Comparing privacy properties and technical measures of eID systems

Research paper

Daniel Ostkamp[1 [0000−0003−0665−5369]] and Erik Poll[1 [0000−0003−4635−187X]]

Radboud University, Nijmegen, the Netherlands
dostkamp@science.ru.nl, erikpoll@cs.ru.nl

Abstract. We compare five eID systems with regard to privacy, incl. the national eID systems of Belgium, Germany, Estonia and the Netherlands. For our analysis, we identify 11 privacy properties.
Our analysis required precise and detailed descriptions of each of the systems. Obtaining these was far from trivial: the descriptions of the systems that we could find were very different in style and did not always provide the necessary detail. We can show many differences between the systems: no system satisfies all properties, and two systems only very few. We also note that systems can use different technical measures to achieve the same privacy property.
Likewise, we assess how the European Digital Identity (EUDI) regulation and accompanying documents propose to protect the privacy of EU citizens. While most of our defined privacy properties must be ensured in EUDI-compliant systems, some are not fully mandated. We recommend that the European Commission adds a section to the "Architecture and Reference Framework" document outlining privacy properties along with technical measures.

Keywords: Electronic Identification · Authentication · Privacy Protection · European Digital Identity

1 Introduction

European citizens increasingly use *electronic identification* (eID) to authenticate to online public services. For instance, in the Netherlands citizens can use the DigiD app to authenticate if they file in their annual tax returns online. Furthermore, foreign nationals can use their national recognized eID system to authenticate to the tax return system. This is thanks to the *electronic IDentification, Authentication and trust Services* (eIDAS) [1] regulation that mandates that one member state must accept eID systems from another member state if the eID system is registered within the EU. For instance, Germans living in the Netherlands could use their eID *neuer Personalausweis* (nPA) to authenticate to the Dutch tax office.

Obviously eID systems employed in the EU have to comply with the *General Data Protection Regulation* (GDPR) [2]. As the name suggests, the GDPR is

a *general* regulation, so it does not contain any sector-specific privacy protection measures. The GDPR does require organizations to implement "appropriate technical and organizational measures" to protect privacy (recital 78 of GDPR) but leaves it open what these are.

To identify such measures for eID systems, we compare five eID systems used in the EU in section 4. We chose systems that make use of an eID app on a mobile device as using mobile apps for authentication is becoming the norm. We analyzed in a harmonized way in appendix A how the selected systems work and process personal data as this is a prerequisite to understand how a system protects privacy. In the comparison we make a distinction between (i) privacy *properties* that state *what* guarantees w.r.t. privacy are made and (ii) the *measures* used to achieve these – i.e. the how rather than the what — those technical measures are *privacy enhancing technologies*. In the end we identify 11 privacy properties (see(section 3). Based on the analysis, we provide recommendations to improve privacy for future eID systems.

In 2021 the EU published a first proposal of the *European Digital Identity* (EUDI) [3] (aka eIDAS 2.0) to amend the eIDAS 1.0 regulation — in the meantime the EU accepted a 1.0.0 version. The regulation itself mentions several times the intent to protect citizen's data. While the regulation itself does not provide details, the accompanying *Architecture and Reference Framework* (ARF) and related implementation acts and annexes do. In section 7 we analyze privacy protection of EUDI based on our privacy properties, and discuss contribute to the public discussion. As the EUDI is a sector-specific regulation for eID, it would be the natural place to provide more guidance on what "appropriate technical and organizational measures" w.r.t. privacy are for eID systems.

Our contributions can be summarized as follows:

- We identify and define 11 privacy properties to determine the level of privacy protection in eID systems (section 3).
- We provide a detailed description of five European eID systems in the same format in appendix A. We found that descriptions of each system vary a lot and the necessary information was sometimes hard to find. The format we used for our descriptions could be used as a template to provide similar descriptions for other systems to complement our analysis.
- We compare five European eID systems based on the privacy properties. In doing so we identify technical measures to achieve them (section 4).
- We provide recommendations to eID system providers based on our observations in section 5.
- We summarize previous work analyzing privacy within eID systems in section 6.
- Finally, we compare the management of privacy protection in the EUDI framework and its accompanying documents to the set of privacy properties. We recommend to add an section to the "Architecture and Reference framework" document to the regulation with focus on privacy. This would provide better guidance for practitioners and EUDI Wallet system providers (section 7).

2 Background about electronic identification

Electronic identification (eID) is needed to ensure authorized access to online services and to carry out electronic transactions. This section fixes some terminology for digital identities and eID systems and explains the distinction between claim-based and network-based eID systems.

2.1 Electronic identity, attributes and pseudonyms

In this paper, we define electronic identity as a set of digital attributes (also referred to as claims) which identifies the user within any set of users [4]. An attribute can either be identifying or non-identifying. Examples of identifying attributes are the social security number or a certificate linked to the user. Non-identifying attributes are, for instance, the current employer of a user, or whether the user is above 18 years old. A set of non-identifying attributes can become identifying.

The use of pseudonyms is a standard technique to improve privacy. Pseudonyms are non-identifying if the association with the corresponding identity is not publicly known, but they can still be linkable. *Scope-exclusive pseudonyms* [5] are pseudonyms that are unique for a specific service provider. This means that conspiring service providers cannot link each others pseudonyms to one particular user, leading to domain unlinkability (as defined in section 3).

2.2 eID system

An *eID system* provides the infrastructure for electronic identification. Figure 1 shows the actors and processes in a typical eID ecosystem. The actors are the entities, and processes are the connectors (solid lines) between the actors.

This involves at least three parties: 1) the *user*, a natural person who wishes to access some service; 2) the *Identity Provider* (IdP) that provides the digital identity to that user; and 3) the *Relying Party* (RP) providing some online service to the user.

Also, we added two parties that are either do not have an active role in the operation of the system or are not involved. First, the eID system provider which provides the required components to run the system. However, the system provider does not need to have an active role during operation. Second, eID systems may involve *brokers*. A broker carries out the task of authenticating users on behalf of an RP. This can save cost or hassle for the RP, especially if the RP has to deal with multiple eID schemes [6]. The RP effectively outsources some work to the broker. This has implications for privacy, as a broker acting for multiple RPs can easily create profiles of users without privacy protection measures.

An eID system implements often the following four processes:

Enrollment The first process is enrollment, in which the user interacts with some central party for either registering the app instance, digitally or in the physical world, or retrieving an ID-card containing her identity.

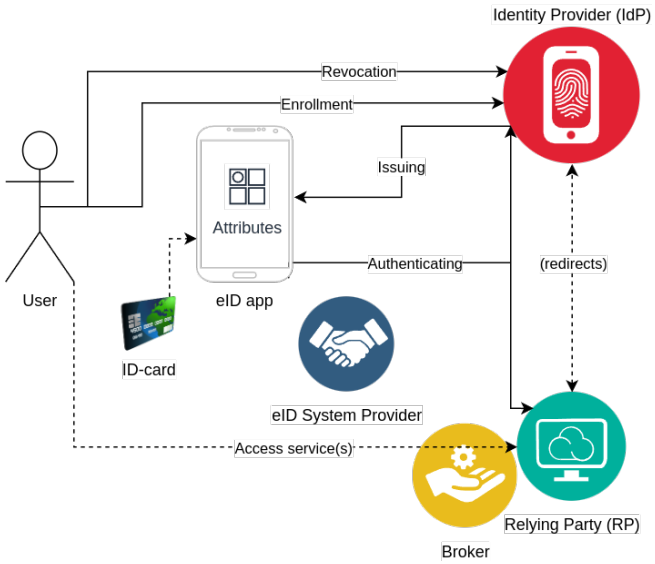

Fig. 1: eID system with actors and processes (solid lines)

Issuance An IdP can issue one or more attributes to a user, which the user subsequently stores within her eID app.

Authentication After having obtained attributes, users authenticate to the RP or broker when they wish to access some services. In some eID systems, the user links her ID-card to the eID app to authenticate. Depending on the eID system type, the user either directly shows the attributes to the RP or broker, or the RP or broker redirects to the IdP where the user authenticates.

Revocation The process of revocation ensures users, in case a user loses her identity or it is stolen, to revoke their identity by interacting with the IdP, such that no one else can use the eID anymore. We decided to exclude revocation from our privacy analysis in order to limit the scope of our study However, we do consider how eID systems — if applicable — perform validity checks during the authentication process, as such checks may have privacy implications.

