EUROPEAN UNION AGENCY
FOR CYBERSECURITY

eIDAS COMPLIANT eID SOLUTIONS

Security Considerations and the Role of ENISA

MARCH 2020

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

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

CONTRIBUTORS

Matthieu GUILLAUME (Wavestone), Saad BOUNJOUA (Wavestone), Claire CLEMOT (Wavestone)

EDITORS

Evgenia Nikolouzou (ENISA), Smaradga Karkala (ENISA), Ioannis Agrafiotis (ENISA), Slawomir Gorniak (ENISA)

ACKNOWLEDGEMENTS

We would like to thank DG Communications Networks, Content and Technology (CONNECT) CNECT.H4 'eGovernment & Trust' and the representatives from the eIDAS Cooperation Network for their valuable comments and contributions in 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

TABLE OF CONTENTS

ACRONYMS

CC: Common Criteria

CEN: European Committee for Standardisation

CID: Commission Implementing Decision

CIR: Commission Implementing Regulation

eID: Electronic Identification

eIDAS: Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market

ETSI: European Telecommunications Standards Institute

ENISA: European Union Agency for Cybersecurity

EU: European Union

FAR: False Acceptance Rate

FRR: False Rejection Rate

GDPR: General Data Protection Regulation

ICAO: International Civil Aviation Organization

ISO: International Organization for Standardization

LoA: Level of Assurance

LoIP: Level of Identity Proofing

MRZ: Machine Readable Zone

NFC: Near-Field Communication

OCSP: Online Certificate Status Protocol

PKI: Public Key Infrastructure

QSCD: Qualified Signature Creation Device

QTSP: Qualified Trust Service Provider

SMS OTP: Short Message Service One Time Password

EXECUTIVE SUMMARY

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereafter the eIDAS Regulation), adopted on July 23rd, 2014, introduces provisions for electronic identification, as being a key lever for the development of a digital single market across Member States. The eIDAS Regulation allows Member States to notify their electronic identification scheme and since September 29th, 2018, the provisions for mandatory mutual recognition of notified eID schemes have come into force. The eIDAS Regulation also introduces 3 levels of assurance, Low, Substantial and High, for the eID means issued under an eID scheme. Finally, it lays down the interoperability framework supporting cross-border electronic identification.

This report provides an overview of the legislative framework under eIDAS for electronic identification, presents the landscape of notified and pre-notified eID schemes and identifies key trends in the electronic identification field. Moreover, it discusses preliminary security considerations and recommendations related to the underlying technologies used for eID means and makes a proposal on the role that ENISA could play in the eIDAS compliant eID ecosystem. Since Germany notified in September 2017 the first European eID scheme under the eIDAS Regulation, an increasing number of countries have started an eID scheme notification process. Other schemes are pre-notified and more will undoubtedly follow, thus demonstrating the success of eID across the European Union.

From historical card-based eID schemes requiring card-readers, Member States and identity providers are moving towards mobile-based solutions, which are more convenient for the end-users. This shift is clearly depicted on the latest notified schemes for which more eID means include the use of smartphone. These eID means can use software applications but can also leverage hardware embedded components such as SIM cards, Secure Element and Trusted Execution Environment for an increased protection against attacks. In the future, it is expected to have more mobile-based eID means relying on such embedded devices. Nevertheless, the security of such an embedded device strongly depends on technology and the actual mobile phone used.

Besides the move to mobile devices, other key trends in the electronic identification field include the increasing use of biometrics and the need to take into consideration users' privacy (protection of the identity data as well as usage of eID means) while building eID schemes. Today, distributed ledger technologies and blockchain for digital identities have also gained momentum, although there are no cases of real world deployements yet.

Security considerations and recommendations

A significant number of published documents already provide relevant and useful guidance on the security of electronic identification means; for instance: ISO standards, NIST Special Publications and European focused documents (including a Guidance Document on Levels of Assurance published by the Cooperation Network, which provides security considerations and examples for a better understanding of the Commission Implementing Regulation 2015/1502).

The reports *of the peer reviews* performed during eID schemes notification processes (some of them being public) and public opinions of the Cooperation Network on notified eID schemes also provide very relevant feedback and key points to be considered while assessing the security of electronic identification means and their compliance with a given level of assurance. It should be highlighted that each peer review report should be considered holistically and judgement on security components can not be drawn in isolation. These reviews and opinions highlight some key security considerations:

- Security of remote identification processes and solutions, as for trust services (e.g. issuance of qualified certificates), is a major concern. There are currently no standards or detailed requirements available to help identify how providers assess their process's compliance with a given Level of Assurance (LoA) based on the classification scale of Regulation CIR (EU) 2015/1502. *However, remote identification requirements for each LoA are currently examined and expected to be formalized in future updates of the document "Guidance for the application of the Levels of Assurance which support the eIDAS Regulation", as* additional guidance and standardization *is needed* in this area.
- A rising number of mobile-based eID solutions require more detailed guidance (especially on cryptographic modules used within the mobile) on their compliance with a given LoA, especially for levels Substantial and High.
- The use of SMS OTP in some eID schemes raises many discussion points regarding the protection it can provide against a potential attack. Specific guidance on this technology may be useful for identity providers.
- As the eIDAS Regulation and CIR 2015/1502 do not require a specific certification scheme for devices used within eID means for LoA High, the security assessment of such devices and the consistency between these assessments may vary. Guidance and further requirements (e.g. from ENISA and the eIDAS Cooperation Network) would be helpful in order to ensure the security level of such devices, and explain how they maintain their security level over time.

It is worth developing guidelines (e.g. ENISA, the Competent Authorities, the eIDAS Cooperation Network) for some of the aforementioned topics to ensure consistency of eID schemes across the Member States. These guidelines would benefit from an overview ofthe eID technology and evolution of threats in this field.

Role of ENISA

Under the Cybersecurity Act, ENISA's role in the eIDAS electronic identification landscape is to support the development and implementation of Union policy, by proving advice and issuing technical guidelines , also for promoting a common understanding of requirements for LoA and to facilitate the exchange of best practices between competent authorities. To that extent, several opportunities to be leveraged by ENISA have been identified, including:

- **Support national initiatives and intiatives of the Cooperation Network on issuing technical and security requirements for eID:** ENISA should work with national competent authorities across the European Union, as well as with the Cooperation Network,to identify their initiatives and facilitate the exchange of best practices on technical and security requirements for the Substantial and High Levels of Assurance of eIDAS.
- **Provide an overview of technological advances and monitor the security of notified schemes:** Due to its mandate to support the European Union to improve cybersecurity, ENISA has a role to play in reporting on the notified security of notified schemes. An overview of technological advances should be carried out and ENISA should facilitate the exahange of best practices and vulnerabilities between the Member States.
- **Publish an annual report on security incidents for eID:** ENISA should publish an annual report aggregating all security incidents which impacted notified electronic identification schemes, alongside with an overview of the threat landscape for eID underlying technologies.
- **Provide guidance on best practice for specific technologies upon request:** ENISA should publish guidelines and recommendations to ensure a consistent understanding of

the requirements of the CIR 2015/1502 of the eIDAS Regulation. These guidelines could include use casesregarding compliance of specific technologies and solutions.

- **Bring insights to the eIDAS review table:** ENISA will also be involved in the eIDAS review process which is due in July 2020. As such, it should bring its technical expertise and insights to define how the Regulation is fit for purpose and identify areas for improvement related to electronic identification.

1. INTRODUCTION

1.1 SCOPE AND OBJECTIVES

Regulation (EU) No 910/2014[1] (hereafter the eIDAS Regulation) regulates the internal market for Trust services in the EU, contributing to the implementation of the European Digital Single Market. Furthermore, the eIDAS Regulation establishes the cross-border recognition of national electronic identification schemes, in cases where Member States have notified these electronic identification schemes.

One of the objectives of this Regulation is to remove existing barriers to the cross-border use of the electronic identification means used in the Member States for authentication, at least for public services. This Regulation does not aim to interfere with electronic identity management systems and related infrastructures established in the Member States. Its goal is to ensure that secure electronic identification and authentication can be used to access cross-border online services offered by Member States.

The mandatory cross-border recognition of notified eID schemes and means applies since September 2018. Following the publication and recognition process of eID schemes, citizens and companies, equipped with a notified eID means, should be able to access online public services in every Member State. The notification process ensures that all notified national eID schemes meet the interoperability and security requirements established in the eIDAS Regulation.

Electronic identification (or eID) constitutes a digital solution, which provides proof of identity for citizens or organisations, to access online services or conduct online transactions. The objective of this report is to overview the state of play of current technologies providing eID solutions, outline the key trends that will guide its evolution, elaborate on security considerations and recommendations on these technologies and provide a first insight into the envisioned role of ENISA in this area. The target audience of the report consists of eIDAS stakeholders and third parties interested in providing eID solutions.

1.2 THE LEGISLATIVE FRAMEWORK

1.2.1 Electronic identification in the eIDAS Regulation

The eIDAS Regulation provides a common foundation for secure electronic interaction between citizens, businesses and public authorities. The Regulation aims at increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union. To this end, it includes provisions for electronic identification and trust services.

The provisions on electronic identification are new as this topic was not addressed in the previous 1999/93/EC Directive superseded by the eIDAS Regulation. These provisions are detailed in Articles 6 to 16 of the regulation and refer to notions of electronic identification, electronic identification means and electronic identification schemes:

- "**Electronic identification**" relates to the process of using personal identification data in an electronic form, uniquely representing either a natural or a legal person, or a natural person representing a legal person.

[1] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

- “**Electronic identification means**” is the material and/or immaterial unit containing the personal identification data and which is used for authentication to an online service, and
- “**Electronic identification scheme**” is the system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons.

The regulation introduces several provisions, which aim to build a framework allowing citizens to use their electronic identification means across borders with a shared level of trust. The provisions primarily encompass the following elements, in particular:

- **Notification**: an electronic identification scheme can be notified to the Commission in order to benefit from cross-border recognition. Member States can submit eID schemes for pre-notification following a pre-defined template that describes the key principles of the scheme. The CID (EU) 2015/1984 defines the circumstances, formats and procedures of notification for eID schemes. It also provides a notification form to be used by Member States. The pre-notified schemes are reviewed by eID experts during a peeriveness review process.The eIDAS Cooperation Network then issues an opinion regarding the compliance of the electronic identification scheme with eIDAS provisions (especially regarding the compliance with the requirements on the claimed LoA). The CID (EU) 2015/296 details the conditions on the cooperation between Member States, including the peer-review of the schemes.
- **Mutual recognition**: electronic identification means that have been issued under notified electronic identification schemes shall be recognised for cross-border authentication to access public online services. This mutual recognition is only mandatory for online services that require electronic identification means with at least a Substantial LoA (meaning Substantial or High) and for eID schemes whose LoA matches the level required by the online service. For instance, a German public service requiring a High LoA electronic identification means shall accept Belgian electronic identification means issued under a scheme notified to the Commission for the High LoA. The CIR (EU) 2015/1501 provides further requirements for the interoperability framework that supports the cross-border authentication.
- **Level of assurance (LoA)**: the Regulation introduces three levels of assurance for electronic identification means issued under notified electronic identification schemes: Low, Substantial and High. 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. The CIR (EU) 2015/1502 describes the minimum requirements to be met for each LoA. It mainly details the requirements expected for the initial identity proofing before issuing the electronic identification means, for the electronic identification means characteristics (design, issuance and activation, lifecycle management), for the authentication process and the general requirements for organisation and management (including requirements for identity providers issuing these electronic identification means).

Figure 1: Main regulatory sources on electronic identification within the eIDAS Regulation

Text	Date	Topic
REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL[2]	July 23rd, 2014	Electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC, hereafter eIDAS Regulation
COMMISSION IMPLEMENTING DECISION (EU) 2015/296[3]	February 24th, 2015	Procedural arrangements for Member States cooperation on electronic identification, pursuant to Article 12(7) of the eIDAS Regulation
COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501[4]	September 8th, 2015	Interoperability framework, pursuant to Article 12(8) of the eIDAS Regulation
COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502[5]	September 8th, 2015	Minimum technical specifications and procedures for assurance levels for electronic identification, pursuant to Article 8(3) of the eIDAS Regulation
COMMISSION IMPLEMENTING DECISION (EU) 2015/1984[6]	November 3rd, 2015	Circumstances, formats and procedures of notification, pursuant to Article 9(5) of the eIDAS Regulation

1.2.2 Focus on the Commission Implementing Regulation (EU) 2015/1502

The Annex of the Commission Implementing Regulation (EU) 2015/1502 (hereafter CIR 2015/1502) details the technical specifications and procedures for each level of assurance for electronic identification means issued under a notified electronic identification scheme. It is organised around 4 main sections:

- Enrolment
- eID means management
- Authentication mechanism
- Management and organisation.

It is worth noting that compliance with a given LoA for an eID means requires compliance with all the requirements for this given LoA (i.e. for the 4 sections). This fact differentiates the eIDAS framework from the NIST SP 800-63-3 framework, which evaluate the identity assurance level (IAL) and the authentication assurance level (AAL) in separate documents[7]. This implies that the “quality” of the identity data verified during the enrolment is correlated with the robustness of the eID means and the associated level of protection against attacks.

The enrolment section details the requirements for identity proofing and verification. Several options can be followed to fulfil the requirements for each level. It is interesting to highlight that a valid eID means can be used during an identity proofing process in order to perform the identity proofing and collect identity data as long as it has at least the same LoA as the eID

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on the electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[3] Commission implementing Decision (EU) 2015/296 of 24 February 2015 on the procedural arrangements for Member States cooperation on electronic identification, pursuant to Article 12(7) of the eIDAS Regulation
[4] Commission implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework, pursuant to Article 12(8) of the eIDAS Regulation
[5] Commission implementing Regulation (EU) 2015/1502 of 8 September 2015 on the minimum technical specifications and procedures for assurance levels for electronic identification, pursuant to Article 8(3) of the eIDAS Regulation
[6] Commission implementing Decision (EU) 2015/1984 of 3 November 2015 on circumstances, formats and procedures of notification, pursuant to Article 9(5) of the eIDAS Regulation

means for which the enrolment is performed. In addition, the enrolement section extends the requirements for legal persons and for the binding between the electronic identification means of natural and legal persons.

The eID characteristics sections detail the requirements for the eID design, issuance, activation and lifecycle management. The following elements can be highlighted:

- eID based on 2 different authentication factors is mandatory in order to reach LoA Substantial.
- For LoA High, the eID means must be protected against attacks with high potential, and against duplication and tampering. However, the notion of high attack potential is not defined in the CIR, but only in the “Guidance for the application of the levels of assurance which support the eIDAS Regulation” to the CIR, issed by the Cooperation Network[8].
- Suspension and reactivation are possible, and the reactivation requires that the same assurance requirements are met as the ones established prior to suspension.
- For the renewal process, the CIR does not explicitly mention a maximum duration validity for an eID means.

Regarding authentication, dynamic authentication is mandatory from LoA Substantial and must precede the release of the identification data. The authentication mechanisms must be capable of resisting attacks with enhanced-basic potential for LoA Low, moderate potential for LoA Substantial and high potential for LoA High respectively.

Finally, the last section on management and organisation details the requirements for participants that are involved in the eID scheme. These requirements cover general provisions for the identity providers, the publication of mandatory information, the information security management, the facility and staff management, the record-keeping, the technical controls and periodic audits.

From a holistic global perspective, it is worth noting that:

- These requirements are agnostic to the underlying technologies used for the eID means. Even if the requirements could, for instance, suggest the use of a dully certified cryptographic module to protect data used in an authentication mechanism for an LoA High eID, no reference to any solution or technology is made, as well as no explicit requirement in terms of certification scheme to be followed for eID means.

- The requirements do not refer to any standards or norms (for instance, ISO 27001 for information security management, etc.) that could be used to ensure compliance. Even if the international standard ISO/IEC 29115 is mentioned in the recitals of the 2015/1502 CIR, no reference to this standard is made in the Annex which details the requirements. Instead, relevant reference is only provided in the “Guidance for the application of the levels of assurance which support the eIDAS Regulation” to the CIR, issued by the Cooperation Network.

1.2.3 Focus on the Commission Implementing Regulation (EU) 2015/1501

The Commission Implementing Regulation (EU) 2015/1501 (hereafter CIR 2015/1501) sets the technical and operational requirements of the interoperability framework in order to ensure the interoperability of the electronic identification schemes which Member States notify to the Commission.

[8] Retrieved from the European Commission website: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents?preview=/40044784/40044786/Guidance%20on%20Levels%20of%20Assurance.docx

It introduces the notion of eIDAS nodes which are used to ensure the connection between Member States. The Regulation elaborates on the requirements that these nodes must satisfy in terms of interoperability, data protection or messages used for communication between nodes, even if no specific standards are mentioned for these purposes. The only standard that has been referenced is the ISO/IEC 27001 for the security management of the node operator. There are no specific requirements for the security of the node regarding the LoA of the electronic identification processed.

The Regulation also mandates the Cooperation Network to issue opinions on technical specifications (see section 2.1.1.2), which could support the interoperability framework, and the Commission to provide a reference implementation as an example, which Member States can apply or use as a sample for testing. The CIR also defines the minimum data set required for person identification in a cross-border context, namely the minimum data set that the eIDAS nodes exchange between them.

