a non-commercial video-conference system following the WebRTC standard. In addition, advanced OCR and biometrics technologies are used to speed up the process and help the identity operator to have more details during the video-session.”

2.3.1.3 Usage of technology for risk analysis

This variation of the video with operator was reported in our survey by a bank. In this scenario, a human operator is responsible for the correct identification of the customers, but technology is used for risk analysis.

2.3.1.4 Complementary use of databases for the verification of documents

In one of the answers we received in our survey, the validation of the natural person identity document is done by the TSP through (a) national identity documents databases, (b) other reliable data sources, or (c) by operator's identification. The verification of a legal person is performed via an official register, based on a unique identifier. The process was certified in accordance with article 24.1(d) of [eIDAS].

2.3.1.5 Acceptance of identity documents with specific security elements only

Some TSPs specified that in the video with operator, they only accept identity documents which contain specific security elements like holograms or other visual security elements. For example, one is using an in-house developed and operated human based, synchronous remote identification process using video and pictures and “traditional” ID documents including a liveliness check and verification of first line authenticity markers on the ID document.

2.3.1.6 Usage of redundant different providers

One of the TSPs described a variation which is based on the use of several remote identity proofing providers, each for a different business case. A human based remote identification using traditional ID documents and a live connection with the customer is applied by all of them.

2.3.2 Remote automatic

Fully automated remote identity proofing is described by a few banks, IDPs and TSPs in our survey. Technology is used in every aspect of the process; for example, a bank describes an AI process which is based on the use of certified third-party software ([NIST SP 800-63A], [ISO/IEC 30107]) integrated with in-house applications to check for liveliness, make face comparison and national card assessment. An IDP uses an asynchronous automated AI-based solution which can be used by TSPs to issue non-qualified certificates.

In general, these solutions are attractive from a business perspective, due to their low cost of operation, scaling and convenience (24/7 available to the user), but they have not become the most popular yet, for a variety of reasons, such as compliance reasons, initial investment, implementation complexity, market fragmentation caused by lack of harmonisation at the Member State level.

The survey states that, with a few exceptions, remote automatic methods based on AI are generally not accepted for the issuance of qualified certificates; some acceptance has been observed in the context of [AML5D]. In most cases, automatic methods are deployed in conjunction with human intervention in some part(s) of the process.

2.3.2.1 Usage of Electronic Machine Readable Travel Documents

One of the TSPs described in our survey a variation which is based on the use of Electronic Machine Readable Travel Document (eMRTD) and online biometric verification. The eMRTD is used to extract the user's data from the ID document. The biometric verification of the applicant is based on the facial image retrieved from data on the eMRTD chip with NFC technology and the facial image captured in the liveness session during registration via mobile phone app using deep learning algorithms. Additional validation against internal databases is supporting the security of this method.

During the identity verification session, the “liveness” of the applicant's facial image is verified. Presentation attack detection (PAD) and face matching controls are used. Technology addresses various presentation attacks (e.g. still or video imagery submission, usage of high-quality masks, replay of a previous video capture). The system is continually monitored and reacts to evolving threats. Face matching algorithm uses the latest advances in deep neural networks, to deliver matching performance with highest level of assurance. It is optimized for ‘selfies’ taken on smartphones and PCs in a huge variety of lighting conditions, poses and facial features.

2.3.2.2 Usage of human verification in case of doubt

This variation is described by banks and IDPs in two cases in our survey. Using a mobile application, the applicant is guided to submit a capture of the identity document and a face-photo. Information is processed by AI based systems to extract identity attributes, validate the identity document submitted as evidence and check the picture extracted from the identity document with the one captured during the application to ensure a correct binding. When the system has doubts or there is a need of an out of band decision, a human operator is called in to make the decision.

In a variant of the above process, a human operator always reviews and takes the final decision. This resembles a combined method (see below).

2.3.3 Electronic identification means

2.3.3.1 Usage of notified [eIDAS] eID means

Based on [eIDAS] article 24.1(b), notified eID means of level substantial or high is used for the issuance of qualified certificates. This is a method which was reported mostly by TSPs in our survey; in particular 6 organizations replied that they have already adopted or plan to adopt this approach, either on their own or by using outsourced solutions.

2.3.3.2 Usage of other eID means

Other eID means have also been suggested in our survey, for use in the banking sector and the provision of certificates under [eIDAS] article 24.1 (b). This includes the use of national ID cards, in the cases described below.

- A governmental CA uses national ID based identification, for the citizen. Citizens who apply for a qualified signature certificate for their Citizen ID Cards have to be identified using the eID function of the Citizen ID Card.
- Other TSPs base the identification on the use of a national electronic ID card and a mobile application.
- In a couple of cases, the TSP offers the option of using the national eID together or as an alternative to the use of bank identities (see the next sub-section).

2.3.3.3 Usage of bank identity

This is another case of using eID means; it is presented separately due to its unique characteristics and popularity among banks and TSPs. In this approach, the bank identity of the person is used as electronic identification means, which can be used to support validation of the applicant's attributes. Typically, the applicant is identified via an identity provided by a bank or financial institution, by logging in to the bank account or by issuing a real time, context based bank transfer. In our survey, the following examples were cited:

- The applicant chooses from the list the electronic bank account, and then the applicant is transferred to the bank account login page. During strong authentication, the bank informs that the applicant's data will be used for identity proofing. The proof contains data of the applicant stored in bank account attributes. This approach was described by two banks and is generally adopted.
- In another case, a bank reported the use of synchronous mode electronic identification means on a level substantial delivered by banks (for use in the initial identity proofing for issuances of qualified certificates for electronic signature).
- A TSP described the usage of verified identity data obtained, verified, and maintained by financial institutions according to Anti-Money Laundering Law [AMLD5].
- A couple of other banks reported their plans to adopt the use of on-line banking or bank account information payment service or electronic identification means provided by banks.

2.3.4 Certificate based

2.3.4.1 Signature with qualified certificate

In the typical scenario, the applicant is identified, on the basis of [eIDAS] article 24.1(c), via either a qualified signature or seal, or an advanced electronic signature based on a qualified certificate.
In our survey, this method was met by a bank and a TSP. The bank described its solution as based on the usage of asynchronous mode qualified certificates for electronic signatures and seals. Requests for certificate issuance are signed by subscribers with their qualified certificates for electronic signatures.

2.3.5 Combined methods examples

2.3.5.1 Multi-factor identification

In a case described by a TSP, remote identity proofing is based on a 3-factor identification process composed of:

- Automatic remote video identity solution
- Identity validation based on bank transfer
- Online human supervision via video communicator.

The applicant uses the provided link to connect with the operator through video communication chat, the operator follows the script and collects all data from documents presented by the applicant. During the process, the applicant receives via SMS a link to start the automatic process for which a smartphone is used. As the final step, the operator sends via email a link to the bank transfer validation which is made and confirmed synchronously in real time. All collected data is checked by the operator who confirms the identity for the issuance of a qualified certificate.

A TSP reported that multi factor remote identity verification is being considered to prevent fraud. More details were provided by another TSP which is working on in-house solution, that will use a combination of checking personal ID documents and photos via video and data verification against an authorized registry.

2.3.5.2 Asynchronous video with final human decision

Several TSPs described the use of asynchronous video with operator where the applicant shows the national ID document and provides proof of liveliness. An automatic AI algorithm helps to check ID document authenticity and person liveliness. All successful decisions are taken by a human operator. For example, a TSP describes asynchronous AI based and human based process: In case of success there is always a human decision. The identification document is checked plus liveliness is verified via a non-predictable video sequence.

Our survey shows that there is a considerable interest in this method, and the majority of TSPs plan to implement this method.

2.3.5.3 Combined AI and human verification

A bank reported using an in-house solution which is a combination of AI and human verification. It asks customers to take a picture of their ID and record a video of their face. A deep neural network processes the evidence and a manual verification of a human operator takes place. The bank works on including a digital layer of eIDs in the process.

Several other variations exist. For example, one bank uses face recognition and document scanning; it collects a photo of the face and photos of an identity document from the user. Another uses face recognition and online ID card verification which is double checked manually.

2.3.5.4 Bank identity plus ID document

In this case, which is reported by a TSP, the applicant will be asked to share identity data from a bank or tax account by signing in to the existing bank/tax account. In addition, the applicant may be asked to create a picture of a valid identity document, a video selfie and to choose a PIN code.

2.3.6 Highlights

Feedback received from Identity Providers, when asked "*Which methods of remote identification do you offer now and which methods do you see in the future?*", has allowed the identification of the following trends and state-of-the-art approaches.

Best of breed method: This practice is based on the combination of different actors, components or techniques, whereas each bequeaths its advantages and qualities to the different parts of the remote identity proofing process; at the same time, fellow actors, components or techniques compensate for its weaknesses. The complementary nature of these measures facilitates robustness and it is important to be combined with simplified customer journeys to avoid unnecessary complexity and phishing attacks. These are some relevant replies we received in our survey:

- Use of a combination of methods is the only way to make a truly reliable remote identification; asynchronous review of video (photo/ID checks are easy to bypass) by fraud experts (to detect sophisticated attacks) and use of AI to automate data extraction, screening and pre-processing.
- The use of a combination of controls to ensure reliability and robustness is the best risk mitigation approach. Apart from more common methods (e.g. face matching, liveliness detection), other checks have also been utilised: detection of documents with the same face photo and different personal data (serial fake IDs production), holograms detection, mask databases for detecting use of latex masks, documents blacklists.
- Use of state-of-the-art techniques including AI for biometric matching, liveness detection, traditional document data extraction and document template validation, all performed synchronously. Use of video agents for extra assurance, particularly in case it is required by (national) legislation.

Mix-and-Match approach: This practice is based on building the technological, organizational and human resources which will allow several implementations targeted for the needs, particularities and regulatory requirements (including LoA) of customers in different sectors or countries. This is normal, because Identity Providers offer their services to different industries; apart from TSPs and banks, their clientele consists of organizations in the gaming and sports betting industry, insurance companies, public administration, hotel industry, human resources, airports, rental companies, public administration, telecoms and others. Each of these sectors may have different regulatory requirements and needs. The same is also true for different national markets. These are some relevant replies we received in our survey:

- Use of dynamic combinations of several components for remote identity proofing depending on the targeted LoA and regulation. Hybrid asynchronous picture/video review supported by 24/7 human-based validation for LoA Substantial, and extra use of NFC for LoA High.
- Targeting several markets segments can only be served by a flexible remote identity proofing system which considers applicable requirements and uses the necessary building blocks and technologies to deliver a solution which integrates into the customer's process; these include AI based video/picture analysis, recognition of eID and traditional document, synchronous and asynchronous steps, different types of devices, level of human participation.
- Use of broad spectre of alternatives to meet different rules per country/industry. This includes use of existing eIDs, reading of chip in passports/ID cards (ReadID partner), optical scanning of identity document with face biometrics and fallback to manual processing, optical scanning of identity document with manual processing, video conference, registry/attribute lookups from various sources, proof of possession (mobile phone, email), NFC chip reading, optical scanning and capturing of selfie in video sequences.

Other: Apart from the above, the survey revealed some other interesting approaches by identity providers.

- **Banks as IDPs for service providers**: Use electronic identification means on a level substantial secured by banks acting as Identity Providers; use of customer data to deliver identification system to any interested service provider (e.g. phone carriers).
- **Use of money transfers for remote identification**: The banking/financial practices and legislation (KYC/AMLD) uses of methods like money verification transfer (data of owner is extracted from money transfer sender data) and AIS (Account Information Services) customer data extraction, based on the fact that comparing to any other method only with money transfer customer will easily see any breach on account (what will not practically happen when using electronic ID means or even digital signature).

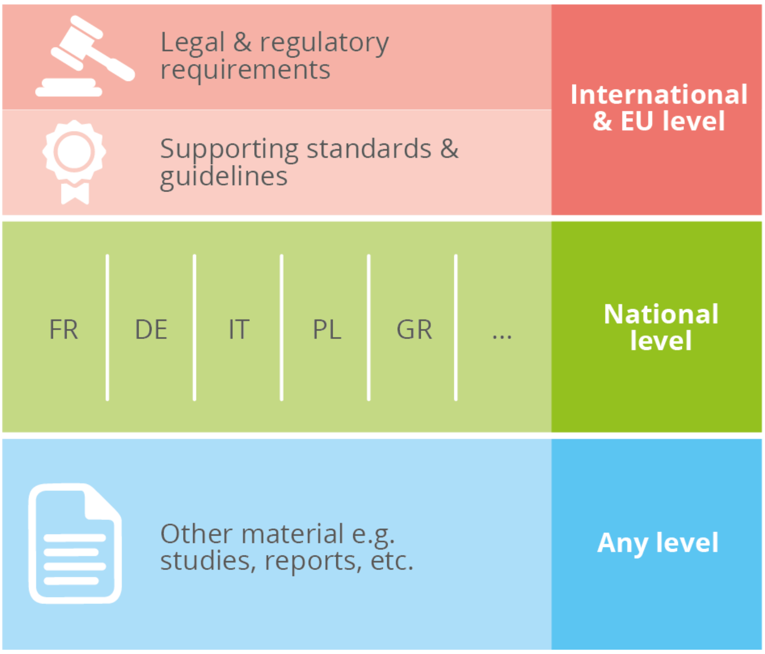
3. LEGAL LANDSCAPE & STANDARDS

3.1 OVERVIEW

This section sketches the current landscape of legal/regulatory environment and supporting standards, guidelines and other material related to identity proofing. It is based on the information received via the questionnaires and also leverages the work delivered in [ETSI TR 119 460].

Several legal frameworks, standards and guidelines have been created to address provision of services which use identity proofing as a trust anchor. The landscape includes regulatory provisions, standards and guidelines at the international and EU level, laws and regulations at the national (MS) level and other supporting material, such as studies and reports (Figure 6). An overview of each item is presented in this section, along with special cases, such as Self-Sovereign Identity (SSI) and blockchain, which are considered with regards to remote identification.

Figure 6: Different types and sources of material for identity proofing


Legal & regulatory requirements
Supporting standards & guidelines
International & EU level
FR
DE
IT
PL
GR
...
National level
Other material e.g. studies, reports, etc.
Any level

Despite the variety of resources available, at the moment, there is no complete set of legal and technical requirements which would receive wide acceptance and adoption in the different use cases and assurance levels with regards to identity proofing or its remote version.

3.2 LEGISLATION AT THE INTERNATIONAL AND EU LEVEL

The lack of jurisdiction at the international level makes it difficult to find universally applied legislation, but it does not hinder the development of international standards. The main legal tools at this level are treaties under the UN or the International Trade Law, bilateral agreements between large ecosystems, markets or countries (e.g. EU, US, China, Japan, Canada) and regulations by international bodies. Standardization efforts of the International Organization for

Standardization (ISO) have provided us with the main international resources of requirements for identity proofing; other standards such as those by ETSI/CEN or governmental guidelines such as NIST have also gained worldwide reputation.

3.2.1 UNCITRAL on Identity Management

The “Draft provisions on the use and cross-border recognition of identity management and trust services” [A/CN.9/WG.IV/WP.162 - UNCITRAL IDM DRAFT] is part of an initiative of the United Commission on International Trade Law, expected to become either a model law or an international treaty subject to ratification by the UN Member States. This is a work in progress document, but it has already received significant feedback by several UN member states and international organisations [A/CN.9/WG.IV/WP.164 - UNCITRAL CROSS DRAFT], which is indicative for the amount of interest in the area of identity management and the need for a solid cross-border legal basis with international recognition.

The scope of the document [A/CN.9/WG.IV/WP.162 - UNCITRAL IDM DRAFT] is more general; it does not technically specifically address identity or remote identity proofing nor does it elaborate on technical requirements or standards, but focuses on legal prerequisites for the mutual legal cross-border recognition of the results of identity determination of natural or legal persons using Identity Management (IdM) systems and of the results of trust services' provision. Thereby it partially replicates [eIDAS] concepts. This document reuses a commonly recognized terminology (with references to eIDAS and ITU-T [A/CN.9/WG.IV/WP.150 - UNCITRAL IDM TC]; where necessary, it introduces additional terms). The cross-border legal recognition of Identity Management (IdM) systems is based on ensuring a substantially equivalent level of reliability. The document describes the collection of attributes, identity proofing and verification, and binding between identity credentials and the person as part of the enrolment of person by an IdM service provider as well as part of the issuing by an IdM service provider (electronic) identity means for a transaction.

The Draft Provisions [A/CN.9/WG.IV/WP.162 - UNCITRAL IDM DRAFT] represent a smaller consensus intersection than [eIDAS] does in the EU/EEA area, but they are currently the only initiative to globalize a mutual, legally significant recognition of identity management systems. They encompass amongst others different levels of assurance of the diverse identity proofing methods and different legal approaches reflecting diverse legal cultures all over the world.

3.2.2 Regulation (EU) No. 910/2014 (“eIDAS”) and Commission Implementing Rules

The [eIDAS] regime has established the legal environment for trust services and electronic identification in the EU/EEA area. It is now considered an international reference point, which is also used by third countries to create compatible or similar ecosystems. One of the main characteristics of the [eIDAS] Regulation requirements is the technological neutrality; different technologies, not necessarily PKI-based, can be mobilized to achieve the necessary security requirements.

The eIDAS Regulation[9] established three Levels of Assurance (LoA) for use in the national electronic identification schemes. LoA characterizes the overall degree of confidence offered to relying parties and it incorporates different elements of the identity lifecycle. It has proven to be a very useful interoperability tool which allowed cross-recognition between different implementations/approaches of MSs, when notified and accepted at the same LoA [eIDAS]. LoAs are a useful interoperability tool, as they allow informed parties to assess immediately the relative strength of the outcome of an authentication process or other qualified services. Also, they have been instrumental in allowing different technical providers to develop solutions that were easy to adapt in different MSs, without any significant technical barriers, and have helped

[9] At the time of this writing [eIDAS] is under review; see section 5.2.3 for more details.

the industry at large in providing more interoperable systems supporting the Digital Single Market strategy. As such, the trend is to define remote identity proofing in terms of these LoAs.

Identity proofing is foreseen in both [eIDAS] pillars; trust services and eID. A two-way connection between the two pillars of [eIDAS] exists: according to article 24.1(b), eID of level substantial or high can be used by QTSPs as a method to verify identity and attributes; at the same time, qualified certificates have been used as authentication means of several eID schemes.

[CIR 2015/1501] provide conditions for the exchange of (natural and legal) person identification data between MSs when used in a cross-border context. The definition of specific minimum and additional person attributes in this exchange (Annex of the CIR), enforces their verification / validation in all eID scenarios. CIR relies upon certification to ISO/IEC 27001 or compliance with equivalent national standard for more general security requirements, such as secure communications. [CIR 2015/1502] sets out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of the eIDAS Regulation. It provides a detailed description of the various steps and conditions required to ensure a given level of assurance for electronic identification means; these include requirements for the enrolment, eID means management, authentication and management and organization. [CIR 2015/1502] is a reference point for the assessment of pre-notified eID schemes, but it is also very useful as a source of guidelines for identity proofing in other contexts (e.g. trust services, KYC).

3.2.3 eIDAS guidance for the application of the levels of assurance

The Cooperation Network (ECN) has issued since 2017 a guidance on the level of assurance [LOA GUIDE] which tries to interpret provisions of the [CIR 2015/1502], with an aim to provide illustrative examples and reasonable expectations (without aiming to enforce these). Use of 'authoritative sources’ and secure communication channels are suggested, by this document, as mitigation controls against inherent risks of the physical and remote identity proofing process, such as those related to presentations attacks (use of masks, makeup, manipulations of ID documents or biometric characteristics). According to the document, depending on the targeted level of assurance, a low false-match rate may be sufficient. For remote identity proofing aiming for a high LoA, it is more difficult than in the case of physical presence to demonstrate that possible manipulations of a video stream by attackers (e.g. real-time re-enactment, synthetic faces) relevant for this level of assurance can be reliably detected. One way of doing so is to demonstrate resistance against ‘attackers with high attack potential’ (though without giving any additional details).

Note: Several changes have been suggested to follow up with the more recent trends and the increasing demand for automated remote on-boarding solutions which use biometrics. A newer version of the guidance document is expected to be published, and is expected to convey the (documented) experience and good practices of MSs to the EU level; [BSI TR-03147] is such an example.

3.2.4 eIDAS guidance on inclusiveness and accessibility

The eIDAS Regulation states per Art. 15 that *“Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.”* This provision stems from the consideration that digital identity is a fundamental tool for an effective online life. This principle requires more thinking when applied in remote identity proofing. In such a case, to provide for more security, the operator could always stop the process if some doubts arise during it. This, coupled with the possibly more difficult identification of people coming from ethnic minorities, could result in a substantial difficulty for these people, preventing them from having a digital identity issued remotely. The same problem could be faced with AI systems, as they might be less trained for ethnic minorities or people with disabilities.