2.3 Types of eID systems: network-based vs. claim-based

Different types of eID systems have evolved over the years. Figure 2 by Alpar et al. [7] illustrates two types of eID systems. We use this classification in our analysis (see section 4), as it highlights fundamental differences in potential approaches to privacy protection. In the *network-based* model, the RP redirects the user to the IdP, where the user authenticates. Then, the RP receives the authentication result from the IdP to decide whether to grant access or not. The authentication result usually identifies the user fully to the RP as the RP wants

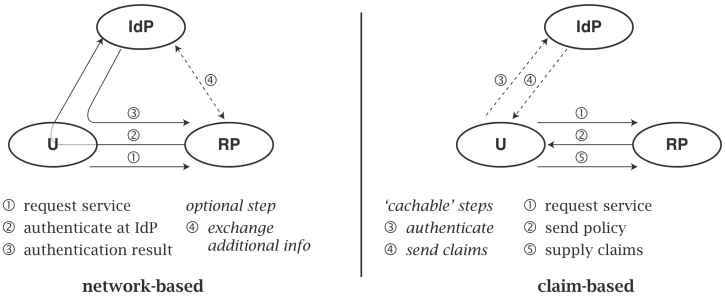

Fig. 2: Types of identity management (taken from Alpar et al. [7])

to know with which user it is communicating. The network-based model is used in federated systems.

In the *claim-based* model, introduced by Cameron [8], during authentication the user provides claims (aka attributes) to the RP without involvement of the IdP. This makes claim-based eID systems automatically more privacy-friendly as the user is unobservable from the IdP's point-of-view. In a network-based system the IdP quickly becomes privacy hotspot as it can observe all the interactions of a user with different RPs.

3 Privacy properties identification

The goal of this section is to identify privacy properties that we can subsequently use to compare eID systems (see section 4). If a system ensures a certain privacy property, it means that this system has one or several technical measures implemented to have this property. The more privacy properties a system ensures, the more it protects the privacy of its users. We looked at existing literature to identify all privacy properties (also referred to as "privacy protection goals") relevant for eID systems.[1] We find that the naming is often not concise across literature. Then, based on the literature research, we provide definitions of 11 properties.

3.1 Existing research on privacy properties

Pfitzmann and Hansen [4] provide us with a terminology about privacy, which is an often cited resource in the privacy research field. While they state that early papers already introduced most terms, they also provide relationships between these terms with the goal to develop a consistent terminology. They define the privacy properties *anonymity*, *unlinkability*, *undetectability*, *unobservability*, *pseudonymity*:

– Anonymity of a user means that the user cannot be identified by any party.

[1] As stated previously, we leave revocation out-of-scope.

- Unlinkability means that an adversary cannot links actions executed by a user to the identity of that user. Hence, there is a relationship between unlinkability and anonymity as anonymity also leads to unlinkability of the user.
- Undetectability means that an adversary cannot sufficiently distinguish whether some action happened.
- Unobservability is derived from undetectability but is more specific in that sense that an adversary knows some action happened, but cannot tell by whom and what it entails.
- Pseudonymity means that in a system pseudonyms are used as identifiers. A pseudonym is an identifier of a user other than the user's real identity. Similarly to anonymity, pseudonymity also lead to some level of unlinkability. Only the party that generates the pseudonym can link it to the user's real identity, provided that the real identity is not disclosed to other involved parties.

In the context of eID, unlinkability is an important property: it prevents parties from linking authentication actions of a user to the actual user. Based on other existing literature [9,10,11], we define three different types of unlinkability that differ in which party cannot link the actions: *multi-show unlinkability*, *domain unlinkability*, *issuer unlinkability*.

Instead of using unobservability as a privacy property, we use the term "avoid privacy hotspot" as we find it a better fit in context of eID — Shrishak et al. [12] and Roelofs [13] used the term previously. A privacy hotspot is a party in a system that collects sufficient identity data of each user leading to issues such as unauthorized access to user identity and transaction data, or misuse of personal information by the issuer. Avoiding a privacy hotspot means that a party participating in the system is not able to collect identity data. In the context of eID, we use two avoiding privacy hotspot properties: *no identity provider privacy hotspot* and *no broker privacy hotspot*.

Zwingelberg and Hansen [14] provide three privacy properties for eID systems on top of the well established CIA (confidentiality integrity and availability) triangle related to information security: Next to unlinkability, they introduce the terms *transparency* and *intervenability*.

Transparency ensures that all parties involved in data processing understand the legal, technical, and organizational conditions that define the scope of processing — before, during, and after it occurs. Transparency by itself does not tell us much about how privacy is protected. Hence, we define three properties that relate to transparency: (1) Users want to ensure that they communicate with the intended party. Within security literature, this property has long been established under the term *mutual authentication* [15]. We also consider it crucial in the context of eID to ensure that no identity data is shared with adversaries. (2) Users desire a *usage history*, an overview which data is shared with which party when, to be able to report unintended behaviour [14]. However, a usage history introduces privacy risks: if the usage history of a user would leak without sufficient protection, their privacy would be violated. (3) Due to the GDPR [2] in

the EU, organizations processing personal data must obtain explicit *consent* and clearly specify which data will be processed before any processing takes place.

Intervenability means that the parties involved in data processing, including the individual whose personal data is processed, have the possibility to intervene where necessary. Within the context of online authentication, the user should have the ability to intervene if authentication is incorrect, by, for instance, revoking their credentials such that it cannot be used anymore in the future. As mentioned earlier, we leave revocation out-of-scope for this work.

To minimize the need for user intervention mechanisms, an IdP must ensure *strong authentication* of a user before enrollment or the issuance of certified identity data. Within the EU, different *level of assurance* (LoA) — the degree of confidence in the claimed identity of a person — are established with eIDAS 1 [16]. The higher the LoA required by the IdP, the harder it becomes for adversaries to enroll as or receive credentials of another person. For instance, with a high LoA often users need to provide a copy of their passport to an IdP.

3.2 Definitions

Based on the previous literature research, we provide definitions for 11 privacy properties in what follows:

PP1: Anonymity No party within the eID system (IdP, RP, broker, and system provider) can identify the user, i.e. to hide the link between the identity used to authenticate and an action executed by the user of that identity.

PP2: Pseudonymity Colluding RPs cannot link two sessions of the same user. Only the party generating the pseudonyms can link it to the real user, in practice often a party under the responsibility of the IdP.

PP3: Multi-show unlinkability It is impossible for an RP to link two sessions of the same user (provided the attributes disclosed to the RP are not uniquely identifying, of course). As a result, the user remains anonymous to the RP, preventing the RP from creating detailed user profiles. In practice, however, often users need to disclose uniquely identifying attributes to RPs which make users linkable.

PP4: Domain unlinkability A RP cannot link the sessions of a user with sessions of that user with another RP by colluding with other RPs (again, provided the attributes disclosed to the RPs are not uniquely identifying).

PP5: Issuer unlinkability An issuer is not able to link a session of a user to the real user by colluding with an RP, where the user authenticated.

PP6: No IdP privacy hotspot The IdP cannot observe interactions of the user with other parties and hence does not become a privacy hotspot. An IdP privacy hotspot means that the IdP collect large amounts of data with the ability to link user identities to their transactions.

PP7: No broker privacy hotspot A broker cannot observe interactions of the user with other parties and hence does not become a privacy hotspot. A broker privacy hotspot means that the broker collects large amounts of data with the ability to link user identities to their transactions.

PP8: Mutual authentication RPs or brokers are authenticated in such a way that users have trust that they disclose their credentials to the intended party.

PP9: Usage history Users can inspect their usage history, i.e. a log of all their transactions with different parties and showing which data has been exchanged. This provides transparency and can help to detect certain types of abuse.

PP10: Consent to disclose data Users are informed about the data to be disclosed to a RP and obtains their explicit consent before any disclosure occurs.

PP11: Strong authentication by IdP An IdP employs an authentication mechanism that ensures sufficient assurance of a user's identity before enrolling or issuing credentials to the user.

4 Privacy comparison of eID systems

In this section we compare five eID systems based on the privacy properties identified in section 3. Appendix A provides the required descriptions of processes of the systems.

We pick the following eID systems used within the EU:

- The German eID system with the mobile app AusweisApp as the the eID system was already established back in 2010, and one of the first systems we are aware of that uses the claim-based model [17].
- The Dutch DigiD Hoog, as DigiD is widely used in the Netherlands to authenticate to a broad range of online services, such as health insurance providers to the municipality one is living. In 2022 more than 500 million times DigiD was used to log in.[2]
- The Dutch Yivi system, as it also uses the claim-based model combined with *Attribute- Based Credentials* (ABCs), to be able to store credentials from different identity providers.[3]
- The Belgian itsme system as it the most used eID system in Belgium. In 2022, in average each citizen used itsme 47 times.[4]
- The Estonian eID system as it is according to Estonia's government "the cornerstone of the country's e-state".[5]

During our analysis we discovered that these five systems provide a wide variety of technical measures.