1.3 OVERVIEW OF NOTIFIED AND PRE-NOTIFIED eID SCHEMES UNDER THE eIDAS REGULATION

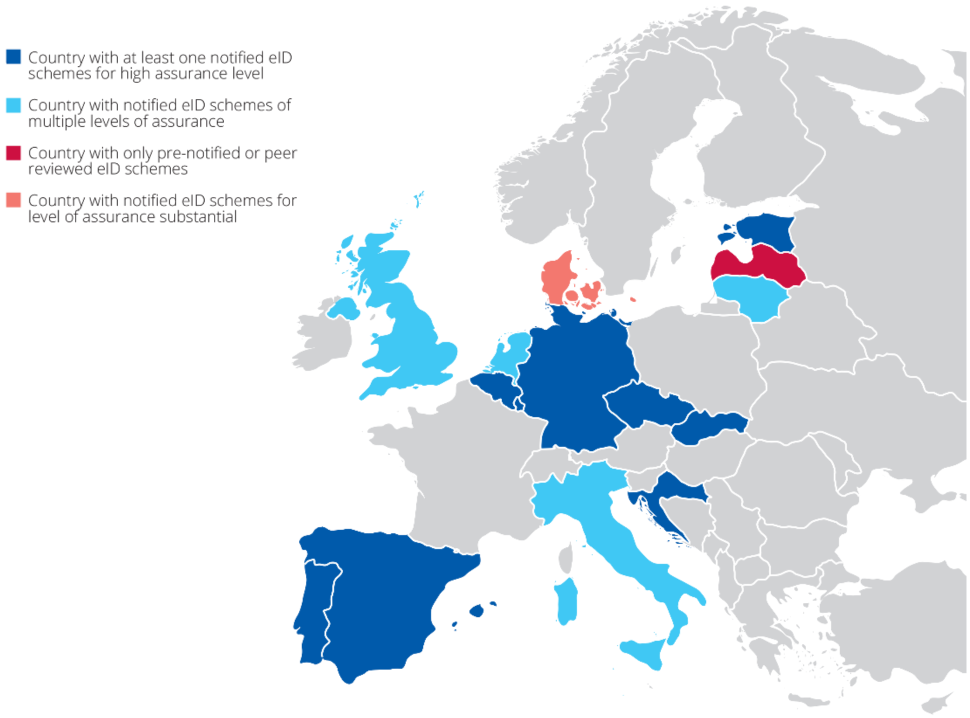
1.3.1 Landscape of notified and pre-notified eID schemes

For many years, certain European countries have been offering digital identities to their citizens. The approach was mainly based on electronic identities supported initially by a national identity card with an electronic chip. For example, Finland was the first country to roll out a national eID card in 1999[9].

Since the eIDAS Regulation has come into force, several Member States have notified an eID scheme. At the time of this report, more than half of European citizens[10] have the ability to use notified (or pre-notified) eID means, thus benefiting from mutual recognition that was made mandatory since 29th September 2018. The notification pace has increased in the last months, and 15 Member States[11] have launched the procedure of notifying and pre-notifying eID schemes. Figure 2 summarises the current state of play regarding notification for Member States under eIDAS.

[9] World Bank Group, 2016. *Digital identity: towards shared principles for public and private sector cooperation.* Retrieved from: http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf
[10] https://twitter.com/Michal_Tabor/status/1133738882586030085
[11] European Commission, 2020. *Overview of pre-notified and notified eID schemes under eIDAS*. Retrieved from: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

Figure 2: Map of notified and pre-notified eID schemes in the European Union


Country with at least one notified eID schemes for high assurance level
Country with notified eID schemes of multiple levels of assurance
Country with only pre-notified or peer reviewed eID schemes
Country with notified eID schemes for level of assurance substantial

In September 2017, Germany was the first country to have a notified eID scheme with eID means based on its National Identity card and its resident permit for the assurance level High. In 2018, the number of notification processes increased notably with six Member States notifying eID schemes between September and the end of December 2018:

- Italy, with its *SPID* scheme, which includes multiple eID means provided by several identity providers for Low, Substantial and High assurance levels (depending on the type of eID means used).
- Estonia, with six eID schemes based on the national identity card, the resident permit card, a dedicated card (*Digi-ID*), the diplomatic card and the e-resident card, as well as a mobile scheme based on a dedicated PKI-enabled SIM (*Mobiil-ID*), all for assurance level High.
- Belgium, Croatia, Luxembourg, and Spain notified eID schemes based on their electronic national identity cards for assurance level High.

In 2019, six more Member States notified their eID schemes for the first time:

- Portugal and the Czech Republic with eID schemes based on the electronic national identity card for the assurance level High.
- The UK with *GOV.UK Verify*, with eID means issued by private players (bank, post office, etc.) appointed by the UK government, for the assurance levels Low and Substantial.
- The Netherlands with a business-oriented scheme (for legal persons) for the levels Substantial and High depending on the identity provider (3 identity providers identified in the schemes providing various eID means).
- Slovakia with an eID card-based scheme for nationals and foreigners for the assurance level High.
- Latvia with a card-based scheme (eID card and dedicated card) as well as a mobile application for the assurance levels Substantial and High.

While also in 2019 two countries notified a second eID scheme:

- Italy with a scheme based on electronic identity cards for the assurance level High.
- Belgium with the FAS/*itsme* scheme, a solution provided by Belgian Mobile ID based on a smartphone application as eID means, for the assurance level High.

In addition, at the delivery date of this report, two schemes were awaiting the completion of the notification process with the publication in the Official Journal of the EU, after the Cooperation Network had already published their corresponding Opinions[12]:

- The *Chave Móvel Digital*, issued by Portugal, notified for the assurance level High, which is based on certificates issued in a remote environment (also providing qualified electronic signature compliant with CEN TS 419 241) and accessed through an authentication mechanism involving a login/password which is coupled with hardware OTP sent through a mobile application (through push notification).
- The *NemID* scheme for Denmark. Similarly to the *SPID* scheme in Italy, *NemID* encompasses a broad set of eID means ranging from basic card code (list of code to be chosen based on a line and a column number) to a smartphone app and hardware OTP generator.

And two more schemes were going through peer review processes after being pre-notified by their respective Member States:

- The *eID / ATK* scheme for Lithuania, based on the Lithuanian national identity card.
- The *DigiID* for the Netherlands, an eID scheme for natural persons based on a smartphone application.

Finally, there is a need for further analysis[13] for the third scheme proposed by Portugal (*Sistema de Certificação de Atributos Profissionais*) to assess whether it meets the definition of an electronic identification scheme, as defined by the eIDAS Regulation. It should be highlighted that each peer review report should be considered holistically and judgement on security components can not be drawn in isolation.

1.3.2 Considerations regarding eID means for notified and pre-notified eID schemes

The first set of eID schemes notified in 2017 and 2018 is mainly based on electronic national identity cards that offer electronic identification capabilities with their chip. This choice was consistent as these countries have a long tradition in issuing these cards with a broad population coverage. This approach takes advantage of an existing physical element, issued during a process which allows strong identity proofing, and does not require additional physical hardware deployment (which will increase logistics concerns and costs) to ensure a high level of security. However, the technical specifications of the applet used on the chip of these cards, for the chip based eID schemes that use this feature, and the way they are used (contact or contactless) may vary from one country to another.

Many countries use chips to perform classic identification, authentication and signature features based on electronic certificates. These cards commonly benefit from a Common Criteria certification (typically with EAL 4 augmented with AVA_VAN.5) [14]. This ensures an adequate level of protection against duplication and tampering and attacks with high attack potential, should the solution be used under the target of evaluation. They also commonly follow

[12] Opinions of the Cooperation Network are publicly available here: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Opinions+of+the+Cooperation+Network

[13] See Opinion No. 06/2018 of the Cooperation Network on the Portuguese eID scheme

[14] https://www.commoncriteriaportal.org/pps/

protection profiles for secure signature creation (such as the Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation[15]). This is, for instance, the case for the notified schemes based on eID cards in 2018 (Italy, Estonia, Spain, Croatia, Luxembourg, Belgium). Portugal also followed this approach for its electronic identity card.

Germany adopted a different approach for its eID scheme notified in 2017. Taking into account strong privacy concerns while building the scheme, the application on the chip follows the BSI technical guidelines TR-03110[16] that extend security mechanisms, which are endorsed by ANSSI and were later described in ICAO (International Civil Aviation Organization) Doc 9303[17] in order to provide electronic identification features. This notably includes PIN management (not managed for Doc 9303 electronic travel document such as a passport chip). During a general authentication procedure, it is ensured that the user correctly knows the PIN code (through password verification using the PACE protocol[18]) and that the terminal trying to authenticate is authorised (through terminal authentication v2 defined in the Technical Report). Data integrity and authenticity of the eIDAS token are also ensured through Passive Authentication and Chip Authentication extended for this TR-03110. In addition, the German eID scheme brings advanced privacy features, such as the ability to perform pseudonymous (sector-specific) identification and signature, in order to avoid the use of a unique identifier. In this scheme, there is no central state-operated identity provider that performs authentication. Any service provider willing to authenticate users based on their eID must be authorised and performs the authentication directly (using a middleware provided by Germany). By 2019, approximately 69 millions German eID cards were issued (the eID application was already enabled on approximately 30 million eID cards)[19]

REMARK

The newly adopted Regulation *(EU) 2019/1157*[20] *on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members* aims at converging towards a common target for national identity cards issued by Member States. The National Identity Cards will, therefore, need to comply with the ICAO Doc 9303, but may contain other applications that use more advanced security mechanisms. Identity cards will contain a chip with an ICAO compliant application that can be used as an electronic travel document, as is already the case for some of the notified eID schemes, which are national eID cards. Member States will implement security protocols described in the Doc 9303 for electronic travel documents (relevant to basic access control, supplemental access control or extended access control for fingerprint protection). As all European identity cards shall be compliant, this could be a lever to develop electronic identity schemes and solutions based on these standards, like the *Alicem* eID solution currently being developed in France (using an ICAO chip on passport or resident permit, with a mobile app and an NFC smartphone), which however has not been pre-notified yet.

It is also worth noting that the Regulation authorises Member States to store data for electronic services such as e-government and e-business in the identity card. Thereby, this does not question the approach of using a national identity card as an eID means.

[15] https://www.commoncriteriaportal.org/files/ppfiles/pp0059b_pdf.pdf
[16] Germany's Federal Office for Information Security, 2016. *BSI TR-03110 Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token*. Retrieved from: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html. See especially part 2 for eIDAS token specification for electronic identification
[17] See relevant part of the Doc 9303 here: https://www.icao.int/publications/pages/publication.aspx?docnum=9303
[18] Password authenticated Connection Establishment, defined in Doc 9303 and here extended with PIN/CAN
[19] According to the data provided by Germany's Federal Office for Information Security, BSI
[20] Regulation (EU) 2019/1157 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 rights of free movement

In addition to the classic eID scheme based on national eID cards, Member States have also notified schemes based on mobile solutions, following usage and expectations of end-users for online authentication. The Estonian *Mobiil*-ID which is card based, the Latvian *eParaksts*, the Portuguese *Chave Móvel Digital*, the Belgian FAS/*itsme* eID, the Danish *NemID,* and some of the eID means issued under the Italian *SPID* scheme are examples, amongst others, of notified or pre-notified solutions that follow this trend. The technologies behind the scheme are thus different.

Mobiil-ID uses a specific SIM-card that is issued by mobile operators under contractual agreement. This SIM card has an embedded dedicated application for electronic identification and electronic signature. SIM cards provided are Common Criteria certified and are QSCD for electronic signature. The part used by the operator of telecommunication services is out of scope of this qualification. The user has two different PIN codes in order to use the authentication certificate for electronic identification or the signature certificate for electronic signature. The solution supports both RSA and elliptic curves for the private key used for authentication and signature.

Regarding *Chave Móvel Digital* or *itsme*, the approach is different as the keys used for authentication are stored in a remote environment. The security of the scheme strongly relies on the authentication mechanism that is used on the mobile device to access these keys when triggering the authentication process and especially on how these devices protect any kind of secret used within the authentication mechanism.

For *itsme*, the solution is based on a smartphone application that needs to be enrolled, either through an authentication solution managed by a registered bank (the registered banks are the IDPs) or by using the national identity card (also notified as an eID means by Belgium). The authentication mechanism requires the user to type a PIN code (chosen during enrolment) in the enrolled application after receiving a notification. The PIN could be replaced by a biometric[21] factor supported by the smartphone (fingerprint or facial recognition depending on the smartphone).

SPID and *NemID* also provide users with a mobile application (amongst other solutions such as hardware token for these “multi eID means” schemes). Mobile applications could be used to generate an OTP to copy on, as it is the case for *SPID* or with an out of band confirmation after receiving a notification and typing a PIN for *NemID*.

1.4 eID KEY EVOLUTIONARY TENDENCIES AND OTHER CONSIDERATIONS

1.4.1 Increasing usage of mobile-based systems

As described in section 1.3, mobile-based identification schemes are already in place in several European countries, including Austria, Belgium, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, Norway, and Sweden.

Other Member States also investigate the use of mobile-based electronic identification schemes, as mobile usage has surpassed desktop usage worldwide (53% of website visits were made via mobile in 2018[22]), the mobile transactions are on the rise and these mobile transactions require a seamless, secure identification, which will perhaps be mobile-based.

[21] The Opinion No. 8/2019 of the Cooperation Network thus indicates, amongst other, that the use of biometric authentication must be disabled to meet requirements for LoA High
[22] Retrieved from *StatCounter* website: https://gs.statcounter.com/platform-market-share/desktop-mobile/worldwide/#yearly-2018-2018-bar

This trend relies on a high and increasing mobile penetration in Europe (85% in 2017 and estimated to go up to 88% in 2025[23]). Mobile identity services are expected to be used across many sectors, from banking to public services. Mobile-based systems have the advantage of offering convenience and security. For example, mobile applications could leverage functionality offered by mobile devices, such as geolocation and biometric features.

Moreover, mobile devices tend to increasingly make use of cryptographic modules, such as Trusted Execution Environments, Secure Elements, eSIMs and iSIMs. eID schemes which utilise these cryptographic modules could thus have an improved security.

1.4.2 Biometrics – shifting towards multimodal and behavioural

Biometric authentication is on the rise: by 2022, 5.6 billion mobile devices will be used to verify 1.37 trillion transactions[24]. These transactions will leverage upon built-in sensors on smartphones.

As using a single biometric modality poses certain weaknesses, multimodal biometric systems and behavioural biometrics are gaining traction. However, it should be noted that behavioural biometrics are not among the authentication factors authorized for eID schemes according to CIR 2015/1502[25]. Single modality, even if used in multi-factor authentication environments, can be hacked or hijacked. For example, authentication mechanisms always revert to a password when a biometric authentication fails (see also section 1.1.1.1AB.3 on additional security considerations regading biometrics). In response, multimodal biometric systems will be increasingly used. The different types of multimodal biometric systems are mentioned in Figure 3.

Figure 3: Types of multimodal biometric systems[26]

System	Definition
Multiple sensors	A system obtaining data through multiple sensors using one biometric feature
Multiple samples	A system with multiple algorithms processing a single biometric feature
Multiple traits	A system consolidating multiple occurrences of the same body trait
Multiple instances	A system using multiple templates of the same biometric method obtained with the help of a single sensor (e.g. multiple fingerprints from different fingers)
Multiple representations	A system combining information about the biometric features of the individual

[23] GSMA, 2018. *The Mobile Economy Europe 2018*. Retrieved from: https://www.gsma.com/r/mobileeconomy/europe/
[24] Alex Perala, 2017. *Shift to cloud-based biometrics is coming: Acuity*. Retrieved from: https://findbiometrics.com/shift-cloud-based-biometrics-acuity-409204/
[25] Commission implementing Regulation (EU) 2015/1502 of 8 September 2015 on the minimum technical specifications and procedures for assurance levels for electronic identification, pursuant to Article 8(3) of the eIDAS Regulation, Annex, article 1. par.2.
[26] CHORAS R, *Multimodal Biometrics for Person Authentication*, 2019, https://www.intechopen.com/online-first/multimodal-biometrics-for-person-authentication

The availability of many features means that multimodal systems become more accurate and reliable, and thus ensure security: if one modality is eliminated, the system can still ensure security by using the remaining modalities.

Behavioural biometrics (see also 1.1.1.1AB.3 for a more extensive definition of behavioural biometrics) are also becoming popular because of their convenience and continuous authentication capabilities. Their collection is transparent for the user: they are, for instance collected through pressure of fingers on the screen, how quickly someone types, the angle at which the device is held, etc. The global behavioural biometrics market is predicted to reach $3,922.4 Million by 2025[27].

1.4.3 Private sector involvement

Traditionally, governments would issue identity documents to citizens who would then use them to prove their identity in the physical world. However, this identity ecosystem is changing with private sector organisations being more and more involved, providing identity solutions or services to both their own customers and other entities.

For example, according to GSMA, banks collectively spent more than $1 billion on identity solutions in 2017[28], making them the world's largest investors, even over public institutions. Financial organisations, post offices and telecommunication operators, traditionally have been conducting identity proofing. They are now leveraging their procedures to resell this service to other organisations that rely on verified identities. Several identity schemes based on a federation of private sector identity providers are already notified under eIDAS, including *SPID* in Italy[29], *GOV.UK Verify* in the United Kingdom[30] and FAS/*itsme* in Belgium[31].

