applied sciences

MDPI

Systematic Review

The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes

Amir Sharif [1,*,†], Matteo Ranzi [2,†], Roberto Carbone [1,†], Giada Sciarretta [1,†], Francesco Antonio Marino [3,†] and Silvio Ranise [1,4,†]

1 Center for Cybersecurity, FBK, 38123 Trento, Italy
2 Department of Information Engineering & Computer Science, University of Trento, 38123 Trento, Italy
3 Polygraphic Institute & State Mint, 00138 Rome, Italy
4 Department of Mathematics, University of Trento, 38123 Trento, Italy
* Correspondence: asharif@fbk.eu
† These authors contributed equally to this work.

Abstract: The eIDAS regulation aims to provide an interoperable European framework to enable EU citizens to authenticate and communicate with services of other Member States by using their national electronic identity. While a number of high-level requirements (e.g., related to privacy and security) are established to make interoperability among Member States possible, the eIDAS regulation does not explicitly specify the technologies that can be adopted during the development phase to meet the requirements as mentioned earlier. To the best of our knowledge, there is no work available in the literature investigating the technological trends within the notified eIDAS electronic identity schemes used by Member States. To fill this gap, this paper analyzes how the different technological trends of notified schemes satisfy the requirements of the eIDAS regulation. To do this, we define a set of research questions that allow us to investigate the correlations between different design dimensions such as security, privacy, and usability. Based on these findings, we provide a set of lessons learned that would be valuable to the security community, as they can provide useful insights on how to more efficiently protect interoperable national digital identities. Furthermore, we provide a brief overview regarding the new eIDAS regulation (eIDAS 2.0) that aims to provide a more privacy-preserving electronic identity solution by moving from a centralized approach to a decentralized one.

Keywords: OAuth 2.0; SAML; OpenID Connect; digital identity; eIDAS

Citation: Sharif, A.; Ranzi, M.; Carbone, R.; Sciarretta, G.; Marino, F.A.; Ranise, S. The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Appl. Sci.* **2022**, *12*, 12679. https://doi.org/10.3390/app122412679

Academic Editor: Luis Javier Garcia Villalba

Received: 4 November 2022
Accepted: 8 December 2022
Published: 10 December 2022

1. Introduction

One of the most important trends in modern online services and applications is accessibility anytime and anywhere from different locations and devices while providing a homogeneous user experience and increasing user trust. This creates a demand for new architectures that are no longer based on the notion of defense perimeter but rather on distrusting any entity (user, device, or application) until it is authenticated at an appropriate level of assurance and has proven to hold appropriate permissions to access resources. As a result, digital identity and consequently identity management (IdM) solutions become the basic building blocks that allow users to access online services, such as those offered by the public administration, in a secure and privacy-preserving way.

The European Commission published the Regulation 910/2014 on electronic identification and trust services (eIDAS) [1] in 2014. This Regulation aims to enable citizens throughout the European Union (EU) to authenticate to and communicate with online services of Member States (MSs) while using an electronic Identity (eID) scheme of their own MS. With eIDAS, the EU has established the necessary foundations and a clear legal framework for individuals, businesses, and government agencies to safely access online services and conduct transactions online in a single "click". To illustrate, let us consider a scenario where a company operating in Italy wants to send its employee to another branch

in Germany. The employee needs to create a bank account in Germany to be able to receive the salary. The employee does not need to travel to Germany to open a bank account, as s/he can utilize the trust services of eIDAS to open it remotely and securely by using their Italian national electronic IDentity (eID scheme). Figure 1 illustrates a general overview of the steps for opening a bank account by utilizing the trust services of eIDAS. In other words, eIDAS provides the foundation for the portability of national digital identities across borders in EU.

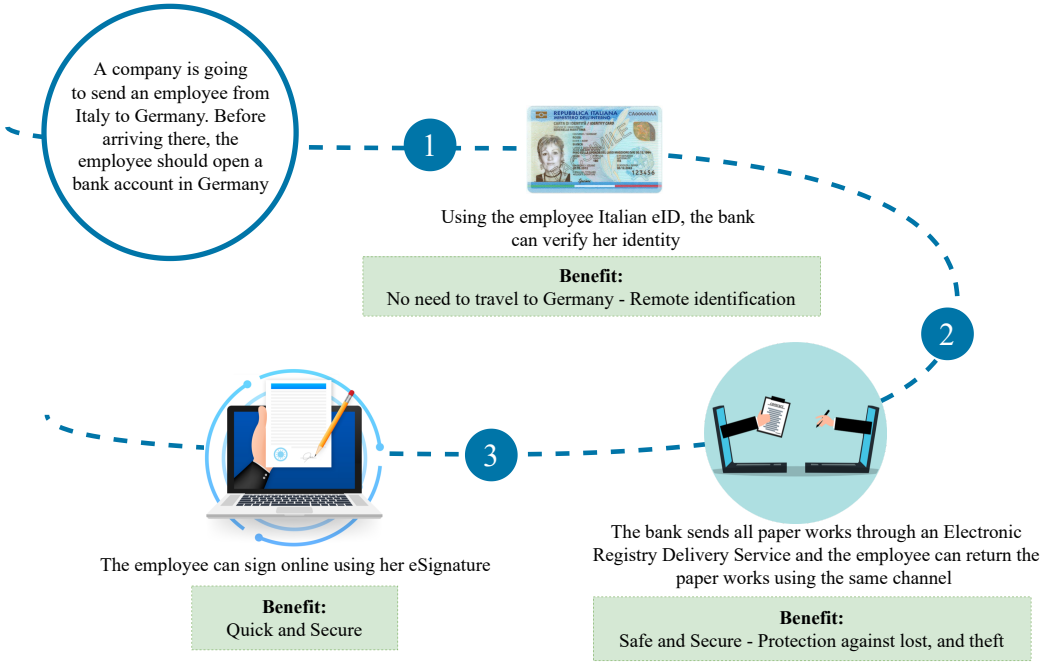

Figure 1. eIDAS in action: opening a bank account.

To make an eID scheme recognizable within other MSs in EU, the European Commission must approve the MS's eID schemes through a notification process. The "Cooperation Network" is an entity which is responsible to perform the notification process and the aim of this process is to check whether the eID scheme meets the eIDAS regulation requirements [1]. Once a MS submits an eID scheme for analysis by the Cooperation Network, it becomes "pre-notified". After the Cooperation Network examines the eID scheme, it turns into "peer-reviewed" and if it passes the analysis successfully and meets the eIDAS regulation requirements, the Cooperation Network announces it as "notified". This means that the eID scheme is qualified and other MSs can integrate it within their services to enable cross-country user authentication.

Although the eIDAS regulation defines a set of security and privacy requirements (e.g., level of assurance and minimal set of user personal data claims that a service can request to identify the user), it does not explicitly specify the technological aspects that developers can adopt during the development phase to meet the aforementioned requirements. While it is desirable that eIDAS is technology agnostic (to accommodate a wide range of current technology and to remain open to those that will be introduced in the future and avoid vendor lock in and related problems), it may make it difficult to understand how to exploit the currently available or new technologies to comply with the eIDAS regulation requirements. To elaborate on this point, let us consider the eIDAS implementation regulation 1501/2015 [2] that defines requirements regarding the three levels of assurance (namely, Low, Substantial, and High). These requirements identify a set of elements needed to reach the desired level of assurance. For example, for a Low level of assurance, the document states: "The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic

attack potential can subvert the authentication mechanisms" [2]. GDPR (The complete list of identified elements for each level of assurance) is available in Appendix A. It is crucial to realize that such requirements can be satisfied using several different technologies, and a wrong design choice may result in a less secure, non privacy-preserving, and difficult to use solution within the MS's eID ecosystem. It is thus crucial to know how the technological choices within the eID scheme implementation can affect security, privacy, and usability. However, to the best of our knowledge, no available work in the literature investigates the aforementioned dimensions within the eIDAS-compliant eID schemes. This motivates our work to understand how to satisfy the requirements of eIDAS regulation by deploying MS eID schemes based on their own national digital identity infrastructures.

More precisely, this work explores the technological choices underlying notified eIDAS-compliant eID schemes, identifies the trends of deploying such schemes that each MS adopts, and discusses how they satisfy the eIDAS regulation requirements. We do this by defining the following research questions along the security, privacy, and usability goals:

- Security and Privacy:
  - Which are the standard authentication protocols adopted by the eID schemes?
  - Which are the crucial implementation choices taken to deploy the identified standard authentication protocols in the previous question by the eID schemes?
- Security and Usability:
  - Which are the adopted authentication methods for three levels of assurance?

The rapid development of mobile technologies has turned these devices from entertainment gadgets to popular and ever-present media. Nowadays, users can manage their banking accounts, control their personal health records, or access public administration services by installing a mobile application. Therefore, it is important to investigate their potential roles in the deployment of MS eID schemes. A key standard for mobile-based eID schemes is OpenID Connect that is an authentication standard [3] used to exchange authentication assertions of users. Furthermore, OpenID Connect is one of the most widely used protocols to support innovative authentication solutions due to the benefits that it provides (e.g., lightweight messages) in comparison with the other available standard authentication protocols. Based on these two observations, we further refine the above-mentioned research questions to investigate mobile- and OpenID Connect-based eID schemes. The refined research questions are detailed in Section 2.2.

The results that we obtain through the investigation of these questions allow us to understand the correlations between security, privacy, and usability, and to provide a set of lessons learned that would be valuable to the security community as they can provide useful insights on how to more efficiently protect interoperable national digital identities.

To summarize, this paper extends our work in [4] with the following main contributions:

1. We extend our analysis regarding different authentication mechanisms chosen by MSs, adopted authentication standards and mobile-based authentication solutions by adding the recently notified eID schemes. More specifically, we add the eID schemes of the Czech Republic (MojeID, MEG), Austria (Austria ID), Sweden (BankID, Freja eID, EFOS), and Malta (Identity Malta);
2. We discuss two new research questions to identify the trends for the eID schemes that provide solutions based on the OpenID Connect. In particular, we investigate the adopted OpenID Connect profiles and implementation choices for these solutions;
3. We refine and extend a set of lessons learned by adding new considerations specific to solutions based on OpenID Connect; and
4. We provide a brief overview of the newly introduced eIDAS regulation (eIDAS 2.0 [5]) and how it is going to address the privacy shortcomings of the previous version of the eIDAS regulation introduced in 2014 [1].

Paper Structure

In Section 2, we introduce the methodology we adopted for analyzing notified eIDAS eID schemes, followed by the identified research questions and data source. Section 3 describes our findings regarding the adopted authentication methods. Section 4 presents the current status in terms of adopted authentication standards for the eID schemes under analysis. Focusing on OpenID Connect, Sections 5 and 6 introduce the current trends regarding the adopted profiles and the implementation choices, respectively. Section 7 presents our findings regarding the technological trends in the authentication mechanism of mobile-based eID schemes, followed by our recent observations in Section 8 on the newly introduced eID schemes by the MSs that were not available during our analysis. Section 9 summarizes the lesson learned that is extracted from our analysis. A brief overview regarding the new version of the eIDAS regulation (eIDAS 2.0) is provided in Section 10. Finally, we summarize the main results and provide insights for future work in Section 11.

2. Methodology

This section presents the methodology we followed to analyze notified eIDAS eID schemes. Section 2.1 summarizes the considered procedure for eID schemes selection. Section 2.2 presents the research questions that we have identified for the analysis of eID schemes. Section 2.3 contains the considered data source.