3.2.5 Directive (EU) No. 843/2018 (“AMLD5 ")

[AMLD5] is EU’s updated legal instrument to prevent the use of the financial system for the purposes of money laundering or terrorist financing, in accordance with the Recommendations of the Financial Action Taskforce [FATF-R]. Among several other provisions, the 5th version of the Directive seeks to enforce stronger customer due diligence controls (Know-Your-Customer / KYC), including verification requirements, and address technological evolutions, such as remote customer onboarding.

Article 13(1) of [AMLD5] brings support for the use of eID means and relevant trust services as set out in the eIDAS Regulation, as an additional tool to identify customers and verify their identity. Apart from that, reliable independent sources may also be sought and accepted at the national level. No acceptance criteria, minimum requirements or guidance is given, apart from the reference to the [FATF-R] and the national KYC regulations, if applicable.[10]

Given the huge demand of remote onboarding solutions by the banking sector, also boosted by the pandemic crisis, it is no surprise that an AML EU Regulation, replacing [AMLD5], has already been suggested by ECOFIN to the EU Commission and is being worked on, as a means to enforce common rules between MSs and allow a satisfactory level of harmonization.

3.2.6 Regulation (EU) No. 1157/2019 on strengthening the security of identity cards

The recent *Regulation 2019/1157 on strengthening the security of identity cards* [SIDCR] specifies security features of national identity or residency documents and how to verify their authenticity. [SIDCR] is aligned with ICAO Document 9303 to ensure global interoperability, for example with regards to data elements included (and thus verified) to identity documents. Reliable identity proofing based on physical presence and use of secure, less vulnerable, breeder documents (i.e. birth certificates) are prerequisites; however, the Regulation leaves this responsibility entirely to each MS.

The use of biometric data, stored in the storage medium of identity cards and residence documents (eMRTD), is both appealing and technically feasible for the efficient capturing of reliable identity attributes. However, under article 11 of [SIDCR], for the protection of the critical biometric data, reading is only allowed to duly authorised staff of competent national authorities and Union agencies, and only after the issuance of Union or national legislation. This heterogeneity makes it difficult to define a uniform remote identity verification process.

3.3 STANDARDIZATION AT THE INTERNATIONAL AND EU LEVEL

3.3.1 ISO/IEC standards

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. The following sector neutral deliverables of the joint technical committee, ISO/IEC JTC 1, *Information technology*, are of particular interest in the area of remote identity proofing:

- ISO/IEC 29115 on entity authentication assurance framework
- ISO/IEC 24760 series on identity management framework
- ISO/IEC TS 29003 on identity proofing
- ISO/IEC 30107 series on biometric presentation attack detection (PAD)

[10] In March 2020, the Financial Action Taskforce (FATF) issued its “Guidance on Digital ID” [FATF-ID-G]. This guidance draws on a number of digital ID assurance frameworks and standards, especially those in place in the United States and the European Union, to draw links between the very technical world of digital ID and those developing policies to combat money laundering and terrorist financing.

ISO/IEC 29115, dated 2013, provides a framework for managing entity authentication assurance. Based on ITU-T Recommendation X.1254 (09/12), it introduced the notion of Levels of Assurance (LoAs) for entity authentication and provided the basis for eIDAS LoAs. Per ISO/IEC 29115, LoA1 is based on self-claiming, LoA2 requires the use of an "authoritative source" and LoA3 additionally requires identity information verification. The standard makes use of an extra LoA4, which, additionally to LoA3, requires the use of multiple authoritative sources and physical (in-person) appearance.[11] Although its threats and controls section is still of some value when considering remote identity proofing, one could refer to the recently released X.1254 (09/20) for more up-to-date guidance.

The ISO/IEC 24760 series specifies fundamental concepts and operational structures (i.e. a framework) of identity management. It is intended to provide foundations for other identity management related International Standards, including ISO/IEC 29115. The series is being updated to reflect recent changes; in particular, the 2019 update of Part 1 promotes a common understanding in the field of identity management by clarifying terminology and concepts, including new sections for identity proofing[12]. ISO/IEC TS 29003 builds upon the aforementioned standards to provide generic concepts and policy requirements of identity proofing. The former includes authoritative and corroborative evidence, actors, identifying and supporting attributes; it also defines three levels of identity proofing (LoIP – low, moderate, high). The latter focuses on the identity proofing policy and requirements of different stages of the process, including attribute collection, determination of the level of identity proofing, binding of the subject with the claimed attributes. The standard does not go into detail with these process requirements, nor does it provide security requirements. However, it includes examples of identity evidence, binding, and also examples of contra-indications and fraud detection (i.e. detective controls).

The ISO/IEC 30107 series includes several standards issued in 2016-2017 by the SC 37, Biometrics Subcommittee. Its focus is on techniques for the automated detection of biometric presentation attacks, meaning attacks specifically on the capture of biometrics at the point of presentation. It contains four parts: in short, part 3 builds on the terms and framework defined in part 1 and on the data formats defined in part 2, in order to establish principles and methods for performance assessment of presentation attack detection (PAD) algorithms or mechanisms; part 4 is a profile that provides requirements for testing biometric PAD mechanisms on mobile devices with local biometric recognition. The ISO/IEC 30107 series is probably the most importance reference on the subject of biometrics security.

3.3.2 CEN/ETSI standards

The European Committee for Standardisation (CEN) and the European Telecommunications Standards Institute (ETSI) are the primary source of European standards in the area of identity proofing. The main drive of these efforts has been to support the European legal framework for trust services, starting from Directive 1999/93/EC in late 2009 and continuing with the eIDAS Regulation, under Standardisation Mandate 460 of the European Commission.

The current ETSI/CEN framework standardizes requirements for a PKI-based implementation of qualified trust services; thus, it is not technology agnostic (as is the case with the eIDAS Regulation). Because of this PKI-based orientation, these standards provide less guidance (or possibly no guidance at all) for "alternative", "innovative" or "creative" implementations (e.g. blockchain-based products or SSI) of the eIDAS requirements.[13]

[11] The newly published ITU-T Recommendation X.1254 (09/20) eliminates this fourth level and uses the more granular entity authentication assurance levels AAL1-3 (component of LoA), in line with the NIST Special Publication 800-63 Digital Identity.
[12] Given the normal 8y lifetime of ISO/IEC standards, Parts 2 (Reference architecture and requirements) and 3 (Practice) should probably be expected in 2023-2024.
[13] Source: ENISA Technical Guidelines on Trust Services

The following standards relate to identity proofing for use in the provision of trust services:

- [ETSI EN 319 411] Policy and security requirements for Trust Service Providers issuing certificates
- [ETSI EN 319 521] Policy and security requirements for Electronic Registered Delivery Service Providers
- [CEN 419 241-1] / [ETSI TS 119 431-1] TSP service components operating a remote QSCD / SCDev

ETSI EN 319 411, parts 1 and 2, builds on the merits of [ETSI EN 319 401] (general policy requirements of TSPs) and provides policy and security requirements for TSPs issuing certificates (non-qualified and qualified respectively). Identity proofing is addressed in section 6.2 *Identification and authentication*; it is part of at least one of processes: certificate application, certificate issuance, subject device provisioning.

Policy identifiers such as LCP, NCP, QCP are used to set the criteria for the different “levels of assurance” of the identity proofing and authentication processes. NCP policy requires that “*evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence*”. For examples of what constitutes “equivalent assurance”, the standard mostly defers to [CA/BF EVCG SSL]. QCP policy is part of [ETSI 319 411-2]; its purpose is to match the eIDAS needs, as expressed in article 24.1(a-d). Again, in this case, the standard focuses on what kind of assurance is required, but not under which criteria this can be done, especially in the case of remote identity proofing.

[ETSI EN 319 521] provides policy and security requirements for the provision of Electronic Registered Delivery Service (ERDS). This service allows *secure and reliable delivery of electronic messages between parties, producing evidence of the delivery process for legal accountability*. Section 5.2 *Users Identification and Authentication* of the standard resembles article 24(1) of the eIDAS Regulation, with some material changes in the case of option (c), in which an NCP-based certificate or a digital signature are sufficient means for identity proofing to be used for qualified ERDS. As in the case of the eIDAS Regulation, option (d) merely allows “*other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence*” (which equivalence must be confirmed by a CAB), without providing implementation details for the TSPs, the national authorities or the CABs.

[CEN 419 241-1] and [ETSI TS 119 431-1] standards rely on the identity proofing process to ensure the sole control of signatories over their private key, when it is stored in a (Q)SCD operated by a (Q)TSP. In this service, the user is recognized by the certificate and thus user enrolment (initial identification and beyond, authentication for day-to-day signature) is a crucial step. With regards to identity proofing, the ETSI technical standard addresses some related notions such as certificate linking, eID means linking and device provisioning, but refers to [ETSI EN 319 411-1] for the core identity proofing process and to [CEN 419 241-1] for the enrolment of the eID means linking. The CEN standard provides more details; it includes an Annex of requirements for electronic identification means, characteristics and design which reflect specific clauses (2.1, 2.2.1 and 2.3.1) of [CIR 2015/1502]. Two levels of Sole Control are defined: SCAL1 and SCAL2; the former is mapped to LoA low or higher, while the latter requires at least LoA Substantial. [CEN EN 419 241-1] standard requires one factor authentication for Advanced Electronic Signatures (AES) and 2-factor authentication of Qualified Electronic Signatures (QES).

ETSI standards are not meant to be used only in the EU ecosystem; they have been designed as international standards which can be utilised by any country or ecosystem aiming to reach the same level of best practices. The significant gap which exists with regards to identity proofing policy and security requirements is expected to be covered by the upcoming [ETSI TS 119 461].

3.3.3 CA/Browser Forum requirements

The Certification Authority Browser Forum (CA/B Forum) is a voluntary gathering[14] of leading Certificate Issuers and vendors of Internet browser software and other applications that use certificates (Certificate Consumers). CA/B Forum maintains a series of requirements and guidelines to be applied by Certification Authorities in the issuance and management of "publicly- trusted" certificates, i.e. digital certificates for server authentication (SSL/TLS), code signing, email protection (S/MIME).

One of the guiding principles of CA/B Forum's documents is that any piece of information must be validated before being included in the certificate; this includes validation of hosts, email addresses, individual identities and/or organization identities, with different levels of scrutiny, depending on the certificate type and the applicable policy. Given the importance of the validation process and the active participation of several stakeholders (e.g. major application providers, certification authorities and the community) in continual material improvement, it's no surprise that identity proofing guidelines are documented very thoroughly. They cover all phases of identity proofing, such as attribute collection, attribute validation and binding with the subject of the certificate. The CA/B Forum repository should be sought as an important and up-to-date source of good practices, especially with regards to identity proofing of legal persons.

3.3.4 US - NIST Special Publication 800-63 Digital Identity

In 2004, the US National Institute of Standards and Technology (NIST) published the initial version of SP 800-63, Electronic Authentication Guideline. Three revisions have been published since then; the latest, revision 3, has been retitled as Digital Identity Guidelines and was published in June 2017.[15] The document is now separated into four volumes:

SP 800-63-3	Digital Identity Guidelines
SP 800-63A	Enrolment and Identity Proofing
SP 800-63B	Authentication and Lifecycle Management
SP 800-63C	Federation and Assertions

Revision 3 retires the concept of a level of assurance (LoA) as a single ordinal that drives implementation-specific requirements. Rather, it takes a more granular approach, by using separate assurance levels for the following components: identity proofing (IAL), authenticators (AAL), and federations (FAL). The objective of this change was to meet matured market needs and allow mix-and-match implementations which allow greater flexibility, more user convenience, enhanced privacy, and reduced risk in accordance with the intended scenario.

Volume SP 800-63A is naturally of special interest with regards to this study. It provides requirements for enrolment and identity proofing of applicants that wish to gain access to resources at each Identity Assurance Level (IAL). IAL1 does not require linking the applicant to a specific real-life identity; this is useful for scenarios which do not require the knowledge of the actual identity of the subject, e.g. petitioning based on the subscriber's home ZIP code. IAL2 supports the verification of identifying attributes in person or remotely to ensure the real-world existence of the claimed identity and the association between the applicant and this real-world

[14] According to its Bylaws (https://cabforum.org/bylaws/) the Forum has no corporate or association status, but is simply a group of Certificate Issuers and Certificate Consumers that communicates or meets from time to time to discuss matters of common interest relevant to the Forum's purpose. The Forum has no regulatory or industry powers over its members or others.

[15] A new Revision 4 https://csrc.nist.gov/publications/detail/sp/800-63/4/draft) is currently underway; draft version was published for comments in June 2020.

identity. IAL3 explicitly requires physical presence and verification of identifying attributes by an authorized and trained Credential Service Provider (CSP) representative; according to the SP, physical presence can also be achieved via remote identity proofing, as long as specific requirements are met.

The SP makes a distinction between supervised and unsupervised remote identity proofing. The former is an equivalent approach to in-person proofing and requires a robust set of features. This includes high-resolution video monitoring through an agency-controlled device (e.g. not an applicant's personal phone), a trained operator on the other end of the video, and a number of other security controls. If there are met, supervised remote identity proofing can achieve IAL3. Supervised remote identity proofing is also perfectly fine for IAL2. Unsupervised remote proofing can be used for IAL2 but not IAL3. It does not require that a remote operator participate in the session with the applicant, and typically involves commodity hardware and services that users and agencies can easily access.

Even though it is a national guideline targeted for US governmental agencies, SP 800-63 is understandably considered and consulted as an international standard with regards to digital identity, including remote identity proofing. According to our survey, in some member states, conformity assessments performed against [NIST SP 800-63] are considered to evaluate conformance criteria until a specific regulation for remote identity proofing is developed.

3.4 NATIONAL LEVEL LAWS, REGULATIONS AND GUIDELINES

This section provides a summary of the different status quo in European countries with regards to their remote identity proofing laws, regulations and practices. It allows quick understanding and comparison while it illustrates the fragmentation since different approaches, rules and adoptions exist among European countries.

When asking conformity assessment bodies "*What are the main difficulties / challenges of evaluating remote identification services / products?"*, most of them (more specifically 80% of the replies) answered the lack of harmonized minimum requirements and/or standards at EU level or even the existence of contradictory national requirements (in few cases). In particular, 40% of the replies highlighted the difficulties in evaluating an enormous variety of remote identity proofing solutions (see Section 2 for different methods) without specialized technical guidelines and standards which cover the process in its entirety

When asked to describe the auditing methodology and standards used for the different types of remote identity proofing (video with operator, remote automatic, etc), the majority of CABs pointed to [eIDAS] and [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2] standards for the issuance of qualified certificates; and [eIDAS] and [CIR 2015/1502] for the issuance of eID. On top of the above, the CABs consider any applicable national regulations, international standards, such as the [NIST SP 800-63] to cover specialised topics, and technical guidelines of other member states, such as the those of Italy and Germany. In some countries, auditing of a remote identity proofing method as a standalone service is available; such a modular evaluation minimizes the overlap between audits, for example when integrating identity proofing services offered by an IPSP to multiple TSPs and banks. Figure 7 presents a geographical map of the current use of remote identity proofing in the provision of regulated services (e.g. trust services, banking, public administration). A similar map, restricted only to the provision of trust services, is presented in Figure 8. There are countries which already make use of such methods and others which are more of "late adopters" (Annex A presents many details for the current regulatory framework in each country). Table 2 presents the current status of European countries with respect to the adoption of laws, regulations, or guidelines specifically for remote identity proofing. Note that there are less countries who have issued national rules compared with the number of countries in which remote identity proofing is practiced.

Comparing the map of countries which exercise, one way or another, remote identity proofing, with Table 2, one may notice that some supervisory bodies have interpreted the lack of national law as not forbidding remote identity proofing practice, whereas others have interpreted it in a stricter manner. This should probably be attributed to the current expression of article 24.1(d) of [eIDAS]. On the question "*What is the current status and the path to improve harmonization of requirements, expectations and processes (for remote identity verification) between the different MS?*" most SBs answered that a clarification of article 24.1(d) of Regulation (EU) No 910/2014 [eIDAS] is needed, as well as European standards on remoted identity proofing. Several pointed the need for an implementing act on how to fulfil the requirements of article 24.1(d) and one proposed to remove the "as recognized on national level" from article 24.1(d). The importance of collaboration between the MSs was also emphasized as well as continuously evaluating the technical development in the area of remote identity proofing. It was also suggested to define requirements for physical identity proofing, and to clarify if the "physical presence" in article 24.1(a) means physical contact between the applicant and the identity proofing operator. It was also not clear for every SB if national recognition of identification methods is compulsory or just optional to allow flexibility. The current study confirms that there are different approaches between the countries with regards to the acceptance of remote identify proofing methods as summarised in Table 3. A more detailed presentation of the information gathered from different countries on this topic is available in Table 4. This presents the current status of remote identity proofing in those European countries for which we received feedback (by the respective national supervisory body).

Table 2: Specific national rules for remote identity proofing

National laws / regulations / guidelines	Countries
Issued	Germany, Greece, Italy, Luxembourg, Portugal, UK
In progress	France, Malta, Romania, Spain
None	Albania, Austria, Belgium, Bulgaria, Cyprus, Estonia, Finland, Lithuania, Netherlands, Serbia, Sweden
Temporary measures to deal with the pandemic crisis	Poland, Norway

Table 3: Allowed remote identity proofing methods per European country[16]

Remote identity proofing method	Countries
Video with operator	Austria, Belgium, Bulgaria, France, Germany, Greece, Italy, Luxembourg, Poland, Portugal
Remote automatic	Bulgaria, Estonia, Greece, Norway
Combined methods	France (underway), Spain (underway)
Other/unknown	Austria, Finland, Latvia, Lithuania, Netherlands, Romania, Sweden, UK

[16] This table reports on the use of remote identity proofing methods in regulated sectors. For private use or other non-regulated cases, several other methods may also apply.