Table 1 shows which system achieves which privacy properties. Then, we describe how a system achieves a set of properties by identifying privacy protection measures (or also *privacy enhancing technologies*), a technical implementation on how to achieve one or more privacy properties.

[2] See `https://vng.nl/nieuws/meer-dan-een-half-miljard-keer-ingelogd-met-digid-in-2022`

[3] See official documentation: `https://irma.app/docs/overview`

[4] See `https://www.itsme-id.com/nl-BE/blog/jaarcijfers2022`

[5] See `https://e-estonia.com/solutions/estonian-e-identity/smart-id`

Table 1: Privacy properties of the eID systems. The † symbol indicates that there is some additional explanation in the associated text about that system in section 4

	Itsme	**Smart-ID**	**DigiD Hoog**	**Ausweis App**	**Yivi**
eID model	network-based			claim-based	
PP1: Anonymity	no	no	no	yes	yes
PP2 Pseudonymity	no	no	yes	yes	yes†5
PP3: Multi-show unlinkability	no	no	no	yes†2	yes†3
PP4: Domain unlinkability	no	no	yes†1	yes†3	yes†2
PP5: Issuer unlinkability	no	no	no	no	yes†2
PP6: Avoid IdP privacy hotspot	no	no	yes	yes	yes
PP7: Avoid broker privacy hotspot	no	no	no	no	no
PP8: Mutual authentication	yes	yes	yes	yes	no†4
PP9: Usage history	yes	yes	yes	no	yes
PP10: Consent to disclose data	yes	yes	yes	yes	yes
PP11: Strong authentication by IdP	yes	yes	yes	yes	yes

4.1 Itsme

PP1 and PP2: There are no possibilities within Itsme to authenticate completely anonymously or using pseudonyms for authentication. *PP3to PP5:* Itsme does not achieve any unlinkability property as the identifier is sent to the IdP during presentation.[6] *PP6:* Itsme employs a network-based model, whereby the user authenticates directly to the IdP. As no additional privacy-preserving measures are applied, the IdP becomes a privacy hotspot. Also,the usage history is visible by the IdP. *PP7:* As the network-based model is employed, the broker receives the user info response which identifies a user.[7] *PP8:* RPs and brokers need to register with Itsme before they can receive a user's attributes. *PP9:* Itsme offers a centralized usage log. *PP10:* The user explicitly needs to consent to the data disclosure to the RP. *PP11:* The user needs to authenticate to her bank before being enrolled with Itsme. Due to regulations and in their own interest, banks usually have high assurances about the identity of the user.

4.2 Smart-ID

PP1 and PP2: There are no options within Smart-ID to authenticate completely anonymously or using pseudonyms for authentication. *PP3 to PP5:* Smart-ID does not achieve multi-show and domain unlinkability as the network-based

[6] See the Itsme documentation for more information: `https://belgianmobileid.github.io/doc/authentication/#authorization-request`

[7] See `https://belgianmobileid.github.io/doc/authentication/#userinfo-request`

model is employed without additional privacy-preserving measures. *PP6:* Smart-ID employs a network-based model, whereby the user authenticates directly to the IdP. As no additional privacy-preserving measures are applied, the IdP becomes a privacy hotspot. *PP7:* We cannot find information about brokers being available for Smart-ID and how they are used. *PP8:* RPs and brokers need to register with Smart-ID before they can receive a user's attributes. *PP9:* The Smart-ID system itself does not provide a usage history, however, Estonians e-government ensures that all personal data transactions are logged in the national citizen portal.[8] *PP10:* The user explicitly needs to consent to the data disclosure to the RP by entering her PIN in the app. *PP11*: The user needs to authenticate to her bank before being enrolled with Itsme. Due to regulations and in their own interest, banks usually have high assurances about the identify of the user.

4.3 DigiD Hoog

PP1: With DigiD Hoog it is not possible to authenticate anonymously. *PP2:* DigiD Hoog supports *scope-exclusive pseudonyms*. *PP3:* DigiD Hoog does not achieve multi-show unlinkability due to the use of *scope-exclusive pseudonyms*. *PP4:* DigiD Hoog achieves domain unlinkability by using *scope-exclusive pseudonyms* if the RP is only allowed to decrypt the encrypted polymorphic pseudonym. As the symbol †1 in table 1 indicates, however, that if the RP is allowed to decrypt the encrypted polymorphic identity, it results in the BSN being revealed, and conspiring RP could link user transactions. *PP5:* If the IdP would conspire with the RP, the IdP can reveal the original BSN used for creating the PI and PP. *PP6:* Although DigiD Hoog employs a network-based model approach, it avoids the IdP becoming a privacy hotspot by using *polymorphic pseudonyms and identities* [18]. None of the IdP parties know when a user authenticates, as only BSNk sends decryption keys to a RP, but does not receive any data. *PP7:* As the broker takes over the role of authenticating the user instead of the RP, the broker would become a privacy hotspot. *PP8:* With DigiD Hoog, the IdP registers an encrypted pseudonym at the *Transaction Log Provider* (TLP). Users can then inspect their usage history at the TLP. Moreover, only with the data stored at the TLP it is impossible to link transactions to an individual user, and hence, the usage history is protected from unauthorized access. *PP9:* The user explicitly needs to consent to the data disclosure to the RP. *PP10:* RPs and brokers need to register with Logius before they can offer authentication by sending the public part of their PKI government-certificate to Logius. During user authentication, the Extended Access Control v2 mechanism ensures that the RP is verified. *PP11:* DigiD Hoog goal is to ensure a high level of assurance of the user's identity. Therefore, users can enroll only with newer Dutch ID-cards or driving licenses. To receive such a card, citizens need to strongly prove their identity.

[8] See `https://www.eesti.ee/en`

4.4 AusweisApp

PP1: With AusweisApp it is possible to authenticate anonymously if a RP requests non-identifying attributes that had been issued to the user. *PP2:* AusweisApp supports *scope-exclusive pseudonyms.*. *PP3:* If a user discloses non-identifying attributes, the RP cannot link the transaction to one user. As the symbol †3 in table 1 indicates, however, in practice, users mostly authenticate to public services. Those public services usually need to uniquely identify the user. *PP4:* Colluding RPs cannot link the identities of a user if pseudonymous authentication is used. As †4 indicates, however, RPs can decide that users cannot authenticate with pseudonyms, and hence, chances increase to uniquely identify the user. *PP5:* As the IdP knows the secret key used on the ID-card, the IdP could know which user authenticates as the pseudonym is derived by using the secret key and the RPs public key. *PP6:* AusweisApp avoids the IdP privacy hotspot by employing the claim-based model. Based on the certificates and keys on the eID, the RP verifies the authenticity of the data. The IdP Bundesdruckerei is not involved during authentication. *PP7:* A broker can identify users in case identifying attributes are used. *PP8:* AusweisApp removed the usage history with version 2.0.0 and we could not find a similar functionality in the online portal.[9] *PP9:* The user explicitly needs to consent to the data disclosure to the RP. *PP10:* RPs and brokers need to request a certificate at the Federal Administration Office before being able to request credentials from any user. *PP11:* Only users with a valid German ID-card can use the AusweisApp. To receive a German ID-card, citizens need to identify themselves in citizens office or in a German embassy.

4.5 Yivi

PP1: With Yivi it is possible to authenticate anonymously if a RP requests non-identifying attributes that had been issued to the user. *PP2:* Pseudonyms are not supported directly in Yivi. However, an issuer could issue several instances of one credential with a different random number as an attribute. Then, user's could disclose a different number each time they authenticate to an RP. *PP3 to PP5* From a technological point-of-view, Yivi achieves all unlinkability properties due to the use of Idemix. As the symbol †3 in table 1 indicates, however, in practice, users mostly authenticate to public services. Those public services usually need to uniquely identify the user. *PP6:* Yivi avoids the IdP privacy hotspot by employing the claim-based model. Even in case of revocation is enabled, an IdP does not learn anything about the user's actions. *PP7:* If a user can authenticate with non-identifying attributes, a broker could not identify the user. However, as often with public services a user needs to be uniquely identified, the broker also learns the users identity, and therefore we do not assign this property to Yivi. *PP8:* Yivi offers a usage history within the Yivi app. The usage history is only stored locally on the user's mobile phone. *PP9:* The user explicitly needs to

[9] See release notes of version 2.0.0: `https://github.com/Governikus/AusweisApp2/releases/tag/2.0.0`

consent to the data disclosure to the RP by entering her PIN. *PP10:* Everyone can setup a Yivi server and can request data from any user. In that case, the RP or broker is not verified by the system provider. However, as †5 indicates, RPs or brokers can register with Yivi to have their name and logo shown in the app: the RP sends its public facing IP address of the Yivi server and a logo to the Yivi system provider. The Yivi system provider subsequently registers the IP address and logo within the scheme, such that if the app connects with that RP, the logo of that RP is shown. *PP11:* Every IdP that issues some credential can have their own identity validation mechanism that can vary in strength.