2.1. eID Schemes Selection

In the eIDAS regulation [1], an *eID scheme* is defined as "a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons", where an *eID means* is "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service". Each MS can notify one or more eID schemes based on one or multiple eID means.

As this work aims to highlight technological trends for eIDAS eID schemes, we focus our analysis on the list of notified eIDAS schemes available on the European Commission's official website (September 2022) [6]. We performed a preliminary analysis in November 2021, and the results are available on our companion website (https://st.fbk.eu/complementary/FARES2022_2, accessed on 1 November 2021). In the following, we report the results of our latest technological trends analysis (September 2022). We aim to check if there are any recently notified eID schemes that we did not consider during the first phase. Figure 2 displays the complete list under analysis, which consists of the eID schemes of 18 (among 27) MSs (There are MSs that, at the time of the analysis (September 2022), still do not have pre-notified, peer-reviewed, or notified scheme. However, based on Article 7 of eIDAS 2.0 [5] regulation, the notification in eIDAS 2.0 becomes mandatory, and each MS MUST have at least one notified scheme) together with the eID scheme of the United Kingdom (Even if, due to Brexit (1st February 2020), the United Kingdom's solution is no longer listed on the European Commission's official website, it was taken into consideration within this analysis since it was formerly notified).

Note that, since some MSs offer multiple eIDAS schemes and/or means (e.g., the Belgian national itsme mobile app and eID Card), we consider a total of 24 eIDAS eID schemes with 40 eIDAS eID means within our analysis. Furthermore, we also consider a solution used in Baltic countries called "SMART-ID". This eID scheme is more recent and may reflect current technological trends. As a final remark, our updated analysis shows an improvement in the status of notified eIDAS eID schemes. While during our first analysis (November 2021), there were 19 notified eID schemes with 31 eID means, in our latest analysis, these numbers changed to 24 notified eID schemes with 40 eID means.

Figure 2. eIDAS notified eID schemes (24 notified eID schemes with 40 eID means).

2.2. Research Questions

Regulation 1501/2015 [2,7] sets out the technical and operational requirements for the eIDAS European interoperability framework. Note that the documents mentioned above only highlight the technical requirements without providing technical details on how to fulfill these requirements. This work aims to cover this gap by looking into the adopted technologies by the eID schemes.

An eID scheme, or more precisely, its related eID means, is used for authenticating citizens in online services. As defined in the NIST Special Publication 800-63 [8], *authentication* is the process of "verifying the identity of a user, process, or device, often as a prerequisite to allowing a system's resource". eID schemes follow *authentication protocols* to perform the user authentication. The authentication protocols specify how the entities involved exchange messages and establish that a person attempting to access an online service has possession and is in control of one or more valid *authenticators* (typically a cryptographic module or password). Every authenticator can attest to one or more *authentication factors* (something you know, something you have, and something you are).

The strength of an authentication process is characterized by an ordinal measurement known as *authentication assurance level* (or Level of Assurance-LoA). In particular, different LoAs provide different security levels based on the difficulty one would have trying to use someone else eID to access online services. With the first research question (RQ1), we will detail the different authentication means chosen by the MSs to comply with the notified LoA.

Different authentication protocols and standards have been defined based on the authentication process. They provide a way to achieve interoperability while facilitating the definition of a set of best practices securing the deployments in different use-case scenarios. The second research question (RQ2) will discuss the different authentication standards adopted in the eID schemes.

Recently, the OpenID Connect authentication standard [3] has gained lots of attraction due to its benefits compared with older standards such as SAML, including using JSON format instead of heavy XML data format for data transition or more straightforward implementation due to its API-based nature. The OpenID Connect Foundation published different OpenID Connect profiles to provide specific guidelines for various scenarios and different kinds of deployments (such as Open Banking and eGovernment) that require a different level of security and privacy. In the third research question (RQ3), we will explore

the different OpenID Connect profiles chosen by MSs within their OpenID Connect-based eID schemes.

The secure implementation of eID schemes based on OpenID Connect is highly dependent on the implementation choices adopted by the MSs. In the fourth research question (RQ4), we will check the adopted implementation choices by the MSs within their OpenID Connect-based eID schemes.

Finally, as mobile use has overtaken desktop users worldwide, transactions via mobile devices are on the rise and require a secure authentication process. In the fifth research question (RQ5), we will compare mobile-based solutions that provide simplicity and security by leveraging capabilities provided by mobile devices, such as biometric characteristics.

Summarizing, we organize our investigation of the technological trends in notified eID schemes around the following five main research questions:

- RQ1. Based on the LoA (Low, Substantial, and High), what are the supported authentication methods in notified eID schemes?
- RQ2. Which standards are used to implement authentication solutions in notified eID schemes?
- RQ3. For the solutions based on OpenID Connect, which are the profiles followed by the notified eID schemes?
- RQ4. For the solutions based on OpenID Connect, which are the implementation choices considered by the notified eID schemes?
- RQ5. Which technologies are used to implement authentication solutions using mobile applications in notified eID schemes?

2.3. Data Source

Our analysis for the selected eID schemes relies on the information collected from the official documentation and official websites of the considered eID schemes [9–25]. Furthermore, we support our analysis with eID scheme-related technical reports and the related OpenID Connect specifications and security best current practices, namely, [3,6,26–33]. We present the list of considered eID schemes and their eID means in Table 1.

Table 1. List of eID schemes and means.

MS	Ref	eID Scheme	ID	eID Means
BE	[9]	Belgian eID Scheme FAS/eCards	1	Belgian Citizen or Foreigner eCard
	[10]	Belgian eID Scheme FAS/itsme	2	itsme Mobile app
CZ	[11]	National identification scheme of the Czech Republic/eID Card	3	CZ eID Card
	[12]	National identification scheme of the Czech Republic/MojeID	4	MojeID
	[34]	National identification scheme of the Czech Republic/MEG	5	MEG
DK	[13]	NemID	6	NemID
DE	[14]	German eID based on Extended Access Control	7	ID/RP/EEA Card

Table 1. *Cont.*

MS	Ref	eID Scheme	ID	eID Means
EE	[6,29]	Estonian eID Scheme /eCards	8	ID/RP/Diplomatic/e-residency Card
	[35]	Estonian eID Scheme/Digi-ID	9	Digi-ID
	[36]	Estonian eID Scheme/Mobiil-ID	10	Mobiil-ID
ES	[6,27,29]	Documento Nacional de Identidad electrónico (DNIe)	11	Spanish ID card (DNIe)
HR	[29,37]	National Identification and Authentication System (NIAS)	12	Personal Identity Card
LV	[26,38]	Latvian eID Scheme/eCards	13	eID/eparaksts card, eparaksts+ card
	[26,39]	Latvian eID Scheme/eParaksts	14	eParaksts
LT	[15]	Lithuanian National identity card	15	Lithuanian National Identity card
LU	[40]	Luxembourg national identity card	16	Luxembourg national identity card
PT	[16]	Cartão de Cidadão	17	Portuguese national identity card
	[41]	Chave Móvel Digital	18	Digital Mobile Key
SK	[17]	National identity scheme of the Slovak Republic	19	Slovak Citizen eCard, Foreigner eCard
IT	[42]	Italian eID based on National ID card (CIE)	20	Italian eID Card
	[43]	SPID	21	Aruba PEC SpA
			22	Namirial SpA
			23	InfoCert SpA
			24	In.TE.S.A. SpA
			25	Poste Italiane SpA
			26	Register.it SpA
			27	Sielte SpA
			28	Telecom Italia Trust Technologies S.r.l.
			29	Lepida SpA
NR	[18]	Trust Framework for Digital Identity	30	eHerkenning
	[44]	DigiD	31	DigiD
UK	[19]	Gov.UK Verify/Post Office	32	Post Office
	[45]	Gov.UK Verify/Digidentity	33	Digidentity
FR	[20]	Franceconnect	34	Franceconnect
	[20]	Franceconnect	35	Franceconnect+
AT	[21]	Austria ID	36	Austria ID
SE	[22]	Swedish eID/BankID	37	BankID
	[23]	Swedish eID/Freja eID	38	Freja eID
	[24]	Swedish eID/EFOS	39	EFOS
MT	[46]	Identity Malta	40	ID/e-residency Card
EE,LV,LT	[25]	SMART-ID	41	SMART-ID

3. RQ1: Authentication Mechanisms Based on LoA

As described in Article 8 of the eIDAS regulation, a notified eID scheme shall specify the corresponding LoA (Low, Substantial, High), which shall meet the following authentication requirements (as defined in the ISO 29115 [47]):

LoA Low (L): comparable with LoA2 of ISO 29115, it provides a limited degree of confidence in the asserted identity of a person, single-factor authentication is acceptable.

LoA Substantial (S): comparable with LoA3 of ISO 29115, at least two authentication factors should be used.

LoA High (H): comparable with LoA4 of ISO 29115, at least two authentication factors should be used, and it should guarantee protection against duplication and tampering by attackers with high potential.

The following sections characterize the adopted authentication methods based on the different LoAs. Table 2 summarizes the results, where the considered MSs are referred to by using the two letters country code based on ISO Alpha-2.

Table 2. Analysis results of notified eID schemes for RQ1, RQ2, and RQ5.

MS	ID	LoA L	LoA S								LoA H				Authn Standard							Mobile Apps				
			Authentication mechanisms								Crypto Auth				SSO				Fed.		Prot.	Storage				
											HW Auth															
		PWD	PWD + SMS	PWD + SW	PWD + MAT	PWD + HW	PWD + QR	PWD + PN	PWD + SK	QR	ID-SC	D-SC	SIM	SK	SW Auth	SAML	OIDC	FIDO	SP-IdP	Direct Login	Bio	PIN	Keystore	SIM	Smart card	MB2App2MB
BE	1	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	Y	-	Y	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	Y	-	Y	-	Y	Y	-	Y	-	Y
CZ	3	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-
	4	Y	-	-	-	-	-	Y	Y	-	-	-	-	Y	-	Y	Y	Y	Y	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	?	?	?	?	?	Y	Y	?	?	-	-
DK	6	-	-	Y	Y	Y	-	-	-	-	-	-	-	-	-	Y	Y	-	Y	-	Y	Y	-	-	-	-
DE	7	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	Y	Y	-	-	-	-	Y	-
EE	8	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-
	9	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-
	10	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	Y	-	?	Y	-	Y	-	-
ES	11	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-
HR	12	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-
LV	13	-	-	-	-	-	-	-	-	-	Y	Y	-	-	-	-	Y ‡	-	Y	-	-	-	-	-	-	-
	14	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y ‡	-	Y	-	Y	Y	Y	-	-	Y
LT	15	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-
LU	16	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-