Figure 7: Geographical map of the remote identity proofing practice for any (regulated) purpose

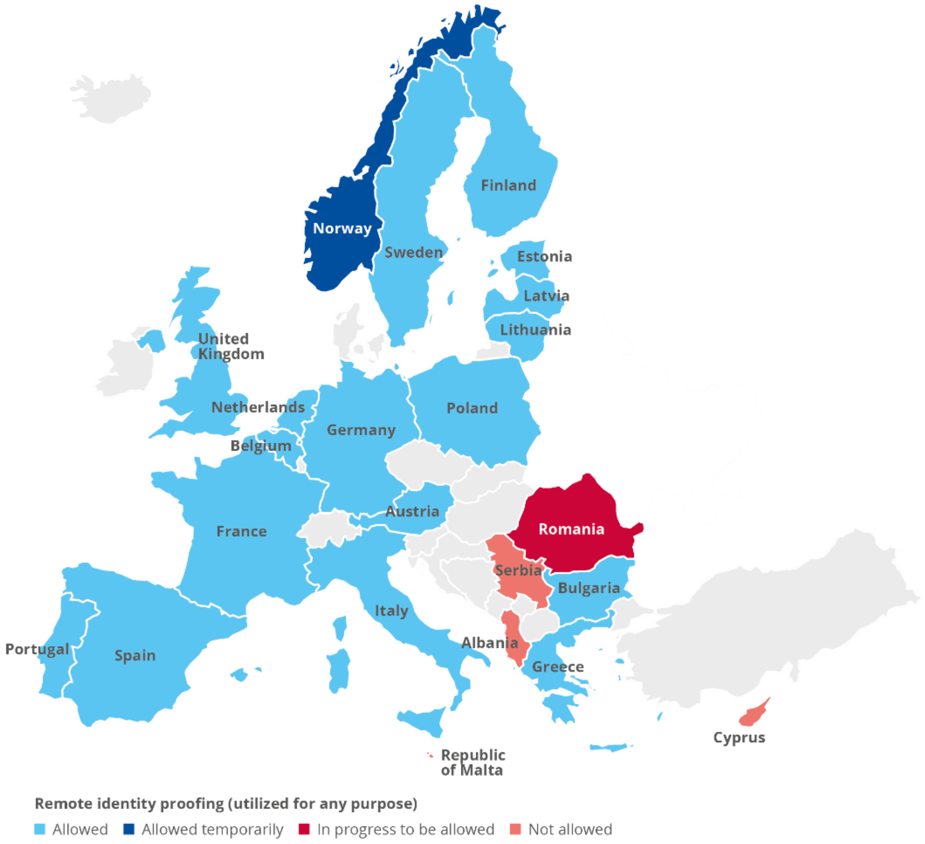


Figure 8: Geographical map of the remote identity proofing practice for trust services only

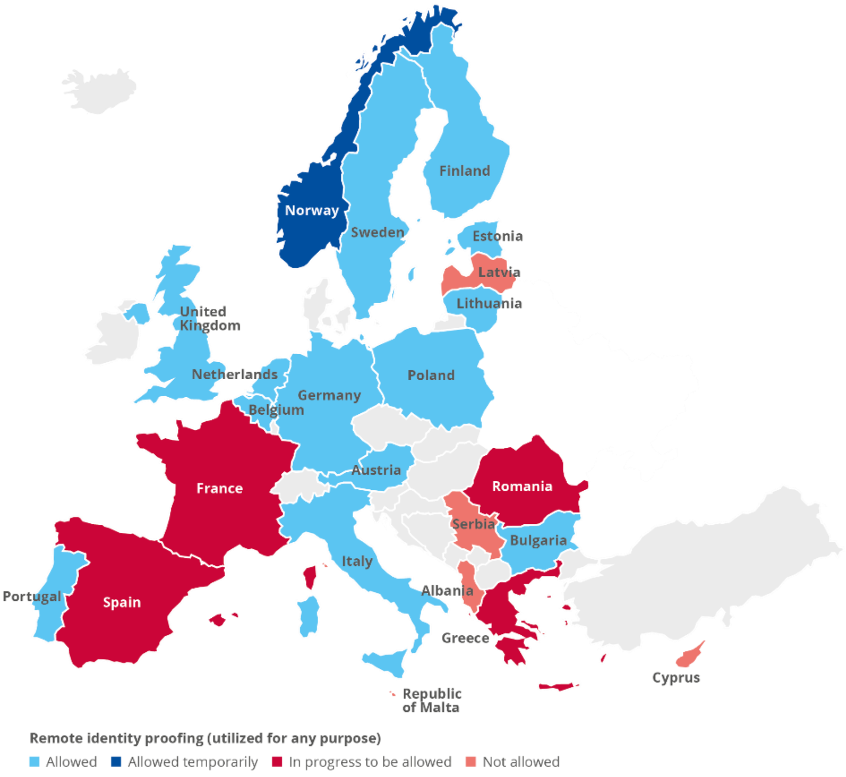


Table 4: Consolidated remote identity proofing status in European countries (November 2020)

Country	National legislation/rules for (Remote) Identity Proofing	Remote Identity Proofing methods allowed (short description)	Criteria/standards
ALBANIA	None specific to remote; law for transposition of eIDAS	None	ETSI standards (EN 319 401, EN 319 411, EN 319 412-1, EN 319 421)
AUSTRIA	None specific to remote; partially covered by national regulation	Decided on a case-by-case basis	Legal requirements, ETSI EN 319 411-1/2
BELGIUM	None specific to remote	Video with operator	eIDAS related ETSI standards (EN 319 401, EN 319 411-1/2)
BULGARIA	None specific to remote	Remote identity verification solutions based on videos, pictures, traditional ID documents	eIDAS related ETSI standards (EN 319 403, EN 319 401, EN 319 411-1/2, EN 319 421, EN 319 102-1, etc.)
CYPRUS	None specific to remote	eID and traditional ID documents only	eIDAS related ETSI standards (EN 319 401, EN 319 411-1/2, EN 319 412-1 to -5)
ESTONIA	None specific to remote; generic law only for national ID documents	eID/traditional ID documents, AI based/human based	eIDAS, eIDAS related ETSI standards (EN 310 403, EN 319 401, EN 319 411-1/2), CAB specific criteria, ISO/IEC 19795-1:2006, ISO/IEC 30107-3: 2017
FINLAND	None specific to remote; generic law only for the accepted ID documents	Allowed; eID/traditional ID documents	None specified
FRANCE	None specific to remote; a new joined decree to transpose AML5 will enable a national certification framework	Will be defined for LoA Substantial: hybrid approach synch/asynch, dynamic presentation solutions Video with operator combined with biometrics algorithm	Draft on requirements for remote identity proofing services is for public review to be published in March 2021. eIDAS, ETSI EN 319 411, ISO 27001, ISO 27002, ISO 27005 and ISO 30107 are also considered
GERMANY	Confidence Services Act	Human based using videos according to linked Order, eID and traditional ID Documents, only synchronous. In the context of qualified certificates, method is usable only for a single transaction.	Confidence Services Act and related additional audit criteria (not publicly available)
GREECE	National laws and regulations issued per sector: currently limited to banking and citizen services. For trust services, recent law provides legal basis; a Ministerial Decree is expected to enable use in trust services.	Banking: video conference or dynamic selfie. Citizen services: video conference. Trust services: Soon to be allowed; SB suggested human based synchronous video identification.	Banking: requirements of the KYC regulation of the banking authority. Citizen services: requirements of national law; not audited. Trust services: requirements of the upcoming Ministerial Decree, plus all other requirements regarding security, GDPR etc.
ITALY	Guideline of the SB with the minimum requirements, no national law	Synchronous remote A/V; asynchronous version to be authorized by the SB soon	Evaluation first by CABs and then by the SB (AgID) based on in-house processes and national requirements

LATVIA	National guidelines limited to the banking / financial sector	Photos against ID	N/A
LITHUANIA	None specific to remote	No restrictions by the national legislation; assessment would be done on a case-by-case basis	eIDAS, SB regulation: Description of the Procedure for Verification of personal identity and additional specific attributes, ETSI standards (EN 319 401, EN 319 411-1/2)
LUXEMBOURG	National law on electronic commerce and trust services	Video identification methods with human interaction	QTSP Procedure n° 005A Recognition of other identification methods at the national level (issued by the national standardisation body - ILNAS)
MALTA	None specific to remote; in progress to create national legislation	None at the moment; aim to be technology neutral, yet ensure equivalency to physical presence	N/A
NETHER-LANDS	None specific to remote; generic law only for national ID documents	No restrictions by the national legislation	eIDAS, national legislation, existing ETSI standards
NORWAY	None specific to remote	Remote automated onboarding based on NFC reading of passport, selfie, biometric face recognition (temporary measure due to the pandemic crisis)	National specifications are being prepared
POLAND	National regulation for use in public electronic identification scheme	Human based, eID documents, video, and must be synchronous, additional verification in public registers, capture recording	Ministerial order to set organisational requirements for public electronic identification scheme Financial Supervision Authority guidance for financial institutions
PORTUGAL	National regulation for use in trust services	Human based, eID documents, video, and must be synchronous	Same national regulation defines the requirements for the service and for the conformity assessment
ROMANIA	None specific to remote	Technical requirements under public consultation: real-time video recording, verification of security elements of the ID card, capture of pictures	The upcoming technical requirement will take into account eIDAS related ETSI standards; Evaluation first by the CABs and then by the SB RO (ADR) based on in-house procedure and national requirements
SERBIA	None specific to remote	Physical presence is required for issuing medium and high assurance level of the eID schemes	N/A
SPAIN	National regulation foresees that the specification of the technical requirements for remote identification may be done by ministerial order	Asynchronous video identification with final human decision and synchronous video identification methods with human interaction	Ministerial order is being prepared to set technical requirements of remote identity proofing
SWEDEN	None specific to remote	No restrictions by the national legislation	eIDAS, ETSI standards (EN 319 401, EN 319 411-1)
UK	National guidelines	Risk-driven approach; all methods are evaluated using a scoring system 1-5 (more granular then LoA)	National guidelines; detailed code of practice is underway to act as supporting reference

3.5 DATA PROTECTION

Identity proofing evidence needs to be stored and processed, to prove that the identity proofing was correctly done, and they contain, for example, copies of identity documents, or videos of the applicant. This data is not needed only for the process of a single identity. For example, effective testing a solution may entail large and different sets of evidence, including actual data.

Protection of personal data is regulated at least in the European Union by the Regulation (EU) 2016/679 [GDPR]. Most DPAs have already been consulted or involved at some point/degree in remote identity proofing concepts. This may include the issuance of guidelines, general consultations, consultations in the preparation of eID schemes and supervision tasks. Few European DPAs have also been consulted for evaluating national laws and regulations specifically for remote identity proofing. Apart from trust service providers and financial institutions, consultation requests may also originate from healthcare organizations, public administration and others.

Banks and TSPs, when asked *"What kind of evidence is stored?*", "*Is this evidence stored by your organisation, an external provider or are they destroyed?*" and "*Are there any national specific regulations?*", stated that the main evidences stored are pictures, videos, but also private data and logs and verification results. Most of them stored evidence internally but some stored it internally and externally. They followed the requirements from their regulator.

When asked "*Have you been already consulted for services providing/evaluating remote identity verification? If yes, which type of sector (trust services, banks, public administration)?*", 3 out of the 4 European DPAs were already consulted for services providing remote identity proofing, some of them on the implementation of the nation eID means, on remote identity proofing in the field of heath care or more specifically on the usage of video identification. On the question ""*Remote identification needs to collect information/records (like video stream, scans/pictures of documents and faces) from processes. What is the position of GDPR regulators regarding this information?",* their general point of view is that assessment is needed to decide which data is really necessary and that no unnecessary data should be kept. Also, data should only be kept as long as needed.

Remote identity proofing by definition involves the collection of large amounts of information/records, including video streams, scans/pictures of documents and faces, etc. All this information are personal data and need to be processed in accordance with the overall principles of the GDPR. In particular, data processing by Identity Providers for the purposes of electronic identification relies on the legal ground provided for by Article 6(1) of the GDPR. Moreover, in case remote identity proofing entails special categories of personal data, such as biometric data, processing is subject to Article 9 of the GDPR and, in some member states, further conditions.

According to the DPAs, only essential data should be processed and it should not be the rule that remote services by-default requires to store additional data. For example, DPAs suggest that if physical meeting is not needed to be recorded, then the same kind of remote meeting should not be recorded either. Additionally, the subject must be aware of the applicable data protection terms, or, depending on the context, explicit consent might be required.

On the other hand, most schemes, including [eIDAS], require the processing and retention of '*sufficient amount of data to prove the validity of the identity proofing'*. For example, not storing the data in a classical verification with physical presence is considered as one of the weakest points of such a process, since there is no later evidence if the check was correctly done. In situations where stakeholders need to be convinced that remote identity proofing solutions are trustworthy enough, it might be necessary to keep more data stored and for a longer period. Given the lack of standardization for remote identity proofing, [eIDAS] regulators put additional pressure in the acquisition of more and more data. This clear 'conflict of interests' requires careful balancing; it should be carefully assessed whether any additional data is required and why. Data controller must make an assessment of any kind of processing that is to be used for remote identification, including categories of personal data that would be required for this, and, when necessary, conduct the data protection impact assessment.

Similarly, GDPR does not forbid data controllers to store personal data if such storage is lawful and necessary. Data controller is obliged to assess and identify which data must be stored, how long and why. In general, the collected data may only be stored as long as it is needed/required. Afterwards, this data must be deleted immediately, instead of retaining 'forever'.

Effective testing of remote identity proofing solutions may entail (in some cases) using/processing real and fake user IDs, archiving results, analysing, etc. This contradicts with the Privacy by Default principle (Article 25 [GDPR]), which requires data involved in testing solutions not to be related to real persons. Priority should always be put on usage of fake data for the testing, unless usage of fakes is not possible and would not meet the purpose. The necessity of using real personal data should always be exceptional and careful assessment should be made in advance. If it is unavoidable to use real data for the tests, it must be protected against misuse by appropriate technical and organizational measures.

3.6 SELF-SOVEREIGN SYSTEMS

In recent years, a new paradigm for the management of digital identities has come to attention, based on the adoption of blockchains and distributed ledger technologies. This paradigm, called Self-Sovereign Identity (SSI) is based on the idea that an identity subject should manage directly his/her identity attributes. These attributes, to be of value, will somehow be certified by a trusted party, but after this the identity subject will be free to present them to any online party during any transaction deemed of value.

SSI is essentially a user-centred management of digital identity attributes, that could employ and benefit a distributed ledger to provide a censor and fault-resistance store of such identity attributes (credentials). By using advanced cryptography techniques, including Zero-Knowledge Proof (ZKP), the owner of such credentials could create a synthetic, cryptographically secure, presentation based on them. A typical example would be that, starting from a birth date, the presentation could just confirm that the subject is an adult without the need to disclose all other information including the exact birth date.

SSI are a promising technology and a more advanced conceptual paradigm for digital identity management, and they possibly have a role in the future eIDAS operational network. For the remote identity proofing process, there are two possible developments and integrations worth noticing. The first relates to the adoption of evidence, stored into a distributed ledger, to be evaluated during the process to support an applicant's claim. The second relates to the actual storage of some or all of the attributes coming from the remote identity proofing process into a distributed ledger for later use.

SSI is still under heavy research, development and standardization activities. The interested reader could check [SSI-EIDAS] for information about possible extensions to the [eIDAS] Regulation to integrate with SSI systems, and [TR23249] for the ISO/TC 307 work in this area. The latter, at the time of writing, is a relatively mature working draft that should be published mid-2021.

4. RISK MANAGEMENT

4.1 INTRODUCTION

Article 19 of [eIDAS] states that qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. This requires TSPs to conduct a risk assessment to ensure that the level of security is commensurate to the degree of risk, and to minimise the impact of security incidents. Many standards already provide guidelines for risk management. One of them is [ISO/IEC 27005]. It provides guidelines for information security risk management in an organization, supporting in particular the requirements of an information security management system (ISMS) according to [ISO/IEC 27001]. This section aims at presenting more specific and practical guidelines for TSP/IDP regarding the management of risks posed to the security of their identity proofing methods based mainly on the requirements of [ISO/IEC 27005] and the risk management process outlined in the [ENISA Security Framework for TSPs].

The methodology adopted to present a more practical approach to apply the risk management process, is done on the basis of examples presenting two different identity proofing processes (Table 5), which were identified in the questionnaires as typical processes. This document provide only an example on how to perform a risk analysis. Every system is different and the corresponding risk analysis must be adapted accordingly.

Table 5: Examples of Identity Proofing Processes

Example 1 : Remote video with the operator for Qualified Certificate registration	Example 2: Remote automatic to enrol a new customer to a service
Process Description	
1. Initiation: The applicant approves the identity proofing policy, and the terms and conditions	**1. Initiation:** The applicant receives the link to download the mobile app supporting the process and launches it. After the installation, the applicant approves Policy, and Terms and Conditions
2. Evidence Collection, Validation and Binding The applicant starts the video call with the operator: a) a. The operator follows the script to check the ID document and binds it to the applicant b) The operator confirms the phone possession by SMS	**2. Evidence Collection, Validation and Binding:** The applicant follows the process: a) captures the identity document which is sent to the system that automatically retrieves the applicant's identity and authenticates the identity document. b) does a dynamic selfie – the captured information is sent to the system that compares the selfie to the picture extracted from the identity document.
3. Issuing identity proof: The operator issues the identity proof	**3. Issuing identity proof:** The system automatically issues identity proof and provides it to the requesting service
Processed Data	
Video recording of the chat session **Private data of the applicant** **Issued proof of the identity**	**Captured images of identity documents** **Captured image of the applicant** **Private date of the applicant** **Issued proof of the identity**

The first example is an identity proofing process using **video with operator** (see section 2.2.2) to identify a physical person (applicant) with the goal of issuing a qualified certificate. This example describes the process already established by many TSPs and used for the issuance of the qualified certificate. This process is based on a video call between an applicant and an operator, where the operator applies a script to collect evidence, validate it, and bind collected evidence to the applicant. The final step of the process is identity proof used by qualified TSP to issue a qualified certificate. The process in this example has applied the following security features: a video recording of the chat session, mobile device SMS based proof of possession, and operators have proof of expert knowledge in the context of identity proofing.

The second example is an identity proofing process using the **remote automatic** method (see section 2.2.3) to enrol a new customer to a service. A remote automatic process, supported by AI is mentioned by TSPs responding to the questionnaires as a planned solution, but most of the banks that have responded use it as the first phase of enrolment to the bank. Communication between the operator and the applicant is performed through an application downloaded to the web browser of the mobile device possessed by an applicant. The process is initialised on the applicant site by the link with unique identification number sent through SMS. The applicant following the link opens the application and is guided automatically to follow the different steps of capturing the ID document image, proofing liveness and capturing image. All computations are done on the backend site of the operator which issues the proof and sent it to the requesting service.

4.2 RISK IDENTIFICATION

[ISO/IEC 27005] states that *"the purpose of risk identification is to determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen"*.

The following sections present risk identification on the basis of the two examples of identity proofing processes described above. The discussion of these examples will focus only on the risks associated with the identity proofing process and it will not identify other operational and technical processes and data that are part of most electronic service providers e.g. human resources processes, system maintenance. It is assumed that these general security controls are already in place. The following sections describe the steps for identifying risks (see [ENISA Security Framework for TSPs] for further details): 1. identification of assets, 2. Identification of threats, 3. Identification of vulnerabilities, 4. Identification of existing security controls and 5. Identification of consequences.

4.2.1 Identification of assets

Based on [ISO/IEC 27005], it is suggested to distinguish between two types of assets:

- **Primary assets** which are processes and information.
- **Secondary assets**, which support primary assets.

The main identified asset in the context of identity proofing is the identity proofing process itself and all evidence processed as part of this process. This asset can be decomposed into more elementary ones for deeper analysis of key steps of the process (as described in section 2): Initiation, attribute and evidence Collection, attribute and evidence Validation, binding and verification, issuing of proof and additional related processes (e.g. OCR recognition, biometric validation).

Processed and stored data and evidences are also recognised as primary assets. The following list presents the most common examples of those assets:

- Private data of the applicant
- Photos (scans)

- Video recording
- Data sent by the applicant in the initiation process
- Data received by the applicant as a result
- Identity proof / assertion.

The identity proofing process is based on many supporting assets which also should be identified, in particular:

- computer systems used for conducting the process including network and software
- the operator workstation equipped with camera and voice devices
- the applicant workstation or mobile device
- communication channels
- internal databases (e.g. logs, archives)
- external registers (e.g. register of stolen identity documents)
- supporting services from external providers (e.g. certificate validation service).

In Table 6 the main primary assets identified for each of the two different identity proofing processes described in Table 5 are given.

Table 6: Example identification of assets

Example	Asset	Example of primary assets
Example 1	Asset 1.1	**Process: The "Video with operator" process.** This process based on the script during the video call between the operator and the applicant
	Asset 1.2	**Data: Video recording** captured during the video call
Example 2	Asset 2.1	**Process: Initiation step** of the process. In this step an individual link containing process identifier is sent to the applicant
	Asset 2.2	**Data: Private data of the applicant**. In this example the private data is captured and optically recognised from the MRZ zone of the ID document

4.2.2 Identification of threats

Risk identification requires awareness of what threats may occur in relation to each identified asset. For the completeness of the risk assessment, the largest possible number of threats (including unlikely ones) should be taken into account.

The operators may consult existing threat catalogues and statistics available from industry bodies, national governments, insurance companies, standardisation bodies. For this purpose, ENISA listed risk assessment tools[17]. Another relevant source is the annual analysis report on the trust services security incidents (with regards to Article 19 of eIDAS)[18].

Table 7 presents examples of potential threats in relation to identified assets. Annex B provides a list of threats related to the identify proofing process which was drawn up by analysing the replies received from the stakeholders as well as other technical documents.

[17] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools
[18] https://www.enisa.europa.eu/news/enisa-news/annual-report-on-trust-services-security-incidents-in-2019

Table 7: Example of threats identification

Example	Asset	Potential threats
Example 1	Asset 1.1 “Video with operator” process	[T_DOC_STOLEN] - Stolen identity document accepted as an evidence [T_DOC_FAKE] Counterfeited or forged identity document accepted as an evidence
		[T_BRIBERY] Bribery of an operator leads to an identity wrongly validated
	Asset 1.2 Video recording	[T_DOC_VIDEO] Video presented instead of genuine document without being detected [T_REPLAY] Interception and replay of captured data is possible and not detected
Example 2	Asset 2.1 Initiation step of the process	[T_PHISHING] User accepts process initiation from attacker
	Asset 2.2 Private data captured form MRZ	[T_DOC_SOFTWARE_PERFORMANCE] Software capability to authenticate identity documents not at the required level.

4.2.3 Identification of vulnerabilities

Identifying possible vulnerabilities is a key step in risk management, as they constitute the possible weaknesses of an asset or group of assets (e.g. all assets related to personnel) that can be exploited by one or more threats. An example of vulnerability in remote identification systems is the inability to verify security features visible in UV light, which may allow the use of a forged identity document. The possibility of exploiting vulnerabilities to the occurrence of a threat is limited by the use of technical and organizational controls. TSPs proving feedback through the questionnaires pinpoint the need for regular and often vulnerability scans and penetration tests. Table 8 presents examples of the vulnerabilities corresponding to identified assets and threats.