Government issued eIDs could also be used to "verify" or "endorse" identities provided by other organisations, including those with Mobile Connect authentication means.

1.4.4 Privacy concerns

Privacy is a key topic driven by user preoccupation, a rights framework and a strong legal framework in the EU[32]. This trend impacts digital identities: sharing a digital identity online is practical to access services, but once authentication is performed, the question is what happens to the shared data. Citizens should have the right to keep control of their personal data and its use. They are entitled to a digital identity under their own control, to use different verified attributes to access a range of services as and when needed. Only information that needs to be shared should be exchanged, and the identity proofing using multiple pieces of personal information should only happen once.

A privacy-centric approach would enable citizens to prove a specific fact instead of releasing the underlying data – for example, proving "I'm over 18" instead of providing the full date of birth or proving "I'm a British citizen" instead of handing over full passport details. These practices are in line with the data minimization principle resulting from the data protection legislation.

Germany's eID takes into account these privacy principles: the unique identifier is only present on the German eID and is never shared with the service provider; only a pseudonym is shared

[27] https://www.alliedmarketresearch.com/behavioral-biometrics-market
[28] https://www.gsma.com/identity/digital-identity-expect-2018
[29] Agenzia per l'Italia Digitale, n.d. Gestori delle identità. Retrieved from: https://registry.spid.gov.it/identity-providers
[30] Governmental Digital Service, 2019. *GOV*.UK Verify overview. Retrieved from: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
[31] Retrieved from *itsme* website: https://www.itsme.be/en/
[32] 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 and Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector.

and this pseudonym is different from one service provider to another[33]. Similar features apply to Luxembourg's eID card, while the UK has made this topic a major trend in their 2019 Call for Evidence around Digital Identity, referencing to security concerns[34].

1.4.5 Self-Sovereign Identities and Verifiable Claims

Privacy concerns described in the previous chapter originated the Self-Sovereign Identities (SSI) approach. This approach is based on the idea that users should manage their own Personally Identifiable Data and make sure that only the pieces of information which are absolutely necessary to to prove their legitimacy will be shared with the service provider in order to access their services. A self-managed identity framework no longer requires centralised systems to manage the lifecycle of identities, and a decentralised system is needed to implement this approach. Blockchain is a technology that offers both a decentralised operating model and immutability ensuring the data integrity. It is thus able to support such an approach (see also B.4.1 for additional details), although it is not the only technology for implementing Self-Sovereign schemes. However, under the eIDAS framework, a central entity, to enrol and verify identity data, is always necessary, as eID under eIDAS is based on verified identities.

One important aspect of the Self-Sovereign Identity approach is the fact that the user can share only relevant personal data to service providers. To illustrate this, we can consider a sport-betting website where only adults can use their services: in a classic authentication scheme, the user will need to communicate his/her date of birth (probably alongside an identity card containing other personal information) to prove he/she is an adult. Thus, realising more information that the website truly needs. The only information the service must know is the answer to the question "Is the user over 18 years old? (or 21, depending on the country)". In a Self-Sovereign Identity scheme, the user will prove he/she is "over the age of 18", without having to share his/her actual birth date. The statement that the user is over the age of 18 is called a "Verifiable Claim" than can be previously validated by a trusted identity provider.

Trust in these Verifiable Claims is necessary for public and private services to use Self-Sovereign Identities. Underlying this trust is the question of where the Personally Identifiable Information comes from and how it was imported. The maturity of Self-Sovereign Identities solutions and the amount of services using this technology will only grow once this question is addressed.

The first implementations of these approaches are already taking place, such as the one being developed by the *Sovrin Foundation*[35]. Canada has also issued a challenge to propose technical solutions to support these approaches[36]. In Europe, the regional Catalan government presented in September 2019 *IdentiCAT*, a decentralized digital identity project based on the blockchain technology, in the form of a mobile application expected in 2020[37].

[33] Federal Office for Information Security, 2017. *German eID based on Extended Access Control v2*. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_LoA_Mapping.pdf?__blob=publicationFile&v=4

[34] GOV.UK, 2019. *Closed consultation on digital identity*. Retrieved from: https://www.gov.uk/government/consultations/digital-identity

[35] https://sovrin.org/

[36] https://www.ic.gc.ca/eic/site/101.nsf/eng/00068.html

[37] https://www.catalannews.com/tech-science/item/catalan-government-presents-identicat-decentralized-digital-identity-project

2. SECURITY CONSIDERATIONS

2.1 DOCUMENTS AND STANDARDS REGARDING eID SECURITY

2.1.1 eID related European documentation: Guidance on Levels of Assurance

The Cooperation Network has released a guidance document[38] for the application of the levels of assurance which support the eIDAS Regulation. This document follows the CIR 2015/1502 plan and provides guidance and examples to illustrate how the requirements described in the CIR could be met (for Low, Substantial and High LoA). The document starts by detailing the applicable definitions from the CIR 2015/1502 Annex:

- Authoritative source
- Authentication factor, including Possession-based authentication factor, Knowledge-based authentication factor and Inherent authentication factor
- Dynamic authentication
- Information security management system.

Following these extensive definitions, the guidance document exhaustively lists the CIR 2015/1502 requirements, following the agenda of the CIR Annex, thus covering the three topics developed during the peer reviews: enrolment, eID means design and authentication, organisation and management. It also provides guidance to help identity providers comply with these requirements.

Regarding the enrolment topic and the comparison between “one or more physical characteristic” of the applicant “with an authoritative source” for the LoA High, the document states that if staff is involved in this comparison, the staff must be “sufficiently skilled” and if automated matching is used, “available best practice should be taken into account”. Best practices about trained and skilled staff are provided in the document, such as possessing knowledge of document design, security features, watermarks and printing techniques, and being able to identify forged and counterfeit documents. However, the current version of the guidance document does not elaborate on best practices and requirements regarding remote identity proofing (performed for instance with videoconference or facial recognition), but a subgroup of the Cooperation Network is currently working on adding parts related to remote identity proofing.

In the electronic identification means characteristics and creation section, examples of protection “against duplication and tampering against attacks with high potential” are provided to satisfy the LoA High:

- Embed cryptographic key material in tamper-resistant hardware security module if possession-based authentication factors are used.
- Liveness detection, trusted environment, low false match rate if inherent authentication factors are used.
- Certification against relevant technical standards (e.g. Common Criteria).

[38] Retrieved from the European Commission website: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents?preview=/40044784/40044786/Guidance%20on%20Levels%20of%20Assurance.docx

The authentication section of this guidance document provides a first insight on how an attack potential could be interpreted and calculated. The potential of the attacks used in the eIDAS Regulation (enhanced-basic, moderate and high) considers examples from ISO/IEC 15408 “Information technology – Security techniques – Evaluation criteria for IT security” and ISO/IEC 18045 “Information technology – Security techniques – Methodology for IT security evaluation”. The document recommends assessing an authentication mechanism taking relevant threats into account (online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading are mentioned in the ISO 29115[39]).

It is worth noting that the document, as it is merely a guidance, provides illustrations and security considerations. However, it does not provide explicit recommendations and mandatory protection measures. Consequently, it is not a framework against which conformity with a given LoA can be assessed. Additionally, guidance is not provided for all the requirements (incl. legal person identity proofing and verification and renewal and replacement) in the current version. Additional examples in the relevant sections (for instance eID means design and authentication) could also be provided in order to give more insights to identity providers and to allow them to consider these recommendations when designing new eID solutions.

Nonetheless, this guidance document is highly beneficial and should be enriched in the next version to be adopted by the Cooperation Network, in order to provide eID solution providers with more examples and guidelines. Some Member States are working on such a guidance framework that could also be used for evaluation at National level[40]. The requirements’ framework prepared by ANSSI follows the same structure as the guidance document but includes more recommendations and requirements that should be applied at national level.

2.1.1.1 Guidance on Notification

The Cooperation Network has also released a guidance document (drafted by Austria, Estonia and the United Kingdom) for the notification process[41], with the objective to provide guidance on how to fill in the notification form. Currently, this document only provides guidance for two sections of the notification form. It could be enhanced by providing guidance for each section of the notification form, taking advantage of the feedback and suggestions of the Cooperation Network and members of peer reviews that have assessed almost 15 notification forms.

2.1.1.2 Interoperability framework for eID

In line with the requirements of the eIDAS Regulation, technical specifications have been developed in order to ensure interoperability and help Member States to implement the eIDAS compliant implementation. The eIDAS Cooperation Network[42] has endorsed a new set of technical specifications (version 1.2) in Opinion No. 5/2019, superseding Opinion No. 2/2016. The specifications have been developed by Member States and the European Commission collaborating in the technical subgroup on eID of the eIDAS Cooperation Network.

To provide a comprehensive framework for interoperability, the current version of the technical specifications consists of four separate documents, each concerning a specific area. This framework, and especially the cryptographic requirements part, provides useful guidance in order to ensure the confidentiality and the integrity of the data exchanged during a cross-border

[39] Refer to section 2.1.2.2 ISO/IEC 29115:2013 – Entity authentication assurance framework for additional information
[40] The requirement framework prepared by ANSSI is not public yet but will be published on the ANSSI website.
[41] Retrieved from the European Commission website: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents?preview=/40044784/52602661/Guidance%20on%20Notification.docx
[42] Cooperation Network established by the Commission Decision EU 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) 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%3A32015D0296

authentication process between the nodes. Even if it does not apply to the eID means itself, it provides key security measures for the eID scheme generally, for the implementation of nodes and the data exchanges between nodes. Moreover, security flaws or vulnerabilities in the implementation of the interoperability framework could endanger the whole electronic identification process.

As a recent example, a vulnerability in the eIDAS node integration package provided by the European Commission was discovered in June 2019 and publicly disclosed on 29th October 2019[43]. This vulnerability , which exploited a bug in the implementation of the system, identified a weak procedure to verify the certificates used to sign SAML responses. By creating a certificate (under relevant assumptions), it was possible to sign SAML responses for which the signature was considered valid by the receiving MS node. By doing so, it was theoretically possible, by forging a SAML response, to impersonate an identity in a cross-border authentication context.

As also explained in section 1.2.3 of this report, the CIR 2015/1501 does not explicitly include security measures for the nodes and node operators other than the adherence to ISO/IEC 27001 or equivalent. As a next step, an assessment could be carried out to include security recommendations for node implementation in the Regulation (as per CIR 2015/1502) in order to align the security of the interoperability part with the one of the eID means.

2.1.2 Other international & third-country frameworks

2.1.2.1 ISO/IEC 29003:2018 – Identity proofing

The ISO/IEC 29003:2018 standard gives guidelines for the identity proofing of a natural person and specifies levels of identity proofing, as well as requirements to achieve these levels.

Identity proofing is the process to verify identifying attributes to be entered into an identity management system and to establish that the identifying attributes pertain to the subject to be enrolled. It includes the collection of identity attributes, the verification of these identity attributes against authoritative sources and proof that the subject is indeed bound to the claimed identity attributes.

This standard defines three levels of identity proofing (LoIP) (see

Figure 4). The levels are described as a combination of the assurance in the existence of the identity and of how it is linked to the applicant. In order to achieve identity proofing at a specific LoIP, the process shall successfully prove the existence of the identity at that LoIP and the identity/subject binding at that LoIP.

[43] See *sec-consult* website: https://sec-consult.com/en/blog/2019/10/vulnerability-in-eu-cross-border-authentication-software-eidas-node/

Figure 4: Levels of identity proofing (LoIP) under ISO/IEC 29003:2018

LoIP	Definition	Requirements regarding the existence of the identity	Requirements regarding the identity/applicant binding
LoIP1	Low confidence in the claimed or asserted identity (identity is unique within the context, there is an assumption the identity exists, and the subject is assumed to be bound to the identity).	The identifying attributes are accepted without carrying any checks.	The binding is accepted without carrying any checks.
LoIP2	Moderate confidence in the claimed or asserted identity (identity is unique within the context, it's moderately established that the identity exists, and the subject has some binding to the identity).	The identifying attributes exist in corroborative evidence.	The binding was checked using one factor.
LoIP3	High confidence in the claimed or asserted identity (identity is unique within the context, it's strongly established that the identity exists, and the subject has a strong binding to the identity).	The identifying attributes exist in authoritative evidence.	The binding was checked using two or more factors.

Levels of identity proofing should be selected based on a risk assessment of the subsequent service and/or credential to be provided.

2.1.2.2 ISO/IEC 29115:2013 – Entity authentication assurance framework

The ISO/IEC 29115:2013 standard provides a framework for entity authentication assurance. An entity can be either a natural person or a legal person, referred to as NPE for Non-Person Entity throughout the document. After defining four levels of assurance (from LoA1 to LoA4) and different actors, the security considerations are organised in three sections: the enrolment phase, the credential management phase and the entity authentication phase. Guidance is also provided regarding management and organisational considerations (e.g. legal and contractual compliance, information security management and audit, external service components).

The four levels of assurance are described as followed:

- 1 – Low: Little or no confidence in the claimed or asserted identity but enough confidence that the entity is the same over consecutive authentication events
- 2 – Medium: Some confidence in the claimed or asserted identity
- 3 – High: High confidence in the claimed or asserted identity
- 4 – Very high: Very high confidence in the claimed or asserted identity.

Levels of assurance are to be selected based on a risk assessment of the transactions or services for which the entities will be authenticated. The standard provides a table to facilitate this risk assessment by suggesting possible consequences and impacts of authentication failure at the various LoAs. For example, if the personal safety of an entity could be substantially impacted by an authentication failure, then the appropriate LoA is Very high.

Security considerations, called controls, are listed relating to threats, i.e. specific examples of what an attacker could do. For enrolment and credential management considerations, these threats are translated into controls based on the level of assurance: security considerations are stronger for a High LoA than for a Low. The authentication phase is described differently: most security considerations are applicable to all levels of assurance and should be applied as determined by a risk assessment.

One key enrolment security consideration is that the enrolment must be completed in person (for a natural person) to reach a very High LoA while it is not a requirement in the CIR 2015/1502 (remote enrolment could be used for LoA High). Another credential management control is that credentials shall be contained on a hardware security module to achieve a very High LoA. On their part, the authentication-related controls range from Multi-Factor-Authentication to the adoption of anti-phishing measures and anti-counterfeiting measures on devices holding credentials.

This ISO standard is quoted in recitals of the CIR 2015/1502, stating it was taken into account for the specifications and procedures set out in the implementing act, but the requirements of the CIR do not reference any specific section or requirement of the standard. Some Member States, however, provide references to this ISO standard in their notification form.

2.1.2.3 NIST SP 800-63 – Digital Identity Guidelines

In 2017, NIST published four volumes to provide technical requirements for American federal agencies implementing digital identity services. The guidelines define technical requirements in the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation and related assertions. These guidelines are agnostic to the vast array of identity service architectures that can be developed and used.

The four volumes are the following:

- SP 800-63-3: Digital Identity Guidelines[44]
- SP 800-63A: Enrollment and Identity Proofing[45]
- SP 800-63B: Authentication and Lifecycle Management[46]
- SP 800-63C: Federation and Assertions[47].

Unlike the eIDAS Regulation where levels of assurance are described in tandem to identity and authentication, the levels of assurance in the NIST document, called xALs, are broken down into independent levels regarding:

- Identity proofing (Identity Assurance Level: IAL)
- Authenticators (Authenticator Assurance Level: AAL)
- Federated assertions (Federation Assurance Level: FAL), referring to the strength of an assertion in a federated environment, used to communicate authentication and attribute information to a relying party.

[44] https://doi.org/10.6028/NIST.SP.800-63-3
[45] https://doi.org/10.6028/NIST.SP.800-63a
[46] https://doi.org/10.6028/NIST.SP.800-63b
[47] https://doi.org/10.6028/NIST.SP.800-63c

Each xAL has three levels, from xAL1 to xAL3. IALs must be selected by service providers based on their risk profile and on the potential harm caused by an attacker making a successful false claim of an identity. AALs must be selected based on the risk profile and the potential harm caused by an attacker taking control of an authenticator and accessing the service. FALs must be selected based on the risk profile and the potential harm caused by an attacker taking control of federated transactions. Flowcharts are made available in the SP 800-63-3 volume to help service providers perform a risk assessment in order to select their three xALs.

It is worth noting that all combinations of Identity Assurance Levels and Authenticator Assurance Levels are acceptable, except AAL1 with IAL1 with personal data, and IAL2 and IAL3, as passwords on their own are not enough to protect personal information according to the E.O. 13681[48] (section 3: "*all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.*").

One topic to highlight in the NIST guidelines is the "in-person proofing". "In-person proofing" is required at IAL3 and can be satisfied in either of two ways:

- A physical interaction with the applicant, supervised by an operator; or
- A remote interaction with the applicant, supervised by an operator, based on a strict set of requirements, including:
  - A seamless monitoring of the credential service provider during the entire identity proofing session from which the application shall not depart, for example, by a continuous high-resolution video transmission of the applicant through an agency-controlled device.
  - A monitoring of the entire identity proofing session by a live operator participating remotely, previously trained to detect potential fraud and to perform a supervised remote proofing session.
  - A digital verification of evidence (e.g. via chip or wireless technologies) performed by integrated scanners and sensors.
  - Communications occurring over a mutually authenticated protected channel.