5 Observations of our analysis and recommendations for eID system providers

Based on our analysis of the five eID schemes in section 4, in this section we discuss our observations and provide recommendations for future eID system providers to improve privacy protection.

5.1 Types of eID systems

We observe that we can group the systems in three different architectural types (see subsection 2.3): the network-based (Itsme and Smart-ID), the network-based with polymorphic pseudonyms and identities (DigiD Hoog), and the claim-based (AusweisApp and Yivi). Each architecture comes with it's own set of properties that can be achieved.

Network-based The network-based systems Itsme and Smart-ID have obvious shortcomings when protecting privacy as they do not achieve PP1 to PP4, PP6 and PP7, as unique identifiers are used for authentication, making it impossible to avoid hotspots, supporting anonymity and pseudonymity, and achieving the unlinkability properties.

Network-based with polymorphic pseudonyms and identities By adding polymorphic pseudonyms and identities, DigiD Hoog avoids some of the limitations of the *pure* network-based systems. DigiD Hoog let users authenticate via pseudonymous (PP4), and thereby achieves domain (PP2) unlinkability if the RP or broker is disallowed to decrypt the polymorphic identity (as it would reveal the BSN). Also, DigiD Hoog avoids the IdP privacy hotspot (PP6).

Claim-based The claim-based model based systems can achieve PP1 to PP6. Yivi and AusweisApp both avoid the IdP privacy hotspot (PP6) due to the claim-based model. However, both apply a different approach of identity data signing.

Yivi is the only system that allows credentials being issued from different IdPs by using *Attribute-Based Credentials* (ABCs), introduced by Camenisch et al. [19]. An ABC is a certified set of attributes of a user, signed by an IdP.

With the signature of an ABC, an RP can verify the authenticity of the attributes without the need to communicate directly with the IdP. ABCs can help to achieve unlinkability [20].

AusweisApp ensures that both the user and RP are authenticated before identity data from the ID-card can be read by the RP due to the *Extended Access Control v2* mechanism. The different approaches can be explained by the fact AusweisApp only works with the ID-card data, and does not support other issuers.

In interactions with a RP the user may only reveal the required subset of information of one or more credentials to the RP; which is referred to as selective disclosure. If those attributes are not identifiable and the signature shared with the RP does not identify the user, anonymity (PP3) can be achieved. If anonymous authentication is possible, also domain and multi-show unlinkability is achievable.

However, currently users mostly authenticate to public services which requires unique identification. In the private sector, however, it could often be sufficient to only disclose parts of your identity that do not reveal identifying information.

Recommendation 1: Either use the claim-based model or the network-based model with polymorphic pseudonyms and identities to avoid the IdP privacy hotspot (PP6), have the possibility to authenticate anonymously (PP1) or pseudonymously (PP2) and achieve unlinkability properties (PP3 to PP5).

5.2 Usage history

Providing a usage history is independent of the chosen type. DigiD Hoog has a usage history (PP9) that is centralized but also protects the user history data, as it can only be accessed by the real user, thereby preventing unauthorized access. With Yivi, the usage history is only visible by the user, as the usage history is only stored locally on the user's mobile phone. However, offering only a local usage history comes with the cost of making it more difficult to detect improper use by some other party. Smart-ID and Itsme have both a centralized usage history, which can be accessed by the IdP.

Recommendation 2: Provide users with access to a usage history that clearly shows when and which data was shared with which Relying Party (RP) for better transparency.

Recommendation 3: If a centralized usage history is used, decouple it from the rest of the system, and limit who can access the data, e.g. only the user and a fraud team, to ensure unlinkability and prevent unauthorized access.

5.3 Mutual authentication

All systems but Yivi guarantees that RPs are authenticated (PP8). Yivi supports verified parties by the IdP but does not guarantee it as everyone can host a Yivi server and any user can disclose attributes to that server. However, RPs can register themselves to have their name and logo shown within the Yivi app.

Recommendation 4: Ensure that RPs or brokers are authenticated if credentials are shared that contain sensitive identity data as otherwise user's risk disclosing attributes to unwanted third parties. In case non-sensitive identity data is shared, such as age, do not enforce of RPs being authenticated to make it less of a burden, for instance, for liquor stores to request the age.

5.4 Avoiding the broker privacy hotspot

The only property no system achieves is PP7: avoiding the broker privacy hotspot. We realize that, In practice, this property is hard to achieve, as the broker has the task to authenticate the user *on behalf* of a RP.

Recommendation 5: Setup agreements with brokers to only allow them to process personal data during authentication, and deny them to store transaction data permanently. Otherwise, there is an increased risk of becoming a privacy hotspot.

6 Previous work on eID privacy analysis

Shrishak et al. [21] investigate privacy protection of five eID systems developed in Europe by using six privacy properties, and conclude that only a few had a privacy-by-design approach in mind. The chosen systems are from Belgian, UK, the Dutch, the German eID scheme and Yivi. The six properties are anonymity & pseudonymity, data minimization, unlinkability, unobservability, and transparency. However, they do not provide an extensive description of properties, but mostly refer to texts of ISO15408-2 [22]. Moreover, they conclude that Yivi (formerly IRMA) is the most privacy friendly system without providing further evidence even though the German system has the same properties. Our analysis is more nuanced and we avoid assigning a clear *winner*.

Khatchatourov et al. [23] assess privacy in eID systems from Estonia, Austria, Germany and Switzerland by defining three inter-related axis, in particular, pseudonymous authentication, attributes location, and authentication schemes. They find that the German eID solution has the best level of privacy protection, but it is also the most complex system. They discuss the difference between actual and perceived privacy protection as they observe that although systems have a higher level of privacy protection, they are not adopted significantly more than systems with less privacy protection. Perceived privacy protections involves factors such as trust in the system and organizations, and reluctance to disclose personal data. For instance, within Germany there exists a clear effect of using the highly personal ID-card in different contexts, even if there is a decent level of privacy protection. Hence, next to actually protecting privacy by implementing privacy preserving measures, governments and providers of eID systems need to take into account the perceived privacy protection of their users. Particularly, the EU should take the notion of perceived privacy protection into account for EUDI. For instance, one explicit goal of EUDI is to increase adoption of eID within the private sector, which can impact perceived privacy protection negatively.

7 Privacy in the EUDI regulation

The goal of this section is to analyze privacy protection within the European Digital Identity (EUDI) regulation. We begin by providing background information on the EUDI regulation and related documents. Next, we examine how the regulation requires future system providers to protect privacy by using our 11 defined privacy properties (see section 3). Thereby, we also highlight shortcomings in the current regulation and related documents. Finally, we offer recommendations to the European Commission.

7.1 EUDI and related documents background information

In 2021 the EU published a first version of the EUDI [3] proposal (aka eIDAS 2.0) to amend the eIDAS 1.0 regulation; in the meantime the EU accepted a 1.0.0 version [24]. An EU evaluation [25] of the eIDAS 1.0 regulation concluded that the current scope of eIDAS is too narrow, leading to minimal usage. EUDI is designed to enable secure user identification and authentication with a high Level of Assurance (LoA) for both public and private online services. With EUDI each EU citizen shall be able to install an identity wallet for free.

The related technical framework is called the *Architecture and Reference Framework* (ARF) [26]. The ARF is still work in progress, the current version at the time of writing is 1.8. It contains details about actors, interactions between actors, common standards and practices. The final version of the ARF will contain legally binding requirements for identity providers issuing credentials and system providers that deliver the identity wallets to EU citizens.

The proposal claims that the framework shall "not allow [...any...] party [...] to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, [...] unless explicitly authorized by the user", and "enable privacy preserving techniques which ensure unlinkability, where the attestation of attributes does not require the identification of the user". Moreover, the ARF states: "In addition, Article 5c(5) provides [..] certification of personal data processing [..]. While this certification is not mandatory, the Regulation (EU) 2016/679 (*GDPR*) requirements fully apply to the EUDI Wallets and their providers". However, several online publications [27,28,29] raise concerns that the current framework weakens the privacy claims made by the proposal. [29] conclude that with the reliance on the proposed cryptographic methods the privacy requirements cannot be fulfilled. Hence, a larger redesign needs to be conducted. [27,28] state that details are missing with regards to unobservability for avoiding privacy hotspots. All in all, there is doubt that the privacy of EU citizens is adequately protected based under the current conditions.