Table 8: Vulnerabilities identification example

Example	Asset	Potential threats	Vulnerabilities
Example 1	Asset 1.1 “Video with operator” process	[T_DOC_STOLEN] [T_DOC_FAKE]	An operator-guided script-based video process makes it possible to use a stolen document. Lack of tools possible to use by an operator allowing verification of the authenticity of the document.
		[T_BRIBERY]	The process allows confirmation of fake identity if an operator accepted a bribery offer.
	Asset 1.2 Video recording	[T_REPLAY]	Video recording if stolen can be reused in other processes.
Example 2	Asset 2.1 Individual link sent	[T_PHISHING]	A fake link to the identity proofing process can be without verification accepted and used by a non-aware user.
	Asset 2.2 Data captured form MRZ	[T_DOC_SOFTWARE_PERFORMANCE]	Data captured from MRZ does not include diacritic letters or can be truncated leading to wrong identity proofing.

4.2.4 Identification of existing security controls implemented

The list of potential vulnerabilities should be contrasted with the list of existing controls. Existing controls are the means of mitigating the likelihood of exploiting potential vulnerabilities as they decrease the level of exposure. The operator should conduct a gap analysis regarding the identification proofing method it uses in order to determine for which vulnerabilities no sufficient controls are in place.

Basing on responses to the questionnaires banks implement security controls basing on requirements provided by their competent authorities. Some Supervisory Bodies also published lists of required security controls for TSPs. These security controls are intended to reduce the possibility of exploiting the vulnerability or even completely prevent its use. Table 9 presents examples of controls; the non-exhaustive list of countermeasures is included in annex C.

Table 9: Security controls identification example

Example	Asset	Potential threats	Vulnerabilities	Existing controls
Example 1	Asset 1.1	[T_DOC_STOLEN] [T_DOC_FAKE]	An operator-guided script-based video process makes it possible to use a stolen document. Lack of tools possible to use by an operator allowing verification of the authenticity of the document.	[S_RECORD_SESSION] Recording and tamper proof storing of the audio and video session
		[T_BRIBERY]	The process allows confirmation of fake identity if an operator accepted a bribery offer.	[S_OPERATOR_VETTING] Operators must be vetted as they perform a security sensitive role
	Asset 1.2	[T_REPLAY]	Video recording if stolen can be reused in other processes.	[S_MORE_EVIDENCE] Define a list of supplemental evidences to strengthen the process, manage corner cases, or when doubts arise
Example 2	Asset 2.1	[T_PHISHING]	A fake link to the identity proofing process can be without verification accepted and used by a non-aware user.	[S_AWARENESS] Have a linear and understandable process.
	Asset 2.2	[T_DOC_SOFTWARE_PERFORMANCE]	Data captured from MRZ does not include diacritic letters leading to wrong identity proofing.	[S_LIST_ID_DOCS] Define the list of identity documents that are allowed for the process.

4.2.5 Identification of consequences

The exploitation of a vulnerability of an asset by a threat may result in consequences, in particular the loss of confidentiality, integrity, and availability on an asset. The consequences in terms of a single asset may have a further impact on the operation of the entire service, in particular operational, legal, financial, reputational, or human consequences.

In addition, the impact can be not only to relation between service provider and user but also on third parties; therefore it is important to identify the impact on relying parties and all users including physical persons and organizations.

Considering that identity proofing includes the processing of personal data, special attention should be paid to the legal effects related to the provisions of the GDPR Regulation. Moreover, the consequences may affect individuals or groups, or the entire dataset and they may vary for each incident scenario.

Some possible examples of consequences linked to incident scenarios are listed below:

- Impact on a single transaction with a single user if identify proofing is used for completing business transactions. This can cause financial consequences.
- False proof of identity in process of qualified certificate issuance has an impact on all transactions where a qualified certificate was used. This has an impact on the operations of a QTSP who is responsible for any damage to relying parties. This can cause legal and financial consequences.
- Identity proofing service unavailability can have an impact on clients and cause legal and reputational consequences.

4.3 RISK BASED SECURITY

Determining the level of risk is the task of the risk analysis process. As a result of the estimation carried out in accordance with the established methodology, values are obtained that allow for the assessment and indication of risks that should be mitigated, accepted, avoided or transferred. One of the outcomes of risk analysis is further risk treatment which can be the application of new security controls (Table 10).

Table 10: Risk treatment example

Example	Asset	Potential threat	Risk treatment
Example 1	Asset 1.1	[T_DOC_STOLEN] [T_DOC_FAKE]	NEW CONTROLS: [S_MORE_EVIDENCE] Define a list of supplemental evidences to strengthen the process, manage corner cases, or when doubts arise [S_LIST_ID_DOCS] Define the list of identity documents that are allowed for the process
		[T_BRIBERY]	NEW CONTROL: [S_RANDOM_OPERATOR] Assignment of registration officer for a specific remote identity proofing should be not predictable.
	Asset 1.2	[T_REPLAY]	NEW CONTROL: [S_RANDOM_ELEMENTS] Introduce some random elements in the identity proofing

Example 2	Asset 2.1	[T_PHISHING]	NEW CONTROL: [S_STANDARDS] Apply standards whenever possible, and follow their development.
	Asset 2.2	[T_DOC_SOFTWARE_ PERFORMANCE]	NEW CONTROLS: [S_MONITOR] Define and implement a monitoring process. [S_TEST_SW_PERFORMANCE] Periodic software performance testing. [S_MORE_EVIDENCE] Define a list of supplemental evidences to strengthen the process, manage corner cases, or when doubts arise

Due to the fact that the [eIDAS] regulation points physical presence as the basic reference model for the security level of identity proofing, risk analysis can be used to compare physical presence and remote processes. In such a case, the risk analysis is based on the analysis of both processes and the comparison of their risks and during this analysis is important to assign the same measures to both processes and obtain an objective result.

5. GAPS AND RECOMMENDATIONS

5.1 OVERVIEW

Regulatory initiatives like [eIDAS] and [AMLD5] have made possible significant breakthroughs for identity proofing. At the same time, several challenges, open issues and difficulties have been observed from practicing under the existing set of requirements.

With regards to remote identity proofing, during this study there have been identified several areas of improvement. For example, there is a significant divergence between rules set by different MSs in their jurisdiction (i.e. lack of harmonization) and a profound demand of specialized standards, boosted by the increasing interest of trust service providers, financial institutions et al, the rapid technological evolvement and the pandemic crisis.

5.2 IDENTIFIED GAPS

Relevant gaps could be organized in areas as follows: gaps which relate to the current legal, regulatory and standardisation context and technical gaps which relate to the technical aspects.

5.2.1 Legal and standardization level

The analysis of information gathered confirms that while a lot of material has been created for the provision of services which use identity proofing as an entry point, only fractions of the remote identity proofing practice have been addressed. The lack of common regulatory requirements and commonly accepted standards between MSs has resulted in a large number of national initiatives which struggle with multiple challenges. Naturally, one may find common elements and diversities in the existing approaches and requirements.

Digital identities, when bound to actual persons at a proper assurance level, serve as a trust anchor and enabler of several kinds of transactions, in the private or public sector, within a country or cross-recognized. Currently, one may find a cross-recognition of eID, trust services and related transactions, but there are no common acceptance and rules for the trust anchor: the remote identity proofing process / service. This lack of harmonization was highlighted in the vast majority of answers received from SBs and CABs and relates to several areas, as illustrated in the figures of Section 3: legislation, acceptance, practice, rules and supervision.

The interoperability and mutual recognition framework introduced by eIDAS relies on uncoordinated national laws and technical specifications, which naturally results in tension (if not contradiction). This leads to regulatory arbitrage opportunities favouring the least demanding national specifications, especially when combined with single market rules (such as the banking passport). If this issue remains unresolved, the tension is likely to prove unsustainable in the long term.

For example, under [AMLD5] a bank may use qualified signatures for remote customer on-boarding and KYC as allowed. This bank, residing in one MS, is forced to do remote onboarding based on qualified signatures with certificates issued by a TSP residing in another MS, because in the country where the bank resides, remote identity proofing for the issuance of qualified certificates is not allowed. This market distortion puts at a disadvantage the TSPs of the less permissive country. At the same time, even if the SB of the MS where the bank resides considers remote identity proofing as less secure than "physical presence", it will not be able to protect its citizens from this technique since the remote identity proofing practice is indirectly used. From the point of view of a single citizen, being forced to be present in person during the original identity proofing process, or the subsequent renewals, results in a lot of unnecessary complications especially after temporarily moving or staying in a country different than those of first emission.

A significant portion of the diversity can be attributed to the approach of [eIDAS]. The first reason is that by design, article 24.1(d), which is used as the legal basis for several remote identity methods, refers to their recognition at the national level. Naturally, this has set the stage for the fragmentation observed by analysing the current landscape in Section 3. The second reason is that Article 24.1 of [eIDAS] allows several different interpretations regarding identity proofing methods (as analysed in Sections 2 and 3):

- Article 24.1(a) requires “physical presence”. This has been interpreted in some cases as a method which requires the applicant to be physically present, but not necessarily on-site with the operator. Indeed, in some countries, a remote identity proofing process is seen as a legitimate case of physical presence.
- Article 24.1(b) refers to remote proofing. It requires electronic identifications means which were issued after “physical presence” and which meet “the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’”. In some cases, this has been interpreted as a clause which requires the use of notified eID means, whereas in other cases any electronic identification mean (e.g. bank identity) which is bound to the person and meets the identity proofing requirements of [CIR 2015/1502] at LoA ‘substantial’ or ‘high’.
- Article 24.1(c) refers to identity proofing “by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b)”. This implies that the TSP is able to identify and accept (for identity proofing) only certificates which were issued after points (a) - (b), but not points (c) – (d). Apart from the technical feasibility, such a distinction is not well understood by all stakeholders (SBs, CABs, TSPs, IDPs).
- Article 24.1(d) refers to “other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body”. Some SBs have interpreted the first sentence in a strict manner: specific legislation is required to allow remote identity proofing; in some other countries, the lack of forbidding legislation is seen as sufficient and thus only a conformity assessment is requested. Section 3 shows that between countries which apply remote identity proofing, only some have done this by issuing specific legislation and/or normative requirements.

Apart from the ambiguity or openness of the language in Article 24.1, one of the main characteristics of the above difference is the level of strictness or creativity that SBs and TSPs apply when interpreting a legal document such as [eIDAS], without guidance (e.g. Commission Implementing Rules) or concrete widely-accepted standards. Some SBs define a "module" audit for an identity proofing method, but others allow only complete evaluations in conjunction with the trust service; this practice decreases harmonisation and puts at disadvantage providers of the less permissive country. Many respondents to the questionnaires have highlighted the lack of specialised standards which address the subject of remote identity proofing. As seen in Section 3, 80% of the CABs have denoted the lack of harmonization as a problem, and 50% raised the issue for the lack of standards.

At the same time, some countries that have authorized emergency adoption of this process during the COVID-19 lockdowns fear that the process could not be very secure and they would prefer to confront themselves with European guidelines and standards. So, the problem can be better described as such: the lack of specialized standards that cover the service in a comprehensive and holistic manner and that are accepted under the selected legal regimes (e.g. [eIDAS], [AMLD5]).

Finally, it is quite problematic to compare different methods employed in different MSs for remote identity proofing, as they are not always framed in the context of [eIDAS] or as result of a specific risk analysis process. This issue is enlarged by the difficulty of establishing a common understanding of the different concepts and methods; for example, the difference between electronic identification (“process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person” [eIDAS]) and remote identification with biometrics (remote identity proofing using biometric characteristics for binding ID attributes to an applicant), video (remote identity proofing using video with operator), bank or fintech identification (remote identity proofing using electronic identification means issued by a bank or a fintech institute) is not always clear to all stakeholders.

5.2.2 Technical level

- **Lack of awareness and understanding** - Remote identity proofing is mostly perceived positively by end users, especially during the COVID-19 crisis. However, in some cases, the users are annoyed by time consuming and complexity of security measures, since they are not aware of the related risks. The faster and the more straightforward the methods are, the better they are received by the clients. Some remote identity proofing methods are stricter than verification with physical presence concerning the acceptable identity document, e.g. expired documents are not allowed, which can lead to dissatisfaction or limited commitment from the user.

  There exists a wide variety of solutions, with a wide disparity not only in technical measures to detect fraud, but with differences in the customer journeys. This might lead to less consistent user experiences, thus making it more difficult for a customer to understand possible fraud. Indeed, higher complexity makes the customers more receptive to accepting changes in the process, and thus more vulnerable to fraud and phishing attacks. Suggested customer journeys could help reduce this risk.

- **Heterogeneity -** Identification documents are an essential part of many remote identity proofing methods, but different countries have different sets of physical documents carrying identification information. [PRADO] shows that many countries in Europe have more than 30 different documents, including identity cards, driving license, residence permits, passports. Specific domains (like higher education) could also have semi-official identity documents. These different documents are the result of different issuing processes and, as such, provide different LoAs that makes them more or less feasible for different contexts (as an example, in many EU countries a driving license could not be considered sufficient to assess the identity of a perspective voter at a polling station). Moreover, the validity of these documents is not uniformly verifiable. [PRADO] provides a list of resources that illustrates this reality.

  This heterogeneity could result in two different kinds of weaknesses for the remote identity proofing process. The first is that less used and more obscure documents could be simpler to counterfeit and more difficult for a registration officer to check due to the lack of proper training, or misevaluated in terms of their intrinsic assurance resulting in a digital identity or certificate that is not grounded on reality. The second problem is that for the operator or the identity proofing service provider it is more difficult to decide how relatively strong is a digital identity or certificate issued from a process based on foreign less standardised physical documents. Also, not all countries manage or provide access to a database of stolen or expired documents.

Reading the chip embedded in electronic documents (eMRTD) may appear to be an efficient way of capturing reliable identity attributes, but such reading, although technically possible, is not permitted by legislation in a uniform manner across the EU. For European identity cards, *regulation 2019/1157 on strengthening the security of identity cards* [SIDCR] unifies the usage of these data. However, this is no uniform legislation for the usage of the date stored in passports. This heterogeneity leads to a difficulty in defining a uniform remote identity verification process.

- **Lack of testing** - Security testing of the solutions (systems, processes) is not always performed to the level required. This may be attributed to the lack of understanding of all security implications, the lack of technical standards and/or the amount of resources and expertise required to perform an effective testing given the technological evolutions pace and the availability of resources and techniques to be used by adversaries. For example, a breakthrough test may require the use of forged or falsified documents, in an attempt to deceive the system or the operator, whereas in most countries the production, possession or use of forged documents is illegal for any purpose.

- **Physical presence per se is not a benchmark -** Using identity proofing with physical presence as a benchmark for remote identity proofing methods is tempting, but it might not be that easy or fair. In fact, it might be psychologically affected or biased by the assumption that pre-existing methods are proven to be secure. Although for remote identity proofing, it might be more difficult to properly verify physical security features of ID document in a video stream or from a picture, in a traditional identity proofing process with physical presence, the actual implementation of the process, i.e. how the operator checks the identity of the person in front of him, is often not disciplined, nor has the operator received specific training. This leads to two relevant elements: the first, that the security of the identity proofing process with physical presence is often assumed to be secure, but is not evaluated against specific metrics and test cases; the second, that the remote identity proofing could be more or less secure than the version with physical presence, according to the specific implementation. It is not the intrinsic nature of the process (with physical presence or remote) that defines the security of the process per se.

5.2.3 Revision of [eIDAS] Regulation

At the time of this writing, the revision of the [eIDAS] Regulation is currently underway. The “EU digital ID scheme for online transactions across Europe” [EU-ID] initiative has published an Inception Impact Assessment that describes three possible options for the revision of the [eIDAS] Regulation:

- Option 1 focuses on the reinforcement of the current regulation in terms of: a) Adoption of additional implementing acts and guidelines (e.g. on identity verification for issuing qualified certificates) on application of specific provisions; b) renewed and stronger commitments from MSs to provide digital identity to their citizens; c) integration and harmonization especially with respect to the Cybersecurity Act; d) allowing private parties to use the eIDAS operational framework.
- Option 2 extends the [eIDAS] Regulation to private parties, introducing new trust services for identification, authentication and for the provision of attributes, credentials and attestations and allowing the provision of identification for devices, within a strong privacy framework to avoid user profiling.
- Option 3 will create a European Digital Identity scheme complementary with eIDAS for citizens to access online public and private services, when identification is necessary.

It is possible that the revision of the current Regulation will combine these three options, that are not mutually-exclusive and could co-exist. From the point of view of this Report, all the options could benefit from the lessons learnt by the different eIDAS stakeholders discussed in this document, as a harmonised remote identity proofing process and relevant security measures would provide valuable insights into all policy options and serve as a valuable building block of the eIDAS architecture.

5.3 RECOMMENDATIONS

The recommendations derive from the stakeholders' responses to questionnaires and the experience of implementing and evaluating remote identity proofing solutions. Most of the recommendations relate to the gaps identified above, thus they are broadly classified into the same areas.

5.3.1 Legal and standardization level

Cross recognition is a key element for an extended use of identity proofing methods in digital services and for cross-border business within the internal market. Cross recognition of identity proofing methods or services means the acceptance of an identity proofing method or service as conforming to the specific regulation in other countries, as soon as it was "accredited" in one country. In case of eID means notified by an EU MS, and for qualified certificates this is already possible based on the [eIDAS] regulation, independent of whether the eID means or the qualified certificate was issued based on remote identity proofing or not.

First of all, to allow successful pan-European cross recognition of remote identity proofing solutions and their usage as part of qualified trust services, it is needed to have standards for the evaluation and rules on auditing remote identity proofing solutions, to be able to evaluate these methods in a comparable way. These standards, in the form of technical guidelines, should be defined at EU level to provide a more or less analogous process for remote identity proofing, fostering the exchange of ideas and cross-fertilization between the different stakeholders, resulting in a more harmonized process. **Evaluation criteria and methodology** should cover the policy and security management areas, the process architecture and also the testing of the actual performance of the service in handling positive and negative cases. Policy and security management are common requirements seen as a good way to achieve mutual recognition. It would also be useful to have some metrics which allows to compare the efficiency of different methods, e.g. the false acceptance rate and the false rejection rate, even if their homogeneous evaluation across solutions can prove to be complex.

To be able to use remote identity proofing solutions in the same way in different countries, it would be needed to have uniform rules on topics like: Is it allowed to use fake identity documents or other fake elements for testing purposes to see if they are recognized? Is it allowed to capture identity attribute by reading the chip embedded in electronic documents (eMRTD)?

In the same way, **article 24(1) of the [eIDAS] regulation should be clarified** to avoid different interpretations on what is "physical presence" (article 24.1 (a)), what eID means are acceptable (article 24.1 (b)), how to verify that a qualified certificate was issued based on article 24.1 (a) or (b) (article 24.1 (c)), and how to evaluate "equivalence assurance in terms of reliability to physical presence" (article 24.1 (d)).

To be able to compare different remote identity proofing methods, it would be useful to have comparable categories. The three different LoAs defined in the [eIDAS] regulation should be the target LoAs of the remote identity proofing. Mapping identity proofing solutions to these levels allows to state that for a specific business process, an identity proofing solution of specific LoA is needed. Note that the future [ETSI TS 119 461] specifies two levels, namely, normalized and enhanced.

Member states should support **automatic and online verification of identity documents**, for example based on a registry of issued, lost and stolen documents.[19] This allows a uniform capability of remote identity proofing services to accept or reject identity documents. Cooperation between MSs and between the different actors within a MS on the topic of remote identity proofing would allow to information sharing and allow for harmonization of the interpretations and requirements. A **central, well-maintained repository with reference material** (laws, regulations, good practices, guidelines) would also be appreciated, in the same way the "Compilation of Member States notification on SSCDs and QSCDs" is maintained.

[GDPR] must be fully embraced by the different stakeholders not only fearing the consequences for not compliance, but as a useful tool that conceptualize the need for security-by-design and privacy-by-design as fundamental blocks for each computing system, including the ones used for the remote identity proofing.

5.3.2 Technical Level

- **Awareness and clear process** - Training (on the operators' side) and awareness (also for subjects) should be duly pursued, especially considering that the process is based on possibly many different identity documents and, from the point of view of users, is relatively new and all of its security implications could be not entirely clear. User awareness on which threats different security measures try to prevent can increase the acceptance of more complex process flows.