Another highlight of these technical guidelines regarding authentication is that authorised authenticator types are listed for each AAL.

Regarding out-of-band authenticators, the document forbids OTPs via email ("[Authentication] methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication") and places restrictions on the use of SMS for OTP[49]. The use of the Public Switched Telephone Network (PSTN) for out-of-band verification is stated as "*RESTRICTED*" and NIST may adjust this status over time based on the evolution of the threat landscape and the technical operation of the PSTN. Implementing a RESTRICTED authenticator requires the agency to assess, understand, and accept the risk associated with that authenticator.

The use of biometrics in the document is only partially supported for authentication because of known limitations of such technologies (need to manage relevant False Match Rate, result of a comparison is not deterministic, risk of theft of biometrics template without possible revocation,

[48] https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions
[49] Referred in the FAQ as authenticators leveraging the public switched telephone network (as for phone OTP as well). Restrictions for such authenticators include to verify that the pre-registered telephone number is associated with a specific physical device, to bind a new authenticator if the registered phone number changes, not to display the authentication secret while the device is locked and to request a PIN, passcode or biometric to view, ask the user to accept the reception of this secret.

etc.). They should only be used as part of a multi-factor authentication process with a physical authenticator, and additional requirements apply[50].

Lastly, privacy is a strong concern of these technical guidelines. Many different measures are listed, for instance:

- The collection and processing of Personally Identifiable Information (PII) shall be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation and verification.
- The Credential Service Provider shall provide explicit notice to the applicant regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.
- Multiple analysis and actions should be performed to frame the use of PII (perform privacy risk assessments, consult with the Senior Agency Official for Privacy, publish a System of Records Notice, publish a Privacy Impact Assessment, etc.).

It is important to note that the NIST SP 800-63[51] provides very detailed and specific requirements that are directly bound to specific types of authenticators or solutions. This is also a noticeable difference with the eIDAS approach which remains technology agnostic. On one hand, it allows very detailed guidelines for identity providers that want to set up an eID scheme. On the other hand, it will require an extensive update process as technologies and solutions evolve very quickly.

2.1.2.4 CEN/TR 419010 – Framework for standardisation of signature – extended structure including electronic identification and authentication

The purpose of this technical report is to analyse the impact of CIR 2015/1501 and 2015/1502 on the already published standards for electronic signature and to analyse if updates or further standards for identification and authentication are needed.

The technical report starts by providing an overview of the CIR 2015/1502 on levels of assurance for eID means and the CIR 2015/1501 on the interoperability framework. The report also mentions that a comprehensive framework for eID interoperability has also been published, covering interoperability architecture, SAML message format, SAML attribute profile and cryptographic requirements for SAML and TLS.

The core of the report describes the potential impact of both CIR 1501 and 1502 on the framework for the standardisation of signature as described in ETSI/TR 119 000. Specifically, it details the foreseen impact or evolution on the six functional areas of the framework:

- Signature creation and validation
- Signature creation and other related devices
- Cryptographic suites
- Trust Services providers supporting digital signature
- Trust application services providers
- Trust service status list providers.

The considerations mainly focus on the cases where the standards could benefit from the provision brought by eIDAS on electronic identification (especially considering interoperability

[50] Refer to NIST SP 800-63B section 5.2.3. for these additional requirements.
[51] The SP 800-63 also includes a FAQ that gives useful examples for a better understanding of the publications.

architecture with 2015/1501 and LoA with 2015/1502). For instance, references to identification and authentication are relevant:

- When an identity proofing is required to issue a certificate or
- When authentication of the signer is required to activate a remote signature process.

The considerations are thus not focused on the eID solution itself. Besides, the CEN/TR 419010 report, published in 2017, references several standards that have evolved since. The analysis could thus be updated to provide a contemporary overview of the standardisation situation and examine how to further expand the existing standards (e.g. by adding references to relevant identification or authentication provisions for instance).

The last section of the technical report identifies possible areas where additional standards could be developed in the field of eID. It notably identifies that standards are needed for identity providers (as for trust services providers). Especially, it could cover technical specifications for:

- Policy requirements for identity providers issuing identification and authentication services for a considered authentication level of assurance.
- Profile for protocol and/or data format for a considered authentication level of assurance for identity providers.
- Compliance testing of these profiles.

The second topic identified as relevant for standardisation is devices supporting identification and authentication. Standards developed around this topic could describe eIDAS compliant eID application profiles and conformity assessment methodologies[52].

2.2 SECURITY CONSIDERATIONS FOR eID SOLUTIONS BASED ON PEER REVIEW FEEDBACK

2.2.1 Introduction

This section highlights the security considerations that emerged from the various peer reviews of the eID schemes which have already been pre-notified to the European Commission by Member States. These considerations are of interest, as they highlight recommendations to be followed for a targeted LoA. These considerations cover the main topics that are studied during peer reviews, following the structure of the CIR 2015/1502:

- Enrolment
- Electronic identification means management and authentication
- Management and organisation.

These considerations and recommendations are not exhaustive and are only examples of topics that raise questions and discussions that could also benefit from further guidance. Further analysis of the technologies used on eID solutions is provided in the Annex “Technological landscape of eID solutions”.

2.2.2 Enrolment

2.2.2.1 Verification of document for identity proofing

Peer reviews have highlighted complexity for the verification and validation of identity documents, especially in the case of foreign identity documents that are used for a request of an eID (as it is the case for some of the already notified eID schemes). As personnel in charge of document verification are not always trained to handle such documents, identification could

[52] Examples of PP given include for instance the PP for German eID (based on TR 03110) and PP EN 419251 (2013).

be difficult. These considerations do not apply to a specific scheme but could be faced by any Member State that needs to verify the identity of non-residents within the scope of their eID scheme. Some recommendations could thus be identified, including:

- International databases such as the Schengen Information System (SIS) or Interpol databases, PRADO database for verification of optical/physical security features of identity documents, iFADO (Intranet False and Authentic Documents Online) should be used to confirm the documents' validity.
- If the verification is performed physically or if the identification is performed solely based on the picture of a document, a professional and trained agent should assess the validity of the document.

Consequently, the robustness of the measures in place could affect the assurance that can be placed in the identification process and thus the associated LoA. This consideration may apply to all Member States with schemes that are opened to foreigners with foreign-identity documents.Therefore an EU-wide approach with shared and common guidance could be of interest for all Member States to address these considerations.

2.2.2.2 Remote identification (video-based) and facial recognition

The use of remote processes for identity proofing before issuing the eID means has been subject to several security considerations across different peer reviews. This topic is of great interest as it is now utilised by more processes, and we can expect this use to increase. Besides the use of remote identification in eID schemes, we can, for instance, mention:

- Digital Bank account (know also as neo-bank account) opening that uses a video call with a bank operator in order to present in front of the camera an identity document and check that the applicant has the alleged identity in the identity document.
- Car-rental websites that enrol customers by scanning their driving licence to perform a facial recognition with liveness detection in order to ensure the customer corresponds to the driving licence.
- Remote identification processes already in use for the issuance of qualified certificates for trust services under eIDAS.

As these processes become more common, we can expect the same for the identity proofing before the issuance of an eID means by an identity provider. This is already the case for some of the notified schemes such as Italy (*SPID*), the Netherlands (*eHerkenning*) or the UK (*GOV.UK Verify*).

The security considerations arising include:

- Using a simple photo of the face and of the document raises some questions and remarks in order to verify if it complies with LoA Substantial. Proven attacks could exist with the manipulation of the image taken without obvious evidence. This risk could be increased if the environment is untrustworthy (e.g. a rooted or jailbroken smartphone or an untrusted webcam on a laptop/desktop).
- Rapid developments in video manipulation attacks, such as video simulation and real-time re-enactement, pose new risks.
- It is currently complex to identify which security measures and requirements should comply with the LoA High, which leads to a non-consensus of experts while evaluating such technologies against the mentioned LoA. Relevant work in progress, guided by the Cooperation Network, is expected to address these issues.
- Especially for facial recognition, it has been noted that evaluation of assurance is unclear as there are no guidelines to relate the FAR of a facial recognition solution to an eIDAS LoA (this is notably mentioned in the publicly available UK peer review).

In the case of video-based identification, verification of the authenticity of the identity document and exploitation of the photo by the agent in charge of the verification also raises questions regarding the associated assurance. In Opinion No. 1/2018[53] for SPID eID schemes, the Cooperation Network has issued its opinion taking into account that Italy will remove video identification for the LoA High. All the above mentioned examples demonstrate the complexity of assessing such solutions and the lack of a framework for assessing it.

Knowing that attack vectors could be used at each step of the process, including fake subject, counterfeit or fake documents presented, manipulation of the video, and the lack of capacity to verify the user identity by agent, some security measures have already been identified such as:

Using liveness detection along with a facial recognition algorithm. For instance, a random motion could be requested to the applicant or selfies could be taken in motion. . It should be noted that liveness detection in this case requires control over the biometric sensor, which in this scenario is under control of the attacker and not the verifier.

- If possible, using a picture already related to the applicant in a national database. Additional security checks could be carried out in case of doubt.
- Verifying the document’s authenticity using Machine Readable Zone (MRZ) or optical security features (photographs, font type, quality, holograms, laminate integrity, spelling mistakes, print quality, etc.). It should be noted however, that most of the optical security features such as holograms cannot be verified properly in the context of remote identification.
- Using a photo extracted from a chip (e.g. passport ICAO chip) with for instance an NFC-ready smartphone to guarantee the integrity of the data. As this photo would be signed, verifying the signature would provide assurances for the authenticity of the photo. The European Regulation standardizing national identity cards[54] is an opportunity as it establishes a common format to protect the photo across Member States.

As the eIDAS Regulation does not prevent remote identification, the Cooperation Network is currently working onproviding guidance on this topic and examining standardisation requirements to help assess the solutions that make use of these technologies. It is also worth noting that this topic already has raised many discussion points between experts as it is also a major concern for trust services such as the issuance of qualified certificates (i.e. how can the identity of the certificate holder be verified remotely). Better guidance, standardisation and conformity assessment practices are highly expected in this area.

2.2.2.3 Qualified electronic signature for enrolment

In case of an identity proofing using a qualified electronic signature, it is relevant to note that eIDAS (Article 24) allows the use of an eID means complying at least with LoA Substantial or High, but only if there was a physical presence during the enrolment. Therefore, in the case of identity proofing for LoA High, some complexity could arise as a qualified signature performed with a qualified certificate issued with a LoA Substantial eID means may not be accepted as proof of identity. This consideration must be taken into account when relevant.

2.2.3 Electronic identification means management and authentication

2.2.3.1 eID means using mail or SMS OTP

[53] See Opinion No. 1/2018 of the Cooperation Network on the Italian eID scheme

[54] 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

SMS or email OTP are known to be subject to various types of attacks (see also annex B.2.1 for an extensive overview of OTP SMS, link to recent attacks and email security considerations). OTP delivered through SMS, for instance, could be attacked with:

- SS7 vulnerabilities with attackers gaining access to the signalling network used for SMS transport.
- Malware attacks on the smartphone used to re-route SMS without any notification of the recipient.
- SIM swapping attacks that are still common today.

However, for SMS OTP, attacks may be technically complex or may require significant effort to target a given user. If combined with another authentication factor (such as a password), they may still remain attractive, providing reasonable protection against several attacks. They are also familiar to end-users as they are extensively used for online banking and payment. In addition, mobile operators could implement more security measures to enhance security (access to SS7 network, identity check for SIM change, check of SIM changes, etc.)[55].

Discussions remain regarding the potential of attacks against which SMS OTP could bring protection. Acceptability of SMS OTP in eID means targeting LoA High, for instance, is subject to discussion (schemes with an authentication using SMS OTP and a second factor to trigger access to keys stored on an HSM). This topic is currently being discussed between experts. Specific guidance could be offered in order to clarify vulnerabilities and secure solutions for SMS OTP.

Regarding mail OTP, these can also be subject to various attacks, the most common being gaining fraudulent access to the webmail of the user. As this attack type is prevalent and can scale (e.g. in case of massive account compromise, this could lead to massive risks for mail OTP), such solutions shouldnot be used even for the Substantial level for eID means.

2.2.3.2 eID mobile-based solutions (software-based, using SE or TEE, SIM-based)

The use of mobile-based eID solutions, in line with end-users' expectations, is increasing and will continue to increase in the coming years following the smartphone penetration rate. As the number of pre-notified and notified mobile-based solutions increases, so do the considerations that can be highlighted from the reviews and opinions.

One of the key security considerations is the protection of the secrets or cryptographic materials used within the solution for authentication. Based on the architecture of the solution, the secrets could be, for instance (the following list is not exhaustive):

- Stored on the mobile device encrypted on software key store
- Stored on the mobile device on hardware key store such as an embedded secure element or secure enclave (SE) and used only in a trusted execution environment (TEE) in order to offer protection of the secrets while stored and used
- Stored on the SIM card of the mobile phone, used as a cryptographic chip.

In all cases, the solution may also store other secrets involved in the authentication process in a remote cryptographic component. The considerations of this section focus on the secrets stored on the mobile part.

[55] According to ENISA's report of March 2018 ("Signalling Security in Telecom SS7/Diameter/5G - EU level assessment of the current situation"), in terms of SS7 minimum security measures are adopted by the majority of the providers, and most operators (87%) implement SMS home routing, to protect their networks against from leaking sensitive information associated with a subscriber, which would help to mount further attacks. This is only applicable if the owner of the eID scheme has a relationship to all MNOs whereby he can validate/enforce the applied security measures.

The latest opinion on the Latvian *eParaksts* scheme and the Belgian FAS/*itsme* scheme (respectively Opinion No. 7/2019 and Opinion No. 8/2019) for the LoA High highlight that such solutions which use smartphone applications should envisage the use of a hardware key store such as SE/TEE. The opinions also raise the question of the certification of such SE as they are mainly not certified against any recognised schemes at the moment, as well as the follow-up of vulnerabilities on such SE in time. However, it should be noted that not all Member States concure on introducing requirements for certified components in an eID scheme. It could be interesting to go further in this analysis by providing an overview of SE/TEE with a list of certified SEs (if any) and of known vulnerabilities on these components. Such lists would benefit identity providers issuing mobile-based solutions and would be consistent with the opinions issued by the Cooperation Network.

Regarding the use of SIM-based solutions to store secrets and cryptographic materials, the approach is currently followed by Estonia with the *Mobiil-ID* solution. This solution has been the subject of discussion during peer review and concerns were raised in Opinion No. 5/2018 regarding the ability of such solutions to be used under the sole control of the user and therefore provide protection against attacks with high potential (larger attack surface). These concerns should also apply to solutions using SE/TEE but do not explicitly appear in the related opinion mentioned in the previous section.

As for the recommendation for SE/TEE, clearer guidance should be provided and it would be helpful for identity providers in order to help them identify under which conditions SIM-based solutions can comply with the LoA High, especially by providing protection against attacks with high potential.

2.2.3.3 Use of biometrics authenticators within eID mobile-based solutions

Consistent with the rise of smartphone-based authentication solutions, the use of embedded biometrics authenticators is now widespread. They mainly consist in biometric sensors for fingerprint or for facial recognition. They are operated directly by the operation system (iOS or Android) and not by the application used for authentication. Commonly, they are used as a replacement of the PIN code. This raises several considerations (see also section B.3 for additional security considerations regarding biometrics):

- The security of the sensors can vary from one device manufacturer[56] to the other with false acceptance and false rejection rates that could differ.
- The solutions often allow to enrol several biometric templates without sufficient checks of the user enrolling a template. Moreover, the application may not choose which templates are used during the authentication process. This is an issue to ensure that the user of an eID is legitimate. In such cases mitigation measures should be applied, as for example advising the user or even deactivating the function if additional templates are enrolled.

The position of the Cooperation Network in the latest Opinions (No.7/2019 and No.8/2019) for the Latvian *eParaksts* and the Belgian *itsme* schemes is aligned with these considerations: to meet the requirements for LoA High, Latvia and Belgium should commit to disable the use of biometric authentication for this LoA.

2.2.3.4 Considerations on other authentication solutions used to trigger access to certificates stored on a remote HSM

Several peer reviews highlighted considerations regarding eID means based on cryptographic materials (such as certificates with private key) stored on a remote environment such as HSM that can be activated only by the user (an approach similar to qualified electronic signature performed on a remote QSCD under the sole control of the user).

[56] See for instance: https://www.zdnet.com/article/google-pixel-4s-face-unlock-works-even-if-you-have-your-eyes-closed/

In this case, the assurance of the authentication required to activate the use of the keys stored in an HSM, is key for the overall security of the solution. Various approaches are used within the schemes notified such as SMS OTP, software OTP (on a mobile app), hardware OTP, virtual smartcard, etc. The above considerations for SMS OTP and mobile-based solutions shouldbe taken into account to assess the compliance with the claimed LoA.

It is certain that this solution type will flourish in the future as it aligns with the eIDAS approach on remote electronic signature. Therefore, it might be possible for Member States to issue guidelines regarding rules and standards against which such solutions could be assessed and the conditions that will make them compliant with the LoA High.