Table 2. *Cont.*

MS	ID	LoA L	LoA S								LoA H				Authn Standard							Mobile Apps				
			Authentication mechanisms								Crypto Auth					SSO			Fed.		Prot.	Storage				
											HW Auth															
		PWD	PWD + SMS	PWD + SW	PWD + MAT	PWD + HW	PWD + QR	PWD + PN	PWD + SK	QR	ID-SC	D-SC	SIM	SK	SW Auth	SAML	OIDC	FIDO	SP-IdP	Direct Login	Bio	PIN	Keystore	SIM	Smart card	MB2App2MB
PT	17	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-
	18	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	Y	-	-	Y	Y	-	-	Y
SK	19	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-
IT	20	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	Y †	-	Y	-	Y	-	-	-	Y	Y
	21	Y	Y	Y	-	Y	-	-	-	-	Y	-	-	-	-	Y	Y †	-	Y	-	Y	Y	-	-	Y	Y
	22	Y	Y	Y	-	Y	-	-	-	-	-	-	-	-	-	Y	Y †	-	Y	-	-	Y	-	-	-	?
	23	Y	Y	Y	-	-	Y	Y	-	Y	?	?	?	-	?	Y	Y	-	Y	-	Y	Y	?	?	?	Y
	24	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y ‡	-	Y	-	-	-	-	-	-	-
	25	Y	Y	Y	-	-	-	Y	-	Y	-	-	-	-	Y	Y	Y †	-	Y	-	Y	Y	Y	?	-	Y
	26	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y ‡	-	Y	-	-	-	-	-	-	-
	27	Y	Y	Y	-	-	-	Y	-	-	?	?	?	-	?	Y	Y ‡	-	Y	-	-	Y	?	?	?	Y
	28	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y ‡	-	Y	-	-	-	-	-	-	-
	29	Y	Y	Y	-	-	-	-	-	Y	-	-	-	-	-	Y	Y ‡	-	Y	-	-	Y	-	-	-	-
NR	30	Y	Y	-	-	Y	-	-	-	Y	?	?	-	-	-	Y	-	-	Y	-	?	?	-	-	?	-
	31	-	Y	Y	-	-	-	-	-	Y	Y	-	-	-	-	Y	-	-	Y	-	-	Y	-	-	Y	-
UK	32	-	Y	Y	-	-	-	-	-	Y	-	-	-	-	-	Y	-	-	Y	-	-	Y	-	-	-	-
	33	-	Y	-	-	-	-	-	-	Y	-	-	-	-	Y	Y	-	-	Y	-	-	Y	Y	-	-	Y
FR	34	Y	?	-	?	?	-	-	-	-	-	-	-	-	-	-	Y	-	Y	-	?	?	-	-	?	-
	35	-	?	-	?	?	-	-	-	-	-	-	-	-	-	-	Y	-	Y	-	?	?	-	-	?	-
AT	36	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	Y	-	Y	Y	Y	-	-	Y
SE	37	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	?
	38	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	?
	39	-	-	-	-	-	-	-	-	-	Y	-	-	Y	-	-	-	Y	-	Y	-	-	-	-	-	-
MT	40	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-
Baltic	41	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y ‡	-	Y ‡	-	?	Y	Y	-	-	-
Total		**12**	**13**	**9**	**1**	**4**	**1**	**4**	**1**	**10**	**16**	**2**	**2**	**2**	**6**	**25**	**20**	**2**	**32**	**9**	**11**	**19**	**8**	**2**	**8**	**10**

Legend: "Y": feature supported, "-": feature not supported, "?": the information is not available, "Y ‡": the eID mean uses OAuth instead of OIDC, "Y †": feature is under implementation, "PWD": Password, "SW": Software, "MAT": Matrix, "HW": Hardware, "PN": Push Notification, "SK": Security Key, "ID-SC": Identity Smart Card, "D-SC": Dedicated Smart Card, "SIM": Crypt SIM, "Auth": Authenticator, 'Authn": Authentication, "SSO": Single Sign-On, "Fed.": Federation, "SAML": Security Assertion Markup Language, "OIDC": OpenID Connect, "FIDO": Fast Identity Online, "SP": Service Provider, "IdP": Identity Provider, "Prot.": Protocol, "Bio": Biometric, "MB2App2MB": Mobile Browser to App to Mobile, "Baltic": EE, LV, LT.

3.1. Authentication Mechanisms: LoA Low

The authentication mechanisms at this level ensure that the subject controls an authenticator registered to the service, requiring single-factor authentication. Based on our analysis (see Table 2, column 2), 12 out of 40 notified eID means under analysis support the LoA Low, and all of them use "Login with Password" as the authentication method (i.e., based on what you know and consisting of a combination of a valid and unique identifier (username) and a secret pass-phrase (password)). Some of them (4 eID means) offer the "Login with QR code" (that will be discussed in the LoA substantial section) as an alternative to password-based authentication. Figure 3 represents this alternative option for the Poste Italiane eID mean. The main reason behind this implementation choice is to provide additional security and, more importantly, usability. Indeed, first of all, it removes the demand to remember the username and password. Secondly, it provides a smoother user experience that demands scanning a QR code using the citizen's pre-registered device and providing a PIN or using biometrics (e.g., touch ID or face ID).

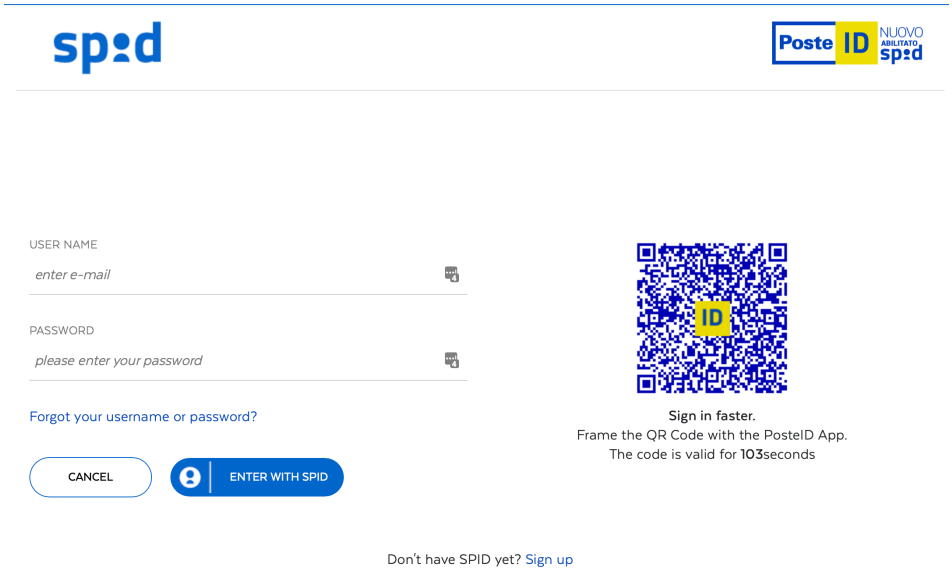

Figure 3. Login with password or login with QR code.

3.2. Authentication Mechanisms: LoA Substantial

The authentication mechanisms at this level provide substantial confidence that the subject controls an authenticator registered to the service. They require two different authentication factors. There are several alternatives, and the authenticator could be a combination of something the citizens know (e.g., a password) with something the citizens possess (e.g., a SIM or a physical document or device) or something the citizens possess (e.g., a mobile application) protected with something the citizens are (e.g., their fingerprint) or know (e.g., a PIN).

In case of possession, to prove the control of an authenticator, usually the authentication protocol requires the exchange of a *One Time Password* (OTP), which is a password that is valid for a short time and can only be used once.

The authentication mechanisms for LoA S based on our analysis results are:

PWD + SMS: username/password (knowledge factor) plus an OTP sent via SMS message to the registered phone number (possession factor) of the user;

PWD + SW: username/password (knowledge factor) plus an OTP generated each time s/he requested it by an OTP software application (possession factor) installed on his/her phone;

PWD + MAT: username/password (knowledge factor) plus a physical document (possession factor), also called "matrix", with the list of codes (OTPs) that s/he has to use to reply to the randomly generated challenge from the online service;

PWD + HW: username/password (knowledge factor) plus a physical electronic device (possession factor) which generates an OTP each time the user requests it;

PWD + QR: username/password (knowledge factor) plus the scan of a QR code from a registered application (possession factor) that then generates an OTP to the online service;

PWD + PN: username/password (knowledge factor) plus the sending of a Push Notification directly to a secure application on the user's device (possession factor), alerting the user that an authentication attempt is taking place. Note that the user should provide a PIN (possession factor) or use biometrics (inherence factor) to complete the authentication after receiving the notification on the registered device;

PWD + SK: username/password (knowledge factor) plus hardware security key (possession factor) that contains a private key (and the corresponding certificate) to send a signed OTP challenge to the authentication server. The user should provide a PIN (knowledge factor) or use biometrics (inherence factor) to complete the user authentication;

QR: is an authentication capability that permits a registered device (possession factor) to scan a QR Code. Then, the user should provide a PIN (knowledge factor) or use biometrics (inherence factor) to complete the user authentication.

Based on our analysis, 20 out of 40 notified eID means under analysis support the LoA Substantial. We report the main results per each eID means in columns 3–10 of Table 2. From the results, we have that:

- Concerning the OTP implementation approaches, SMS (13 out of 20) is the most adopted approach, and PWD + Matrix, PWD + QR Code, and PWD + HW SK (1 out of 20 eID means) are the least adopted ones within the eID means;
- None of the eID means under analysis support the Email within their OTP implementation approach;
- Only 4 out of 20, and 10 out of 20 eID means under analysis support the push notification and Login with QR Code mechanism, respectively.

Our latest analysis in September 2022 highlights a new technological trend within the implementation of eID schemes. Some solutions use the hardware security key (possession factor) as the second authentication factor to satisfy the requirement of LoA Substantial. As we will discuss later in Section 9, the usage of a hardware security key can increase the level of security and usability of an eID scheme.

3.3. Authentication Mechanisms: LoA High

The authentication mechanisms at this level provide high confidence that the subject controls an authenticator registered to the service, by requiring the proof of possession of a cryptographic authenticator. A cryptographic authenticator leverages a Public Key Infrastructure (PKI), by storing the user's private key (and the corresponding certificate). The authentication mechanisms are thus based on a challenge-response protocol. According to our analysis, the cryptographic authenticators used in the notified eID means are as follows:

1. **Hardware Authenticator (HW Auth):** indicates the support of login by using hardware authenticators (e.g., smart cards) by the eID means under analysis. Note that the hardware authenticator in LoA H refers to a hardware device that can securely store a client certificate. In contrast, the PWD + HW in LoA S refers to a hardware device capable of generating an OTP. We detected the following HW Auths:

- **Smart card** indicates the support of login by using a physical smart card (SC). In our analysis, we distinguish two types of SC, namely: dedicated SC (D-SC) and identity cards (ID-SC);
- **SIM (Crypt SIM)** indicates the use of SIM as a secure element to store secrets and electronic certificates, which are used during the authentication process. The Crypt SIM embeds additional applets (w.r.t. the ones used by network operators) to provide the functionalities for storing authentication and signature certificates;
- **Security Key (SK)** indicates the support of login by using a hardware security key (e.g., FIDO security key). The difference between SK in this category and the PWD + HW SK as defined in LoA S lies in the hardware requirements that the SK satisfies. To elaborate, let us consider the certification requirements defined for FIDO SKs in [48]. To be suitable for LoA H, the SK must have a restricted operating environment (e.g., Secure element), while this condition is not necessary for SKs that are recognized for LoA S;

2. **Software Authenticator (SW Auth)**: indicates the login support by using software authenticators storing the electronic certificate associated with the user's digital identity. To elaborate, let us consider the SPID Poste Italiane eID means. In this scenario, a key pair is generated in the citizens' device (PosteID app) that is protected by a user-selected 8-digit PIN during the setup phase.