  Having a straight forward identity proofing process with a clear user journey does not only increase the user experience, but makes the user less vulnerable to phishing attacks, since the user could more easily recognize differences from the normal process.

- **Uniformity through risk analysis -** Risk analysis should be done in a systematic way, to provide for a secure remote identity proofing process, align the different implementations and result in more comparable outcomes. A regular review of risks and a sharing of security incidents between the different actors should further strengthen convergence for processes with comparable LoAs. This approach facilitates standardization and harmonisation without hindering creativity and innovation which promote user experience and provide additional value to the service.

- **Uniformity through equal access to government data** - Many identity documents store electronic data that can be used and validated during the identity proofing process. Technical support from issuers of those documents is needed to allow identity proofing service providers a secured access to those documents' electronic data (including software libraries and common API interfaces when not standard, CA's certificate, etc.). Access to lost/stolen/invalid identity document online service is also needed to be able to verify the validity of the document produced during identity proofing process.

- **Putting the test first -** Testing should have a relevant role in the analysis, implementation and continuous monitoring of these systems, as it is often overlooked while it is a critical security tool. A good way to compensate for the weakness of specific remote identity proofing methods, is to combine several methods of complementary natures. This can be done for example by combining an asynchronous review of a video by fraud experts and the use of AI to automate data extraction, screening and pre-processing. Another example would be the usage of several identity sources that can be checked and compared against each other. For identity providers

[19] Such registries are typically managed by the state who is the issuer of the identity document. The use of registries which are managed by the private-sector on behalf of the state, or even private-sector registries, could also be considered in case they are legally allowed and provide the same level of assurance as those provided by the state.

targeting different industries it is useful to have different solutions for different use cases, since not all of them have the same security requirements, or the same target applicants.

- Remote identity proofing is a solution that will develop very dynamically in the coming years, therefore it is necessary to **collect information and report incidents**. It is crucial to exchange information about incidents at the EU level, in a similar way to what is done for qualified trust services.

- **Test data –** A remote identity proofing system could leverage AI for cost savings. An AI system is usually trained using a limited set of data, and a EU-wide dataset would be beneficial in terms of actual comparisons of different AI-based systems. This dataset should be defined considering not only the implications in terms of [GDPR] – a general problem with training set for AI – but also how properly represent (in the training set) people from ethnic minorities and with disabilities, to avoid that a poorly trained system is biased against people coming from these groups.

6. BIBLIOGRAPHY/REFERENCES

6.1 ENISA PUBLICATIONS

ID	Description
eIDAS COMPLIANT eID SOLUTIONS	eIDAS COMPLIANT eID SOLUTIONS, Security Considerations and the Role of ENISA, March 2020
ENISA Security Framework for TSPs	Security Framework for Trust Providers, https://www.enisa.europa.eu/publications/security-framework-for-trust-providers/

6.2 APPLICABLE LEGISLATION / REGULATION

ID	Description
AMLD5	Directive (EU) 2018/843 of the European Parliament and of the Council amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('AMLD5') https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843
CIR 2015/1501	Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0001
CIR 2015/1502	Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R1502
eIDAS	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. OJ L 257, 28.8.2014, p. 73–114. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
EU-ID	EU digital ID scheme for online transactions across Europe https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-
FATF-ID-G	The FATF Digital Identity Guidance, issued in March 2020 http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html
FATF-R	The FATF Recommendations as amended June 2019 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

LOA GUIDE	Guidance of the European Cooperation Network on the application of the levels of assurance which support the eIDAS Regulation https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance%20on%20Levels%20of%20Assurance.docx
SIDCR	Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 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:32019R1157
A/CN.9/WG.IV/WP. 164 - UNCITRAL CROSS DRAFT	UNICTRAL Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services – synthesis of comments submitted by States and international organizations https://undocs.org/en/A/CN.9/WG.IV/WP.164
UNCITRAL E-COMMERCE	UNCITRAL Working Group IV: Electronic Commerce https://uncitral.un.org/en/working_groups/4/electronic_commerce
A/CN.9/WG.IV/WP. 162 - UNCITRAL IDM DRAFT	UNCITRAL Draft Provisions on the Use and Cross- border Recognition of Identity Management and Trust Services (A/CN.9/WG.IV/WP.162, April 6-9, 2020) https://undocs.org/en/A/CN.9/WG.IV/WP.162
A/CN.9/WG.IV/WP. 150 - UNCITRAL IDM TC	UNCITRAL Terms and concepts relevant to identity management and trust services, (A/CN.9/WG.IV/WP.150, February 6, 2018) https://undocs.org/en/A/CN.9/WG.IV/WP.150

6.3 STANDARDS AND OTHERS

ID	Description
ANSSI PVID	Prestataires de vérification d'identité à distance - Référentiel d'exigences - Version 1.0 du 19 novembre 2020 https://www.ssi.gouv.fr/uploads/2020/11/anssi_pvid_referentiel_exigences-v1.0.pdf
BSI TR-03147	BSI TR-03147 (v1.0.4) "Assurance Level Assessment of Procedures for Identity Verification of Natural Persons"
CA/BF BR CS	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
CA/BF BR SSL	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
CA/BF EVCG SSL	CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates
CEN 419 241-1	CEN 419 241-1 "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements"
CC	Common Methodology for Information Technology Security Evaluation
ETSI TS 119 431-1	ETSI TS 119 431-1 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".
ETSI TS 119 431-2	ETSI TS 119 431-2 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation"
ETSI TR 119 460	ETSI TR 119 460 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects"
ETSI TS 119 461	ETSI TS 119 461: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects" which will be published after the present report. (for public review before publication)

ETSI EN 319 401	ETSI EN 319 401 (v2.2.1): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
ETSI EN 319 411-1	ETSI EN 319 411-1 (v1.2.2): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
ETSI EN 319 411-2	ETSI EN 319 411-2 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
ETSI EN 319 521	ETSI EN 319 521 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".
ETSI EN 319 531	ETSI EN 319 531 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC 27001	ISO/IEC 27001:2013: "Information technology -- Security techniques -- Information security management systems -- Requirements".
ISO/IEC 27005	ISO/IEC 27005:2018: “Information technology — Security techniques — Information security risk management”
ISO/IEC TS 29003	ISO/IEC TS 29003:2018: “Information technology — Security techniques — Identity proofing”
ISO/IEC 29115	ISO/IEC 29115:2013 “Information technology — Security techniques — Entity authentication assurance framework”
ISO/IEC 30107	ISO/IEC 30107-1:2016 Information technology — Biometric presentation attack detection — Part 1: Framework ISO/IEC 30107-2:2017 Information technology — Biometric presentation attack detection — Part 2: Data formats ISO/IEC 30107-3:2017 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting ISO/IEC 30107-4:2020 Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices
M/460	Standardisation mandate to the European Standardisation Organisations in the field of information and communication technologies applied to electronic signatures https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=442
NIST SP 800-63-3	NIST SP 800-63-3: “Digital Identity Guidelines”
NIST SP 800-63A	NIST SP 800-63A: “Digital Identity Guidelines; Enrollment and Identity Proofing Requirements”
PRADO	PRADO – Public Register of Autenthic travel and identity Documents Online https://www.consilium.europa.eu/prado/en/prado-start-page.html
PRADO GLOSSARY	https://www.consilium.europa.eu/prado/en/prado-glossary/prado-glossary.pdf
SSI-EIDAS	SSI eIDAS Legal Report, How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market
TR23249	ISO Technical Report 23249 “Overview of Existing DLT systems for identity management”

A ANNEX: DETAILED SITUATION IN DIFFERENT STATES

A.1 ALBANIA

In Albania, national laws[20] have done a partial transposition of the eIDAS Regulation; these include Law no. 9880/2008 “On electronic signature”[21] as amended by the Law no. 107/2015 “On electronic identification and trusted services"[22] and Decision No. 69/2016 of the Council of Ministers "On the approval of the regulation ’On electronic identification and trusted services’“[23]. According to article 7 of Law no. 107/2015 “On electronic identification and trusted services”, the initial identification of person requesting electronic identification tools is done only by physical presence of a natural/legal person.. The common ETSI European Norms for TSPs are used. In the absence of an accredited CAB in Republic of Albania the audits are being performed by the Supervisory Authority (National Authority on Electronic Certification and Cyber security).

A.2 AUSTRIA

Related to eIDAS, Austria has requirements on identification in general, but not specifically on remote identification. The only related provisions are those of Article 8 of the Signature and Trust Services Act[24], and Article 3 of the Signature and Trust Services Regulation[25]). According to the latter, in order to determine the identity of the person applying for the certificate, the following are required:

1. an official photo ID or
2. proof which certifies that identity has at least been verified with that level of reliability as is observed with a registered personal delivery (§ 21 of the Service of Documents Act)

The data contained in the official photo ID or the other proof (§ 8(1) first sentence of the Signature and Trust Services Act) must be recorded and documented with the application, unless this information has already been documented. The information may also be recorded just electronically and the documentation needs only be in electronic form. The Austrian SB does not decide in advance on specific types of solutions. So far, the remote identification methods used in the country are human (not AI) based, using video (no still pictures) and traditional ID documents (no eID yet). Both synchronous and asynchronous methods are in use.

Under anti-money laundering laws, Austria issued an “Online Identification Ordinance” (Online-Identifikationsverordnung) that has specific rules on remote-identification. The Ordinance has inter-alia provisions on operator training, using dedicated operator rooms, recording of audio-

[20] https://cesk.gov.al/publicAnglisht_html/legjislacioni/index.html
[21] Law no 9880/2008 “On electronic signature”: https://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/ligji9880.pdf
[22] Law no. 107/2015 "On electronic identification and trusted services": https://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/ligji107.pdf
[23] DCM No. 69/2016 "On the approval of the regulation 'On electronic identification and trusted services'": https://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/VKM69.pdf
[24] Signature and Trust Services Act, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009156, and unofficial translation to English: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2016_1_50/ERV_2016_1_50.pdf
[25] Signature and Trust Services Regulation, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009619, and unofficial translation to English: Regulation http://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2016&num=149&dLang=EN

video sessions, audio and video quality, what features of an ID document need to be checked, or when a session has to be discontinued.

A.3 BELGIUM

In Belgium there are no existing or upcoming specific national regulations, requirements or guidelines for remote identity proofing in the scope of remote identity vetting services.

However, the Supervisory Body allows video identification methods with a human operator. The applicant presents an identity document and must have human interaction with the operator. The Belgian SB does not allow pre-recorded videos. It attaches great importance to the risk analysis carried out by the TSP as to the management of these risks. Not all identity documents are accepted. The TSP is requested to operate a white list with the accepted identity documents, this list may evolve. This method is used by a Belgian TSP for the issuance of qualified certificates for electronic signatures.

Remote identity proofing methods are audited against the usual ETSI standards for TSPs (EN 319 401, EN 319 411-1 and -2) but the Supervisory Body welcomes any new standard dedicated to remote identity proofing.

A.4 BULGARIA

Bulgaria has not defined any national requirements specifically for remote identification. The TSPs fulfil the requirements of the eIDAS Regulation. At the moment of writing, there are no restrictions regarding the types of solutions which can be applied. Verification solutions based on videos, pictures and traditional documents are already in use. One of the Bulgarian TSPs uses a remote video identification system for the verification of the identity of natural and legal persons, and, if necessary - of specific attributes related to the persons. The remote identification system has been verified and certified by a Conformity Assessment Body as a system ensuring a level of security equivalent to physical presence, pursuant to article 24.1(d) of Regulation (EU) 910/2014. Additional authoritative sources are also used in the process: the national identity documents database (for natural persons) and the official register (for legal persons).

A.5 CYPRUS

Cyprus has not issued any national laws on remote identity proofing, but generally plans to do so. The Supervisory Body currently allows the use of eID and traditional ID documents for identity proofing.

A.6 ESTONIA

Estonia has not yet adopted specific national regulations, criteria or obligatory requirements for physical and remote identity proofing in electronic identification services. Legislations and requirements for identification and verification are currently established only for the issuance of National Identity Documents which are based on certain procedure and apply only for issuer (Estonian Police and Border Guard Board) of identity documents. In general, provided identification services are different and based on a principle that a person must be thoroughly verified by secure authentication processes, systems, technologies and products that are protected against modification and are in accordance to the assurance level of security (low, substantial or high) and other requirements that are required for this service.

Estonia's approach is to try to keep up to date with new technologies, solutions and their usages in identity verification solutions for issuing qualified certificates, which also will lead to creating or updating requirements on national level. The country is at a very preliminary planning phase to find the options on how to regulate remote identification solutions which are based on biometric identity verification[26, 27, 28.]

National ID-card, Mobile-ID and ABIV have been audited as parts of trust service, TSP and their involved subcontractors have been subject of conformity assessment according to eIDAS and ETSI EN 319 411-1/2 (and subsequently ETSI EN 319 401, GDPR), which was carried out by an accredited conformity assessment body. In addition, TSPs' conformity assessment body has rated controls performed in the course of the Subscriber's biometric identity verification compared the controls provided by a typical average human based face2face identity verification.

The NPL, the official national UK research lab, specialized and recognized for evaluation of biometric methods, considered that the methodology for testing and reporting (error rates specified, etc.) biometric verification performance conforms to the relevant requirements of ISO/IEC 19795-1:2006, and that the methodologies for testing and reporting presentation attack detection sufficiently conform to ISO/IEC 30107-3: 2017 to support the facial recognition performance claims.

A.7 FINLAND

As per the issuance of certificates, Finland has not issued any legislation nor criteria complementing eIDAS article 24.As per eID, there is national legislation on electronic identification services and the requirements are aligned with eIDAS regulation. Remote identification based on presenting identification document is allowed in legislation, but the criteria is not elaborated. Issuing eID is also allowed based on another already registered eID with the same LOA. For foreigners representing a foreign organisation, there is special legislation for issuing eID for foreigners based on certain procedures that are more lightweight than issuing eID on LOA substantial or high. The use of these eIDs is restricted to certain services, where the risk is acceptable.

If verification is based on presenting identity documents, the acceptable documents are defined in the Act on Strong Electronic Identification and Electronic Trust Services. Otherwise, there are no specified requirements in the general eID context. Possible recent PSD2/AMLD -eKYC developments have not been researched yet. There are very preliminary plans to define criteria in the context of verification of identity when issuing eID means, but at the moment no legislative initiatives are underway.[29, 30, 31]

A.8 FRANCE

As part of the transposition of AMLD5, the French decree n° 2020-118 of February 12, 2020 extends the scope of ANSSI's (i.e. the National Cybersecurity Agency) competence. This decree provides that financial organizations, to verify the identity of their customers, can: "*5° Use a service certified as compliant by the ANSSI, or a certification body that this agency authorizes, at the level substantial of the requirements relating to proof and verification of identity, provided for in the annex to the implementing regulation (EU) 2015/1502 of September*

[26] Identity Documents Act, https://www.riigiteataja.ee/en/eli/504022020003/consolide
[27] Electronic Identification and Trust Services for Electronic Transactions Act, https://www.riigiteataja.ee/en/eli/ee/527102016001/consolide/current
[28] Information security standard (ISKE) developed for the Estonian public sector. The goal of implementing ISKE is to ensure a security level sufficient for the data processed in IT systems, https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html
[29] Act on Strong Electronic Identification and Electronic Trust Services (section 17 Identifying a natural person applying for an identification means) , https://www.finlex.fi/en/laki/kaannokset/2009/en20090617.pdf
[30] Traficom Guideline 211/2019 EN Assessment guideline for electronic identification services (3.10, About initial identification based on an identity document using a remote connection), https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Assessment_guideline_for_electronic_identification_services_211_2019_O_EN.pdf
[31] Specific eID for foreigners representing a foreign organisation, https://dvv.fi/en/-/-korvaa-katso-tunnistuksen-ulkomaalaisen-yrityksen-edustajalle

8, 2015. A joint decree of the Prime Minister and the Minister of the Economy specifies the procedures for applying this 5°".

ANSSI has already provided this type of evaluation with regard to the eIDAS regulation since 2016:

- the evaluation of electronic identification means under the eIDAS regulation
- the qualification of trust services under the eIDAS regulation for which remote identification is a possibility

The evaluations have so far been carried out thanks to informal partnerships with experts in the various fields considered (such as the Ministry of Interior). No standards only criteria based on risk analysis and confidence in the qualified trust provider who carries the solution and an evaluation of the identity document fraud by competent authorities. Based on this first operational experience, the decree offers the opportunity to build a certification framework and requirements for remote identification to take into account in particular, the evaluation of facial and living recognition.

ANSSI is currently working on establishing this new certification framework. A first draft[32] of requirements for remote identification has been published on the 1st of December 2020 for public review until the end of January 2021. The final version is expected in March 2021. These requirements will also address the eIDAS regulation (evaluation of electronic identification means and the qualification of qualified trust services under the eIDAS). The framework will specify the type of remote identity verification solutions allowed at the eIDAS level substantial and high. Given the current perspectives and analysis, the services applying for substantial level certification will need to have the following characteristics:

- On the one hand, a hybrid approach (both automatic and human based, human action being mandatory for each identity proofing), synchronous or asynchronous
- On the other hand, dynamic presentation solutions for the user's identity title and face (using videos).
- Chip reading for electronic identity documents is also considered.

Subject to evaluation, ANSSI will accept "video with operator" methods, if combined with the use of biometrics algorithm in the remote identification process.

A.9 GERMANY

Two Gazzettes (BNtA 126/2017, BNtAg 208/2018) and one technical guideline (TR-03147) are part of Germany's regulatory framework. *The analysis below makes use of selected parts of ETSI TR 119 460.*

BNtA 126/2017[33]: In 2017 a revised German Telecommunications Act (TKG) was adopted as part of national and EU efforts to fight international terrorism. The Act includes the requirement to collect specific subscriber data for prepaid mobile communications services (i.e. SIM Cards). This means the customer must now present proof of their identity prior to the purchase of any SIM card.

Verification can now be carried out by other "suitable methods", including digitally. The remote video identification verification procedures are specified in detail through the Federal Network Agency (BundesNetzAgentur) as Gazette 126/2017. The Gazette details what needs to be

[32] In French only. Appel public à commentaires sur le référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID) https://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/

[33] BNtA 126/2017 - 1 Konsolidierte Fassung der geänderten Verfügung der Bundesnetzagentur gemäß §111Absatz1Satz4 Telekommunikationsgesetz (Stand: 22.11.2017), https://www.bundesnetzagentur.de/SharedDocs/Downloads%20/DE/Sachgebiete/Telekommunikation/Unternehmen_Institu%20tionen/Anbieterpflichten/OeffentlicheSicherheit/Verfuegun%20g111/verfuegung.pdf

validated for the specific purpose of identity verification in relation to a specific sector, namely digital interactions in telecommunications. The document supports remote identity verification procedures consistent with the research of this study.

BNtAg 208/2018 on eIDAS[34] :The German law implementing the EU eIDAS regulation was laid out and approved jointly by the Federal Network Agency and the Federal Office for information Security (BSI). It is known as the eIDAS Implementation Act of July 2017. The core part of the law is known as the “Confidence Services Act” (VDG), and it replaces the previous German Signature Act (SigG).

The VDG is the German law for the application of electronic signatures, seals and time stamps (trust services). The VDG gives the BundesNetzAgentur and BSI the right to determine which other identification methods within the meaning of eIDAS article 24(1) d are recognized and the required procedures that apply.

The hearings between BSI and the Federal Network Agency on identification methods were published as a ruling to endorse the eIDAS Regulation and this document outlines specifications under Section 11 (1) of the VDG as an Official Gazette 11/2018 (notification no. 208). The Video identification requirements for issuing qualified web authentication certificates or qualified certificates for electronic signature are usable for a single transaction. The provisions are similar to the BaFin 03/2017 Circular on Video identification requirements. This document does not provide complete procedural details like the BaFin Circular, rather it endorses the procedures and lists requirements.

TR-03147[35]: This technical guideline outlines a threat / risk perspective to identity proofing. Based on threats to identity checks, requirements for identity checks have to be defined and implemented. Document provides the technical guideline for minimum levels of assurance for E-Government / Business functions (Bundesamt für Sicherheit in der Informationstechnik). This is a complimentary document to guideline [TR-03107-1] (Electronic Identities and Trust Services in E- Government). The document covers eIDAS application inside the German framework. The document provides tables and specifications for definitions and assessment methodology, proof of Identity, trustworthiness of ID documents, security of transmission channels, checking of ID documents, comparison of persons with ID document data, correct registration of the required ID attributes, and safeguarding process integrity.