2.2.3.5 Certification of devices usedin eID means

The certification of the eID means (being smartcard, HSM or other cryptographic module-based) used is a key consideration in order to ensure trust in the ability of a solution to offer protection against a given attack potential.

Among the pre-notified and notified schemes, several certification schemes are highlighted by Member States to demonstrate the security of devices:

- Common Criteria certification is a basis and devices are mainly being certified CC EAL4 augmented with AVA_VAN.5.
- QSCD certification under eIDAS Regulation is often done and is used to demonstrate the security level of the chip used. It is thus widespread for eIDs based on national eID cards already used for electronic signature purposes. It should be noted nonetheless, that the certification scope for local chip QSCD strongly varies from that for remote QCSDs.
- Protection profiles are also referenced and used as a base for QSCD certification.

Some public peer-review reports[57] have highlighted the need for periodical certification and not only to rely on an initial certification. In the context of the ROCA vulnerability, this approach is indeed relevant as it appears that a certification that ensures a protection against a given attack potential at the time of its issuance may not provide the same assurance a few years later (as attacks methods and the threat landscape evolve quickly).

It would be relevant to have additional guidance for devices used within eID means regarding needs in terms of certification (including the scope of the certification) and maintenance in time. Nevertheless, some Member States have already put approaches in place at national level, in order to review the evaluation of security components on a regular basis (vulnerability assessment, cryptography evaluation, etc.). This is the case in France for instance where ANSSI promotes its “qualification” approach.

2.2.4 Management and organisation

2.2.4.1 Certification of identity providers issuing eID means

The topics related to management and organisation are generally the ones raising the least comments in peer review reports. Some recommendations have already been given by the Cooperation Network in their guidance document. There are existing standards (against which certification is possible) that could be followed by identity providers or third parties involved in the eID means management for compliance with some of the requirements of the CIR.

Such standards which are highlighted in notification forms or supporting documentation provided for schemes pre-notification include for instance:

[57] See for instance the peer review reports for the Croatian and Luxembourgish schemes, publicly available on the European Commission website.

- ISO/IEC 27001:2013 for fulfilment of requirements on information security management, record keeping, facility and staff and technical controls
- Relevant ETSI standards such as ETSI EN 319 401 and ETSI EN 319 411-1 and ETSI EN 319 411-2.

Guidance could be provided in order to help identity providers match the requirements covered by a certification they already have (as per the mapping already proposed in the current version of the guidance document of the Cooperation Network). For instance, a provider already certified as QTSP could easily benefit from all the requirements already covered by the qualification and the ETSI standards against which it has been assessed. Such standards, if relevant, could eventually be referred to in the legislation.

3. NEW OPPORTUNITIES FOR ENISA UNDER THE CYBERSECURITY ACT

According to the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification[58] (hereafter Cybersecurity Act), ENISA's role is in line with achieving "*a high common level of cybersecurity across the Union, including by actively supporting Member States, Unions institutions, bodies, offices and agencies in improving cybersecurity"*. ENISA shall also "*act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders"* (Article 3(1)).

ENISA's role is to contribute to a coherent European cybersecurity landscape regarding electronic identification.

In Article 4(6) of this Regulation, it is stated that ENISA "*shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market"*. In the eID landscape, The Commission and ENISA could coordinate the pursuit of consistency across national competent authorities that have issued or are still working on detailed technical and security requirements based on the Commission Implementing Regulation 2015/1502.

COORDINATE NATIONAL INITIATIVES ON ISSUING TECHNICAL AND SECURITY REQUIREMENTS FOR eID

ENISA could work with national Competent Authorities across the European Union to identify their initiatives and share their views on technical and security requirements for the Substantial and High Levels of Assurance of eIDAS.

It is also stated in this Regulation, in Article 5(5), that ENISA *"shall contribute to the development and implementation of Union policy and law […] in the field of electronic identity and trust services, in particular by providing advice and issuing technical guidelines, as well as by facilitating the exchange of best practices between competent authorities"*. To this end, ENISA could carry out a periodic technological overview on electronic identification means and solutions as well as on the evolution of the threat landscape in this area. In case of a vulnerability, ENISA could put in place communication means between Member States and provide its expertise.

PROVIDE AN OVERVIEW OF TECHNOLOGICAL DEVELOPMENTS AND REPORT ON SECURITY INCIDENTS OF NOTIFIED SCHEMES

ENISA has a role to play in reporting on the security incidents of notified schemes. An overview of technological advances could be carried out and ENISA could facilitate the exchange of best practices and vulnerabilities between the Member States.

Along the same lines, it could also be interesting to extend Article 10 of the eIDAS Regulation focusing on security breaches and stating, "*where either the electronic identification scheme […] or the authentication […] is breached or partially compromised […], the notifying Member States […] shall inform other Member States and the Commission.*" Indeed, Member States have a

[58] https://eur-lex.europa.eu/eli/reg/2019/881/oj/

similar obligation regarding trust service providers: supervisory bodies "*shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust providers*" (Article 19 of the eIDAS Regulation). Accordingly, ENISA prepares an annual report aggregating these breaches to show root causes, statistics and trends. A similar report could thus be made available to Member States and interested eID stakeholders, summarising security breaches and incidents of notified electronic identification means and identity providers issuing these electronic identification means. This report could also include a threat overview of underlying authentication technologies, which would benefit from the technological watch proposed in the foregoing provision.

PUBLISH AN ANNUAL REPORT ON SECURITY INCIDENTS FOR eID

ENISA could publish an annual report aggregating all security incidents which impacted notified electronic identification schemes, alongside with an overview of the threat landscape for eID underlying technologies.

Besides, leveraging technological advances and security concerns of eID schemes and underlying technologies, ENISA could provide further guidance, including on the definition of the levels of assurance and attack potential to ensure a consistent comprehension of the topic from one Member State to another. The NIST guidelines have,for instance, developed flowcharts to help define which level of assurance is required per use case. Moreover, as stated in section 2.2, ENISA could go one step further and publish recommendations on specific topics, including OTP SMS and remote identity proofing, in close collaboration with Competent Authorities and the Cooperation Network.

PROVIDE GUIDANCE TO MS COMPETENT AUTHORITIES

ENISA could publish guidelines and recommendations to ensure a consistent understanding of the requirements of the CIR 2015/1502 of the eIDAS Regulation. These guidelines could include use cases by levels of assurance to further detail their definition, as well as recommendations regarding compliance of specific technologies and solutions.

Finally, as the eIDAS Regulation must be reviewedby July 2020 by the Commission (Article 49 of the eIDAS Regulation), ENISA couldbring insights on what the review of the eIDAS Regulation should include in the electronic identification area. Towards this end, this report could form the baseline for ENISA's feedback, as ENISA continues to delve into this topic in the first semester of 2020. The Commission haspublished the eIDAS review roadmap[59] stating that reports and studies prepared by ENISA will be fully included in the initial step of the evaluation process.

BRING INSIGHTS TO THE eIDAS REVIEW

ENISA will be involved in the eIDAS review process which is due in July 2020. As such, it should bring its technical expertise and insights to define how the Regulation is fit for purpose and identify areas for improvement related to electronic identification.

[59] Retrieved from https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2019-6019401_en

A ANNEX: OVERVIEW OF OTHER EID SCHEMES

This section offers an overview of other relevant eID schemes,that are not pre-notified or notified at the time of writing this report. It is worth to notice that all the considerations and analysis of the eID schemes made in this report are based on publicly available information.

A.1 SMART-ID

Smart-ID is an eID solution currently in use in Estonia, Latvia and Lithuania. It is based on a smartphone mobile application. From an end-user perspective, the user experience is quite similar to a push authentication mobile application. When trying to access a service or confirm a transaction, the user receives a notification on the enrolled application and can perform the authentication by typing a PIN code. The user has two separate PIN codes, one for authentication purposes and one for digital signature purposes. From a design standpoint, the solution offers an interesting perspective. In order not to rely only on the user device (i.e. the mobile phone with the application), or server signing services (i.e. remote HSM for server signing, which raises questions on the initial authentication of the user), the solution provides an alternative by sharing the risks and responsibilities between these two components. The private keys used for authentication and signature are generated in a shared manner, following threshold-signature scheme protocol principles. By doing so, each secret sharing of the key (one stored in an encrypted format in the application with the PIN and the other stored on the HSM) is used to produce a signature without the need to combine the private keys in a single location. The signature shares are then combined on the server-side to create the final composite signature.

Regarding the enrolment, the solution can be activated while deriving the digital identity of the Estonian eID or *Mobiil-ID* (for Estonian users).

From a signature perspective, this approach is inspired by the protection profile[60] *EN 419 241 – 2 Trustworthy Systems Supporting Server Signing Part 2: Protection Profiles for QSCD for Server Signing* but differs in the use of the threshold signature scheme protocol as it does not use the classic server signature solutions. The server part of the *Smart-ID* solution (the secure-zone on the server-side connected to the HSM through a secure channel) has been certified against Common Criteria for EAL 4+ augmented with AVA_VAN.5 and constitutes a QSCD.

In addition to these principles, *Smart-ID* also includes interesting security measures:

- Verification codes are generated to bind the context of the session on the relying party with the authentication session on the mobile application (also used, for instance, within the Estonian *Mobiil-ID*). Such features are always useful to avoid approval from the user without being fully aware of the transaction context.
- There are clone detection mechanisms to detect duplication of the Smart-ID application with a parallel use. For this purpose, one-time material is generated by the Smart-ID server and is expected to be provided by the mobile application for the next interaction.

[60] Retrieved from BankID A Protection Profile (PP) is a document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC). As the generic form of a Security Target (ST), it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements. A PP is a combination of threats, security objectives, assumptions, security functional requirements (SFRs), security assurance requirements (SARs) and rationales.

A.2 BANKID IN SCANDINAVIAN COUNTRIES

Both Sweden and Norway have an electronic identification scheme where banks act as identity providers to access public administration websites and private sector websites in these countries. Both schemes are called BankID but are based on different technologies.

A.2.1 Swedish eID

The Swedish eID system relies on eIDs that have been issued by the private sector since 1999. The main solution is BankID and is in operation since 2003. This eID scheme is based on a network of 11 banks and has the same value and functionalities, regardless of which bank has issued it. It can be used for login and identification as well as to perform digital signatures. Every individual who has a Swedish social security number can obtain BankID e-credentials through their bank. In 2019, BankID is estimated to have been used on almost 4 billion occasions[61].

BankID is available in 3 forms: a physical smart card (BankID on a card), an application on a smartphone or tablet (mobile BankID) and a computer software (BankID in a file). Service providers can choose to accept one or all forms for different services.Identity providers also select which forms of eID they offer[62]. By the end of 2019, it is estimated that 8 million of Sweden's inhabitants will own a BankID, of which approximately 7.5 million will have a mobile BankID[63].

BankID credentials are ordered via an Internet bank. The process differs between banks: some require a face-to-face meeting at a bank office with an approved Swedish ID document, while others require users to only login in the Internet bank and order a BankID online.

Authentication with mobile BankID either requires the user to enter an identification number and a password or to scan a QR code on the service provider website with the mobile application. Mobile BankID works only on the initial mobile phone that it was installed on: if a user changes his/her mobile phone and tries to restore it from an old laptop, the mobile BankID will not work and new credentials must be sought from the bank.

A.2.2 Norwegian eId

Mobile BankID was launched in 2009 as a joint initiative between DNB Bank, a leading Norwegian bank, and Telenor, the country's largest mobile operator. Mobile BankID is an electronic identification scheme, supporting authentication and digital signature across online services through the users' mobile phones. Today, all five of Norway's mobile operators offer Mobile BankID to their customers, leading to a full market coverage. BankID in Norway has a total of 4 million subscribers[64]. Mobile BankID uses PKI technology and stores bank-generated certificates on the SIM card. A PIN code is used for authentication and validation purposes.

[61] Retrieved from *BankID* website: https://www.bankid.com/om-bankid/detta-ar-bankid
[62] Retrieved from *BankID* website: https://www.bankid.com/kontakt/utfaerdare
[63] Retrieved from *BankID* website: https://www.bankid.com/assets/bankid/stats/2019/statistik-2019-08.pdf
[64] Retrieved from the *BankID* website: https://www.bankid.no/en/company/

B ANNEX: TECHNOLOGICAL LANDSCAPE OF EID SOLUTIONS

The following technological landscape of eID solutions is built by regrouping in clusters the underlying technologies used in all eID solutions including both notified or not eID schemes.

Four broad technological clusters are detailed in the following subsections:

- Cards and other hardware authenticators (incl. contact and contactless smart cards)
- Mobile-based solutions (incl. OTP, cryptographic SIM and Mobile Connect)
- Biometrics (incl. fingerprints and face recognition)
- Prospective technologies (such as self-sovereign identity and analytics).

B.1 CARDS AND OTHER HARDWARE AUTHENTICATORS

B.1.1 Physical identity document and visible digital seals

A physical identity document is any document which may be used to prove a person’s identity without an electronic component. They can, for example, be ID cards made of plastic. They display personal information such as name, address, date of birth and a photograph.

What are the potential use cases regarding eID in an eIDAS ecosystem?

Physical ID cards cannot be used as an electronic identification means since they don’t offer useful electronic features. However, since they usually contain a picture of the cardholder, they can be used during the identity proofing process during a face-to-face verification The unique identification number located on every card can also be used during an identity claim validation by an appropriate authority.Most eID schemes use these documents in face-to-face identity proofing if such enrolment processes are used. They can also be used in remote enrolment processes where identity documents are photographed, recorded or shown during a videocall by the users performing the enrolment. However, most physical security features are designed for verification in a face-to-face scenario and are not suitable for duplication by photography or video recording.

To further improve the security of identifying attributes retrieval, visible digital seals on physical documents can be used. Visible digital seals are cryptographically signed data structures containing document features, encoded as a 2D bar code and printed on a document. This 2D bar code includes the signed biographic data located on the card. The signature is performed by document issuers (usually issuing state), using the private keys corresponding to the bar code signer certificates. The integrity of the data contained in such 2D bar codes is thus ensured, as detection of the forged digital visible seal would be easy (not signed by the issuing state CA for instance). It is also a way to check that the data stored in the digital visible seal and on the card match, helping the identification of counterfeit cards. It is worth noting that these bar codes are easily decoded by off-the-shelf smartphones or scanners as long as publicly available algorithms are used to create the seal.

These digital visible seals do not replace the security features of microchips, do not enable dynamic authentication and do not protect against duplication. However, they strengthen the security of the retrieval of information during an enrolment phase.

What are the applicable standards that are related to this technology?

To automate the data capture and to reduce human errors, bar codes (example of an algorithm for 2D code: PDF417, BSI TR-03137, ANTS 2D-DOC, etc.) located on physical cards can be used. The use of these bar codes is not harmonised, as the ISO/IEC 7810[65] standard only specifies physical characteristics for identification cards (dimensions, resistance to bending, toxicity, etc.).

Regarding visible digital seals, the ICAO has published a technical report called *Visible Digital Seals for Non-Electronic Documents*[66] describing these seals, including the container format of a digital seal, how it should be encoded, and the use-case of digital seals applied to travel documents. This report states the added value of these visible digital seals for breeder documents[67] and temporary visas while specifying that travel documents should, whenever possible, employ microchips.

In this ICAO report, the 2D bar codes that can be used as the printed representation of visible digital seals are the ones specified as an ISO standard, including DataMatrix (ISO/IEC 16022), Aztec Codes (ISO/IEC 24778), and QR Codes (ISO/IEC 18004). ISO/IEC 15415 is also referred to regarding the print quality of these bar codes.

These visible digital seals or secured bar codes have been further developed at national level. For instance, Germany's cyber security authority, BSI, has published technical guidelines[68] on the topic, and France has developed a framework called 2D-Doc[69] based on this principle to ensure the integrity of public documents. These two documents were the basis of the ICAO report.

What are the network and information security considerations regarding this technology?

While network and information security considerations do not apply to physical cards, it is essential to recall that the security level of these cards is closely related to the printed security of the cards.

The operators verifying those cards in face-to-face processes must be trained and equipped to recognise and verify the printed secure elements to make sure the cards are not forged.

Identity documents printed without a cryptographic element remain more prone to falsification and counterfeiting, and the guarantee they can provide during an identity proofing process remains very limited. The usage of a visible digital seal enhances the security of this process.

B.1.2 Contact Smart Cards

A smart card is a device including an embedded integrated circuit chip (ICC). A contact smart card needs to be inserted in a card reader to operate the transmission of commands and data.

[65] https://www.iso.org/standard/31432.html
[66] https://www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Visible%20Digital%20Seals%20for%20Non-Electronic%20Documents%20V1.7.pdf
[67] Documents that can serve as a basis to obtain other identification documents, i.e. a birth certificate that is used to obtain a passport.
[68] BSI TR-03137 Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal), see https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03137/BSITR03137.html
[69] https://ants.gouv.fr/Les-solutions/2D-Doc (in French)

These smart cards usually carry cryptographic functions such as key generation (including random number generation), encryption and signature.

What are the potential use cases regarding eID in an eIDAS ecosystem?