The ARF [26] is complemented with additions, called annexes, technical specifications, and implementing regulation documents. [10] Among others, those documents provide requirements for EUDI system providers. The fragmentation of documents complicates efforts to ensure privacy protection within EUDI-compliant eID systems

7.2 Privacy analysis of EUDI

In the following, we present our privacy analysis of the EUDI regulation. To maintain a focused scope, we concentrate our analysis on Annex 2, as it outlines normative requirements categorized according to the RFC 2119 requirement levels [30]. In section B, we map these EUDI requirements to our defined set of privacy properties (see section 3) if they are somehow related. Based on this mapping, we discuss the resulting implications. Specifically, we assess whether EUDI-compliant systems are required to uphold certain privacy properties and, if so, provide possible details on how this is enforced. Our goal is to assist practitioners and identity wallet implementers in better understanding how privacy should be protected in EUDI-compliant systems.

Anonymity and Unlinkability In theory, PP1 , PP3, PP4, and PP5 are all achievable as selective disclosure is a technical measure systems need to support. However, the actual credential and wallet instance may be identifiable and thus, linkable to an actual user. The *cryptographers feedback* [29], published in June 2024, recommends the use of *anonymous credentials* (synonymous with attribute-based credentials). With anonymous credentials the only information revealed to an RP is the attributes the user chooses to reveal and who issued the credential, but no identifiers that could identify the user. One technology to realize anonymous credentials is *Zero Knowledge Proofs* (ZKP), as used by Yivi. In March 2025, a

[10] See for instance `https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-european-digital-identity-wallets`

section about Zero Knowledge Proofs (ZKP) has been added to annex 2, which outlines requirements in case ZKP is used within a wallet system.[11] Therefore, it seems, the cryptographers feedback has been taken into account.

Pseudonymity Pseudonymous authentication (PP2) is clearly a requirement. Yet, as epicenter.works points out in their most recent analysis [31], in the current draft of implementing regulation documents, there is no clear distinction between cases where a RP is legally required to identify users and other situations where such identification is optional. The right to use a pseudonym for authentication depends on this distinction. Therefore, it is important to allow RPs to indicate whether such a legal obligation applies.

Privacy hotspots With the current annex 2, as wallets need to support the "OpenID for Verifiable Presentations" standard [32], a claim-based architecture is mandatory. Consequently, IdP privacy hotspots are avoided (PP6). However, brokers are not mentioned, and hence, broker privacy hotspots may emerge (PP7).

Mutual authentication and consent A wallet instance need to ensure that RPs are authenticated (PP8). Also, the requested attributes by the RP should also be visible, before the user provides consent to disclose the data (PP10). Interestingly, the ARF mentions (section 6.6.3.3) that a user needs to be informed in case an RP requests attributes that were not previously documented within the RP's registration certificate. This mitigates the risk of over-sharing [33], as then users does not need to educate themselves about the RP they are communicating with whether they trust them and that the RP only requests the required set of attributes.

Usage history A dashboard functionality need to be available in any identity wallet, which provides a usage history (PP9). However, no details are provided how to guarantee privacy protection. If no measures are taken, this can lead to a privacy hotspot.

Strong authentication by IdP If an IdP issues "personal identification data" (PID), which contains similar data as a passport, that IdP needs to ensure the identity of the user in compliance with LoA high (PP11). In other cases, it depends on the IdP how strong the authentication of the user needs to be.

Summary All in all, we can state EUDI-compliant systems do not need to ensure all the 11 privacy properties that we identified. PP2, PP6, PP8, PP9, PP10, PP11 are clearly properties that future EUDI-compliant wallets need to ensure. Brokers are not mentioned at all in any EUDI-related document, hence PP7 does

[11] There is also a lively discussion about ZKP on the ARF's GitHub page: `https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/408`

not need to be ensured. PP1 , PP3, PP4, and PP5 in theory can be ensured as selective disclosure is a mandatory measure. However, as [29] also criticize, the actual credential and wallet instance still could be identified and linkable to the user.

7.3 Recommendations for the European Commission

Due to fragmented documentation, it remains difficult to fully understand how privacy should be protected in EUDI-compliant systems. The ENISA Digital Identity Standards report [34] similarly calls for a standardized privacy evaluation methodology. We recommend that the EU adds a new section to the ARF focused on privacy, including a clear list of privacy properties and corresponding technical measures for wallet providers — our work can help shape this guidance. Additionally, once systems are deemed EUDI-compliant, a public report should explain how they ensure privacy properties for transparency.

In the same direction as [29] , we strongly advise to add additional requirements for making credentials and wallet instances unlinkable. Also, from our recommendations (see section 5) number 3 and 5 are not explicitly mentioned in annex 2. Hence, we advise to take them into account in future versions of the ARF.

8 Future work

We analyzed five eID systems, but there are obviously many more in use within the EU. We would like to extend our comparison to more systems, especially to identify other technical measures that improve privacy protection. This might allow us to refine our recommendations.

Avoiding the broker privacy hotspot is the most difficult property to achieve: none of the systems we analyzed achieves it. Grassi et al. [6] proposed scenarios for privacy-preserving brokers that do not become privacy hotspots. One year later, Brandão et al. [35] provided recommendations and concerns about this paper. Using this research as a starting point, future work could develop proof of concepts for different approaches to realize privacy-preserving brokers.

Future research could look into how to protect personal data in centralized usage histories as it can lead to privacy hotspots. DigiD Hoog shows how to implement a centralized usage history that protects the data from unauthorized access. It would be interesting to identify and compare other scenarios.

9 Conclusion

In this paper, we identify 11 privacy properties (section 3) for eID systems to subsequently compare five eID systems used in the EU (section 4). Table 1 provides an overview of properties a system has. We also show that some properties are achieved with different *technical measures* (also *privacy enhancing technologies*). One challenge in this research was describing the systems we analyzed in

a uniform way, as detailed descriptions were hard to find for some systems and are very different in nature.

A more fundamental challenge was coming up with a good, complete and clearly-defined set of privacy properties relevant for eID systems. After looking at the literature, in particular [9,11,36,14,10,12], it remains hard to argue that our set of privacy properties is complete. Nevertheless, we have shown that it is rich enough for a good comparison of eID systems, as four out of five systems satisfy different sets of properties.

For future eID system providers we provide recommendations in section 5. The claim-based model clearly has some benefits over the network-based model with regards to privacy protection, as the claim-based model avoids the IdP privacy hotspot. An interesting aspect of the Dutch DigiD Hoog is that it offers privacy benefits typical of claim-based systems, despite using a network-based approach. By combining this model with polymorphic pseudonyms and identities, it avoids common network-based drawbacks, notably the IdP privacy hotspot. As brokers are not recognized by any system, we recommend to setup agreements with them to deny them storing any identity data after processing.

In section 7, we analyze how privacy should be protected in *European Digital Identity* (EUDI)-compliant identity wallet systems. Our analysis concludes that EUDI-compliant systems are not required to fulfill all of our 11 privacy properties. Since brokers are not referenced in any EUDI-related documents, avoiding the broker hotspot is not applicable. Although anonymity and the unlinkability properties could theoretically be supported through the mandatory use of selective disclosure, we highlight that credentials and wallet instances may still be identifiable and linkable to users in practice. To better support EUDI system providers, we recommend that the European Commission include a dedicated privacy section in the technical framework, clearly outlining relevant privacy properties and possible technical measures that can ensure those properties.

References

1. European Parliament and of the Council of the European Union, "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 and repealing directive 1999/93/ec," https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1502, 2014.
2. European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," https://data.europa.eu/eli/reg/2016/679/oj, OJ L 119, 4.5.2016, p. 1–88, 2016.
3. European Commission, "European Digital Identity," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en, 2021.