A.10 GREECE

In the trust services sector, recently issued national legislation (Law 4727/23.09.2020) recognises remote identification as an acceptable identification method for the purposes of issuance of qualified TS certificates according to Article 24 1(d) of eIDAS Regulation. Nevertheless, an implementation Act (Ministerial Decree) that will set the terms and conditions of the method is still pending. [36]￼ of its proposal. EETT is in favour of human based synchronous video identification using traditional ID documents.

In the public sector, the Greek Ministry of Digital Administration has made available a new digital platform which allows the public to remotely conduct several transactions with the Public Administration. The platform allows the public to submit applications from their home during a

[34] NtAg 208/2018 on eIDAS - Verfügung gemäß § 11 Absatz 1 VDGs, https://www.bundesnetzagentur.de/SharedDocs/Downloads/%20DE/Sachgebiete/QES/Verf%C3%BCgungIdentmethoden/Ers%20tverfuegung2018.pdf;jsessionid=4352CCD9F3A53FDE2A26C356F59D2DE3?__blob=publicationFile&v=5

[35] Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons (version 1.0.4), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publica%20tions/TechGuidelines/TR03147/TR03147.pdf?%20blob=publication%20File&v=1

[36] Results of the public consultation and EETT’s proposal to the Ministry, https://www.eett.gr/opencms/opencms/admin/News_new/news_1187.html

scheduled video call with employees of Citizens' Service Centers. The service is based on newly introduced legislation: Law 4704/14.07.2020[37] and Ministry Decision 20530 EX 2020/21.7.2020, which allows video-based (synchronous) identification by a human agent. In the banking sector, the Bank of Greece laid down the terms and conditions for digital customer onboarding by banks and other supervised entities via the Executive Committee Act issued in May 2020[38].

The Act contains a combination of organisational, technical and procedural measures that ensure a reliable identity verification of natural persons and are designed to prevent identity fraud. Two methods of digital onboarding are envisaged: (a) by video conference with a trained agent, which provides the greatest safeguard of security; and (b) an automated procedure via a dynamic selfie, subject to additional safeguard measures.

The identification documents for natural persons that are acceptable are those incorporating enhanced security features, most notably passports. Exceptionally and only as part of the video conference method, ID cards issued by the Hellenic Police, with data written in Latin characters, may be accepted subject to validity and authenticity check through the central portal of the public administration.

More recent developments include:

- Law 4557/30.07.2018 as amended by Law 4734/08.10.2020[39] incorporates the provisions of AMLD5 and AMLD4, and thus enables the eIDAS toolbox for electronic identification to verify the customer's identity due diligence processes.
- Board Decision 4/894/23.10.2020 of the Hellenic Capital Market Commission, published in the Government Gazette no.5008/23.11.2020[40], aligns remote identity proofing requirements for "e-money" providers (e-wallets, virtual currencies) with those which apply to the traditional banking sector.

A.11 ITALY

In Italy, there are no national laws regarding specifically remote identity proofing, but the Italian SB (AgID) has released a guideline, containing the minimum requirement in order to obtain the authorization for the use of A/V remote identification procedure. AgID is currently drafting a technical document concerning A/V procedures, requirements, risks and countermeasures. It is likely to be published by the end of next year.

Until now, AgID has only authorized remote synchronous remote A/V identification, lasting about 20 minutes, for the release of both qualified certificates and SPID identities (eID). It is about to authorize, by the next weeks, some asynchronous A/V procedures lasting 10 sec, with a later control of the operator and some other reinforcement measures (bank transfers, witnesses, usage of eIDs).

[37] Law 4704/14.07.2020 on digital governance and simplification of citizen services, http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wHUdWr4xouZundtvSoClrL8NXGWS3cU8Kt5MXD0LzQTLWPU9yLzB8V68knBzLCmTXKaO6fpVZ6Lx3UnKl3nP8NxdnJ5r9cmWylq-BTkXB0ftEAEhATUkJb0x1LIdQ163nV9K--td6SIuQQz_MAyRfEhwZeksFj4hiU3__gO-yJL47OeoTCdy-aJ

[38] Executive Committee Act 172/1/29.05.2020 regarding remote identify proofing, https://www.bankofgreece.gr/RelatedDocuments/EXECUTIVE_COMMITTEE_ACT_172.pdf

[39] Law 4734/08.10.2020 on AMLD5 transposition, http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wHUdWr4xouZundtvSoClrL8H69BYATHe5V5MXD0LzQTLWPU9yLzB8V68knBzLCmTXKaO6fpVZ6Lx3UnKl3nP8NxdnJ5r9cmWylq-BTkXB0ftEAEhATUkJb0x1LIdQ163nV9K--td6SIufZCx3uo5L5jBeXfj7sQOLGKeF-okwx7jUf11XWSFIVL

[40] Board Decision 4/894/23.10.2020 of the Hellenic Capital Market Commission, http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wHUdWr4xouZundtvSoClrL8-AbDqCH5J4nuFUDqazHcNeJInJ48_97uHrMts-zFzeyCiBSQOpYnTy36MacmUFCx2ppFvBej56Mmc8Qdb8ZfRJqZnsIAdk8Lv_e6czmhEembNmZCMxLMtRBCZzLZsboz_elGwVfbZ41Vq--A1dGO5LwzOf1ApM1w

In Italy, it is also possible to obtain a QES remotely, using a CIE, the national notified electronic ID or another FEQ (Qualified Electronic Signature) or the CNS (national electronic services card). The use of remote identity proofing (both A/V and other) is widely spread over the QTSPs and the SPID IDPs of the country. To be authorised, a solution is evaluated first by an accredited CAB and then by AgID based on in-house processes and national requirements.

A.12 LATVIA

Ceiling law regarding electronic identification in Latvia is Law on Electronic Identification of Natural Persons[41]. This law doesn't prescribe remote identification as a measure to be used in adopting natural persons to eID scheme. However, there are guidelines from the national Finance Sector authority - The Financial and Capital Market Commission[42], since remote identification is to some extent used in the banking sector in Latvia. The same applies in the case of prevention of money laundering and proliferating where distant identification methods are mentioned[43]. Currently, there are no plans to update legislation regarding remote identity proofing.

A.13 LITHUANIA

Remote identity proofing methods are allowed in Lithuania. There are no specific national laws or requirements related to the use of remote identity proofing in the trust services area; the current legislation does not put any restrictions. Discussions are being held to update legislation, but at the moment no timeline is set.

The main audit criterion is the "Description of the Procedure for Verification of personal identity and additional specific attributes by issuing qualified electronic signatures, electronic seals, website authentication certificates" approved by Order No. 1V-1055[44] of the Director of the Communications Regulatory Authority on 26 October 2018. This above SB regulation specifies that remote identity proofing is framed in accordance with eIDAS article 24.1. No TSP uses such methods at the moment.

A.14 LUXEMBOURG

Luxembourg's legislation has foreseen remote identification since the Amended E-Commerce and Trusted Services Act of August 14, 2000. A newer amendment was issued on July 17, 2020. ILNAS, the national supervisory body for trust service providers, has issued the "QTSP Procedure n° 005A Recognition of other identification methods at the national level"[45] which lists the current requirements for remote identity proofing methods; the requirements mainly correspond to the requirements of the Bundesnetzagentur (Germany) on video identification methods. The allowed remote identity proofing method[46] is based on video identification with human interaction. The main usage scenarios include the issuance of qualified certificates for electronic signatures and the issuance of qualified certificates for electronic seals.

A.15 MALTA

No national legislation exists on remote identity proofing. The SB has proposed and drafted the relevant laws and they are currently being reviewed by the government. The plan is to proceed with Public Consultation this year. Remote identity proofing is not allowed at the time of writing.

[41] Law on Electronic Identification of Natural Persons, https://likumi.lv/ta/en/en/id/278001-law-on-electronic-identification-of-natural-persons
[42] The Financial and Capital Market Commission remote identification guidelines (in Latvian), https://www.fktk.lv/wp-content/uploads/2019/05/Ieteikumi_neklatienes%20identifikacija_18.09.2014.pdf
[43] Republic of Latvia Cabinet Regulation No. 392 Procedures by which the Subject of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer, https://likumi.lv/ta/en/en/id/300147-procedures-by-which-the-subject-of-the-law-on-the-prevention-of-money-laundering-and-terrorism-financing-performs-the-remote-identification-of-a-customer
[44] Order No. 1V-1055 of the Director of the Communications Regulatory Authority on 26 October 2018, https://www.e-tar.lt/portal/lt/legalAct/cc076bf0d91111e89a31865acf012092
[45] QTSP Procedure n° 005A Recognition of other identification methods at the national level version 1.3, https://portail-qualite.public.lu/fr/documentations/confiance-numerique/surveillance-psc.html
[46] Remote identification methods recognized in LU, https://portail-qualite.public.lu/fr/confiance-numerique/prestataires-services-confiance/remote-identification-methods.html

Per the ongoing process of creating the national legislation, the SB plans to be as technology neutral as possible whilst ensuring the chosen method is equivalent to physical identification.

A.16 NETHERLANDS

At the moment of writing, in the Netherlands there is no specific law on remote identification or plans to create one. The generic law on identification of natural persons does apply (e.g. on the use of official ID documents). The current interpretation of Netherlands for the eIDAS regulation is that all identity proofing methods are allowed as long as they meet requirements in eIDAS and national law. At the moment there are no restrictions on specific methods in eIDAS or national law. So, all methods should be allowed, as long as their implementation does not violate other requirements in eIDAS or national law.

Two TSPs have notified for the use of remote identity proofing: one is using live video interaction with a human operator in a controlled environment; the other using a mobile app solution based on AI technology without operator interaction. Formally these are audited against eIDAS and national legal requirements. Typically, the ETSI standards framework for trust services is used, although specific ETSI standards for (remote) identification of trust service subjects are still pending.

A.17 NORWAY

In Norway, no approved guidelines or rules exist against eIDAS Article 24.1.d or otherwise. Video interview is not an option in the country; common practice is physical presence, usually either at a bank branch office or a post office.

Due to the pandemic crisis, the supervisory authority temporarily approved, earlier this year, a solution using remote automated onboarding (NFC reading of passport, selfie, biometric face recognition). This solution targets foreign workers that have rights to unemployment or social benefits from Norway and that had to (or desired to) go to their home country when the pandemic started. It allows these people to remotely onboard using their national passport (Polish, Lithuanian, other) and obtain an eID proving their Norwegian national ID number via a lookup in the Norwegian population register. Then, they can digitally access the services of the social welfare agency to claim their rights. This is primarily an eID at level “high”, which includes a qualified certificate for advanced electronic signatures.

On a more permanent basis, a project is in progress on a specification for KYC in the financial sector. This will include issuing an eID of level “high” (BankID), which includes a qualified certificate for advanced electronic signatures. The technical approach is similar to the one described in the previous paragraph (NFC reading of passport, selfie, biometric face recognition). Once the specification is completed, it shall pass through the approval of the relevant authorities.

A.18 POLAND

In Poland, there is no specific national level recognition of identification methods. For trusted services, Poland considers eIDAS Regulation to be part of its internal legal system. Since there is no national legislation nor criteria complementing article 24 of eIDAS, the SB relies on certification by conformity assessment bodies. Remote identity proofing is already applied for the provision of qualified certificates at least by one Polish QTSP.

Human-based remote identity proofing using national eID documents and synchronous video (tele-conferencing) is possible in electronic identification scheme called Trusted Profile. The electronic identification means issued under that system can be used only in public online services.

These possibility has been introduced by national legislation[47] as a response to the threats of COVID-19 posed by confirmation of identity during physical presence.

An additional important provision specified in the Act is the possibility for a person confirming identity, to verify data in public registers, including a photograph entered in the Register of Identity Cards. Recording from video tele-conference has to be preserved for six years. Nowadays the Trusted Profile issued based on remote identity proofing is temporary (3 months validity automatically renewed to the end of formally announced epidemic threat), but the evaluation of the remote identity confirmation process will be carried out ex post.

Banks and financial institutions according to [AMLD5] are allowed to offer services to new customers remotely if identity is confirmed via the video identification process. The Polish Financial Supervision Authority issued guidance for all financial institutions[48], with requirements to the remote process.

A.19 PORTUGAL

In Portugal, a regulation[49] has been published by the Supervisory Body regarding the identification of individuals through remote identification procedures using videoconferencing. This regulation defines the requirements for the videoconferencing identification procedures and systems, as well as the certification and conformity assessment of the videoconferencing identification procedures and systems, for the purposes defined in article 24.1(d) of the Regulation eIDAS.

At the moment of writing, the only acceptable remote identity proofing is human-based, with the use of eID documents and synchronous video (tele-conferencing). In the next months, the country intents to publish requirements for automated systems, which will allow asynchronous AI-based remote identity proofing which will make use of video, pictures and biometrics.

A.20 ROMANIA

At the time of writing, Romania has not issued national legislation but is in the process of creating technical requirements for remote identity proofing. In particular, the Agency for the Digitalisation of Romania has recently submitted for public consultation a draft of a normative act50 regarding technical rules on the procedure for identifying a person remotely using video means. It replicates some requirements from BaFin Circular 03/2017 on Video Identification. The solution is expected to be based on real-time video recording, verification of security elements of the ID card, capture of pictures.

A.21 SERBIA

Republic of Serbia transposed eIDAS Regulation 910/2014 on Law no.107/2015 “On electronic identification and trusted services”[51] through adoption of Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (Official Gazette No.94/2017).

[47] Act of introducing IT technologies for the activities of entities performing public tasks http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20050640565

[48] Financial supervision guidance, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf

[49] Dispatch 154/2017 - Identification of individuals through distance identification procedures using videoconferencing, https://www.gns.gov.pt/media/10442/Despacho-154-2017-ID-Videoconferencia.pdf

[50] Proiectul de Hotărâre de Guvern privind norme tehnice referitoare la procedura de identificare a persoanei la distanță utilizând mijloace video, https://www.adr.gov.ro/transparenta-decizionala

[51] Official Gazette of the RS No.24/17 - Law on electronic document, electronic identification and trust services in electronic business, https://mtt.gov.rs/en/download/1(2)/Law%20on%20electronic%20document%20electronic%20identification%20and%20trust%20services%20in%20electronic%20business.pdf

Requirements for issuing electronic identification schemes are different depending on the assurance level of the electronic identification schemes (low/basic, medium/substantial or high level) and physical presence is required for issuing medium and high assurance level of the electronic identification schemes.

Requirements are regulated in accordance with article 18 of the Law and articles 4, 5and 6. of the Regulation on more detailed Regulation of the Mandatory Requirements for Electronic Identification Schemes for Specific Assurance Levels[52,53]. For the moment, there are no plans for updating existing national laws and requirements.

A.22 SPAIN

The current national law on electronic signature[54] foresees that the specification of the technical requirements for remote identification may be done by ministerial order. The Ministry of Economic Affairs and Digital Transformation is currently working on a draft of the order. The public consultation[55] has ended on November 11, 2020 and publication is expected in March or April 2021.

The above-mentioned ministerial order includes synchronous and asynchronous identification through video streaming. An artificial intelligence algorithm could also be used but always with the verification by a qualified agent, also in asynchronous mode. In the banking sector, SEPBLAC (the financial supervisory body) has authorized video-identification and videoconference. SEPBLAC authorizations[56] are sector oriented, thus not directly applicable to trust services.

A.23 SWEDEN

Sweden has not issued national legislation or regulations for remote identity proofing; there is also no plan to do so in the near future. Given that there are no national legal requirements, the SB allows all identity verification solutions as long as they conform to the applicable requirements in the eIDAS regulation. For example, a QTSP recently received their qualified status for their CA service, using remote identification in accordance with article 24.1(d). ETSI standards (EN 319 401, EN 319 411-1) are used for the evaluation of the identity proofing service or service component.

A.24 UK

At the end of 2018, the UK government (in particular the Cabinet Office, Government Digital Service, and National Cyber Security Centre) published a collection of documents which provide "*Guidance on how to prove someone's identity or give them access to your service or organisation*" [57]. This includes Good Practice Guides (GPG) for issues like natural person ID proofing (GPG 45) and legal person ID proofing (GPG 46). This guidance is aligned with all the major international standards and regulations: eIDAS Regulation, Digital ID and Authentication Council of Canada (DIACC), Pan Canadian Trust Framework Model, ISO/IEC 29115 and NIST 800-63.

[52] Official Gazette of the RS No.60/18 - Regulation on more detailed Regulation of the Mandatory Requirements for Electronic Identification Schemes for Specific Assurance Levels, https://epotpis.mtt.gov.rs/download/regulation-on-more-detailed-regulation-of-the-mandatory-requirements-for-electronic-identification-schemes-for-specific-assurance-levels-official-gazette-60-18/?wpdmdl=546&refresh=5f990f39bbc961603866425

[53] Register of Electronic Identification Service Providers and Electronic Identification Schemes, https://epotpis.mtt.gov.rs/eng/register-of-electronic-identification-service-providers-and-electronic-identification-schemes/

[54] Documento BOE-A-2020-14046: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-14046

[55] Public consultation on the Draft Order on remote identification methods for the issuance of qualified electronic certificates: https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/SEDIA_OM_identificacion_remota.aspx

[56] SEPBLAC authorizations:
https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf
https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf

[57] UK guidance on Identity proofing and authentication, https://www.gov.uk/government/collections/identity-proofing-and-authentication

The guides define and make use of a multi-parameter scoring system, which is aimed in quantifying different aspects of the identity proofing process. Scores 1 (lowest) to 5 (highest) are defined to assess different kinds of ID supporting evidence, including the type of the issuing organization, and different types of the validity check of this evidence. For example, an eID issued under an eIDAS scheme, scores 2 if it is notified / accepted at LoA 'Substantial', but 3 if it is a LoA 'High'. Scores 4 and above normally involve biometric information and cryptographic security features.

The ID proofing process is broken down to five (5) modular parts; each is evaluated and scored separately. "Identity profiles" are defined for the different combinations of the ID proofing process; each profile provides a different level of overall confidence (low to very high). Instead of defining specific security requirements, the guidelines suggest this process to be viewed from a risk management perspective.

A British Standard is also underway on the Design and operation of online user identification systems (OUIs); BS 8626[58] (ready for approval at the time of writing). It is a Code of Practice document; it is designed to be used as a reference by different stakeholders, instead of defining requirements. The standard includes comprehensive guidelines on functional, organisational and technical aspects. It contains recommendations for almost all steps of the process, for the material involved and for the management controls. For example, it provides an extensive list of tests to determine whether the evidence is genuine. Overall, BS 8626 is an up-to-date document which covers all key aspects of identity proofing, and thus it is valuable material in this area.

[58] Draft BS 8626 Design and operation of online user identification systems – Code of practice, https://standardsdevelopment.bsigroup.com/projects/2018-01712

B ANNEX: THREATS AND VULNERABILITIES

This annex provides a non-exhaustive list of threats and vulnerabilities to remote identity proofing systems. It should only be seen as a starting point for identifying threats and vulnerabilities since, on the one hand, each system is concerned by particular threats or vulnerabilities and, on the other hand, threats evolve extremely rapidly in this field. One need only consider for instance the rapid evolution of AI in the field of presentation attacks to be convinced of this. This list was drawn up by analysing, exploiting and detailing the replies received from the stakeholders to the questionnaire submitted to them. This analysis was completed by taking into account various existing technical reports dealing with identity proofing[59] or technical components reported to be used during identity proofing by stakeholders[60]. Annex C of [ISO/IEC 27005] also proposes categories of threats and origins. Some threats and vulnerabilities have been inferred from guidance. Some of these threats are often common with face-to-face identity verification, but the fact that identity is verified remotely introduces new methods of exploitation for attackers.

This list may be supplemented by the list of threats presented in the annex to [ENISA Security Framework for TSPs]. As stated in the same document, these threats can be categorized by root cause and associated to an origin. [ENISA Article 19 incident reporting] proposes five root cause categories that may apply to TSPs:

- **Human error**: includes incidents caused by human error during the operation of equipment or facilities, the use of tools, the execution of procedures, etc.
- **System failures**: includes incidents caused by failures of a system, for example, hardware failures, software failures or errors in procedures or policies.
- **Natural disaster**: includes incidents caused by severe weather, earthquakes, floods, wildfires, and so on.
- **Malicious actions**: includes incidents caused by a deliberate act by someone or some organisation.
- **Third party failures**: includes incidents where the cause was not under the direct control of the provider, but some third-party.

Each threat is described in such a way as to provide an understanding of its operating context. Possible vulnerabilities associated to each threat have been listed following that description.