Contact smart cards can be used for both identity proofing and electronic identification means. Depending on the use case, the maturity level of the ecosystem and used endpoints, using a contact smart card can be more or less appropriate for those two purposes.

- In countries where citizens possess an electronic national identity card including a microchip, many public services (healthcare, voting, etc.) and private services (electronic banking, signing contracts, etc.) can allow the use of these microchips as electronic identification means for citizens. In a mature ecosystem where every citizen has a contact smart card reader, they can use their electronic national identity card to access those electronic services.
  In Europe, most countries provide their citizens with electronic identity cards and allow citizens to access e-gov services with digital identities based on these identity cards (see also section 1.3 for an overview of eID solutions).
- In an ecosystem where the use of a microchip as an electronic identification means is not widely supported, or where electronic services are used from endpoints for which using a microchip is difficult, not user friendly or not possible (absence of card readers, from mobile devices, etc.), eID cards can be used to strengthen a remote initial identity proofing during a registration process with an identity provider. For example, Estonian and Lithuanian ID cards can be used as identity proofing documents by reading the microchip to enrol the *Smart-ID* solution, a third-party electronic identification means based on a mobile application (see also section **Error! Reference source not found.**)[70]. As another e xample, the Belgian *itsme* eID solution can be activated after carrying out an identity proofing based on the Belgian national eID card.

What are the applicable standards related to this technology?

The ISO/IEC 7816 standard defines contact smart cards. This standard specifies many aspects such as the physical characteristics, dimension, and location of the contacts parts, electrical interface and transmission protocol, personal verification through biometric methods (e.g. Match on Card). For some specific use cases, additional standards can be required, such as EMV for payment cards, or UICC for SIM cards.

In terms of technology, electronic certificates are commonly used on the chip to provide eID features.

What are the network and information security considerations regarding this technology?

The microchip security level is usually evaluated against the Common Criteria framework with an Evaluation Assurance Level (EAL), with potential augmented requirements. For instance, smart cards are commonly assessed for EAL4 augmented with AVA_VAN.5 (Vulnerability Assessment and Analysis) to ensure protection against attackers with high potential. The Common Criteria framework benefits from mutual recognition agreements such as the SOG-IS in Europe and the CCRA (Common Criteria Recognition Agreement).

In addition to the Common Criteria, some countries are also using national qualification frameworks. For instance, it is the case in France with the ANSSI qualification process that

[70] See also https://www.smart-id.com/help/faq/registering/how-to-register-a-smart-id-account-using-an-id-card

aims, in addition to the Common Criteria, to ensure the security level of the assessed product in time (cryptographic review, yearly supervision report, periodic recertification).

Cryptographic modules are also commonly certified as QSCDs under the eIDAS Regulation, as are most of the national eID cards used in Europe. Several protection profiles have been defined and certified.

Because of its relevance for the smart cards industry, it is worth mentioning the Federal Information Processing Standards (FIPS) developed by the American National Institute of Standards and Technology (NIST), which are standards and guidelines for federal computer systems, often used also by the private sector. The 140-2 Security Requirements for Cryptographic Modules standard[71] specifies the security requirements that must be satisfied by a cryptographic module utilised within a security system protecting sensitive but unclassified information. The standard provides four increasing, qualitative levels of security. The requirements to satisfy a level of security are partially based on the Common Criteria framework: level four, for instance, relies on the EAL4 (or higher).

B.1.3 Contactless Smart Cards

A contactless smart card is also a smart card with an embedded microchip like the contact smart card described above. However, it also embeds an antenna and only requires close proximity to a card reader. They communicate using radio frequency (RF), and this electromagnetic signal derives power for the internal chip.

What are the potential use cases regarding eID in an eIDAS ecosystem?

Just as contact smart cards, contactless smart cards can be used for both identity proofing and as an electronic identification means. They offer an advantage over contact smart cards regarding compatible devices due to the ability of many smartphones to read contactless smart cards. Those cards are used, for example in *Alicem*, a French eID solution, where contactless passports (or residence permit for foreigners) are used during identity proofing along with facial recognition mechanism via a smartphone as a card reader. These cards can also be used as electronic identification means, which is also the case in *Alicem*, where contactless passports can be used during electronic identification via the mobile application.

Electronic travel documents standardisation thanks to the ICAO document about Machine Readable Travel Documents (Doc 9303 ICAO[72]) has made the reading of identity information and the photo highly standardised and easily to be included in eID applications on mobile phones. It thus strengthens the security of the process to derive an identity from an identity document.

These usages can be developed as more and more smartphones are NFC compatible. Android phones have long been known to have NFC capabilities as NFC became available on some Android devices in 2012. Today, all the top ten manufacturers sell NFC phones[73]. With iOS 13, iPhones can now read NFC tags, and mobile applications are coming to the App Store in order to read electronic identity documents[74]. Since 2018, there is an Android mobile application from the UK Home Office to facilitate applications for residency in the UK after it leaves the EU, by quickly and securely confirming identities[75]. In October 2019, the UK Government has introduced an iOS version of this app[76]. The German eID can also be used efficiently on Android and iOS devices without any additional deviced required.

[71] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
[72] https://www.icao.int/publications/pages/publication.aspx?docnum=9303
[73] https://learn.seritag.com/nfc-enabled-phones
[74] https://techcrunch.com/2019/06/12/nfc-gets-a-lot-more-powerful-in-ios-13/
[75] https://play.google.com/store/apps/details?id=uk.gov.HomeOffice.ho1&hl=en_GB
[76] https://www.nfcw.com/2019/10/21/364763/uk-government-includes-iphone-nfc-passport-reading-in-ios-brexit-app/

What are the applicable standards related to this technology?

The ISO/IEC 14443 standard defines contactless smart cards. This standard specifies many aspects such as physical characteristics, radio frequency power and signal interface, transmission protocol.

These identity documents are generally compliant with ICAO's Doc 9303. The document is divided into 12 parts. For instance, part 10 of the document defines the logical data structure for data storage in the contactless integrated circuit, and part 11 defines the security mechanisms for machine-readable travel documents (MRTDs).

What are the network and information security considerations regarding this technology?

Considering the microchip itself, the same considerations as for contact smart card defined in section B.1.2 apply (the ISO standard, the Common Criteria framework, etc.).

It is worth noting that an ICAO compliant chip (for electronic MRTD) itself only provides one authentication factor, as the ICAO applet does not manage PIN. If used as part of an electronic identification means, they need to be associated with another authentication factor.

Contactless smart cards are mainly vulnerable to non-authorised readings by a close reader (less than 10 centimetres) when no countermeasures are deployed (access control, random UID), allowing the tracking of identity information and people's movements. ICAO compliant chips require at least to use the barcode to access the identity information (non-sensitive) with protocols such as PACE. Sensitive information such as biometric template (fingerprint) are protected using Extended Access Control that requires mutual authentication with the inspection system accessing the information. These protocols are described in the Doc 9303 and aim at local reading. For remote reading, there exist references to the extension of the protocols in BSI/ANSSI TR-03110.

B.1.4 FIDO Authenticator

The FIDO Alliance is an open industry association that develops open standards for authentication intending to replace passwords to promote more secure and convenient authentication. The association members include authentication specialists, industry companies, GAFAM (except Apple) or payment companies.

FIDO authentication standards are based on public-key cryptography. The main principle behind the protocol is the use of a key pair associated with each FIDO compliant relying party that the user wants to access. The relying party stores the public key along with a credential ID to identify its owner. The authentication process is performed through the signature of a challenge by the private key, ensuring the possession of this private key.

Several authentication factors (or form factors) are supported to unlock access to the private key during the authentication process such as biometrics (e.g. embedded on a smartphone), a USB second factor, and a contactless authenticator. Moreover, the way private keys are created, managed and stored depend on the implementation chosen by each factor's vendor. Indeed, FIDO does not specify exactly how to perform these operations, but rather gives a set of security requirements to comply with, which do not currently align with eIDAS requirements[77].

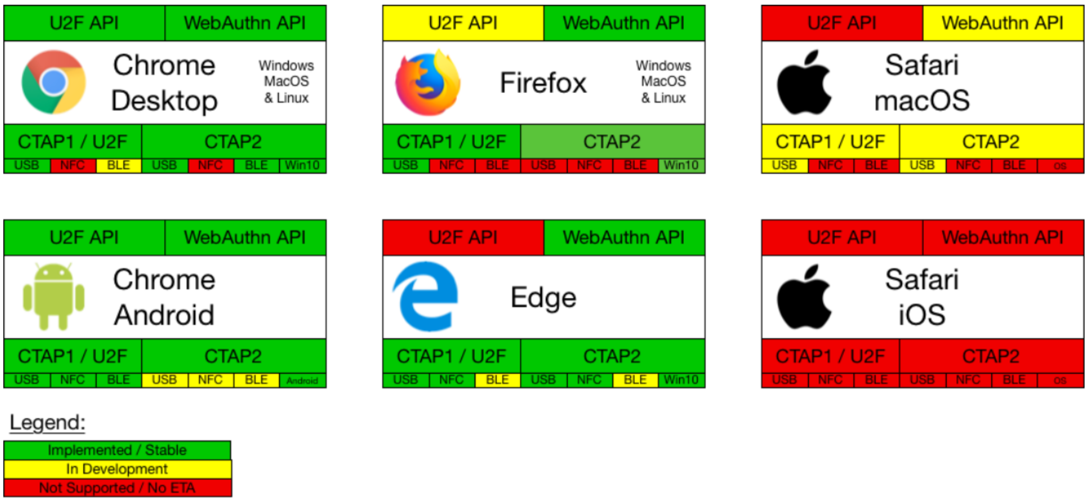
[77] https://fidoalliance.org/specs/fido-security-requirements-v1.0-fd-20170524/fido-authenticator-security-requirements_20170524.html

What are the potential use cases regarding eID in an eIDAS ecosystem?

FIDO is an industry authentication standard that benefits from a broad coverage by all major browsers (Chrome, Safari, Edge, Firefox) and Operating Systems (Android, Windows).

Being an authentication standard, a FIDO authenticator in itself does not manage identity but only authenticates a registered user. An Identity Verification and Binding Working Group[78] (IDWG) has been created within the FIDO Alliance and is working on improving identity proofing mechanisms, based for example on biometrics or government-issued identity documents remote verification. The compliance to eIDAS requirements appears not to be at stake for now. It could be therefore interesting to study the outputs of this working group, even to discuss with the working group, and check proposed identity proofing mechanisms against eIDAS Regulation or way to bind FIDO authenticator with identity data for instance.

Figure 5: Browser and operating system coverage of FIDO ecosystem (Source FIDOalliance.org)



What are the applicable standards related to this technology?

Historically, the FIDO Alliance has developed two authentication standards:

- FIDO UAF (Universal Authentication Factor): the FIDO UAF protocol was designed to provide a “passwordless” experience while authenticating on online services. It requires the use of a device supporting FIDO UAF stack (FIDO client and FIDO authenticator on the device, mainly a smartphone). Depending on the FIDO compliant authenticators supported on the device, several form factors for authentication can be used such as fingerprint biometrics, facial recognition, voice recognition and the use of a PIN. Authentication unlocks access to the private key used for signing. Confirmation is then transmitted to the FIDO server-side that checks the validity of transmitted information.
- FIDO U2F (Universal 2nd Factor): The FIDO U2F protocol was designed for strong authentication to provide a second factor with a FIDO U2F device that can be used through USB (insert and press a button on the USB device) or NFC or BLE (Bluetooth Low Energy) (tapping the NFC or BLE device). It should be used in conjunction with a username/password as a second factor to provide strong authentication. The FIDO U2F device implements the same concept, generating a key pair which is relying party specific

[78] https://fidoalliance.org/identity-verification-binding/

and that is used for signature during the authentication process. The FIDO U2F protocol is now relabelled as CTAP1 as part of FIDO2.

In order to rationalise the standards used, the FIDO Alliance is now promoting FIDO 2 which is comprised of:

- Client To Authenticator Protocol CTAP 1 (the new label of U2F) and CTAP2 (extension of U2F to include mobile devices as external authentication factors). These protocols manage the interaction between a FIDO authenticator and a FIDO client (browser, native application).
- WebAuthn (Web Authentication) is a web-based API that allows websites to support FIDO-based authentication on supported browsers and platforms. It has been developed with the World Wide Web Consortium (W3C) and was officially recognized as a W3C web standard in March 2019.

What are the network and information security considerations regarding this technology?

Being based on asymmetric cryptography, with keys stored on software or hardware key stores, security considerations are related to considerations that could apply for mobile based solution with SE or smartcards, such as:

- Cryptographic mechanisms and algorithm used
- Protection of the authenticator against tampering, duplication, attack to steal the private keys stored, etc
- Certification of the authenticator if any to ensure resistance against a given attack potential.

It is worth noting that the German BSI has released a protection profile for a FIDO U2F based authenticator: *FIDO Universal Second Factor (U2F) Authenticator BSI-PP-CC-0096-2017*[79]. The target of evaluation described in this protection profile can be on a contactless of a contact secure chip. It has been evaluated for EAL4 augmented with AVA_VAN.5 to ensure resistance against high potential attacks. Further security concerns consider the use of embedded biometric sensors and futher details can be found in Section 2.2.3.3.

B.2 MOBILE-BASED eID SOLUTIONS

Mobile technologies related to identity consist of phone and tablet-based hardware and software solutions used to register, authenticate, and verify an individual’s identity.

B.2.1 SMS and email OTP

One-time password (OTP) is a single factor of authentication, commonly used for a single authentication in addition to a static password or PIN to implement two-factor authentication with a possession-based factor (something a person has, such as a specific phone number) and a knowledge-based factor (something a person knows, such as the PIN). For the user to authenticate, a single-use password is generated centrally and sent to the registered phone number through SMS or to the registered email address through email.

What are the potential use cases regarding eID in an eIDAS ecosystem?

OTP SMS or email can be used in the enrolment process to prove the user performing the enrolment process indeed possesses the phone number or email address. Such validated contact information can then be used later for authentication purposes. Still, during an eID

[79] More information on: https://www.commoncriteriaportal.org/files/ppfiles/pp0096b_pdf.pdf

enrolment process, it is also commonly used to send activation codes (for instance to activate a card issued after a face-to-face identity proofing).

SMS or email OTP is also used during authentication. When used as a second factor, it provides a layer of security on top of static user-created passwords which can be weak and/or reused across multiple accounts.

Examples of SMS OTP use as part of eID schemes are numerous across Europe. For instance, it is currently used in Spain through the Permanent *Cl@ve*[80] identification scheme where an OTP is sent by SMS to the mobile phone to access electronic administration services that require a high level of security. A similar authentication flow is used by Norway's *MinID*[81] identification means to access more than 1,000 different services from government agencies. This identification scheme gives access to online public services at a "medium-high level of security"[82] (level 3 out of 4 on the Norwegian ID-porten scale). Numerous other examples of the usage of SMS OTP can be found for various usages (social network, banking, etc.).

What are the applicable standards related to this technology?

There is no standard per se describing the use of OTP SMS or email. OTP SMS is delivered to mobile phones through the global SS7 (Signaling System 7) network of mobile operators, and OTP email is delivered through the Internet (refer to section 2.2.3.1 for additional standards and security considerations regarding OTP SMS and email).

What are the network and information security considerations regarding this technology?

Email OTP is problematic regarding the risks linked to a mail account takeover by an attacker. Indeed, a mailbox is attractive to an attacker, and a successful phishing attack can't be overlooked. Therefore, this technology is not massively used anymore in eID schemes and should not be promoted.

Regarding OTP transmitting via SMS, this technology can be considered too reliant on the network's operator processes. Recent examples of SIM swapping (incl. Twitter's CEO on 31st August 2019[83]) show the danger of having a mobile number both as identifier and authenticator[84].

Moreover, the SS7 protocol used by telecommunications companies to coordinate how texts and calls are rooted has a long-known security flaw allowing malefactors to send commands and route text messages as they wish. It has already happened in 2017 and 2019 when bank customers from Germany[85] and the UK[86] were victims of fraudulent transfers that exploited this SS7 vulnerability. Mobile operators could implement additional security measures, but according to ENISA's report of March 2018 ("Signalling Security in Telecom SS7/Diameter/5G - EU level assessment of the current situation") security measures are already in place:

- In general, most of the operators have implemented basic security measures especially for SS7,
- Most operators (87%) implement SMS home routing, to protect their networks against from leaking sensitive information associated with a subscriber, which would help to mount further attacks.

[80] https://clave.gob.es/clave_Home/en/Clave-Permanente.html
[81] http://eid.difi.no/en/minid
[82] http://eid.difi.no/en/security-and-cookies/information-about-levels-security
[83] https://www.theverge.com/2019/8/31/20841448/jack-dorsey-twitter-hacked-account-sim-swapping
[84] https://www.wired.com/story/phone-numbers-indentification-authentication/
[85] https://www.kaspersky.com/blog/ss7-attack-intercepts-sms/16877/
[86] https://www.kaspersky.com/blog/ss7-hacked/25529/

- More than 84% of our respondents are applying different analysis techniques for SS7 interconnect traffic in order to detect abnormal activities.
- More than 80% of the respondents monitor for abnormal SMS activities.