Our analysis shows that 25 out of 40 notified eID means, and the Baltic eID scheme under analysis support the LoA High. We report our findings per each eID means within columns 11–15 of Table 2. From the results, we have that:

- 18 eID means under analysis adopt login with a smart card (identity or dedicated) within their solutions;
- 6 eID means under analysis adopt the login with a software authenticator within their solutions;
- 2 eID means under analysis adopt the login with SK within their solutions.

We provide an overview of the authentication mechanisms adopted by MSs for each LoAs in Figure 4.

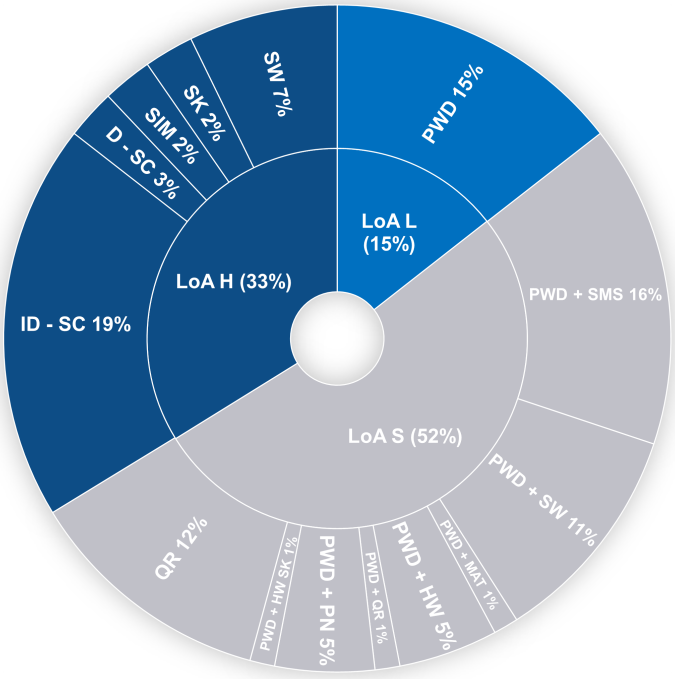

Figure 4. Overview of Authentication Mechanisms based on LoAs adopted by MSs.

Our updated analysis in September 2022 highlights a new technological trend toward using the security keys (e.g., FIDO keys) to satisfy the requirement of LoA H. As we will discuss later in Section 9, using security keys can increase the level of security and usability of the eID scheme.

4. RQ2: Authentication Standards

In this section, we will explore the authentication standards adopted by the notified eID schemes. To reach this goal, we investigate the solutions provided by eID means under analysis and, as a result, we identify the following features:

SSO Protocols: Single Sign-On (SSO) is an authentication method that lets users access multiple applications and services using a single login credential. The adopted SSO standards based on our analysis are the following:

1. **SAML (Security Assertion Markup Language 2.0) [49]:** is among the most widespread standards used to exchange authentication and authorization assertions (in XML formats). SAML requires that the User (called Principal) is registered with an Identity Provider (IdP), which, after receiving a request message from a Service Provider (SP), will respond with an authentication result (called assertion). An assertion contains information that SP uses to evaluate whether to give or deny the Principal access to a particular resource;
2. **OIDC (OpenID Connect) [3]:** is a most recent authentication standard for user authentication that is designed for the same purpose as SAML. In contrast to SAML, which uses heavyweight XML messages, the OIDC uses the lightweight JSON message format. OIDC is an authentication layer developed on top of the OAuth 2.0 standard. It requires that the User (called Resource Owner in the context of OIDC) is registered with an IdP, which after receiving a request message from a relying party (RP in the context of OIDC) will respond with an authentication result (called ID Token). An ID Token is one of the main features that is added by the OIDC and contains information about the authentication process that enables the RP to evaluate whether to give or deny the resource owner access to a particular resource. In addition to the ID Token, the OIDC adds the userInfo endpoint into the OAuth standard as well, which is a protected OAuth Resource Server that releases identity-related claims to RPs (e.g., the email and address). The terms RP in the OIDC and SP in the SAML refer to the same entity. Hereafter, we use the term SP;
3. **FIDO (Fast Identity Online) [50]:** is a protocol that uses standard public key cryptography techniques to provide stronger authentication. During the registration with an SP, the user's device creates a new key pair. It retains the private key and registers the public key with the SP. Authentication is completed by the user's device proving possession of the private key to the SP by signing a challenge. The user's private keys can be used only after they are unlocked locally on the device. The local unlock is accomplished through a user–friendly and secure action, such as swiping a finger, entering a PIN, inserting a second–factor device, or pressing a button.

SP-IdP Federated: indicates whether a federation is required through the registration phase of SP at the IdP to obtain SP-specific credentials and IdP metadata, where federation can be expressed as an agreement between parties that trust each other. The SP-IdP federation applies only in the case of SSO protocols.

Direct Login: indicates whether the eID means under analysis does not use any federation mechanism, meaning that all identification and authentication communication occurs directly between the user and the SP.

We report the main results per each eID means within columns 12–16 of Table 2. According to our investigation, 29 out of 40 notified eID means use at least one authentica-

tion standard (SAML, OIDC, FIDO) to provide an SSO service and 9 eID means use the direct authentication model. From the results, we have that:

- 72% of notified eID means use at least one of the SSO protocols;
- 62% of notified eID means use SAML standard within their solutions;
- German eID means is the only eID means that provides a hybrid solution to support both federated and direct authentication;
- Latvian and Lithuanian eID means are the only solutions under analysis that adopt OAuth 2.0 protocol instead of OIDC for authentication. To the best of our knowledge, the usage of OAuth for authentication can lead to several vulnerabilities [51–53];
- The solution of Baltic countries (SMART-ID) and the Italian CIE/SPID eID schemes published their national OIDC specification [25,54] and they are in the process of implementing the OIDC within their eID schemes;
- The Swedish OIDC working group, in collaboration with Swedish eID means, is working on the definition of the Swedish OIDC profile. This profile is going to be adopted by the notified Swedish eID means [55];
- None of the notified eID means use Mobile Connect as an authentication standard. Mobile Connect [56] is an authentication mechanism based on OIDC, where the federated telco operators perform the user authentication;
- The eID means of Czech Republic (mojeID) and Sweden (EFOS) are the only available solutions that support FIDO [6].

Our updated analysis in September 2022 highlights a new trend related to FIDO: however, in our preliminary analysis in November 2021 [4], none of the considered eID means supports FIDO, in our latest analysis, two eID means (Czech Republic (mojeID) and Sweden (EFOS)) are supporting it, probably because this is an emerging technology [6].

5. RQ3: OpenID Connect Profiles

This section explores the OIDC profiles that the eID schemes have adopted. We spot the following features:

OIDC Core Profile [3]: provides guidelines regarding the core OIDC functionality and how to achieve the baseline security;

OIDC International Government Assurance (iGov) Profile [30]: is based on the OIDC Core and aims to increase baseline security, provide greater interoperability, and structure deployments for public administration and governmental domains;

OIDC Financial Grade API (FAPI) Profile [57,58]: is a highly secured OIDC profile that aims to provide specific implementation guidelines for security and interoperability. This profile can be applied to any market area that requires a higher level of security than the one provided by standard OIDC Core;

OIDC Identity Assurance (IDA) Profile [31]: aims to provide SPs with identity information, i.e., verified claims along with an explicit statement about the verification status of these Claims (what, how, when, according to what rules, using what evidence). It enables use cases requiring strong assurance, like compliance with regulatory requirements such as anti-money laundering laws or access to health data, risk mitigation, or fraud prevention.

We report the main results per each eID means considering only the adopted features by these solutions within columns 2–3 of Table 3. From the results, we have that:

- The Italian CIE and SPID eID means define their national OIDC specification based on the OIDC iGov profile, and they will be the only solutions within the eID means under analysis that follow the OIDC iGov;
- None of the eID means under analysis support either OIDC FAPI [57,58] or OIDC IDA [31] profiles.

Table 3. Analysis results of OIDC-based eID schemes for RQ3 and RQ4.

MS	ID	OIDC Profiles		OIDC Implementation Choices								
				Client authn Method								
		OIDC Core	OIDC iGov	PKCE	ACR Values	sub=pairwise	Client Secret	Client Secret JWT	Private Key JWT	Request	Request uri	Claims
BE	2	Y	-	Y	Y	Y	-	-	Y	Y	-	-
CZ	4	Y	-	-	-	Y	Y	Y	Y	Y	-	Y
DK	6	Y	-	Y *	Y	Y	Y	-	-	Y	-	-
IT	20	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	21	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	22	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	23	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	24	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	25	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	26	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	27	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	28	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
	29	-	Y †	Y †	Y †	Y †	-	-	Y †	Y †	-	Y †
FR	34	Y	-	-	Y	Y	Y	-	-	-	-	-
	35	Y	-	Y	Y	Y	Y	-	Y	-	Y	Y
AT	36	Y	-	Y	-	Y	Y	-	-	-	-	Y
Baltic	41	Y †	-	-	Y †	?	Y †	-	-	?	?	?
Total		**7**	**10**	**13**	**15**	**16**	**6**	**1**	**13**	**13**	**1**	**13**

Legend: "Y": feature supported, "-": feature not supported, "?": the information is not available, "Y *": eID means supports the feature but is not mandated within the implementation, "Y †": feature is under implementation, "OIDC": OpenID Connect", "iGov": International Government Assurance, "PKCE": Proof Key for Code Exchange", "sub": Subject identifier, "authn": Authentication, "JWT": JSON Web Token, Baltic": EE, LV, LT.

6. RQ4: OpenID Connect Implementation Choices

In this section, we investigate the OIDC implementation choices adopted by the eID means under analysis. We identify the following features:

Proof Key for Code Exchange (PKCE) [32]: indicates whether the eID means support PKCE. This extension was created to secure the OIDC implementations against several attacks such as code interception in the OIDC authorization code flow [3]. In simple words, code interception attack refers to scenarios in which the attacker can obtain the authorization code somehow and then sends it to an IdP to exchange it for an Access Token. An attacker may use several available ways to steal the code (Section 4 in OAuth Security BCPs [33]). To mitigate this attack, the PKCE extension introduced three query parameters to provide a way for the SP to prove to the IdP that the authorization code belongs to the SP, namely: (*i*) `code_verifier`, (ii) `code_challenge`, and (iii) `code_challenge_method`. The `code_verifier` is a dynamically created cryptographically random key, which is unique per request. The `code_challenge` is a transformation of the `code_verifier` by using the method that is declared in `code_challenge_method` (e.g., `Plain` or `S256`). Thus, an attacker needs to know the value of the `code_verifier` for the intercepted request to be able to exchange the authorization code for an Access Token, which is not as simple as code interception;

acr_values [3]: indicates whether the eID means under analysis support `acr_values` to define the level of assurance within the authentication context, where `acr_values` enabling SPs to request IdPs strong authentication methods to harden intrusion attempts against users by mandating additional authentication factors;

subject identifier (sub)=pairwise [30]: indicates whether the eID means under analysis adopt the `pairwise` value for the subject identifier, where the subject identifier is an attribute within the IdP for the User. The `sub` claim is returned from the IdP to SP either directly in the ID Token or as a response from the userInfo endpoint;

client authentication method [3]: indicates the client authentication method used by the SP at the IdP token endpoint to authenticate the SP and avoid releasing Access/ID Tokens to a not legitimate SP. This feature can have the following values:

- **client secret** SP uses the `client_secret` received from the IdP during the registration phase to perform the client authentication;
- **client secret JWT** SP creates a JSON Web Token (JWT) using an HMAC SHA algorithm, which uses the `client_secret` issued by the IdP during the registration phase for the HMAC calculation that is used for the client authentication;
- **private key JWT** SP creates a JWT using asymmetric algorithms and signs the JWT with its private key to perform the client authentication;
- **mTLS** [59] SP provides a mechanism for authentication to the IdP using mutual TLS based on either self-signed certificates or public key infrastructure (PKI).

request [3]: indicates whether the eID means under analysis support the `request` OIDC parameter. It provides a way to encapsulate all the authorization request query parameters inside a single object which can be signed and optionally encrypted to provide integrity;

request_uri [3]: indicates whether the eID means under analysis support the `request_uri` OIDC parameter. In the same way as the OIDC `request` parameter, it provides a way to encapsulate all the authorization request query parameters inside a single object which can be signed and optionally encrypted to provide integrity. However,, in the case of `request` parameter, the object is directly included within the authorization request, in the case of `request_uri`, it is retrieved from the defined URL;

Token Binding (DPoP/mTLS) [59,60]: indicates whether the eID means under analysis are using any techniques for binding the issued Access Tokens, such as: Demonstrating Proof of Possession (DPoP) or mutual TLS (mTLS) to avoid the misuse of a stolen Access Token by other SPs. DPoP is a JWT created by the SP and sent with an HTTP request using the DPoP header field to demonstrate to the IdP that the SP holds the private key that was used to sign the DPoP-proof JWT. DPoP enables IdP to bind issued Access Tokens to the corresponding public key. Furthermore, DPoP enables Resource Servers to verify the key-binding of Access Tokens that it receives, which prevents said tokens from being used by any entity that does not have access to the private key. mTLS is an alternative way to reach the same goal by using the application's mutual-TLS certificate. Such a binding is accomplished by associating the certificate with the Access Token in a way that the protected resource can access. One possible way of doing this is to embed the certificate hash in the issued Access Token.

claims [3]: indicates whether the eID means under analysis support the `claims` OIDC parameter, which enables the SP to explicitly request individual claims to be returned in the ID Token and/or userInfo response to satisfy data minimization. The top-level members of `claims` OIDC parameter JSON object are:

- `userInfo`: requests that the listed individual claims be returned from the user-Info endpoint. If present, the listed claims are being requested to be added to any claims that are being requested using the OIDC `scope` parameter. If not

present, the claims being requested from the userInfo endpoint are only those requested using the values defined in the OIDC `scope` parameter;
- ID Token: requests that the listed individual claims be returned in the ID Token. If present, the listed claims are being requested to be added to the default claims in the ID Token. If not present, the default ID Token claims are requested.

We report the main results per each eID means considering only the features implemented by the eID schemes under analysis within columns 4–12 of Table 3. From the results, we have that:

- 76% of eID means support and mandate the usage of the PKCE within their solutions;
- Danish eID means (NemID) is the only solution that optionally supports the PKCE within its solution;
- 88% of the eID means under analysis support the usage of `acr_values` within their OIDC implementations;
- 94% of the eID means under analysis (for which we could find information) use the pairwise subject identifier;
- `private_key_JWT` and the `client_secret` are the two most widely used client authentication methods within eID means;
- None of the eID means support the mTLS client authentication method [59];
- 82% of eID means support either the `request` or `request_uri` OIDC parameters;
- 76% of the eID means under analysis (for which we could find information) support the usage of `claim` parameter within their solutions;
- None of the eID means under analysis support token binding methods based on DPoP [60] or mTLS [59].

As a final remark, in Figure 5, we provide an overview of OIDC profiles and OIDC implementation choices adopted by MSs.

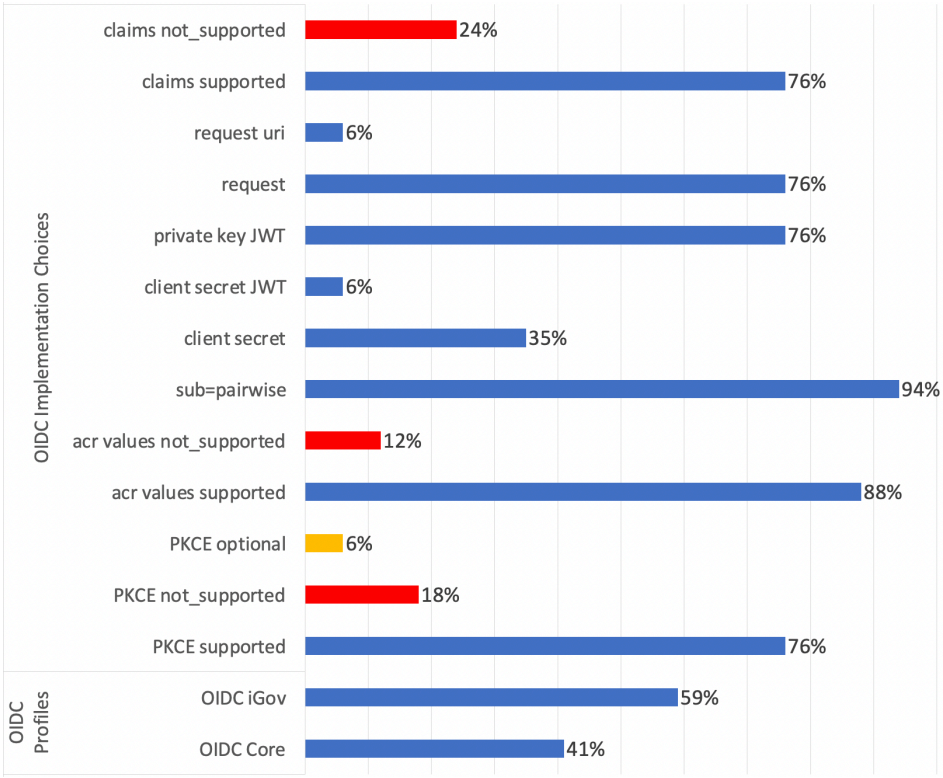

Figure 5. Overview of OIDC profiles and OIDC implementation choices adopted by MSs.

7. RQ5: Mobile-Based Authentication Solutions

This section analyzes the adopted technologies by notified eID schemes to implement authentication solutions based on mobile applications. As a result, we can determine the technological trends concerning the authentication mechanisms based on mobile applications. Given that, we identified the following features based on the analysis of notified eID means:

Mobile app protection: indicates whether the mobile application is protected with a security mechanism, such as biometrics (fingerprint, face recognition), and/or PIN;

Secure storage for mobile apps: in the cases in which the mobile application leverages a cryptographic authenticator, we analyzed the storage location of the user's private key. In our analysis, after the investigation of notified eID means, we identified the following locations:

- Keystore (Key SW): the private key of the user is stored in the user's mobile phone within Keystore;
- SIM (crypt SIM): it is used to store secrets and electronic certificates to be used during authentication processes or, in this case, they embed additional applets than the ones used by network operators, for instance, to have a PKI-based SIM that stores authentication and signature certificates;
- Smart card: the NFC reader or Bluetooth connectivity of the mobile phone is used to interact with the smart card, which stores the private key;
- Security key: the user's private key is stored in the hardware security key (e.g., FIDO security key). During the authentication, the user inserts the security key into the device and provides access to the private key by entering a PIN or using biometrics.

Mobile browser to app to mobile browser (MB2App2MB): it represents the scenario where the user starts the authentication process within the mobile browser. S/he performs the login on the mobile browser and is redirected to an app for 2nd-factor authentication (e.g., using a national eID card). After the user successfully finishes this step, the app will redirect the user to the mobile browser to complete the authentication process and obtain the token to access the services.

Based on our analysis, 18 out of 40 notified eID means, and the eID scheme of Baltic countries (SMART-ID) provide mobile-based solutions for authentication. We report the main results per each eID means within columns 21–26 of Table 2. From the results, we have that:

- 4 eID means that provide card reader mobile applications do not have any mobile app protection mechanism;
- Concerning the secure storage solution used by mobile applications:
  - Estonian Mobiil-ID and Belgian itsme eID means are the only solutions that use cryptographic SIM to secure the PKI keys;
  - 8 eID means use the Mobile NFC or Bluetooth connectivity to read the information from the smart card;
  - 8 eID means for which we could find the information use the SW Keystore to secure the private key within their solutions;
  - None of the eID means for which we could find information uses either Secure Enclave/Element (SE) or Trusted Execution Environment (TEE) to secure the private key; SE would provide CPU hardware-level isolation and memory encryption by isolating application code and data; similarly, TEE would offer a secure area of the main processor, protecting the confidentiality and integrity of the executed data;
  - None of the eID means for which we could find information uses the security key to store the private key within their solutions;

- 10 eID means support the MB2App2MB scenarios.

8. Additional Information

The technical details of the eID means in our analysis are available at our companion website (https://st.fbk.eu/complementary/MDPI2022, accessed on 1 September 2022) for interested readers.

In the following, we would like to share some of our recent observations on the newly introduced eID means by the MSs that either were not available during September 2022 or were recently introduced:

- Denmark announces its new eID mean "MitID" that aims to address the development complexity of "NemID" and unify the two different systems that NemID provides for the public and private sectors. The scheme supports LoAs S and H and provides different authentication mechanisms, such as PWD + SW and PWD + HW. This eID scheme supports both SAML and OIDC authentication standards;
- Poland, Liechtenstein, and Bulgaria eID means—Trusted/personal profile, Li-eID, and Evrotrust eID—completed the peer-reviewed process in the eIDAS framework;
- The Norway eID means (BuypassID, BankID) completed the peer-reviewed process in the eIDAS framework and are in the process of becoming notified eIDAS solution. Both eID means are based on LoA H. Both eID means support the OIDC authentication standard and follow the OIDC Core profile.

9. Lessons Learned

As we mentioned in Section 1, the eIDAS regulation [2,7] does not define the specific technologies to address the reported technical requirements for different levels of assurance. Thus, there are different dimensions that the MSs should consider during the development of their eID schemes, such as security, privacy, and usability. In the following, we summarize our insights based on our eID scheme analysis w.r.t. above-mentioned dimensions.

9.1. Security Considerations

Based on our analysis in Section 3, 90% of eID means under analysis support either LoA substantial and/or high. This implies that these eID means to protect the service by demanding two authentication factors, which makes it difficult for an attacker to use someone else eID means. To provide a general comparison among the various technologies adopted by each eID means per LoA regarding the security level and resistance against different types of attackers, we leverage the MuFASA [61] tool. This tool aims to assist normal users and security experts—during the design phase of Multi-Factor Authentication (MFA) protocols—by providing a high-level report regarding possible risks associated with the specified MFA protocol and its resistance to a set of attacker models. Note that the tool supports a subset of attacker models defined in [8], namely: Device Thief (DT), Authenticator Duplicator (AD), Eavesdropping Software (ES), Shoulder Surfer (SS), Social Engineer (SE), Man in the Browser (MB), and Man in the Mobile (MM). The interested reader can refer to the NIST specification [8] and MuFASA document for the definition of the attacker models. In the following, we highlight some of the interesting findings by analyzing the eID means using MuFASA (Interested readers can refer to our companion website for checking the reports generated by MuFASA, regarding the security analysis of the solution).