[59] [NIST SP 800-63A] is reviewed and documents from SBs as listed in Annex A
[60] [ISO/IEC 30107] Biometric presentation attack detection, [ISO/IEC 19795] Biometric performance testing and reporting

B.1 INITIATION STEP THREATS AND VULNERABILITIES

Threat	Possible Vulnerabilities
[T_POLICY_FLAW] Policy flaw. A remote identification proofing process has to take into account a large number of different contexts and when some are not correctly understood when defining the policy, this can lead to several vulnerabilities.	A method used for validation or verification doesn't satisfy the requirements of the targeted LoA.
[T_PHISHING] User accepts process initiation from attacker. Some remote identity proofing may be exposed to phishing attacks. This is for example the case in processes with interruptions and reconnections using SMS or email.	A fake link to the identity proofing process can be without verification accepted and used by a non-aware user. User is not aware how to verify the correct service.

B.2 ATTRIBUTES AND VALIDATION STEP THREATS AND VULNERABILITIES

Threat	Possible Vulnerabilities
[T_DOC_WEAK] Insufficiently secured Identity document. Some identity documents which are still valid in Europe do not have remotely verifiable security features strong enough to achieve the expected level of assurance.	The system is misconfigured to accept such a document, whether it is an automatic system or a guidance to an operator. Lack of knowledge about identity documents leads to not being aware of this problem.
[T_DOC_IMPRECISE] Insufficiently precise Identity document. Some identity documents which are still valid in Europe do not include all the information necessary to uniquely and positively identify the applicant. Some do not have a unique identifier of the person and the information mentioned is not sufficient to avoid duplicates. For example, on the French identity card in force at the date of writing of this report, only the surname, first name, sex, date and name of the commune of birth appear. Cases of perfect duplicates on these elements are obviously common.	User can impersonate someone else with whom she shares the same attributes. The system is misconfigured to accept such a document without collecting more information, whether it is an automatic system or a guidance to an operator.
[T_DOC_STOLEN] Stolen or revoked identity document. This case refers to an attacker using a stolen authentic document. This is a common identity theft scenario, most often combined with a presentation attack on the verification stage to deceive the software or the person who is going to verify that the picture on the identity document matches the person presenting it.	Lack of tools possible to use by an operator allowing verification of the validity of the document. Document not listed as stolen whatever the reason. Lack of automatic access for the system to a service allowing verification of the validity of the document.
[T_DOC_FAKE] Counterfeited or forged identity document. A counterfeited document is a complete reproduction of an identity document while a forged document is an original document on which an attacker has modified one or more elements. In some cases, it may also be a stolen blank document personalised by the attacker. The imperfections of a counterfeited or forged document may be easier to conceal in the case of remote verification. See T_QUALITY_ALTERATION.	The process or tool for the detection of false documents is non-existent or inoperative.

[T_DOC_FANTASY] Fantasy or non-recognised identity document . A fantasy document is a document created from scratch without reference to an existing type of document. It is generally of a fairly coarse quality, although there are some relatively likely production channels for fancy documents. Identity documents issued by non-recognised states or by states that no longer exist can be classified in the same category.	The list of accepted documents defined is not correctly enforced, thus making possible to use a fantasy or non-recognized document.
[T_DOC_HUMAN_CAPABILITIES] Lack of operator capability or knowledge about [some] accepted identity documents. If an operator is involved in the data validation or verification phase, he may not have the capability or competence to perform this task satisfactorily. For example, he may be unfamiliar with the document or data source presented to him. An attacker will seek to produce a forged document relating to a type rarely encountered by operators to take advantage of their lack of expertise.	Operators not trained well enough. Lack of evaluation after training. Operators not provided with the right tools. They lack a reference database with genuine documents templates and a guide on how to authenticate each identity document.
[T_DOC_HUMAN_ERROR] Non-handled human error. If an operator is involved in the data validation or verification phase, he may make an error.	The process is not human error proof.
[T_DOC_SOFTWARE_PERFORMANCE] Software capability to authenticate identity documents not at the required level. If a software component is involved in the data validation or verification phase, it may not be able to validate or verify adequately the identity document it is presented. Indeed, there are hundreds (or even thousands if one takes into account every single model variation) of valid identity document in use around the world. Software could support documents in an uneven way. An attacker will seek to produce a forged document relating to a more permissive document type.	The software is not able to authenticate a given type of identity document with the expected accuracy. The software is not able to extract information from identity document with the expected accuracy. Data captured from MRZ does not include diacritic letters leading to wrong identity proofing.
[T_DOC_CHIP_READING_NOT ALLOWED] Chip reading not allowed. Reading the chip of an eMRTD (electronic Machine-Readable Travel Document; most passports are compliant with this standard) if done carefully is a good way to recover identity attributes with a high level of assurance. However, this operation, while technically possible in accordance with ICAO9303, is not always legally possible in some EU countries such as France.	eMRTD chip reading used in the process although not allowed by law.
[T_QUALITY_ALTERATION] Artificial image or video quality alteration. When data collection is performed remotely, transmitted identity document image or video is altered in such a way as to degrade its quality to the point of making it difficult or even impossible to detect a forged or counterfeit document or to identify with confidence the applicant. This can be exploited by acting on the quality of the transmission, for example by artificially limiting the bandwidth, or by acting on the capture conditions, for example by reducing lighting. This is usually exploited in combination with one or more of the following to increase the likelihood of success.	Operator or software does not [sufficiently] take into account image or video quality when reviewing evidences.

[T_DOC_IMAGE] Image presented instead of genuine document. The attacker may attempt to mislead the system by using photos instead of legitimate document. This type of attack is particularly common on fully automatic systems that require a picture of the identity document. For example, the attacker will present a photo of a forged identity document. For this type of attack, a screen is usually placed in front of the camera in the place of the applicant.	Operator or software fails at detecting an image presented as a genuine identity document.
[T_DOC_VIDEO] Video presented instead of genuine document. The attacker may attempt to mislead the system by using a video instead of legitimate document. This type of attack is particularly common on fully automatic systems that require a dynamic capture of the id document. For example, the attacker will present a video of a forged identity document including simulated OVD (Optically Variable Device are security features which show different information depending on the viewing angle and/or lightning conditions such as holograms, iridescent ink, etc.). For this type of attack, a screen is usually placed in front of the camera in the place of the applicant.	Operator or software fails at detecting a video presented as a genuine identity document.
[T_DOC_AI] AI generated video presented instead of genuine document. The attacker may attempt to mislead the system by altering the signal using a video manipulating technology in order to make it look like a genuine document. For instance, an AI-based software can generate data corresponding to an original identity document (for instance by including all artifacts produced by OVDs). This attack can be prepared in advance when the scenario is predictable or generated on the fly. It can use a screen or projector placed in front of the camera or directly replace the video stream generated by the camera. The possibilities of applying AI in the field of presentation attacks are significant and rapidly evolving.	Operator or software fails at detecting a software generated or altered video presented as a genuine identity document.
[T_DATA_INJECTION] Data injection. When a data capture system is set up, the possibility for the attacker to inject data directly by bypassing the capture system makes it possible to avoid the validation treatments that could be carried out on the applicant's equipment and to industrialise replay or AI-based presentation attacks.	API keys are not protected.
[T_DATA_ALTERATION] Data alteration before it is sent to the system. It may allow an attacker to modify the captured data. This vulnerability is particularly severe when part of the validation operations is carried out on the applicant's equipment.	Mobile application is not protected against decompilation and modification. API keys are not protected.
[T_REPLAY] Interception and replay of captured data . This can allow an attacker to carry out a replay attack. A loophole allows the attacker to capture data collected when verifying the identity of a legitimate applicant. Possibly through a Man In The Middle. The replay attack consists of using the captured data by presenting it again to the system, thus impersonating the legitimate applicant.	Protocol vulnerability allows data capture between client and server part of the capture software. User provided with a cloned application/website mimicking the legitimate one. Malicious software installed on user’s device captures data.

B.3 BINDING AND VERIFICATION STEP THREATS AND VULNERABILITIES

Threat	Possible Vulnerabilities
[T_FACE_IMAGE] Image presented instead of applicant's face. The attacker may attempt to mislead the system by using photos instead of the genuine face of the legitimate applicant. This type of attack is particularly common on fully automatic systems that require a picture of the applicant for binding with the presented identity document. For example, the attacker will present a photo of the legitimate applicant. For this type of attack, a screen or a printed photo can be placed in front of the camera in the place of the applicant's face. Several photos can be used to mislead systems that require some actions to be performed by the applicant (such as smile, close an eye, etc.)	Operator or software fails at detecting a photo or series of photos presented as a legitimate user's face.
[T_FACE_VIDEO] Video presented instead of applicant's face. The attacker may attempt to mislead the system by using a video instead of genuine face of the legitimate applicant. This type of attack is particularly common on fully automatic systems that require a dynamic capture of the applicant's face for binding with the presented id document. For example, the attacker will present an edited video of the legitimate applicant performing the actions sequence requested by the system. For this type of attack, a screen is usually placed in front of the camera in the place of the applicant.	Operator or software fails at detecting a video presented as a legitimate user's face. User's device system is modified to take a video as the camera output.
[T_FACE_MASK] Mask. The attacker uses a mask usually to impersonate a person whose identity has been provided with a stolen identity document [T_DOC_STOLEN]. There is a wide variety of techniques easily available to produce a mask to match a person, ranging from a simple cut-out photo to a more realistic latex or silicone mask.	Operator or software fails at detecting a mask is used to impersonate the legitimate user.
[T_FACE_AI] AI generated video presented instead of applicant's face. An AI-based software can generate in real time a video of the legitimate applicant mimicking the behaviour of the attacker. This attack can be prepared in advance when the scenario is predictable or generated on the fly. It can use a screen or projector placed in front of the camera or directly replace the video stream generated by the camera. The possibilities of applying AI in the field of presentation attacks are significant and rapidly evolving.	Operator or software fails at detecting a software generated or altered video presented as a legitimate user's face. User's device system is modified to take a video as the camera output.
[T_FACE_HUMAN_CAPABILITIES] Lack of operator's abilities to identify a person. If an operator is involved in the binding and verification step, he may not have the capabilities or competence to perform this task satisfactorily. For example, he may not have the ability to reliably identify a person from another ethnic group. This situation may be exploited by an attacker.	Operator not trained enough. There is a lack of evaluation after training. Operator recruitment process not taking into account that ability.
[T_FACE_LOOKALIKE] Similar looking person. Solutions using biometrics to perform the binding step are vulnerable when people with strong similarities to the legitimate applicant attempt to mislead the system. This is the case, for example, with twins or even members of the same family when the identity documents used as a reference are a little old.	Similar looking persons mistaken whether the similarity is natural or artificial.

[T_FACE_OLD_REFERENCE] Old identity document. Even if it is not a good practice, identity documents can be valid during a long period (up to 15 years in France at the time this report is written for example). As a result, the time lapse between the date on which the photo on the identity document is taken and the date on which the verification is carried out may be significant and the appearance of the applicant may have changed significantly, especially for young people.	Software wrongly finds that two faces are identical because it does not take into account the lapse of time between the two photos during training.
[T_FACE_POOR_QUALITY_REFERENCE] Poor quality photo on the identity document. Photographs on identity documents can be small, of poor quality, sometimes in shades of grey. This can be exploited for a "lookalike" attack.	Software doesn't take into account picture quality
[T_FACE_SOFTWARE_PERFORMANCE] Performance of facial recognition software not at the expected level. When facial recognition is done or assisted by software, possible lack of performance of the software is a vulnerability. Indeed, the context (reference photo from an identity document and possibly a relatively old one) may lead to favouring the FRR (False Rejection Rate, i.e., the proportion of people who should have been accepted but were unduly rejected) rather than the FAR (False Acceptance Rate, i.e., the rate of people who should have been rejected but who nevertheless broke into the system).	Software wrongly finds that 2 faces are identical because it favours a low FRR.
[T_DATA_INCONSISTENCY_INACCURACY] Inconsistency or inaccuracy of reference data. When reference data is used to validate or verify an identity, it is possible in some configurations to find cases of inconsistent or incomplete reference data, for example, differences in transliteration, homonyms, etc. For instance, during the remote identity proofing for a legal person, identification of a legal representative is key and it may occur that the person being the legal representative is not uniquely defined by the registered identity attributes thus allowing legal person impersonation by anyone sharing the common set of registered identity attributes. The management policy (automatic or manual) of these cases can constitute a loophole that can be exploited by an attacker.	Operator or software matches applicant's identity with a given identity although the identity attributes collected from the applicant or the identity attributes of the person she is pretending to be are not precise enough to identify her uniquely.
[T_SOCIAL ENGINEERING] Social engineering. If an operator is involved in the data validation or verification phase and interaction with the applicant is part of the process, it is possible for an attacker to convince the operator to improperly validate an identity verification operation, for instance by appealing to his sensitivity.	Operator is not sufficiently made aware of this type of fraud. Process is not sufficiently enforced, allowing the operator to bypass some instruction.
[T_BRIBERY] Bribery of an operator. If an operator is involved in the data validation or verification phase and interaction with the applicant is part of the process, it is possible for an attacker to convince the operator to improperly validate an identity verification operation by bribing him.	The process allows confirmation of fake identity if an operator accepted a bribery offer. Too low salary makes an operator accepting bribery offer.
[T_INSIDER] Insider. If an operator is involved in the data validation or verification phase and interaction with the applicant is part of the process, it is possible for an attacker to have the remote identity proofing service provider hire a malicious operator who will validate identities that should normally have been rejected.	Lack of controls during the recruitment process. Lack of follow-up of employees.
[T_REVOKED_CERTIFICATE] Revoked certificate. Use of revoked certificate as a proof of identity without checking its status.	Not checking the status of the CA. Not checking the status of the certificate against CRL/OCSP.

[T_EMRTD_WEAK_IMPLEMENTATION] eMRTD weak implementation. Security of eMRTD relies on the country or organisation certificate. There is no complete official master list of these certificates. Using an unsecure list of certificates or not using that security make the system vulnerable to forged eMRTD. A poor implementation of security mechanisms ensuring data integrity and chip presence makes the solution vulnerable to various attacks such as Man in the middle, eMRTD cloning, etc.	Lack of validation against master list of certificates. No or non reliable verification of data integrity.
[T_BLACKBOX] Blackbox. eID, IdP, or any other digital proof of identity related threats should be handled as a blackbox threat. Any vulnerability on these systems may lead to a vulnerability on the remote identity proofing system.	Any vulnerabilities in the communication protocols exposed by these blackboxes. Any vulnerabilities affecting the blackbox itself.

B.4 GENERAL THREATS AND VULNERABILITIES

Threat	Possible Vulnerabilities
[T_CONSTRAINT] Applicant under constraint. During remote identity proofing, the applicant may be threatened and perform this operation under constraint. This vulnerability, which also exists in face-to-face interviews, is made easier to exploit in the context of a remote verification.	Legal weakness of the proof if the applicant is physically threatened. Legal weakness of the proof if the applicant is blackmailed.
[T_PROCESS_FLAW] Process flaw. Generally speaking, any flaw/inaccuracy in the remote identity verification process can constitute a loophole that can be exploited by an attacker.	Process contains an interruption with recovery mechanism from the previous step and is vulnerable to attacks using a poorly secured recovery mechanism. A process hypothesis is not verified, controlled or made mandatory. For example, a control is supposed to be carried out by an operator but nothing is done to ensure that the control has indeed been carried out. Missing evidences (due to process flow or technical flow) do not lead to a rejection.
[T_DELEGATION] Delegated operator. Delegation of responsibilities could weaken the process. If the remote identity proofing is delegated to another organization (e.g. a bank asking an identity provider to do so, or a parent company with respect to a more specialized subsidiary), it is possible that some ambiguity in this outsourcing arises as soon as organizational boundaries are crossed. This could loosen the security of the entire process, including making the risk analysis performed as discussed in section 4 less focused.	The requirements for the delegated operator are not clearly defined or not verified. The risk analysis wrongly assumes that a similar risk analysis is carried out for the delegated operator.

C ANNEX: SECURITY CONTROLS

This annex provides a non-exhaustive list of security controls, elements of the remote identity proofing process that are subjected to specific constraints in order to contrast a possible attack. This list has been drawn by analysing the answers that the different stakeholders have submitted to the questionnaires. The answers, in many cases, pointed to specific national legislation or guidelines, that have been analysed to extract, relevant to this section, the different security controls that have been put in place in the different countries, for the countries that are allowing remote identity proofing.

In fact, there are almost three group of countries with respect to the adoption of remote identity proofing: countries that are allowing for it and standardize it (at a national level), countries that do not allow for it, and countries that have temporarily allowed it during the lockdowns experienced in contrasting COVID-19. While the security controls could be defined only from the analysis of technical guidelines as adopted by remote identity proofing-friendly countries (or, at least, from countries temporarily allowing this process), many countries have highlighted the need to define some specific guidelines following standards, exchanging ideas and experiences from others. This common approach has been guided us in the definition of the different security controls, as we have tried to accommodate and encapsulate differences, providing a reasonable level of detail to allow for an effective understanding of the different specific processes that are implemented all over Europe.

This section provides a list of such security controls, as said not exhaustive and focused on the specifics of the remote identity proofing process, considering it a kind of cyber physical system that requires specific security measures.

This section is organized as follows:

- Some consideration regarding the adoption of these security controls given the LoA of the remote identity proofing system are given, to provide a more robust conceptual model and avoid that unnecessary or overtly complex security controls are implemented when they are not really needed; this integrates with section 4 on security aspects and methodology;
- The security controls are provided as classified in different groups. These groups are for organizational, technical and process controls, and they are mostly for the easiness of reading, as this classification is at a very coarse grain, and the different groups are partially overlapping. A sound security policy should consider this list as a general starting point that must be detailed and tailored to the specific organizational and technical security context. Testing, that is often overlooked, is provided within a specific section;
- This Appendix ends with a table relating the security vulnerabilities as discussed in appendix B with the security controls that could mitigate them.

C.1 ATTACK POTENTIAL AND LEVELS OF ASSURANCE

According to [ISO 15408] part 1, attack potential is defined as measure of the effort to be expended in attacking a Target of Evaluation (TOE), expressed in terms of an attacker's expertise, resources, and motivation. In the context of this report, the TOE is the remote identity proofing process. A thorough assessment of the attack potential should consider resources from different categories. As described in [CC], appendix B, these factors ought to be considered during the analysis of an attack potential required to successfully exploit a vulnerability:

a) Time taken to identify and exploit (Elapsed Time);
b) Specialist technical expertise required (Specialist Expertise);
c) Knowledge of the TOE design and operation (Knowledge of the TOE);
d) Window of opportunity;
e) IT hardware/software or other equipment required for exploitation.

[BSI TR-03147] frames these elements in the context of the remote identity proofing process, while the overall assessment of the attack potential for a successful attack against a TOE should be evaluated using the [CC], appendix B, section B.4.

Broadly speaking, the attack potential tries to assess the amount of resources that an attacker has to employ to successfully circumvent a TOE. In the context of remote identity proofing process, this usually means associating a digital identity to an applicant that is not the legitimate natural person that should be associated with this digital identity.

The same TOE could be used, with specific different operational parameters, to provide digital identities with different LoAs. The eIDAS Regulation by itself considers three different LoAs, but a remote identity proofing system could be employed by a complex organization, like a bank, adapting to domain or organizational specific LoAs.

The attacker gains some advantage by circumventing the TOE, and the attack potential is somehow the cost that the attacker has to pay for gaining this advantage. So, a successful strategy for contrasting attacks is to have an attack potential higher than the benefits resulting from it. Both of these two elements have to be tailored with the LoA that the attacker pursues, and the TOE provides. This strategy is implemented with an appropriate risk analysis, as described in section 4. On practical terms, if the specific remote identity proofing process that is being performed could result in a digital identity with an high LoA, the TOE LoA must implement more security controls, in a more thorough manner, than if the outcome of the process would have been a digital identity with a lower LoA.

This balance is not static in time, as the evolution of technology, the discovery of new vulnerabilities and the more pervasiveness of the digital identity to access more online services are all factors that could make more convenient for an attacker circumventing the TOE, as both the attack potential has lowered or the benefits have increased. Following the same rationale, the same approach should be followed for testing, so a TOE providing digital identities with higher LoAs must be more tested than a TOE providing lower LoAs ones. As such, a risk analysis process should be done on a regular periodic basis, to reflect the evolution of the different risks. Also, in order to make more comparable different TOEs operating under different jurisdictions, the specific metrics adopted to evaluate the robustness of these systems should be the same, tailored to the different LoAs, which should also be categorized in accordance with the eIDAS framework.