4. A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," 2010.
5. J. Camenisch, "Concepts Around Privacy-Preserving Attribute-Based Credentials," in *Privacy and Identity Management for Emerging Services and Technologies*. Springer, 2014, vol. 421, pp. 53–63.
6. P. Grassi, N. Lefkovitz, and K. Mangold, "NIST privacy-enhanced identity brokers," *NIST-NCCoE*, vol. 19, 2015.
7. G. Alpár, J.-H. Hoepman, and J. Siljee, "The Identity Crisis Security, Privacy and Usability Issues in Identity Management," *Journal of Information System Security*, vol. 9, no. 1, pp. 23–53, 2013.
8. K. Cameron, "The laws of identity," *Microsoft Corp*, vol. 12, pp. 8–11, 2005.
9. S. A. Kakvi, K. M. Martin, C. Putman, and E. A. Quaglia, "SoK: Anonymous Credentials," in *Security Standardisation Research*, ser. LNCS, vol. 13895. Springer, 2023, pp. 129–151.
10. J.-H. Hoepman, "Privately (and unlinkably) exchanging messages using a public bulletin board," in *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, 2015, pp. 85–94.
11. K. Kluczniak, J. Wang, X. Chen, and M. Kutyłowski, "Multi-device anonymous authentication," *International Journal of Information Security*, vol. 18, no. 2, pp. 181–197, 2019.
12. K. Shrishak, Z. Erkin, and R. Schaar, "Enhancing user privacy in federated eid schemes," in *2016 8th IFIP international conference on new technologies, mobility and security (NTMS)*. IEEE, 2016, pp. 1–5.
13. F. Roelofs, "Analysis and comparison of identification and authentication systems under the eIDAS regulation," Master's thesis, Radboud University, 2019.
14. H. Zwingelberg and M. Hansen, "Privacy Protection Goals and their implications for eID systems," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Springer, 2011, vol. 375, pp. 245–260.
15. D. Otway and O. Rees, "Efficient and timely mutual authentication," *ACM SIGOPS Operating Systems Review*, vol. 21, no. 1, pp. 8–10, 1987.
16. EU, "eIDAS Levels of Assurance," https://ec.europa.eu/digital-building-blocks/wikis/digital-building-blocks/wikis/display/DIGITAL/eIDAS+Levels+of+Assurance, 2014.
17. K. Bräunlich, A. Kasten, and R. Grimm, "Der neue personalausweis zur authentifizierung bei elektronischen wahlen," *Sicher in die digitale Welt von morgen*, pp. 211–225, 2011.
18. E. R. Verheul, "The polymorphic eID scheme," Ministry of Interior and Kingdom Relations, Tech. Rep., 2019.
19. J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, K. Rannenberg, and H. Zwingelberg, "D2.1 Architecture for attribute-based credential technologies," *Deliverable, ABC4Trust EU Project*, 2011.
20. A. Sabouri and K. Rannenberg, "ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-Life," in *Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Springer International Publishing, 2015, vol. 457, pp. 3–16.
21. K. Shrishak, Z. Erkin, and R. Schaar, "Enhancing privacy of users in eID schemes," *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, 2016.
22. ISO/IEC, "ISO 15408: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security," ISO, Geneva, CH, Standard, 2022.

23. A. Khatchatourov, M. Laurent, and C. Levallois-Barth, "Privacy in Digital Identity Systems: Models, Assessment, and User Adoption," in *Electronic Government*, ser. LNCS. Springer International Publishing, 2015, pp. 273–290.
24. The European Parliament and Council, "2024/1183 regulation (eu) 2024/1183 of the european parliament and of the council amending regulation (eu) no 910/2014 as regards establishing the european digital identity framework," https://eur-lex.europa.eu/eli/reg/2024/1183/oj, 2024.
25. European Commission, "Evaluation commission staff working document accompanying the document report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 eIDAS," 2021.
26. European Commission, "The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework," 2024, version: 1.8. [Online]. Available: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework
27. epicenter.works, "EU Digital Identity Reform: The Good, Bad & Ugly in the eIDAS Regulation," https://epicenter.works/en/content/eu-digital-identity-reform-the-good-bad-ugly-in-the-eidas-regulation, Nov. 2023.
28. epicenter.works, "eIDAS: Implementing acts - european digital identity wallets," Sep. 2024. [Online]. Available: https://epicenter.works/fileadmin/medienspiegel/user_upload/epicenter.works_-_eIDAS_implementing_acts-rv1.pdf
29. C. Baum, O. Blazy, J. Camenisch, J.-H. Hoepman, E. Lee, A. Lehmann, A. Lysyanskaya, R. Mayrhofer, H. Montgomery, N. K. Nguyen *et al.*, "Cryptographers' feedback on the eu digital identity's ARF," *Tech. Rep.*, 2024.
30. S. Bradner, "RFC2119: Key words for use in RFCs to indicate requirement levels," 1997.
31. epicenter.works, "eIDAS: European digital identity wallet: Analysis and amendments to the implementing acts 2," https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_iA_-_amendments-rv5.pdf, 2025.
32. K. N. Chadwick and J. Vercammen, "Openid for verifiable credentials," *OpenID Foundation*, 2022.
33. H. M. M. Klenk, M. de Reuver, and N. Bharosa, "How does the EU digital identity wallet change the risk of over-sharing data? a Dutch perspective," 2024.
34. I. Alamillo, S. Mouille, A. Röck, N. Soumelidis, and M. Tabor, "Enisa digital identity standards," https://www.enisa.europa.eu/sites/default/files/publications/Digital_Identity_Standards.pdf, 2023, [Accessed 16-04-2025].
35. L. T. Brandão, N. Christin, and G. Danezis, "A Public Comment on NCCoE's White Paper on Privacy-Enhancing Identity Brokers," 2016.
36. J. Camenisch, R. Leenes, M. Hansen, and J. Schallaböck, "An Introduction to Privacy-Enhancing Identity Management," in *Digital Privacy: PRIME - Privacy and Identity Management for Europe*, ser. LNCS. Springer, 2011, pp. 3–21.
37. S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)," Internet Engineering Task Force, Tech. Rep. RFC 6960, 2013.
38. E. R. Verheul and B. Jacobs, "Polymorphic encryption and pseudonymisation in identity management and medical research," *Nieuw Archief voor Wiskunde*, vol. 18, pp. 168–172, 2017.
39. D. Kuegler and Y. Sheffer, "Password Authenticated Connection Establishment with the Internet Key Exchange Protocol version 2 (IKEv2)," Internet Engineering Task Force, Request for Comments RFC 6631, 2012.
40. BSI (Federal Office for Information Security), "German eID based on Extended Access Control v2," Tech. Rep., 2017.

41. IBM, "Specification of the Identity Mixer cryptographic library, version 2.3.4," 2012.
42. J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," in *Advances in Cryptology – CRYPTO 2004*, ser. LNCS. Springer, 2004, pp. 56–72.

A eID system descriptions

In this section we describe for each system the enrollment, issuing (if applicable), and authentication process.

A.1 Itsme

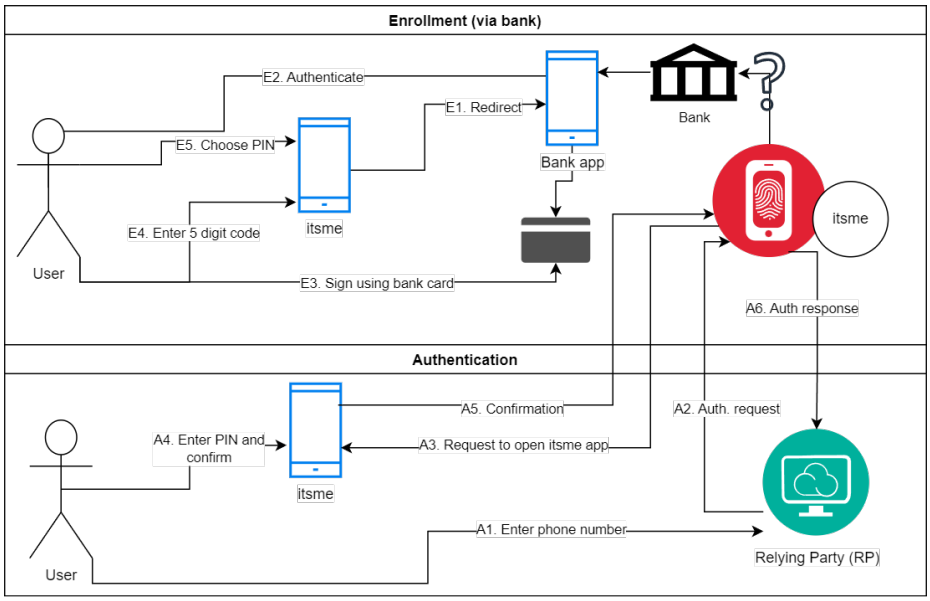

Fig. 3: Itsme enrollment and authentication process

Figure 3 shows the enrollment and authentication process of Itsme. Itsme is developed by the Belgian Mobile ID, a consortium of the seven biggest banks in Belgium. Itsme is the eID system provider and IdP.

Enrollment Initially, a user can choose to either enroll via her bank account or ID-card. We leave enrollment via the ID-card out of scope. In case of enrollment via bank, the Itsme app redirects the user to their mobile banking app (E1). After authenticating to the bank (E2), the user signs the Itsme session by using the bank card and the bank's card reader (E3). The interaction between the bank and IdP is unknown to us but not relevant for our privacy analysis. Then, the user receives a 5-digit code, which she needs to enter within the Itsme app to activate the app (E4). Last, the user chooses a PIN code to secure the app (E5).