- All the eID means, independently of their adopted authentication factors, are not resistant against the (extremely powerful) MB attacker model;
- 12 eID means use PWD, which is the least secure authenticator and exposes these solutions to ES, SE, MB, and SS attacker models. However, it is worth mentioning that all the 12 eID means offer an additional authentication mechanism that provides a higher LoA, which can be used when necessary;

- Concerning the eID means with LoA S, the eID means that are using PWD + QR (1 eID mean) and/or PWD + PN (4 eID means) are more secure in comparison with the eID means that are using other authenticator types for LoA S (reported in Table 2). The main reasons are: (i) the number of successful attackers with higher risk is less than the other methods, and (ii) these methods are not susceptible to the ES attacker model, while this is not the case for the other available authenticator types for LoA S;
- Concerning the eID means with LoA S that are using PWD + SW and/or PWD + HW (13 eID means), the security of their solution can increase according to the features of the OTP generation provided by the SW/HW. In the case that the generation of OTP output is uniquely associated with the ongoing operation—dynamic linking [62]—the solution would be more secure in comparison to the one that does not consider dynamic linking. The main reason for the improvement of the security is related to the fact that: (i) the generated OTP is unique for that specific operation, and (ii) at the time of the operation, the identity of the demandant is displayed to the user and the user has to explicitly agree on the ongoing operation to generate the OTP;
- Concerning the eID means with LoA S that are adopting QR as an authenticator (10 eID means), the mobile app protection mechanism can affect the security level of the solution. Based on the results of our analysis using MuFASA, the usage of the fingerprint can improve the security w.r.t. the usage of PIN.

In the following, we provide specific security considerations for the eID means using QR and/or PWD + SMS within their solutions.

The QR authentication factor must be used with caution as this method is vulnerable to phishing attacks, as explained by the authors in [63,64]. It is worth mentioning that some measures can be considered by the eID means to reduce such kinds of attack, namely [54]: (i) the eID means app can show the origin of the request (e.g., the domain where the response will be sent) and/or ask the user to confirm this origin. In an attack, this origin would be different from the attacker's origin, where the QR code is displayed to the user; (ii) the authentication request can be made short-lived. An attacker would have to request a new authentication request (e.g., QR code) frequently and update it on its website as well; (iii) the eID means app can warn the user when logging in at a new application for the first time; (iv) the eID app can create user-specific QR codes that the attacker cannot generate; and (v) the eID means may demand the user to provide an additional authentication factor after the usage of QR code.

Concerning the solutions that are using PWD + SMS, we would like to elaborate on some security considerations in their case. The OTP sent through SMS is susceptible to various kinds of attacks, such as SS7 vulnerabilities, malware attacks on smartphones, and SIM swapping [65,66]. This is the main reason why both NIST and PCI-CSS [8,67] deprecate the use of SMS. However, this solution is still the most often used implementation within MSs eID means (13 eID means). We identify the following two reasons for this choice. First, SMS is easy to integrate into user experiences based on the use of smartphones. Second, SMS can easily support scenarios where the user has a mobile phone that is not a smartphone with internet connectivity.

As a final remark, we would like to highlight some security considerations specific to the implementation choices of solutions based on OIDC. Most of the solutions under analysis are secure against code interception/replay attacks [32,52] due to the adoption of PKCE. Furthermore, most of the solutions are adopting the usage of `request` or `request_uri` OIDC parameter and the `private_key_jwt` client authentication methods. These parameters can play an essential role in the security improvement of the solutions. The former provides a way to encapsulate the authorization query parameters in a single object to avoid tampering and provide message integrity. The latter provides a higher level of protection in comparison with symmetric methods (e.g., `client_secret`) as reported in [33] due to the lack of demand for storing secret keys at the authorization servers.

9.2. Privacy Considerations

As we mentioned in the Introduction (Section 1), the Regulation 1501/2015 [7] defines only data minimization (minimal set of personal user data claims that each eID scheme shall release to online service) as a privacy requirement within the eIDAS framework. This would be the main reason why only two eID schemes (Gov.UK Verify, and German eID) consider additional privacy considerations within their solution's design even though there exist proposals for some authentication standards (e.g., SAML profiles [49]) to provide a privacy-preserving solution. The Gov.UK Verify eID scheme uses an intermediary HUB to prevent the eID scheme provider from knowing which application the user is using and hence exploiting this information for commercial gain, and the same goes for the application side. In the case of Germany, the key privacy enabler is supporting pseudonym transactions, which issues a unique user identifier for every application, thereby avoiding colluding applications to breach privacy by linking the transaction histories of any given users.

In the following sections, we first elaborate on the implementation choices that should be considered during the development of all eID schemes to preserve privacy. After that, we provide the specific considerations for the eID schemes that are based on the OIDC.

9.2.1. General Considerations

In the following, we highlight how the "Accountability" and "Federated or Direct Login" implementation choices can affect privacy level of the eID schemes.

- **Accountability**: in some use cases, the service providers may need additional information to precisely identify users to provide access to their resources. Thus, based on the form of identifier (e.g., pseudonymized identity) that is considered in the eID schemes, there could be greater accountability or privacy;
- **Federated or Direct login**: Federated solution means a centralized system exists to handle the identification and authentication. While it can simplify the management of authentication for the service providers, it will come with the cost of user tracking across the system if no other measures against that are in place. In the case of direct login, there is not a single entity that can know about a user's authentication actions. Thus, in this way, it can increase the user's privacy by preventing an entity from learning about all the user's activity across different service providers. However, this comes with the cost of handling the authentication and all the relevant overhead that comes with it on service providers. Furthermore, it has the problem of interoperability issues with the other eID schemes. Regarding interoperability, the eIDAS framework implements a proxy to solve the problem, with the cost of creating a federation at the eIDAS level [27].

9.2.2. OIDC-Based Considerations

This section highlights the implementation choices that should be considered within the implementation of OIDC-based eID schemes to provide "Data Minimization" and "Unlinkability".

- **Data Minimization**: it means asking only for the required claims. Indeed, OIDC Core recommends minimizing the amount of information requested from the user. This is possible by the usage of the OIDC "`Claim`" parameter that returns the information explicitly declared using this parameter;
- **Unlinkability**: is to prevent users from being identified across different SPs. In the context of OIDC solutions, the users can be identified by SPs through the usage of subject identifier (`sub`) in the ID Token. Using the pairwise value for the subject type can help to protect the users against tracking by SPs as it will assign different values to the same user across different SPs. Thus, it can avoid user tracking across SPs.

In the light of the GDPR, privacy is turning into a hot topic, and that is the main reason why the European Commission is trying to address the major privacy shortcoming

of eIDAS in the revised eIDAS framework (eIDAS 2.0 [5]) by promoting the transition from federated to decentralized solutions that aim to give back the control of data to the user. Section 10 provides a brief overview of the eIDAS 2.0 regulations.

9.3. Usability

The usability of the eID schemes is another important factor that must be considered during the implementation of the eID means. In particular, it is essential to provide a balance between security and usability concerning access to various service providers. Based on our analysis, some of the eID schemes (e.g., Italian SPID) make various authenticators available to users. Indeed, it lets the user choose a method they trust and are comfortable with. This is beneficial to the user experience and, at the same time, enables the different level of security that is needed to access various services on the service providers. However, our analysis reveals that some eID schemes (e.g., Spain) do not provide various authenticators, and the user is forced to use the only authenticator available in the eID scheme. Although it might be good from a security perspective, it does not provide the best user experience for the user.

In light of the security and usability considerations described above, Figure 6 provides a pictorial overview of the relation between security and usability of the various authenticators used within eID means under analysis. While being qualitative, Figure 6 shows the important trade-off between ease of use and security level associated with each authentication mechanism.

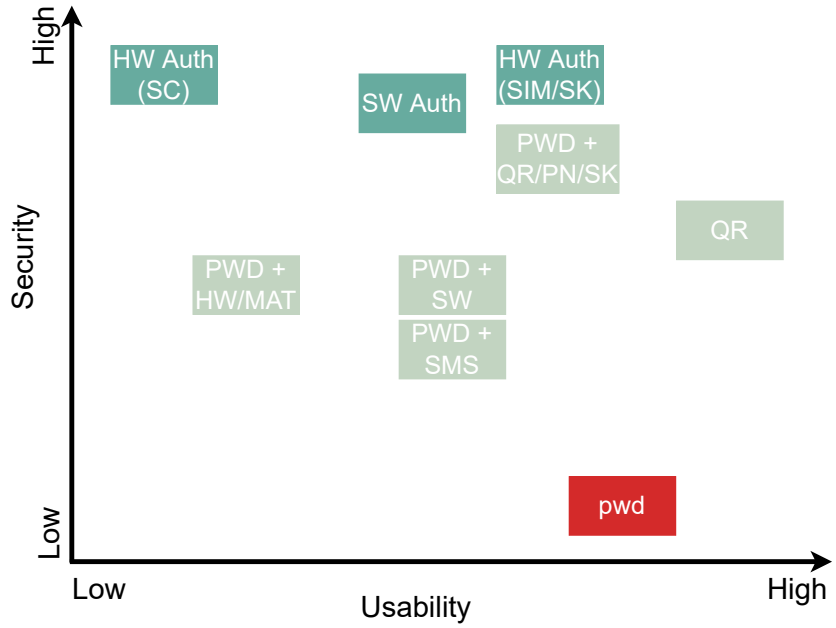

Figure 6. Authenticators' security vs. usability trade-off.

10. eIDAS 2.0 Regulation

The digital identity landscape has evolved through time, beginning with the most basic model (Centralized identities) and progressing through several stages as additional models are introduced. These methods, as illustrated in Figure 7, are briefly explained in the following:

Centralized identities: Entities such as administrators manage centralized identities at the system level (e.g., active directory). As a result, the user's identity is determined by these entities and can only be deleted through them. Reliance on a centralized entity frequently leads to a lack of interoperability. The main reason is due to the fact that the user's identity cannot be transferred without further ado, and it must be recreated for another service provider;

Federated identities: aims to break down the hierarchies based on a single authority by providing a central-login solution (IdP) to enable the users to share their identities with different SPs using only one registered credential at the IdP. This solution can solve the problem of password fatigue by providing a Single Sign-On experience and interoperability, but, still, the problem of tracking users across multiple SPs remains unsolved. Indeed, it is possible for the IdP to aggregate information from numerous SPs to generate user profiles, which might cause several privacy issues [68];

Self-sovereign identities: is the next and most recent stage of digital identity management that aims to solve the privacy issues in the previous models by giving the users back control of their own data. The main idea is to shift the control from the centers of the network to the edge of the network to enable direct interaction [69].

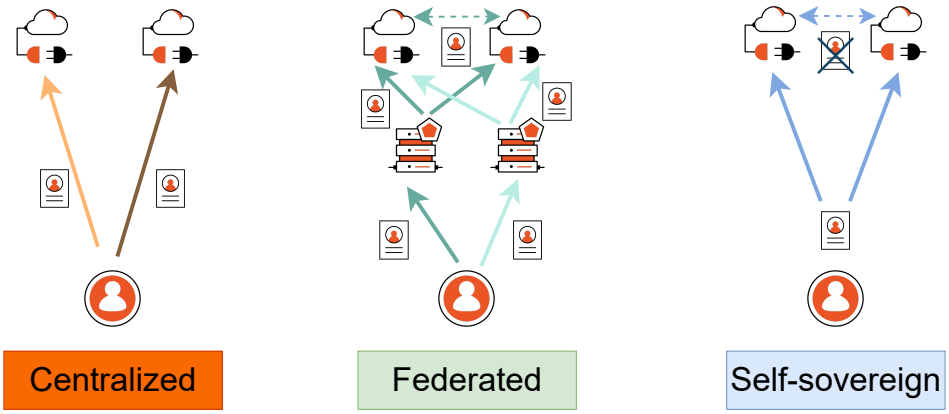

Figure 7. Comparison of different identity management systems.