By the analysis of the current national regulation and guidelines that have been adopted by the different Supervisory Bodies, it has emerged that some of them, to provide an effective remote identity proofing process during the lockdowns following the COVID-19 pandemic, have chosen to temporarily allow for remote identity proofing by adding some restrictions to the validity of the issued digital identities. Examples of limitations applicable to these identities include access to only some specific services, or limited temporal validity. These measures could be conceptualized in the framework described above, as they are reducing the value, as perceived by an attacked, of circumventing the TOE. At the same time, a more structured and long-standing approach could be more beneficial in terms at least of a more thorough analysis of the attack potential, resulting in more secure TOEs.

C.2 ORGANIZATIONAL CONTROLS

These controls are more related to the staff employed in the remote identification proofing process.

[S_STANDARDS] Apply standards whenever possible, and follow their development. Standardization is a useful tool to provide cybersecurity features for a digital product or process, as it allows for a continuous exchange of ideas and lessons learnt by other practitioners that are then distilled into technical guidelines, also providing for a shared understanding of the specific portion of the world being standardized and a common terminology. This is even more important for the remote identity proofing process, whose results (digital identities) could be consumed in a cross-border scenario.

[S_STOP] Allow the operator to stop and void the remote identification proofing should any suspicion come to his/her mind, without the need to provide any justification to the applicant. In a traditional face-to-face identity proofing process, the operator could hesitate to deny the applicant the requested digital identity for a variety of reasons. As an example, the operator could be embarrassed for the time and effort the applicant has spent in undergoing the face-to-face interview, or he could feel some coercion or even fear physical retaliation. Many of these elements are not applicable in a remote identity proofing setting, resulting in an increased security. To take full advantage of this context, the operator must be always allowed to stop the process and require the applicant to go into a face-to-face setting, without the need to provide any justification or having any kind of personal or performance based impact coming from this decision.

[S_RANDOM_OPERATOR] Assignment of registration officer for a specific remote identity proofing should not be predictable. If the pool of operators is sizable, the specific operator asked to follow the remote identity proofing for a specific applicant should be chosen in a non predictable way, to contrast collusion.

[S_TRAINING] Provide proper and continuous training to the operators. Each one of the EU MSs has many different identity documents, as shown in [PRADO]. Operators should be properly trained for all the relevant identity documents considered as legitimate source of identity for the remote identification proofing. The training should focus on spotting counterfeiting techniques, understanding the psychology and reaction patterns of the subject, and finding evidence of the most typical technical tools adopted by attackers. All these elements are changing over time due to context or technological updates, so the training must be performed regularly.

[S_MONITOR] Define and implement a monitoring process. The remote identity proofing implemented according to these (and other more general) security controls requires some time to be properly performed. As such, monitoring the throughput coming from a specific operator provides a first immediate view on the effective respect of all the security controls. In the same way, monitoring other **process metrics** (e.g. number of rejected identifications) could provide better process analytics and insights useful to spot ongoing weaknesses. Metrics (like false acceptance rate, FAR, and false rejection rate, FRR) are of particular importance if the remote identity proofing leverages on biometrics.

[S_WORKPLACE] Provide a secure and well-organized workplace for the operator. The operator should work from a specific office with physical access control, where he could focus on the task at hand, without any distraction. If he works remotely from home, specific considerations should be made regarding the confidentiality of the process and the absence of distractions.

[S_OPERATOR_VETTING] Operators must be vetted as they perform a security sensitive role. Operators are central to the identity proofing process, especially when it is performed in a completely manual way. For a hybrid process, or even in a fully automated setting based on AI techniques, operators could decide or guide the automatic system when critical situations are flagged. As such, these people must be vet before being hired and, when possible according to the applicable legislation, they could be periodically checked, as requiring penal certificates on regular basis. Note that this kind of control should not result in disqualifying a person that would be otherwise legitimate in issuing face-to-face digital identity, or even traditional identity documents with the same LoAs, were this specific security control not put in place.

[S_AWARENESS] Have a linear and understandable process. It has to be always considered that, the more the remote identity proofing is complex, the more it could be difficult to be followed either by the operator and the subject. A complex process could result in a loss of awareness of what is at stake during each step, and which is the advised line of action or the expected results. This impacts both on the operator and on the subject.

C.3 TECHNICAL CONTROLS

These controls relate to technical elements underpinning the process, and they are usually quantified according to some specific technical metrics.

[S_AUDIO_VIDEO] Define a minimum acceptable level of audio and video quality, and Internet bandwidth and latency. This control allows to discriminate between video artifacts resulting from a limited yet acceptable bandwidth and the forced downgrading of the video quality resulting from the limited resources employed by the attacker. Attacks that are based on the counterfeiting of identity documents, wearing of face masks or quasi real time digital effects are susceptible to be better spotted if the audio and video quality of the session is reasonably high, and if many parameters of the audio and video stream (including latency, adoption of proper audio or video codecs) are monitored. It has to be noted that the cost of CPU power to mount a digital effect attack decreases with time and, as such, these quality levels should increase over time, matching the corresponding evolution and availability of better video and audio cameras and Internet connections.

[S_ACCEPT_CRITERIA_ID_DOCS] Define the acceptance criteria for the validity of the different identity documents. There are two kinds of criteria that must be defined. The first relates to the information stored in the identity documents, including date of issuance and expiration, nationality, and all of these information must be valid (e.g. the document is not yet expired), and checked directly from the document and, if possible also against some specific service made available to legitimate parties (e.g. a national list of stolen documents, or the civil registry to assess the validity of a residence address). The other kind of criteria relates to the physical information from the document. An identity document usually provides a list of anti-counterfeiting features. These are typically grouped in diffractive features (e.g. holograms, identigrams, kinematic structures), personalization technology (multiple laser images, secure typographic elements), material based (optically variable ink) or afferent to the printing (guilloche structures or microlettering). If an MRZ is available in the document, it should also be evaluated, possibly using an OCR working on a screenshot of the document. The remote identity proofing process must require that some of these features are evaluated by the operator, in good lighting conditions, not relying on screenshots but in an interactive process where the identity document(s) is moved on the screen and it interacts with the applicant. The acceptance criteria could be adaptive, when more checks are needed, and they should target different features, providing an intrinsic element of randomness in the process but also covering for all of the security features of the identity document(s) that are acceptable for the remote identity proofing process.

C.4 PROCESS CONTROLS

These controls relate to the actual remote identification proofing process.

[S_LIST_ID_DOCS] Define the list of identity documents that are allowed for the process. As EU MSs have many different identity documents, with different security features and different level of assurance, the IPSP must accept only a specific subset of them, according to their security level and security strength. As an example, in many European countries the driving license is not considered a proper identity document, while some other identity documents (e.g. paper based identity cards) could be considered as not sufficient identity documents per se because they might lack suitable informative image elements such as guilloche structures and micro lettering. In these cases, the operator could ask to provide different additional identity documents to corroborate the identity claim.

[S_MORE_EVIDENCE] Define a list of supplemental evidences to strengthen the process, manage corner cases, or when doubts arise. Instead of relying on a single identity document, the remote identity proofing could be based on some other trust anchors, including but not limited to: other identity or personal documents (e.g. driving license, health card), physical evidence (witnesses), documents from reliable parties (e.g. bills from a bank), general means of authentication (e.g. an SMS OTP, authentication over another digital identity system). These supplemental evidences could be provided as standard part of the procedure (especially for digital identities with a high LoA), or to discriminate some corner-cases or when the operator has some suspicions or doubts. This control includes also the possible access to specific databases like stolen documents, sanctions list, list of wanted people or domain-specific black lists.

[S_BINDING_OUTSOURCE] Define the rights and obligations of all the participating and relying parties. If the identity proofing party uses an external service to carry out the remote identity proofing, it must ensure that the latter implements all the security controls that would be requested, defining in a clear way the rights and obligations of all parties, avoiding that the outsourced process is provided with a lower level of security and trustworthiness.

[S_REALTIME] Request that the remote identity proofing process happens in real time when it requires the participation of the subject, but allow for asynchronous evaluation of its trustworthiness. The interaction between the operator and the applicant must happen in real time, to avoid the possibility for the attacker to mount a staged attack. On the contrary, the evaluation of the trustworthiness of the specific remote identity proofing could be partially delegated to an asynchronous process, where more detailed analyses are performed.

[S_BEHAVIOUR] Verify the behavioural patterns of the subject. The operator must check, as much as possible, that the applicant is not coerced into doing so, acts willingly, and she understands the implications of the process. This control could also comprise the reading of small, random text, to check that the participant has a clear mind.

[S_RECORD_SESSION] Recording and tamper proof storing of the audio and video session. If the remote session is stored and archived for a long period of time, exceeding the validity of the digital identity that is the result of the remote identity proofing, it would be always possible to check later if the entire remote identification proofing has been carried out according to the specific rules of conduct, or if on the contrary some kind of highly sophisticated attack has been gone undetected. This control allows to avoid collusion of the operator (that, in a traditional face-to-face session could always participate in a scam, relying that there are no proof of his/her behaviour during the identification phase). Also, having an integral copy of the video session allows to perform further checks in the future, if needed, to analyse the video and audio stream to identify patterns resulting from some kind of physical (face masks, make up) or digital (digital double, digital morphing) counterfeiting.

These analyses could be most difficult or even impossible to do at the time of the remote identity proofing, but they could be manageable offline or when more advanced computing power or detection algorithms come into the availability of the IPSP or any legitimate party.

[S_ACTIVE_ROLE] Require active participation of the applicant, including some speech. The counterfeiting of someone's voice is a complex process, and if there is an audio recording it is usually possible, by specialized forensic tools and practitioners, to determine if the voice is from the applicant whose digital identity is under scrutiny or not. The spoken part could be not only subject's name or general data (like what day and time it is) but also some random text, to provide for a longer audio segment and some unpredictable variance of the process.

[S_RANDOM_ELEMENTS] Introduce some random elements in the identity proofing. If the process follows the same script, an attacker could pre-define specific elements (like a pre-recorded video) to be played later as requested by the operator. On the contrary, if there are some random elements (like changing the order of the questions or asking out of the blue to raise a hand, rotate the face and similar gestures) this line of attack fails. Also, when these random elements relates to other body parts, they make more costly creating some kind of physical or digital artefact replacing the real subject, as they could make clearer that the applicant is wearing a face mask, or that the digital artefact that is in front of the camera has not been modelled to include the other body parts. This control also contrasts replay attacks.

C.5 SECURITY TESTING

This is an overview of different tests that should be implemented in the context of remote identity proofing. Not all of them may be applicable depending on the mechanisms implemented. Security testing is a core part of the security process for a remote identity proofing solution.

The evaluation of remote identity verification solutions requires regular testing of many aspects of the overall solution: algorithmic performance, operational, technical, sociological. While these tests should of course be measured internally, it is advisable to use external test providers on a regular basis to reduce bias.

A security testing policy needs to be defined and implemented and this section aims to provide initial elements for its development. Although certain tests are indeed part of the elements carried out by the evaluators, there are still too few requirements for regular testing and evaluation in the standards while a security testing policy seems indispensable to guarantee the proper functioning of such services.

C.6 SOFTWARE PERFORMANCE TESTING

As soon as automatic systems (whether AI-based or not) are used to make automatic decisions or to provide decision-making elements to an operator, it is essential to test the performance of the algorithms in conditions as close as possible to reality in order to have an accurate evaluation of the FAR (False Acceptance Rate) and FRR (False Rejection Rate). This evaluation is traditionally carried out during the development of algorithms, but it must be possible to revise it in real conditions. Test campaigns can be implemented either by using representative data sets or by sampling real cases.

While datasets exist for testing technologies related to facial recognition and presentation attack detection, it is much more complicated to test solutions for authenticating identity documents. Indeed, the possession or fabrication of false identity documents is generally not allowed, or at least restricted. It is therefore difficult to set up a dataset including a significant number of counterfeit or forged documents. Moreover, as attackers' techniques are constantly evolving, the threat is also constantly evolving. Difficult as it may be to achieve, the constitution of this set of data is essential in order to be able to measure the performance of the solutions. Of course, both ID document data sets and biometric data sets will have to be created in accordance with GDPR.

[S_TEST_SW_PERFORMANCE] Periodic software performance testing. A periodic software performance testing and monitoring should be put in place using real-like data. It should take into count any bias due to the specific situation. For example, in the case of facial recognition from a photo on an identity document, the dataset will have to reflect the specific nature of this problem.

[S_TEST_MONITOR_SW_PERFORMANCE] Periodic software performance monitoring. If, in the course of the process, the software's verdict needs to be confirmed by an operator, measuring discrepancies in results can be a good way of monitoring the software's performance. The analysis of these discrepancies can identify vulnerabilities, for example on a particular type of document or a particular pattern.

C.7 BREAKTHROUGH TESTING

Since the solution requires information that is provided by the end user, it is important to test the system from end to end by a malicious user. These tests should be performed periodically to take into account the evolution of threats and techniques available to attackers.

[S_TEST_BREAKTHROUGH] Breakthrough testing. These tests must take into account all means of penetrating the system, whether it is to exploit software flaws or to deceive the software or the human making the decision. In particular, the validation of evidence and verification phases will be subject to tests using false documents, presentation attacks, etc. The effort made to break through the system must be consistent with the level of assurance targeted by the service. It is important that this test is carried out at least by a separate team, and if possible, by an external provider, so as not to introduce bias into the means deployed to break into the system. It is this type of test that will uncover flaws in the process itself.

C.8 SOFTWARE SECURITY TESTING

The system as a whole will be regularly tested to ensure that its technical components do not cause security breaches that could be exploited by an attacker.

[S_TEST_VULNERABILITY_SCANS] Vulnerability scans. Vulnerability scans should be performed on a regular basis, both authenticated and unauthenticated in order to detect system weaknesses. In addition, a permanent watch integrated to the software development pipeline should ensure that algorithms and libraries used by the solution do not have any exploitable vulnerabilities.

[S_TEST_PENETRATION] Penetration testing. A periodic penetration test should be performed. These tests must take into account all technical means of penetrating the system. There are several regularly updated security penetration testing methods to refer to (OSSTMM, OWASP, etc.). Ethical hacking or a bug bounty program can also be considered.

[S_TEST_CODE_REVIEW] Code review. Reviewing the code is important to ensure that there are no vulnerabilities in the code developed or integrated to deliver the service. This practice must be supported by the use of tools in the software development pipeline to analyse the code and ensure its quality.

C.9 SOCIOLOGICAL TESTING

As soon as operators are involved in the decision-making process, it is essential to test in real conditions. These tests must be designed to verify that threats have been correctly addressed. These tests must of course be carried out transparently for operators so that they do not adapt their behaviour accordingly.

[S_TEST_DUPLICATE_PROCESSING] Duplicate processing. A statistical performance test can be carried out by sampling cases that will be handled in duplicate, either during a test campaign or permanently. This will measure the rate of cases wrongly accepted and the rate of cases wrongly rejected and will help to identify problems or training deficiencies. The sampling of these tests must be carried out carefully so as to address vulnerable points even if they are poorly represented in the totality of the files. It must therefore take into account specific vulnerabilities, for example on certain types of identity documents or on certain more vulnerable stages of the process.

[S_TEST_SOCIAL_BREAKTHROUGH] Social breakthrough testing. A test can be carried out in the form of a sociological breakthrough test campaign during which testers will try to convince operators to wrongly validate an identity by playing on emotions, for example. This will make it possible to determine possible training actions or instructions to be put in place to avoid social engineering cases. As a side effect, operating this test will increase operators' awareness to this kind of attack. This type of test must be carried out with special care to prevent operators from detecting the test campaign and adapting their behavior.

C.10 CONTRASTING THREATS AND VULNERABILITIES

The set of threats and vulnerabilities discussed in annex B, and the security controls just presented, are naturally related to each other. A security control is justified if it contrasts some threats and/or keeps under control some vulnerabilities, and at the same time a threat or a vulnerability should be properly addressed by a security control. Table 11 provides this correlation in a tabular format, excluding from the list the testing controls (whose names start with S_TEST), as they are more cross-boundary and as such should be always implemented.

Table 11: Contrast of threats and vulnerabilities by security controls

THREAT AND VULNERABILITY	SECURITY CONTROL(S)
T_POLICY_FLAW	S_STANDARDS
T_PHISHING	S_AWARENESS, S_STANDARDS, S_MORE_EVIDENCE
T_DOC_WEAK	S_ACCEPT_CRITERIA_ID_DOCS, S_LIST_ID_DOCS, S_MORE_EVIDENCE
T_DOC_IMPRECISE	S_ACCEPT_CRITERIA_ID_DOCS, S_LIST_ID_DOCS, S_MORE_EVIDENCE
T_DOC_STOLEN	S_ACCEPT_CRITERIA_ID_DOCS, S_MORE_EVIDENCE, S_BEHAVIOUR
T_DOC_FAKE	S_ACCEPT_CRITERIA_ID_DOCS, S_LIST_ID_DOCS, S_MORE_EVIDENCE, S_BEHAVIOUR
T_DOC_FANTASY	S_ACCEPT_CRITERIA_ID_DOCS, S_LIST_ID_DOCS, S_MORE_EVIDENCE, S_BEHAVIOUR
T_DOC_HUMAN_CAPABILITIES	S_STOP, S_ACCEPT_CRITERIA_ID_DOCS, S_LIST_ID_DOCS, S_TRAINING

T_DOC_HUMAN_ERROR	S_STOP, S_ACCEPT_CRITERIA_ID_DOCS, S_LIST_ID_DOCS, S_TRAINING, S_WORKPLACE, S_RECORD_SESSION
T_DOC_SOFTWARE_PERFORMANCE	S_MONITOR, S_LIST_ID_DOCS
T_DOC_CHIP_READING_NOT ALLOWED	S_ACCEPT_CRITERIA_ID_DOCS, S_LIST_ID_DOCS
T_QUALITY_ALTERATION	S_AUDIO_VIDEO, S_REALTIME
T_DOC_IMAGE	S_ACTIVE_ROLE, S_RANDOM_ELEMENTS
T_DOC_VIDEO	S_ACTIVE_ROLE, S_RANDOM_ELEMENTS, S_BEHAVIOUR
T_DOC_AI	S_AUDIO_VIDEO, S_REALTIME, S_ACTIVE_ROLE, S_RANDOM_ELEMENTS
T_DATA_INJECTION	S_AUDIO_VIDEO, S_REALTIME, S_ACTIVE_ROLE, S_RANDOM_ELEMENTS
T_DATA_ALTERATION	S_MORE_EVIDENCE, S_STANDARDS
T_REPLAY	S_ACTIVE_ROLE, S_RANDOM_ELEMENTS
T_FACE_IMAGE	S_ACTIVE_ROLE, S_RANDOM_ELEMENTS, S_BEHAVIOUR
T_FACE_VIDEO	S_AUDIO_VIDEO, S_REALTIME, S_ACTIVE_ROLE, S_RANDOM_ELEMENTS
T_FACE_MASK	S_STOP, S_ACTIVE_ROLE, S_RANDOM_ELEMENTS
T_FACE_AI	S_ACTIVE_ROLE, S_RANDOM_ELEMENTS
T_FACE_HUMAN_CAPABILITIES	S_STOP, S_TRAINING, S_WORKPLACE
T_FACE_LOOKALIKE	S_STOP, S_ACCEPT_CRITERIA_ID_DOCS, S_ACTIVE_ROLE, S_MORE_EVIDENCE
T_FACE_OLD_REFERENCE	S_ACCEPT_CRITERIA_ID_DOCS, S_MORE_EVIDENCE
T_FACE_POOR_QUALITY_REFERENCE	S_STOP, S_ACCEPT_CRITERIA_ID_DOCS, S_MORE_EVIDENCE
T_FACE_SOFTWARE_PERFORMANCE	S_MORE_EVIDENCE
T_DATA_INCONSISTENCY_INACCURACY	S_STOP, S_MORE_EVIDENCE
T_REVOKED_CERTIFICATE	S_ACCEPT_CRITERIA_ID_DOCS, S_MORE_EVIDENCE

T_EMRTD_WEAK_IMPLEMENTATION *	S_STANDARDS, S_ACCEPT_CRITERIA_ID_DOCS
T_BLACKBOX	S_TEST_SW_PERFORMANCE
T_CONSTRAINT	S_STOP, S_TRAINING
T_SOCIAL_ENGINEERING	S_STOP, S_TRAINING, S_WORKPLACE, S_RANDOM_OPERATOR, S_MONITOR
T_BRIBERY	S_MONITOR, S_RANDOM_OPERATOR, S_RECORD_SESSION, S_OPERATOR_VETTING
VT_INSIDER	S_RANDOM_OPERATOR, S_MONITOR, S_OPERATOR_VETTING
T_PROCESS_FLAW	S_STANDARDS, S_MONITOR
T_DELEGATION	S_BINDING_OUTSOURCE

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union’s infrastructure, and, ultimately, to keep Europe’s society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000