Issuing After enrollment, it is not possible with Itsme to receive additional attributes.

Authentication The user clicks on the *Itsme* button on the website of the RP and enters her phone number (A1). The RP then establishes a session with the IdP by sending an authentication request (A2). The IdP subsequently sends a notification to the app instance, which subsequently opens automatically on the user's mobile device (A3). Itsme does not document how revocation of the user attributes works, however, as Itsme is both eID system provider and IdP, it can easily revoke a user's identity if the user requests it.[12] The user enters the previously chosen PIN code (A4) and confirms the authentication (A5). The IdP sends the auth. response to the RP (A6). Finally, the RP verifies the signature of the payload with the public key of the Itsme IdP.

A.2 Smart-ID

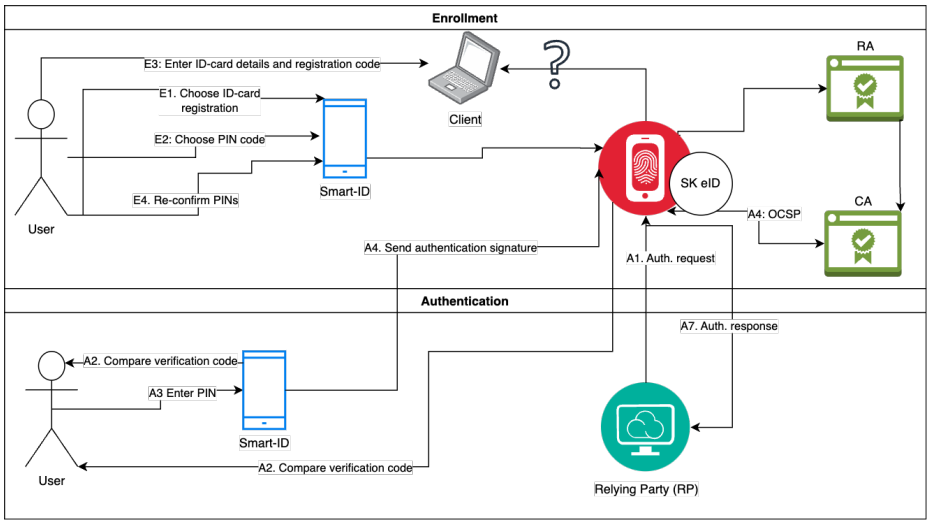

Fig. 4: Smart-ID enrollment and authentication process

Figure 4 shows the enrollment and authentication process of Smart-ID. *SK eID* is the eID system provider and IdP.

Enrollment To enroll, one of several methods in Estonia can be used: either by using a citizen's ID-card or Mobile-ID or biometric identification. Mobile-ID is a solution where the identity is linked to a custom SIM card, provided by some mobile operators in Estonia. For biometric identification in Estonia a citizen needs to use their passport, as well as a NFC compatible phone and phone

[12] A RP can request to revoke a session token: `https://belgianmobileid.github.io/doc/authentication/#revoke-request`

camera such that the app can compare your actual face with the photo on the passport. We chose to describe the enrollment via the citizen's ID-card.

The user chooses to register via ID-card initially (E1). Then, she must choose two PIN codes, one for authentication, and one for signing (E2). Subsequently, she must enter ID-card details and the registration code shown in the app on the Smart-ID website shown on the client (E3). After confirmation, the user needs to re-confirm the PIN codes on the mobile phone (E4). How exactly the website communicates with the IdP, and how the IdP communicates with the RA and CA is unknown to us.

Issuing After enrollment, it is not possible with Smart-ID to receive additional attributes.

Authentication After requesting to login at the RP, the user is redirected to the IdP (A1) whereby the identifier is passed on.[13] Subsequently, the IdP sends a request to the mobile device to open the Smart-ID app, and a verification code is shown on the screen and within the mobile app (A2). The citizen should ensure that the codes are the same, and confirms it by entering her PIN (A3). The app then sends the authentication signature to the IdP (A4). The IdP checks the validity of the transmitted signature at the CA by following the *Online Certificate Status Protocol* (OCSP) (A5). OCSP is described in RFC 6960 [37].

A.3 DigiD Hoog

Figure 5 shows the enrollment and authentication process of DigiD Hoog.[14] Logius is the system provider and IdP of DigiD, and part of the state government in the Netherlands. DigiD Hoog employs polymorphic pseudonyms and identity; for an in-depth explanation see [18]; [38] contains a summarized version. Overall, for each user, a pseudonym is derived from the Dutch social security number, BSN, and stored on the ID-card, which is used during authentication.

Enrollment To enroll in DigiD Hoog, a user requires owning an ID-card handed out after 13-03-2021, as it contains a *polymorphic card application* (PCA). To obtain such an ID-card, the user first needs to authenticate to the *Rijksdienst voor Identiteitsgegevens* (E1). After successful authentication, the Rijksdienst sends the BSN to the IdP *BSN linking service* (BSNk) (E2). BSNk generates two structures: First, a Polymorphic Identity (PI), an encrypted identity, containing the BSN . Second, a Polymorphic Pseudonym (PP), containing the encrypted base pseudonym, which is a keyed hash value of the BSN. Both PI and PP are sent to the Rijksdienst (E3). Moreover, the BSNk generates a PP for the status

[13] See the Smart-ID documentation: `https://github.com/SK-EID/smart-id-documentation#22-relying-party-rest-interface`

[14] Hoog is Dutch for high. There are three variants of DigiD offering different levels of assurance, with Dutch Hoog offering the highest level. The levels are based on the three eIDAS levels of assurance.

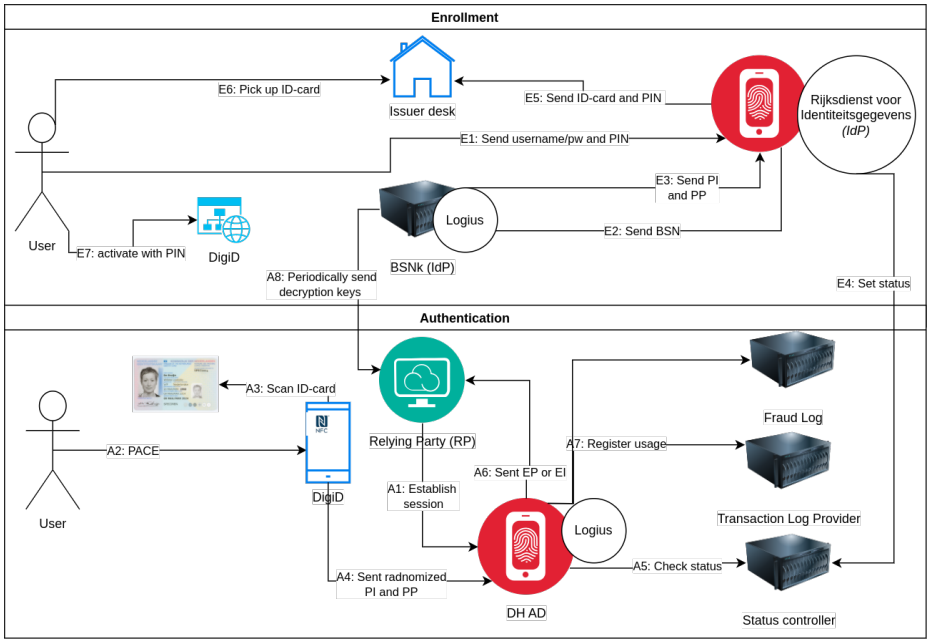

Fig. 5: DigiD Hoog enrollment and authentication process

controller such that the *Status Controller* cannot collude with other components to identify a user. The Rijksdienst tracks the status and monitors status transitions, and updates this data in the status controller (E4). The resource issuer produces the ID-card and sends it to an issuance desk (mostly the municipality the user is registered) together with the PIN (E5), where the user needs to pick it up (E6) Finally, the user activates the ID-card by visiting the DigiD website and entering the PIN (E7).

Issuing After enrollment, it is not possible with DigiD Hoog to receive additional attributes.