At the European level, a concrete effort to provide a European interoperable solution started in 2014 by publishing eIDAS 910/2014 [1] based on a federated identities model. However, as we mentioned earlier, major privacy shortcomings exist within the eIDAS 910/2014 regulation, which is the main reason why the revised eIDAS framework (eIDAS 2.0) promotes the transition from a federated to a self-sovereign identity model. The eIDAS 2.0 amendment proposal [5], published in June 2021, aims to:

- Provide a highly secure and trustworthy electronic identity solution that enables the user to share only the minimum set of identity data needed by the SP to provide the service requested by the user;
- Introduce a so-called "European Digital Identity Wallet (EUDIW)," which may be provided by public authorities or by private entities recognized by MSs and link a citizen's national digital identity to other personal attributes (e.g., driving license or bank account);
- Enhance privacy by decoupling credential issuance from its presentation to SPs; This can blind the IdP from the SP the user interacts with and vice versa.

The eIDAS 2.0 proposal defines the EUDIW as "a product and service that allows users to store identity data, credentials and attributes linked to their identity, to provide them to SPs on request and to use them for authentication, online and offline, and to create qualified electronic signatures and seals." Based on the eIDAS 2.0 proposal, the EUDIW plays the role of an eID means to receive, store and share Personal Identification Data (PID), (Qualified) Electronic Attestation of Attributes (Q)EAA, and any other personal data.

The European Commission road map for the adoption of the eIDAS 2.0 regulation is presented in Figure 8. To provide a set of common standards, technical specifications, and best practices to serve as a basis for an interoperable, secure, and privacy-preserving implementation of EUDIW, the EU Commission published a first draft of the "Architecture and Reference Framework (ARF)" in [70]. The ARF provides a set of functional and non-functional requirements that, by the time of writing this work, are quite abstract, and it

does not provide any insights regarding how to satisfy the requirements. To elaborate on this point, let us consider the following example. The ARF document states "Secure access to locally or externally stored cryptographic functions will be necessary to implement most of the functionalities of the EUDIW (e.g., qualified electronic signature, authentication, selective disclosure). In the case of externally stored cryptographic functions, the wallet shall provide a minimum set of local cryptographic functions that enable secure access to them. Overall cryptographic methods and functions shall fulfill existing and upcoming requirements originating in standards, implementing acts and certifications based on these." However, what would be beneficial is to provide some insights regarding the technical aspects that should be considered to implement this functionality in a secure way. In the following, we highlight some challenges derived from the ARF and eIDAS 2.0 proposal [5,70], which are important to be considered in the EUDIW implementation to avoid possible failure as it has happened for the German digital driver's license and the ID Wallet app [71].

- **Persistent and unique identifier:** Article 11a of eIDAS 2.0 regulation states that the minimum data set of user identification data shall contain a unique and persistent identifier for all European citizens and residents. This parameter should design carefully as it can create additional privacy risks and allows online services to track the user's activity. A more privacy-friendly approach would be adopting a service-specific pairwise identifier model or pseudonymization;
- **Standards and technology immaturity:** To support the implementation of different functionality requirements of EUDIW, new standards and technologies are needed. There are different working groups, such as Decentralize Identity Foundation (DIF) (https://identity.foundation, accessed on 1 November 2022), OpenID Foundation (OIDF) (https://openid.net, accessed on 1 November 2022), World Wide Web Consortium (W3C) (https://www.w3.org/Consortium/, accessed on 1 November 2022), and ISO 18013-5 [72] to name a few of them, which are working on this dimension to provide the basic building blocks to build the EUDIW on top of it. However, most of these standards are in their early stages;
- **Interoperability:** It is worth mentioning that the current eID schemes that are operating within the MSs will continue to operate for quite some time after the final release of EUDIW. This can lead to potential challenges for SPs that are supporting several eIDs, including the EUDIW, for their services. A possible solution to this issue would be using an identity gateway (a.k.a broker) between the EUDIW and/or governmental eID means and the SPs. However, it is important to design the identity gateway based on privacy-by-design principles to prevent the identity gateway from profiling the user's online activity. A potential solution can be the adoption of a blind broker architecture model [73].

As a final remark, it is worth mentioning that, while in the case of eIDAS regulation [1] the notification process of eID means was not necessary, this has been changed in the eIDAS 2.0 regulation [5], and all MSs must notify at least one eID means. The European Commission road map for the adoption of the eIDAS 2.0 regulation is presented in Figure 8.

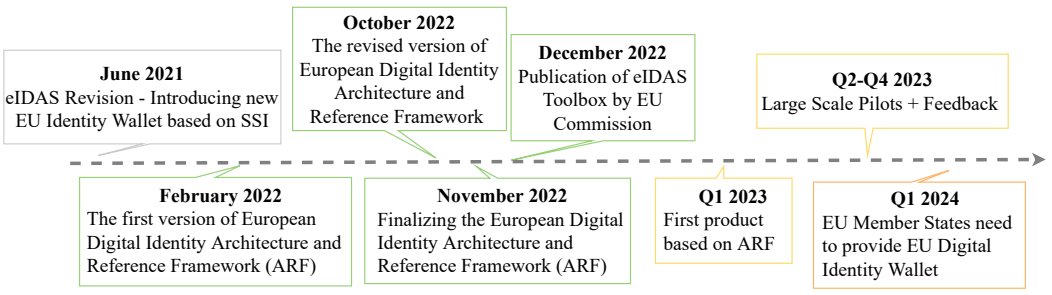

Figure 8. Timeline of new eIDAS 2.0 regulation adoption by MSs.

11. Conclusions

This paper considers the technological trends of notified eIDAS electronic identity schemes used by Member States. We do this by defining a set of research questions that allow us to investigate the correlations between different design dimensions, such as security, privacy, and usability. Based on these findings, we provide a set of lessons learned that the security community can use to protect interoperable national digital identities more efficiently. Furthermore, we provide a brief overview of the new transition from a federated to a decentralized model due to the release of a revision on the eIDAS regulation—eIDAS 2.0—which aims to address one of the main shortcomings of the previous eIDAS regulation concerning user's privacy. Furthermore, we highlight some of the important challenges to consider for the EUDIW implementation. These challenges can provide various interesting research directions. In the case of standards, they need in depth security and privacy analysis that are missing by the time of writing this paper to check if they are satisfying the security and privacy principles. In the case of new technologies, zero-knowledge proofs gain a lots of attraction to satisfy the data minimization requirement of EUDIW by providing the selective disclosure mechanism. While the zero-knowledge proof approach has the potential to significantly improve the protection of personal data in the context of EUDIW, it must be carefully assessed how reliable it is and for which use cases it could be applied. It is worth mentioning that the zero-knowledge proof is not the only option to provide the selective disclosure mechanism and there are other available methods such as atomic credentials and hashed values as defined in [74]. In future work, we plan to (i) investigate the state of the art of European digital identity wallet solutions, to have an overview of their requirements (e.g., storing and sharing of identity data), the technologies used within their implementations (e.g., protocols used for sharing identity data between the wallet and SP), and how the adopted technologies satisfy the identified requirements introduced by the eIDAS 2.0 [5], and (ii) investigate different cryptographic mechanism for selective disclosure to provide an overall comparison between them based on their capabilities and performance, such as: cryptographic agility, proof size, offline usage, and presentation unlinkability.

Author Contributions: A.S.: Methodology, Investigation, Writing—original draft, Writing—review and editing. M.R.: Methodology, Investigation, resources. R.C.: Supervision, Methodology, Writing—review and editing, Validation. G.S.: Supervision, Methodology, Writing—review and editing, Validation. F.A.M.: Methodology, Writing—review and editing, resources. S.R.: Supervision, Conceptualization, Methodology, Writing— review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Data is contained within the article or supplementary material

Acknowledgments: This work has been partially supported by "Futuro & Conoscenza Srl", jointly created by the FBK and the Italian National Mint and Printing House (IPZS), Italy.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. eIDAS Identified Requirements per Assurance Level

Table A1 provides a set of identified requirements per each assurance level as mention in Regulation 1501/2015 [2] to enable citizens to confirm their identity using their owned eID means.

Table A1. Regulation 1501/2015 [2] Requirement per each LoA.

Assurance Level	Elements Needed
Low	The authentication mechanism should implement security mechanisms for the verification of eID means in a way that the authentication mechanism is resistant against guessing, eavesdropping, replay, or manipulation of communication by an attacker with enhanced-basic attack potential.
Substantial	The authentication mechanism should implement security mechanisms for the verification of eID means in a way that the authentication mechanism is resistant against guessing, eavesdropping, replay, or manipulation of communication by an attacker with moderate attack potential.
High	The authentication mechanism should implement security mechanisms for the verification of eID means in a way that the authentication mechanism is resistant against guessing, eavesdropping, replay, or manipulation of communication by an attacker with High attack potential.

References

1. Union, E. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. *Off. J. Eur. Union L* **2014**, *257* .
2. Union, E. Council regulation (EU) no 1502/2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to article 8(3) of regulation (eu) no 910/2014 of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market. *Off. J. Eur. Union L* **2015**.
3. Sakimura, N.; Bradley, J.; Jones, M.; De Medeiros, B.; Mortimore, C. *OpenID Connect Core 1.0 Incorporating Errata Set 1. Specification*; The OpenID Foundation: New York, NY, USA, 2014, Volume 335.
4. Sharif, A.; Ranzi, M.; Carbone, R.; Sciarretta, G.; Ranise, S. SoK: A Survey on Technological Trends for (pre) Notified eIDAS Electronic Identity Schemes. In Proceedings of the the 17th International Conference on Availability, Reliability and Security, Benevento, Italy, 29 August–1 September 2022; pp. 1–10.
5. Union, E. Regulation of the European Parliament and of The Council Amending Regulation (Eu) No 910/2014 as Regards Establishing a Framework for a European Digital Identity. *Off. J. Eur. Union L* **2021**.
6. EuropeanCommission. Overview of Pre-notified and Notified eID Schemes under eIDAS. 2022. Available online: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (accessed on 1 September 2022).
7. Union, E. Council regulation (EU) no 1501/2015 on the interoperability framework pursuant to article 12(8) of regulation (eu) no 910/2014 of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market. *Off. J. Eur. Union L* **2015**.
8. Grassi, P.A.; Garcia, M.E.; Fenton, J.L. Digital Identity Guidelines. *NIST Spec. Publ.* **2017**, *800*, 63–3.
9. BelgianeID. Belgium eID card. 2022. Available online: https://www.ibz.rrn.fgov.be/fr/documents-didentite/eid/(accessed on 1 November 2021).
10. BelgianMobileID. Itsme Developer Documentation-Authentication Service Documentation. 2022. Available online: https://belgianmobileid.github.io/slate/login.html (accessed on 1 November 2021).
11. CzechGovernment. Czech Republic eCitizen. 2019. Available online: https://info.identitaobcana.cz/eop/, (accessed on 1 November 2021).
12. CZNIC. MojeID Solution. 2022. Available online: https://www.mojeid.cz/en/egovernment/ (accessed on 1 September 2022).
13. NemID. NemID eID Solution. 2019. Available online: https://www.nemid.nu/dk-en/get_started/index.html (accessed on 1 November 2021).
14. BSI. German eID-Overview of the German eID System. 2017. Available online: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf?__blob=publicationFile&v=1 (accessed on 1 November 2021).