Also, the PSD2 Regulation requests strong authentication to perform online payments over Internet and to access a bank account. The combination of the card details printed on the card and SMS OTP, very popular to validate online payments, would not be compliant anymore for strong customer authentication under this directive[87]. This directive might then indirectly reduce the usage of the combination of the card details printed on the card with SMS OTP. However, as stated in the EBA Opinion[88] on the implementation of the RTS (paragraph 35), a device could be used as evidence of possession, provided that there is a 'reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device'. Evidence could, in this context, be provided through the generation of a one-time password (OTP), whether generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification. In the case of an SMS, and as highlighted in Q&A 4039, the possession element 'would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number'. (paragraph 25). So, the PSD2 Regulation does not preclude the usage of SMS OTP in addition to a static password or PIN to implement two-factor authentication[89]..

In summary, OTP sent via SMS remain interesting as it is a very known and straightforward way to perform 2FA at large scale. However, long-known multiple weaknesses should be addressed, although these weaknesses only benefit an attacker targeting a specific user.

B.2.2 Soft OTP

Another implementation of one-time passwords uses mobile applications or hardware security tokens. In both cases, they are generated using Hashed Message Authentication Code (HMAC) and a moving factor - such as event counter (HOTP) - or time-based information (TOTP). In two-factor authentication scenarios, a user must enter a traditional, static password as well as a time-based one-time password to gain access to a digital service. Typically, a time-based temporary passcode expires after 30, 60 or 120 seconds.

Historically, hardware security tokens (e.g. an RSA token) were used, but the focus here is on one-time passwords generated by mobile applications (e.g. Google Authenticator).

One-time passwords can also be challenge-based, where the resource being accessed provides a challenge needed to generate the OTP. The challenge can be meaningless or related to the transaction. To increase the security of the process, a PIN on the smartphone or the hardware token can be required to trigger the generation of the OTP. In this case, the process provides two authentication factors from different nature: knowledge of the PIN and possession of the smartphone with the enrolled application.

What are the potential use cases regarding eID in an eIDAS ecosystem?

Event-based OTP, time-based OTP and challenge-based OTP can all be used as a second factor in an electronic identification process, or as a comprehensive authentication solution if a PIN is required to trigger the OTP generation. For instance, *SPID*, the Italian notified eID

[87] See European Banking Authority opinion, accessible here https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2 and UK's local decision https://www.finextra.com/newsarticle/34047/fca-delays-introduction-of-strong-consumer-authentication-rules
[88] "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2." - from 21 June 2019, https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf
[89] There are commercial PSD2-compliant offers based on SMS OTP, like for example https://www.twilio.com/blog/how-twilio-can-help-strong-customer-authentication-psd2.

scheme, offers such processes, including mobile OTP on a smartphone application and hardware OTP generators, depending on the identity provider.

What are the applicable standards related to this technology?

OTP generation methods are described in several RFC:

- RFC 4226 – HOTP: An HMAC-Based One-Time Password Algorithm[90]
- RFC 6238 – TOTP: Time-Based One-Time Password Algorithm[91]
- RFC 6287 – OCRA: OATH Challenge-Response Algorithm[92].

What are the network and information security considerations regarding this technology?

If the device is stolen, the PIN code may be known by the attacker as well, and in this case, the security value of this soft OTP is nullified. If this soft OTP is combined only with biometrics without a PIN code, this weakness is nullified, but this is rarely the case as many countries require alternative authentication solutions to biometric ones.

As the one-time code generally is generally entered on the login page of the accessed service, there also is a risk of interception with fake login pages (phishing) that could allow an attacker to reuse the intercepted code during its validity window. This attack type could be executed by using challenge-based OTP generation mechanisms.

However, the solution, even with a challenge-based approach could remain vulnerable to targeted social engineering, as there is also a lack of information regarding the context of the transaction that requires the generation of an OTP.

Finally, the Soft OTP token is also vulnerable to any malware that extracts or duplicates the underlying key in the device. The security of the environment storing secrets is fundamental for the overall resistance against attackers (software or hardware key store. Also, the use of embedded biometrics sensors for such applications raises security concerns.

B.2.3 Mobile authentication with push notification

Specific mobile applications can be used to enable authentication on online service for a citizen. The implementation may vary depending on the provider. Sometimes, the mobile application manages the authentication from end to end, and sometimes it calls cryptographic elements on the smartphone and/or in a server-side HSM. The authentication and cryptographic processes are often provided as an SDK from security providers and sometimes embedded in a smartphone application offering more services. Banking institutions have been following this model in order to provide a secure but seamless user experience to their customers.

This approach now supersedes the classical soft OTP approach by bringing a better user experience with:

- Push notifications to advise the user of a pending approval
- Transparent and over the air transmission of the signed challenge to the server without needing to copy the OTP on the page of the accessed services
- Allowing to replace the PIN code in the app with biometrics leveraging sensors embedded on the smartphones.

[90] https://tools.ietf.org/html/rfc4226
[91] https://tools.ietf.org/html/rfc6238
[92] https://tools.ietf.org/html/rfc6287

What are the potential use cases regarding eID in an eIDAS ecosystem?

Such applications are used as an electronic identification means when citizens need to authenticate on an online service.

Smart-ID[93] is an electronic identification app available on tablets and smartphones. It enables authentication of users seeking to access online services. Users register their devices through the app using their digital ID cards and digital certificates. Once the registration is complete, they can use *Smart-ID* to authenticate themselves for various services and digitally sign documents. In the Baltic countries, 2 million people are using *Smart-ID*. They perform 40 million transactions a month with the application, used for entering e-services, confirming transactions and digitally signing documents.

Other examples in Europe use a similar application, such as *Mobile BankID*[94] in Sweden, *L'Identité Numérique La Poste*[95] in France and *itsme*[96] in Belgium.

What are the applicable standards related to this technology?

Depending on the technology used in the mobile application, different standards can apply.

What are the network and information security considerations regarding this technology?

As this eID technology is based on mobile applications, the security of the mobile environment storing secrets is key for the overall resistance against attackers (software or hardware key store) (refer to section 2.2.3.2 for additional considerations). Also, the use of embedded biometrics sensors for such applications raises security concerns (refer to section 2.2.3.3 for a detailed description).

The application or devices that contribute to the authentication process could implement several security measures to offer protection against duplication and tampering. Moreover, certification against schemes such as Common Criteria could bring confidence on the assurance level of the solution.

Finally, it is interesting to note that providing end-users with the context of the authentication they are performing (e.g. access to a given website, approving a payment for a given amount, etc.) offers additional protection against social engineering attacks. End-users are indeed more aware of the operation they are approving and therefore can identify more easily operations they have initiated.

B.2.4 Cryptographic SIM or smartphone secure element

As a hardware component in the form of a chip used in smartphones, SIM cards can be used to store secrets and electronic certificates to be used during authentication processes. They can also embed additional applets than the ones used by network operators, for instance to have a PKI-based SIM that stores authentication and signature certificates (as for Estonian *Mobiil-ID* for instance).

Besides SIM cards, modern smartphones now directly integrate in the device additional components that could be used to store secrets, sensitive materials or perform operations in trusted environment such as:

[93] https://www.sk.ee/en/News/smart-id-now-has-2-million-users/
[94] https://www.bankid.com/en/
[95] https://lidentitenumerique.laposte.fr/
[96] https://www.itsme.be/

- Embedded SIM (eSIM)
- Integrated SIM (iSIM)
- Trusted Execution Environment (TEE)
- Secure Enclave (SE)
- Secure Element (SE)

Embedded SIMs are typically physical SIMs soldered into the device, enabling storage and remote management of multiple network operator profiles. Integrated SIMs offer further optimisations while retaining SIM security: the SIM moves from a separate chip into a secure enclave. It is worth noting that eSIMs and iSIMs are secure, dedicated physical circuits rather than software-based SIMs.

A hardware security module, a smart card, a trusted execution environment, a secure enclave and a secure element are all computing environments designed for secure execution and the storing of cryptographic keys. Their properties in common include their isolation from unsecured environments with a degree of tamper resistance, the impossibility to clone them as they hold unique cryptographic keys and their limited set of interfaces to reduce the attack surface.

What differentiates them is their form factor, which directly impacts their isolation and their resistance to attacks. The differences between Trusted Execution Environments (TEE), Secure Enclaves (SE) and Secure Elements (SE) are described below:

- A secure element is soldered to a board or part of a system-on-chip package. It is isolated from other computing environments on the same board or package but may not be resistant to physical tampering.
- If the secure element is inside the same chip package as the main processor, it's called a secure enclave.
- A trusted execution environment is a software environment which runs on the same processor as a less-secure environment, sometimes called Rich-OS Execution Environment (REE) on smartphones. It's isolated by a piece of software relying on hardware functionality (e.g. Arm TrustZone or Intel SGX).

GlobalPlatform[97] is currently working on standardising both SEs and TEEs. The defined security features for TEEs are[98]:

- Isolation from the Rich OS – all trusted applications and their related data are separated from the rich environment.
- Isolation from other Trusted Applications (TAs) – TAs are isolated within the TEE, and from the TEE itself.
- Application management control – any modification of the TA and the TEE can only be performed by the authenticated entity.
- Identification and binding – where the boot process is bound to the System-on-Chip, enforcing the authenticity and integrity of TEE firmware and TAs.
- Trusted storage – TA and TEE data is stored securely to ensure integrity, confidentiality and binding to the TEE (or anti-cloning).
- Trusted access to peripherals – the TEE offers APIs accesses to trusted peripherals such as the screen, biometric sensors and SEs, under the control of the TEE.
- State of the art cryptography – random number generation, cryptography and monotonic timestamps are key assets for value-added services.

[97] https://globalplatform.org/
[98] https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf

Regarding smartphones, Android-based devices are equipped with TEE and iOS-based devices are equipped with a Secure Enclave within the System-on-Chip. The iOS Secure Enclave is also responsible for processing fingerprint and face data from the Touch ID and Face ID sensors. The Apple Secure Enclave Processor (SEP) has a U.S. Federal Information Processing Standards (FIPS) 140-2 validation.

What are the potential use cases regarding eID in an eIDAS ecosystem?

Electronic identification schemes already use a PKI-enabled SIM card. In Estonia, *Mobiil-ID*[99], a PKI-enabled SIM card, received when requested to the mobile operator, can be used to access secure e-services, digitally sign documents and facilitates the enrolment flow to the *Smart-ID* application[100]. In Finland, a PKI SIM card, called *Mobile eID,* is also used for electronic identification. Moldova followed Estonia's example with a mobile e-ID called *Me-ID*[101], existing since 2011. It operates the same way as the Estonian *Mobiil-ID*.

What are the applicable standards related to this technology?

SIM cards are defined by the TS 102 221 – Smart cards; UICC-Terminal interface; Physical and logical characteristics[102] and the TS 131 102 – Universal Mobile Telecommunications Systems (UMTS); LTE; Characteristics of the Universal Subscriber Identity Module (USIM) application[103] standards. As described above, GlobalPlatform is currently working on standardizing SEs and TEEs.

What are the network and information security considerations regarding this technology?

This technology was used in several notified and pre-notified schemes (refer to section 2.2.3.2 for the security recommendations on this topic discussed during peer reviews).

B.2.5 Mobile Connect

Mobile Connect is a global open and common framework developed by the GSM Association (GSMA) in cooperation with leading mobile operators. The standard is already supported by 60 mobile operators in 30 countries[104].

The framework offers authentication, authorisation, identity and attributes sharing or verification for service providers, although for now, only one operator offers services related to identity and attribute sharing, all others being focused on authentication. Mobile Connect's prerequisites are that the mobile phone uses a compatible SIM card and that the mobile operator supports Mobile Connect.

The authentication process can work using several authenticators:

- A seamless check by the mobile operator that the mobile phone is connected to the network
- A verification link sent by the operator through SMS
- A USSD session initiated by the operator allowing the users to verify themselves by typing a PIN that is stored server-side by the operator
- A SIM applet used to authenticate the user on his mobile phone, with an authentication request triggered by the mobile operator. The verification then requires either only to

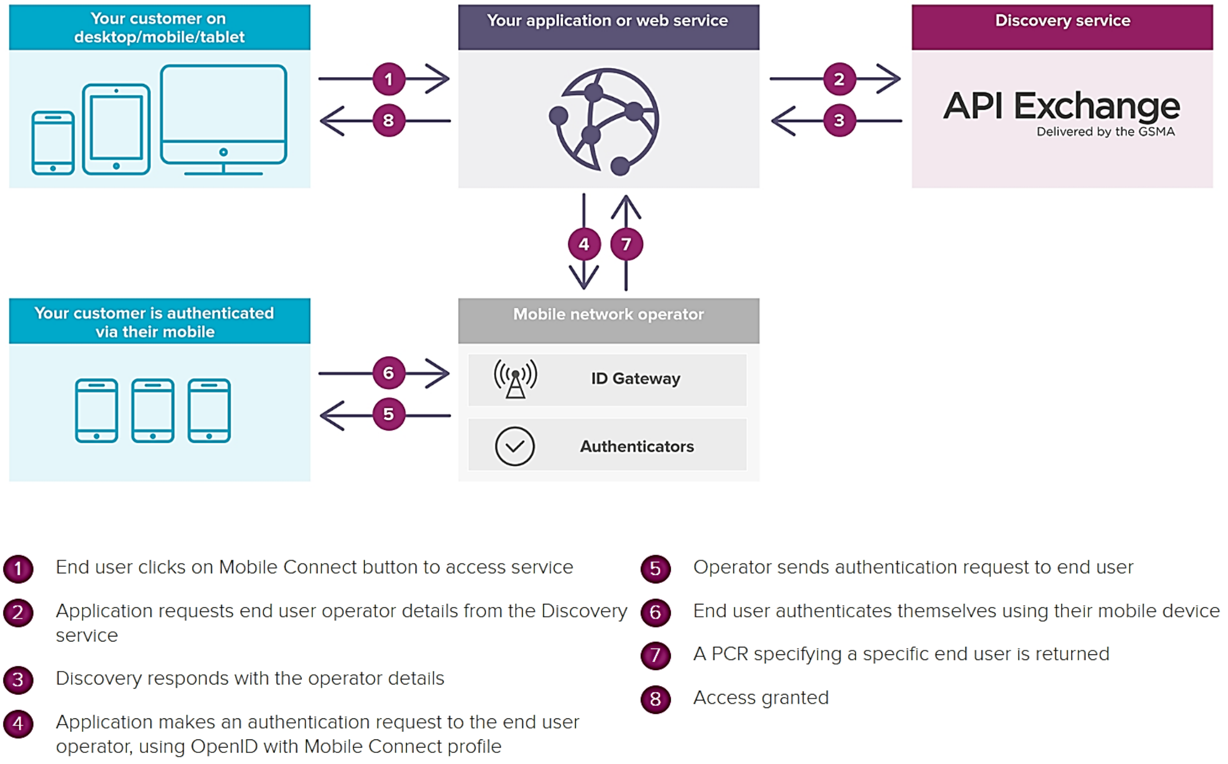
[99] https://e-estonia.com/solutions/e-identity/mobile-id/
[100] https://www.smart-id.com/help/faq/registering/can-use-mobile-id-register-smart-id-account
[101] http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf, Annex Moldova
[102] https://www.etsi.org/deliver/etsi_TS/102200_102299/102221/11.00.00_60/ts_102221v110000p.pdf
[103] https://www.etsi.org/deliver/etsi_ts/131100_131199/131102/13.05.00_60/ts_131102v130500p.pdf
[104] Source: https://mobileconnect.io/

approve the authentication process or to require an additional PIN code, verified locally on the SIM applet.

The last authentication mode is the most interesting offered by the Mobile Connect framework as it offers additional security with the usage of the SIM applet on the SIM card, which is a secure element. For this authenticator, a SIM toolkit session is initialised by the SIM card and generates the information prompted to the user, either to confirm an authentication or to type a PIN code chosen at the service activation. This process thus uses the SIM applet directly, without relying on a native smartphone application.

In addition to the Mobile Connect API used for authentication, the GSMA has also developed a Discovery API (API Exchange) that can be used by a service provider (or a third-party identity provider) to discover the mobile operator of the user trying to authenticate with Mobile Connect.

Figure 6: Mobile Connect standard authentication process[105]


Your customer on desktop/mobile/tablet
Your application or web service
Discovery service
API Exchange
Delivered by the GSMA
1
8
2
3
4
7
Your customer is authenticated via their mobile
Mobile network operator
ID Gateway
Authenticators
6
5

1. End user clicks on Mobile Connect button to access service
2. Application requests end user operator details from the Discovery service
3. Discovery responds with the operator details
4. Application makes an authentication request to the end user operator, using OpenID with Mobile Connect profile
5. Operator sends authentication request to end user
6. End user authenticates themselves using their mobile device
7. A PCR specifying a specific end user is returned
8. Access granted

In the process described previously, it is worth noting that identity attributes are not stored on the user's SIM card, as it would require additional storage space on the SIM which has limited capabilities. Mobile Connect offers identification based, for instance, on identity attributes gathered by the mobile operator, potentially shared with the service provider for which the authentication is performed. However, the way Mobile Connect is deployed and used today is more focused on authentication. Either way, in order to link the user with a persistent unique identifier for non-ambiguous authentication purposes, Mobile Connect manages a PCR (Pseudonymous Customer Reference). The mobile operator generates this PCR during the first successful authentication of a user with Mobile Connect. This PCR remains unchanged for the combination of an end-user and the application or web service, even if the user switches operators.