15. LithuanianGov. Lithuania Identity Card and Electronic Signature. 2019. https://www.nsc.vrm.lt/ (accessed on 1 November 2021).
16. AMA. Authentication.gov-Authentication Provider of the Portuguese Public Administrator. 2021. Available online: https://www.autenticacao.gov.pt/documentos (accessed on 1 November 2021).
17. SlovacianGovernment. Slovakia eID card. 2019. Available online: https://www.slovensko.sk/sk/eid/_eid-karta/ (accessed on 1 November 2021).
18. eHerkening. Eherkenning Overview. 2019. Available online: https://www.eherkenning.nl/leveranciersoverzicht (accessed on 1 November 2021).
19. Whitley, E.A. *Trusted Digital Identity Provision: GOV. UK Verify's Federated Approach*; Minister of UK: London, UK, 2018.
20. FranceConnect. Franceconnect Documentation. 2021. Available online: https://api.gouv.fr/les-api/franceconnect (accessed on 1 November 2021).
21. A-SIT. Austria ID Solution. 2021. Available online: https://www.a-sit.at/ (accessed on 1 Septmeber 2022).
22. BankID. BankID Solution. 2022. Available online: https://www.bankid.com/en/utvecklare/guider/teknisk-integrationsguide/rp-introduktion (accessed on 1 September 2022).
23. FrejaID. FrejaID Solution. 2022. Available online: https://frejaeid.com/en/home/ (accessed on 1 November 2022).
24. EFOSID. EFOSID Solution. 2022. Available online: https://www.forsakringskassan.se/myndigheter-och-samarbetspartner/e-tjanster-for-myndigheter-och-samarbetspartner/e-identitet-for-offentlig-sektor-efos/allman-information-om-efos (accessed on 1 September 2022).
25. SmartID. Smart ID Solution. 2021. Available online: https://www.smart-id.com/about-smart-id/ (accessed on 1 November 2021).
26. ENISA. eIDAS Compliant eID Solutions: Security Considerations and the Role of ENISA. 2020. Available online: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions/view/++widget++form.widgets.fullReport/@@download/ENISA+Report+-+eIDAS+Compliant+eID+Solution.pdf (accessed on 1 November 2021).
27. Roelofs, F.; Verheul, E.; Jacobs, B. *Analysis and Comparison of Identification and Authentication Systems under the eIDAS Regulation*; European Commission: Brussels, Belgium, 2019.
28. FutureTrust. Overview of eID Services. 2017. Available online: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b52e19d7&appId=PPGMS (accessed on 1 November 2021).
29. Commission, E. Overview of Member States' eID strategies v3.0. 2021. Available online: https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/364643428/eID_Strategies_v4.0.pdf (accessed on 1 November 2021).
30. Internet-Draft. *International Government Assurance Profile (iGov) for OpenID Connect 1.0*; Minister of UK: London, UK, 2018.
31. Lodderstedt, T.; Fett, D. OpenID Connect for Identity Assurance 1.0. *The OpenID Foundation, Specification*; New York, NY, USA, 2022.
32. Sakimura, N.; Bradley, J.; Agarwal, N. Proof Key for Code Exchange by OAuth Public Clients (RFC7636). *Internet Eng. Task Force (IETF)* **2015**.
33. Lodderstedt, T.; Bradley, J.; Labunets, A.; Fett, D. OAuth 2.0 Security Best Current Practice (draft-ietf-oauth-security-topics-21). *Internet Eng. Task Force (IETF)* **2022**.
34. CzechGovernment. eGovernment Mobile Key. 2022. Available online: https://info.identitaobcana.cz/mep/, (accessed on 1 September 2022).
35. EstonianGovernment. Estonian Digital ID (Digi-ID). 2018. Available online: https://www.politsei.ee/en/instructions/digital-id (accessed on 1 November 2021).
36. EstonianGovernment. Mobiil-ID. 2018. Available online: https://www.politsei.ee/en/instructions/mobile-id (accessed on 1 November 2021).
37. CroatianGovernment. Croatian Electronic Identity Card. 2018. Available online: https://www.eid.hr (accessed on 1 November 2021).
38. LatvianGovernment. Latvian Electronic Identity Card. 2019. Available online: https://www.pmlp.gov.lv/lv/jaunums/eid-karte-erts-un-dross-personu-apliecinoss-dokuments (accessed on 1 November 2021).
39. LVRTC. eParaksts. 2019. Available online: https://www.eparaksts.lv/en/ (accessed on 1 November 2021).
40. LuxGov. The Luxembourg Electronic Identity Card. 2019. Available online: https://ctie.gouvernement.lu/en/dossiers/eID/eID.html (accessed on 1 November 2021).
41. AMA. Chave Móvel Digital. 2021. Available online: https://www.ama.gov.pt/web/english/digital-mobile-key (accessed on 1 November 2021).
42. ItalianGovernment. Italian eID Card. 2019. Available online: https://www.cartaidentita.interno.gov.it/en/citizens/cie-id/ (accessed on 1 November 2021).
43. AGID. Public Digital Identity System (SPID). 2018. Available online: https://www.spid.gov.it (accessed on 1 November 2021).
44. DutchGovernment. DigiD eID Scheme. 2020. Available online: https://www.eherkenning.nl/leveranciersoverzicht (accessed on 1 November 2021).
45. DigIdentity. Digidentity 2018. Available online: https://www.digidentity.eu/en/govuk-verify/#how-it-works (accessed on 1 November 2021).

46. MaltaGovernment. Maltese eID Card and E-Residence Documents. 2021. Available online: https://www.identitymalta.com/unit/e-id-cards-unit/ (accessed on 1 November 2021).
47. ISO/IEC. Information Technology—Security Techniques—Entity Authentication Assurance Framework. 2013. Available online: https://www.iso.org/standard/45138.html (accessed on 1 November 2021).
48. FIDO. Certified Authenticator Levels. 2021. Available online: https://fidoalliance.org/certification/authenticator-certification-levels/ (accessed on 1 November 2021).
49. Cantor, S. SAML Version 2.0 Errata 05. *Retriev. March* **2012**, *18*, 2015.
50. Alliance, F. Specifications overview **2016**. https://fidoalliance.org/specifications/overview (accessed on 1 November 2021).
51. Chen, E.Y.; Pei, Y.; Chen, S.; Tian, Y.; Kotcher, R.; Tague, P. Oauth demystified for mobile application developers. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 892–903.
52. Sharif, A.; Carbone, R.; Sciarretta, G.; Ranise, S. Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients. *J. Inf. Secur. Appl.* **2022**, *65*, 103097.
53. Sharif, A.; Carbone, R.; Ranise, S.; Sciarretta, G. A wizard-based approach for secure code generation of single sign-on and access delegation solutions for mobile native apps. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications-SECRYPT, Prague, Czech Republic, 26–28 July 2019; Volume 2, pp. 268–275.
54. Yasuda, K.; Jones, M. Self-Issued OpenID Provider v2. 2022. Available online: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html (accessed on 1 September 2022).
55. OIDCSweden. Sweden OIDC Working Group. 2021. Available online: https://github.com/oidc-sweden/specifications (accessed on 1 September 2022).
56. GSMA. Mobile Connect Universal Log-in Profile. 2021. Available online: https://mobileconnect.io/specifications/ (accessed on 1 November 2021).
57. Sakimura, N.; Bradley, J.; Jay, E. Financial-grade API - Part 1: Baseline. *Internet Eng. Task Force (IETF)* **2021**.
58. Sakimura, N.; Bradley, J.; Jay, E. Financial-grade API - Part 2: Advanced. *Internet Eng. Task Force (IETF)* **2021**.
59. Campbell, B.; Bradley, J.; Sakimura, N.; Lodderstedt, T. OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens (RFC8705). *Internet Eng. Task Force (IETF)* **2020**.
60. Fett, D.; Campbell, B.; Lodderstedt, T.; Jones, M.; Waite, D. OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP) (draft-11). *Internet Eng. Task Force (IETF)* **2022**.
61. Sinigaglia, F.; Carbone, R.; Costa, G.; Ranise, S. Mufasa: A tool for high-level specification and analysis of multi-factor authentication protocols. In *Proceedings of the International Workshop on Emerging Technologies for Authorization and Authentication*; Springer: Berlin, Germany, 2019; pp. 138–155.
62. European Commission. European Banking Authority: Directive 2015/2366 of the European Parliament and of the Council on Payment Services in the Internal Market (PSD2) 2015. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&qid=1653045761540&from=EN (accessed on 1 November 2021).
63. Yong, K.S.; Chiew, K.L.; Tan, C.L. A survey of the QR code phishing: the current attacks and countermeasures. In *Proceedings of the IEEE 2019 7th International Conference on Smart Computing & Communications (ICSCC)*; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.
64. OWASP. QRLJacking-A New Social Engineering Attack Vector. 2020. Available online: https://github.com/OWASP/QRLJacking (accessed on 1 November 2021).
65. Fox-Brewster, T. Watch as hackers hijack whatsapp accounts via critical telecoms flaws. *Forbes*, 1 June 2016.
66. Lee, K.; Kaiser, B.; Mayer, J.; Narayanan, A. An Empirical Study of Wireless Carrier Authentication for SIM Swaps. In Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), Boston, MA, USA, 10–11 August 2020; pp. 61–79.
67. standards council, S. Information Supplement-Multi- Factor Authentication. 2017. Available online: https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf (accessed on).
68. Ehrlich, T.; Richter, D.; Meisel, M.; Anke, J. Self-sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Prax. Wirtsch.* **2021**, *58*, 247–270.
69. Kubach, M.; Schunck, C.H.; Sellung, R.; Roßnagel, H. Self-sovereign and Decentralized identity as the future of identity management? In *Open Identity Summit 2020*; Springer: Berlin, Germany, 2020.
70. EuropeanCommission. European Digital Identity Architecture and Reference Framework– Outline. 2022. Available online: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline (accessed on 1 September 2022).
71. Zeit. Digitale Führerschein-App defekt. 2021. Available online: https://www.zeit.de/mobilitaet/2021-09/verkehrsministerium-digitaler-fuehrerschein-app-defekt-andreas-scheuer (accessed on 1 November 2021).
72. ISO. Personal Identification—ISO-Compliant Driving Licence—Part 5: Mobile Driving Licence (mDL) Application. 2021. Available online: https://www.iso.org/standard/69084.html (accessed on 1 September 2022).
73. Boysen, A. Decentralized, self-sovereign, consortium: The future of digital identity in canada. *Front. Blockchain* **2021**.
74. Sporny, M.; Longley, D.; Chadwick, D.; Terbu, O.; Zagidulin, D.; Zundel, B. Verifiable Credentials Implementation Guidelines 1.0. 2022. Available online: https://w3c.github.io/vc-imp-guide/ (accessed on 1 September 2021).