[105] Retrieved from mobileconnect.io

Besides, Mobile Connect could also benefit from contextual information captured by mobile operators in its network to help identify risky situations and provide a risk-based approach. The contextual data could include the SIM's location, roaming, recent changes and more. Finally, in terms of standards, it is also worth noting that the API provided with Mobile Connect for exchanges between the service providers and the mobile operators uses Open ID Connect.

Building a comprehensive eID solution with Mobile Connect indeed requires defining how identity attributes are collected, how the initial identity proofing functions, and how identity attributes are issued once the authentication is performed.

An example of a Mobile Connect integration in an eID scheme: *Mobile Connect et Moi*

Mobile Connect et Moi is a French identity provider that is part of *FranceConnect* (the French state-operated identity federation service). *Mobile Connect et Moi* offers a mobile app, used for the initial identity proofing and the collection of identity attributes. The whole process is remotely performed and requires taking a photo of a valid identity document and performing a facial recognition (with liveness detection) to verify the requester's identity. After this process, the Mobile Connect service is activated on the SIM card and the user can choose the associated PIN code. *Mobile Connect et Moi*, as the identity provider, stores the identity attributes previously collected.

During the electronic identification process, the user enters his mobile phone number and then performs a Mobile Connect authentication with the SIM applet and the PIN code. The PIN CODE is verified locally on the SIM card. After the authentication confirmation, Mobile Connect et Moi shares the identity attributes to FranceConnect, using Open ID Connect, that verifies them and sends them to the service provider.

Mobile Connect eIDAS pilot

GSMA with its Mobile Connect technology was involved in an eIDAS pilot initiative which started in 2015 to demonstrate how Mobile Connect can be used to identify a citizen of one EU Member State in order to gain access to a public service of another Member State. Other stakeholders were involved, such as mobile operators, technology companies and government services. This pilot demonstrated the ability to support eIDAS compliant cross-border authentication with eID means based on Mobile Connect, including the identity provider *Mobile Connect et Moi*. The pilot was designed using the eIDAS reference architecture based on eIDAS nodes, with a proxy/connector approach, as developed by the European Commission and the Member States technical sub-group of the eIDAS Expert Group (see section 2.1.1.2 Interoperability framework for eID).

What are the applicable standards related to this technology?

As Mobile Connect is a framework developed by GSMA, there is no applicable standard related to this technology other than the Mobile Connect standard itself.

What are the network and information security considerations regarding this technology?

During a Mobile Connect API authentication request, the application declares the degree of confidence that is required in the returned asserted identity. The recommended Level of Assurance depends on the risk associated with an erroneous authentication: the greater the risk, the higher the Level of Assurance. These Level of Assurance are defined in the ISO/IEC 29115 Standard, described in section 2.1.2 Other international & third-country frameworks.

Mobile Connect supports Level of Assurance 2 and 3, i.e. some and high confidence in the asserted identity. A Mobile Connect authentication for LoA2 means the user needs to prove he is in possession of the device, playing the role of the credentials. A Mobile Connect authentication for LoA3 means the user needs to enter a secret PIN or use biometric factors on the enrolled mobile device.

B.3 BIOMETRICS

Biometric recognition uses an individual's unique physiological and behavioural attributes to identify and authenticate his or her identity. Physiological attributes include elements related to the shape or composition of the body, such as fingerprint ridges, iris patterns, or facial characteristics. Examples of behavioural attributes include gait, signature, keystroke patterns, and mouse usage. The type of attribute collected and matched is called modality. For example, fingerprint and iris are different biometric modalities.

A practical biometric modality should meet the specified recognition, accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.[106]

During an enrolment process, physiological and behavioural biometric characteristics are acquired through adequate sensors extracting distinctive features in order to form a biometric template. At the time of verification, the system processes another biometric input which is compared against the stored template, yielding acceptance or rejection.[107] Biometrics can also be used in an identification mode where a system recognises an individual by searching the templates of all the users in the database for a match.

Biometrics can be classified into two categories, primary and soft biometrics:

- Primary biometrics are modalities such as fingerprint, face, and iris recognition. They yield accurate results for identification (relatively low FARs and FRRs).
- Soft biometrics relate to an individual's behaviour and includes keystroke dynamics, signature analysis, and gait analysis. They are rarely used for identification purposes as error rates are high to identify a user. However, these modalities are currently more and more used for continuous authentication to verify the identity of a user throughout a session.

What are the applicable standards related to this technology, for all modalities?

Biometric information protection is defined in the *ISO/IEC 24745:2011 – Information technology – Security techniques – Biometric information protection* standard. It guides the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, it provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information. This standard is currently under review[108].

Requirements of biometric information protection include (ISO/IEC 24745:2011):

- *Confidentiality*: "to protect biometric references against access by an unauthorised outsider resulting in a privacy risk, biometric references shall be kept confidential".
- *Irreversibility*: "to prevent the use of biometric data for any purpose than originally intended, biometric data shall be processed by irreversible transformations before storage". It thus should be computationally hard to reconstruct the original biometric template from the protected template, while it should be easy to generate it.

[106] JAIN AK, ROSS A, PRABHAKAR S, *An introduction to biometric recognition*, 2004, https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf
[107] RATHGEB C and UHL A, *A survey on biometric cryptosystems and cancellable biometrics*, 2011
[108] https://www.iso.org/standard/52946.html

- *Unlinkability*: “the stored biometric references shall not be linkable across applications or databases.” Accordingly, different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching (diversity).

ISO/IEC 30107:2016 focuses on presentation attacks and their automated detection. A presentation attack is a presentation to the biometric capture subsystem to interfere with the operation of the biometric system.

What are the network and information security considerations regarding this technology, for all modalities?

Biometrics, in general, have a crucial security consideration to keep in mind: they are uniquely and permanently linked to the person. The direct consequence is that if biometric template data is revealed in some way, from a data breach, for instance, or if it can be copied, then the security of this technology is nullified. Unlike passwords that can easily be changed, getting a new fingerprint or face is impossible.

Concepts such as cancellable biometrics and biometric cryptosystems[109] were thus investigated and developed:

- In cancellable biometrics, complex mathematical functions are used to transform the original template data of a scanned fingerprint or face. This transformation is non-reversible, meaning it’s impossible to turn back the transformed template data being into the original fingerprint or face scan. If the database holding the transformed template data is breached, these transformed templates can be changed for new ones, as each enrolment results in a new unique template, even if the same finger or face is used.
- Biometrics cryptosystems combine the strengths of both cryptography and biometrics by dynamically generating keys with the help of biometrics to secure the template and biometric system.

B.3.1 Fingerprint Recognition

Fingerprint recognition is one of the most popular biometric techniques used in personal identification. Each individual has unique fingerprints, the pattern of ridges and valleys on the surface of a fingertip. There are three basic patterns of fingerprint ridges: the arch (a pattern where the ridge enters one side of the finger), the loop (the ridge enters one side of the finger, then forms a curve and exists on the same site of the finger from which it entered) and the whorl (the ridges form circularly around a central point)[110]. Ridge ending (the point where a ridge ends abruptly) and ridge bifurcation (the point where a ridge forks or diverges into branch ridges) are collectively called minutiae[111].

Depending on the business needs and on the level of assurance needed, the number of fingerprints captured and matched for an individual can be from one to all ten fingers. Multiple sensors can capture fingerprints:

- Optical sensors capture an image, mostly a photograph, and use algorithms to detect unique patterns by analysing the image’s lightest and darkest areas[112].

[109] https://www.researchgate.net/publication/257879510_A_survey_on_biometric_cryptosystems_and_cancelable_biometrics
[110] http://www.biometric-solutions.com/fingerprint-recognition.html
[111] ZAERI Naser, *Minutiae-based Fingerprint Extraction and Recognition* DOI: 10.5772/17527, 2011. Retrieved from: https://www.intechopen.com/books/biometrics/minutiae-based-fingerprint-extraction-and-recognition
[112] https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

- Capacitive sensors use electrical current to form an image of the fingerprint by tracking the changes in the charge stored in the capacitor when a ridge is placed over the conductive plates whereas it stays unchanged with an air gap.
- Thermal sensors read the temperature differences on the contact surface between fingerprint ridges and valleys.
- Ultrasonic sensors send high-frequency sound waves to penetrate the skin and get absorbed or bounced back based on the fingerprint pattern. They thus read the fingerprint on the dermal skin layer, eliminating the need for a clean and free of scares surface.

What are the potential use cases regarding eID in an eIDAS ecosystem and the related security considerations?

At first glance, it looks like fingerprint recognition could be used for identity proofing as well for authentication.

Indeed, another eID scheme or identity document storing fingerprints could be used to validate an identity enrolling to another eID. However, fingerprints are subject to enhanced security due to their sensitivity: they are, for example, protected with Extended Access Control on electronic travel documents. Their access is regulated and restricted, which makes it *a priori* impossible to use them to enrol a new eID.

Smartphone-embedded biometrics directly operated by the mobile operation system (e.g. iOS and Android) also seem like they could be used as an authentication means (to protect secrets stored in a smartphone or to unlock sensitive application such as the ones described in section B.2.3). However:

- Multiple fingerprints can be stored in Touch ID or equivalent, and they can belong to more than one person.
- Even if a specific fingerprint was saved during the enrolment phase, there is no way to associate it with a specific action and to force its use as an authentication factor linked to an eID means. Embedded biometrics sensor works with all stored biometrics templates regardless of under which circumstances they have been enrolled. Mitigation measures to avoid such situations are advising the end-user (similarly to advising smartcard users not to disclose their secret PIN) or deactivating this functionality if additional templates are enroled.

It is thus assumed that the owner of the smartphone is the one enrolling the templates and is responsible for it. Therefore, in case of eID means using such biometrics sensor as an authentication factor, there is no assurance that the templates enrolled match actually the identity of the user that has been issued the eID means.

Moreover, fingerprint recognition technology is not immune to circumvention, i.e. the system being fooled using fraudulent methods. A study has recently shown that fingerprint recognition is vulnerable to dictionary attacks based on MasterPrints (real or synthetic fingerprints that can luckily match with a large number of fingerprints, constructed with a Generative Adversarial Network[113]).

Besides, fingerprints raise privacy concerns as their collection is simple and transparent for the end-users. Therefore, fingerprints could be collected without the person knowing it.

The combination of these security and privacy concerns result in fingerprint recognition being more and more abandoned in favour of face recognition for electronic identification.

[113] https://arxiv.org/abs/1705.07386

B.3.2 Face Recognition

Face recognition is the process of identifying or verifying the identity of a person using their face. First, the face needs to be detected, then captured and finally matched.

To capture a face, 2D or 3D sensors can be used. The “face” is then transformed into digital template by applying an algorithm before comparing the image captured to those held in a database.

Face recognition uses features of the face such as the distance between the eyes, the width of the nose, the depth of the eye sockets, the shape of the cheekbones and the length of the jawline. These features do not change significantly over time[114].

What are the potential use cases regarding eID in an eIDAS ecosystem?

Face recognition could be used in the enrolment phase as well as the authentication phase.

France, for instance, is currently developing *Alicem* eID scheme which use facial recognition during the enrolment phase. This eID scheme is in test mode. Facial recognition is used during enrolment to make sure that the applicant matches the photo stored on the ICAO chip of the passport. If they match, the facial recognition will validate the identity and enrol the identity on the smartphone application.

What are the network and information security considerations regarding this technology?

Facial recognition brings up multiple security and privacy considerations (Refer to section 2.2.2.2 for additional security considerations regarding face recognition that have arisen during the conducted peer reviews), including:

- Algorithms are often proprietary and difficult to rate, so their selection is complicated. NIST is for instance maintaining a program to assess facial recognition algorithm quality[115]
- Morphing pictures (creating a photo ID containing a graphical representation of several faces, which enables multiple individuals to share credentials) is a way to bypass facial recognition if the picture source is not managed correctly (i.e. if there is no existing relationship between the picture and the identity, for example, through a national database)
- According to the GDPR, a freely given, specific, informed and unambiguous consent must be granted to approve the usage of biometric features[116]. As it should be a freely given consent, an alternative to facial recognition must be offered.

B.4 PROSPECTIVE TECHNOLOGIES

B.4.1 eID using Blockchain/Distributed Ledger Technology

The blockchain is a technical solution that leverages the notion of distributed ledgers technology (DLT) that was popularised by the bitcoin phenomenon born in 2009. A distributed ledger is a replicated set of data across multiple actors. In the case of bitcoin, only the transactions are shared and replicated. Distributed ledgers were created to ensure trust between actors without the need for a third-party trusted by all the stakeholders.

[114] For adult. For Children, facial recognition may not be suitable.
[115] See for instance: https://www.nist.gov/programs-projects/frvt-11-verification
[116] 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, Article 9, https://eur-lex.europa.eu/eli/reg/2016/679/oj

Blockchains are created around a few fundamental properties:

- Distributed and shared: for records to be consigned, the main actors of the blockchain are required to know and witness that data is being recorded. All parties are therefore required to be online and participate in giving the consensus to publish new records;
- Immutable: the blockchain records integrity is based on an uninterrupted chain since the beginning of the blockchain. This chain ensures the immutability of data recorded but requires establishing a consensus to add a new block to the chain consistently. As a consequence, records cannot be modified, but new records can be added to the chain to describe modifications to existing ones;
- Ordered: as the records are chained, they are ordered one after the other, which can be used for proof of anteriority.

Blockchain technology can be leveraged to implement the immutable property of Self-Sovereign Identity approach and the need of a distributed system to support it. It also serves as a container for the Verifiable Claims that goes along with the SSI. Those two evolutionary tendencies are introduced in chapter 1.4.5.

What are the potential use cases regarding eID in an eIDAS ecosystem?

Blockchain-based eID solutions can be used as electronic identification means, once the identity information is proofed using a third party eID solution. In this case, the trustworthiness of the identity information or verifiable claim a user can share is inherited from the authority that proofed that piece of information. It may appear inconsistent to rely on trusted third parties to proof identities to be used in a decentralised system, but blockchain-based eID solutions offer a standard cross-platform technology independent from the eID solutions that trusted third parties could offer and manage.

Identity proofing for blockchain-based eID solutions can be performed when the identity information is first inserted by the owner, or later when the user wants to verify it against a certain level of assurance requested by a service provider. This identity proofing can be achieved through two mechanisms under the eIDAS framework[117]:

- Authentication with a notified eID scheme
- Electronic signature using electronic certificates issued by trust service providers.

What are the applicable standards related to this technology?

Blockchain and distributed ledgers technologies are based on a set of technical specifications including cryptography operations. Some initiatives are launched to work on standards related to blockchain-based applications. For example, ETSI launched in 2018 a new Industry Specification Group on Permissioned Distributed Ledger[118]. The IEEE has been actively pursuing blockchain standardisation efforts through various activities in multiple industry sectors[119].

When it comes to eID solutions as a blockchain application, the main initiatives are:

- The one related to the Self-Sovereign Identity approach using Decentralized Identifiers (DIDs), which are “a new type of identifier for verifiable, decentralized digital identity.

[117] https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf
[118] https://www.etsi.org/newsroom/press-releases/1473-2018-12-press-etsi-launches-new-industry-specification-group-on-blockchain
[119] https://blockchain.ieee.org/standards

These new identifiers are designed to enable the controller of a DID to prove control over it and to be implemented independently of any centralized registry, identity provider, or certificate authority." Data Model and Syntaxes used in Decentralized Identifiers are specified by W3C[120]

- The one related to the Verifiable Claims to "provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable"[121] specified by W3C as well.

What are the network and information security considerations regarding this technology?

A first security consideration to keep in mind is related to the blockchain technology itself and its vulnerability to what is called the "51% attack", where an attacker controlling a majority of the nodes can record incorrect data to the chain. In this case, the attacker focusses on corrupting the nodes, which is less complicated than attacking the cryptography behind the blockchain itself. The more the blockchain nodes network is vast, the more this attack is complex to carry out because of the higher number of nodes to corrupt.

Another issue regarding this technology is related to one of its inherent properties, immutability: once identity information is added to the blockchain, they cannot be removed. If today it is assumed that cryptographic mechanisms used with the blockchain are secure enough for current attacker's capabilities, no one can know for sure when technology breakthroughs will be made available to overcome those cryptographic mechanisms, especially with the rise of Quantum Computing[122]. When that happens, personal data stored in the blockchain would be made public. To mitigate this risk, personally identifiable information and biometric information should never be stored on a blockchain[123].

One last issue to consider is related to the decentralisation aspect of the blockchain: the features usually delivered by centralised systems are now to be managed by the users themselves. The most striking example of these features is the recovery of lost or forgotten private keys: in the blockchain, recovery of these pieces of information is not available, and users must find a way to do it outside the blockchain, for example by using centralised systems to manage their private keys, which goes against one of the reasons to use blockchain as an eID solution.

[120] https://w3c-ccg.github.io/did-spec/
[121] https://www.w3.org/TR/vc-data-model
[122] https://medium.com/fintech-kellogg/quantum-computing-is-it-the-end-of-the-blockchain-10fa7e222b0a
[123] http://documents.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

XX-00-00-000-XX-X

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber 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