Authentication After the RP established a session with the authentication service *DH AD* (A1), the user must connect the ID-card to her mobile device (A2), and enter the PIN (A3) to establish a secure channel between ID-card and DigiD app via the *Password Authenticated Connection Establishment* (PACE) protocol [39]. Then, the *Extended Access Control* mechanism is applied to ensure a secure connection between the DigiD app and the RP and restricts access to identity data on the ID-card. *Extended Access Control* comprises Terminal Authentication, where the chip authorizes the eID server to access the identity data; Chip Authentication, where the eID server verifies the authenticity of the ID-card; and Passive Authentication, which proves that the information on the ID-card is authentic and unaltered. After scanning the QR code, the app sends

a randomized PI and PP to the authentication service *DH AD* (A4). Then, the DH AD asks the status controller for the status of the ID-card, i.e., whether the ID-card is valid and not revoked (A5). With the *re-keying* operation the PI or EI is made decipherable for the intended RP by DH AD, leading to *Encrypted Identity* (EI) resp. the *Encrypted Pseudonym* (EP), whereby DH AD does not have access to the plaintext data itself. Then, DH AD sends either the EI or EP to the RP (A6), depending on whether the RP requests the identity or pseudonym. The EI is only used if the RP is granted permission to process the BSN. Then, for both the *Transaction Log Provider* and the *Fraud Log* (A7) a unique PI is generated, preventing that those components can link transaction to a user. Subsequently, the authentication session is logged at both parties. Finally, the RP periodically receives keys from the BSNk, which the RP uses to decrypt the EP or EI (A8), thereby preventing user identification at the BSNk. Moreover, other RPs cannot decrypt the EP or EI with their decryption keys.

A.4 AusweisApp

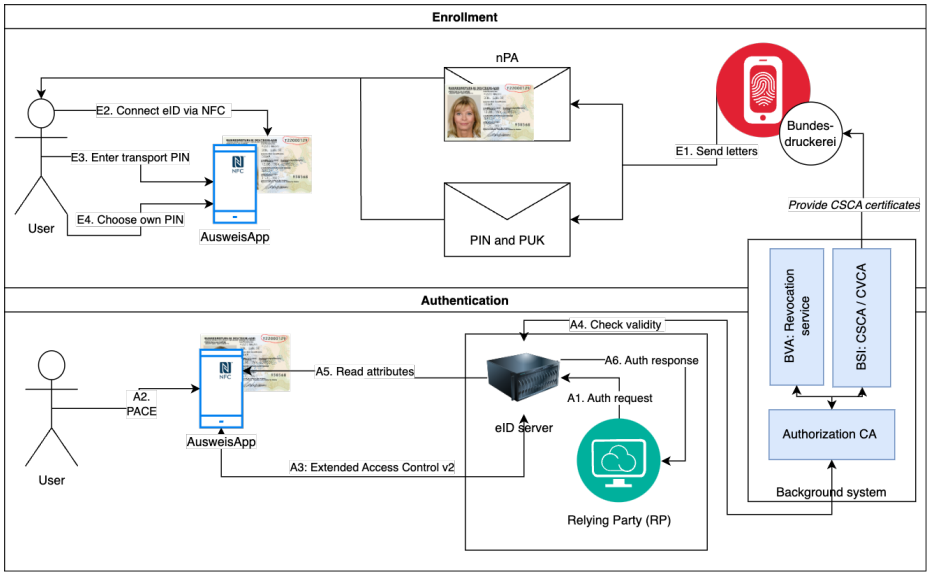

Fig. 6: AusweisApp enrollment and authentication process

Figure 6 shows the enrollment and authentication process of AusweisApp. The eID system provider of AusweisApp is Governikus.[15]

[15]See Governikus website: `https://www.governikus.de/`

Enrollment To be able to use the AusweisApp, the German ID-card is required.[16] The chip of the nPA holds a static Diffie-Hellman key pair and a certificate containing the public key signed by the Bundesdruckerei, whereby the root certificate is provided by the *Country Signing Certification Authority* (CSCA). Parallel to the ID-card being sent to the user via mail, another mail is sent containing a PIN for activation (E1). To activate the eID function, the user needs to connect the ID-card with her mobile device via NFC (E2) and enter the activation PIN (E3). Then, the user chooses her own PIN to secure the app (E4).

Issuing After enrollment, it is not possible with AusweisApp to receive additional attributes.

Authentication As a prerequisite, in case another client than the mobile device is used to access some service, the client and AusweisApp must be in the same network. Also, the client needs to have the AusweisApp installed. Then, the two app instances need to be paired by enabling pairing and entering the pairing code from the mobile app instance in the client's app instance. When the user requests some service, the RP creates the authentication session on the eID sever (A1). The PACE protocol is implemented to establish a secure channel between AusweisApp and the ID-card, relying on the user's PIN [40] (A2). Then, three protocols are performed [40] as part of the *Extended Access Control v2* mechanism (A3), resulting in the establishment of a authenticated TLS channel between the ID-card and eID server: First, the terminal authentication protocol authenticates the RP. Second, the passive authentication protocol proves authenticity of the data stored on the ID-card. Third, the chip authentication provides proof that the eID contains the correct private key (corresponding to the public key), and together with passive authentication verifies the authenticity of the eID. Only after all protocols are successfully completed, the RP can read the personal data. Subsequently, the eID server verifies that the eID is not revoked nor expired (A4), after which the data is read from the ID-card and transferred to the RP (A5). Finally, the eID server responds to the RP with the requested data (A6).

The German eID offers the *Restricted Identification* protocol for pseudonymous authentication.[17] The pseudonyms are derived by the ID-card based on the unique secret key of the ID-card and the public key of the RP, resulting in a *scope-exclusive pseudonym*. Importantly, although the chip on the ID-card is authenticated to the RP during chip authentication, the ID-card's public key is shared among a large group of eID cards, which does not uniquely identify the ID-card.

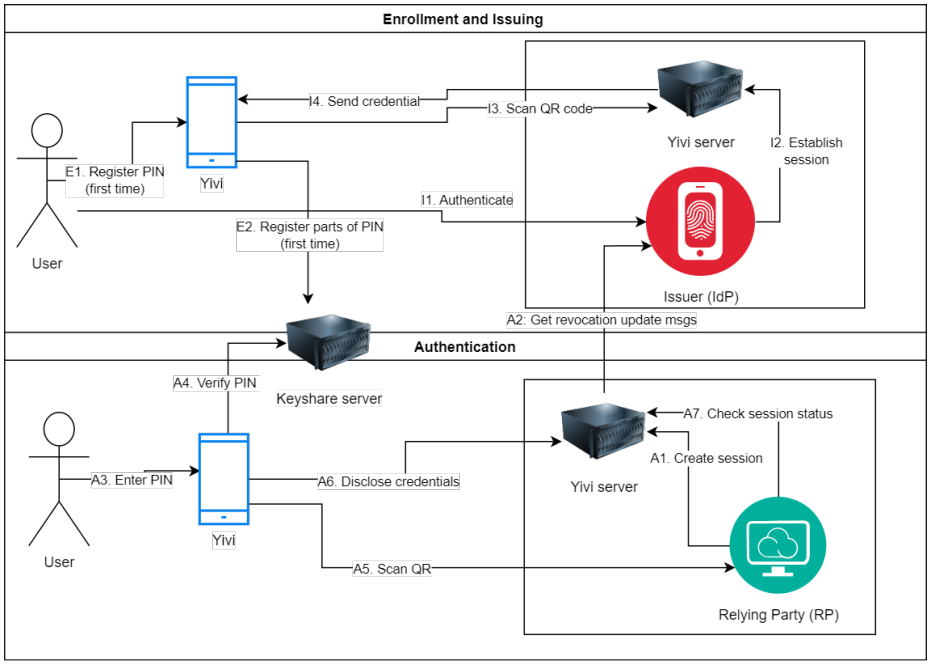

Fig. 7: Yivi enrollment, issuing, and authentication process

A.5 Yivi

Figure 6 shows the enrollment and authentication process of Yivi. Yivi is owned by the privacy by design foundation (Pbdf); the Pbdf is the eID system provider.[18]

Enrollment When using the Yivi identity wallet app for the first time, the user is asked to choose a PIN (E1), whereby parts of the PIN are registered at the keyshare server (E2)[19].

Issuing A Yivi user can receive attributes from different IdPs, the official Yivi scheme contains a list of all official IdPs.[20] Hence, Yivi itself is not solely responsible for providing attributes to the user. After a user authenticated to the IdP in question (I1), the IdP establishes a session with its Yivi server (I2). Then, the user scans the QR code with the Yivi app (I3) to establish the session

[16] See the website of the Bundesdruckerei: `https://www.bundesdruckerei.de/en/digitale-identitaeten`

[17] See `https://www.personalausweisportal.de/Webs/PA/EN/business/technology/pseudonym/pseudonym-node.html`

[18] See the Pbdf website: `https://privacybydesign.foundation/`

[19] For more details see `https://irma.app/docs/keyshare-protocol`

[20] See official scheme: `https://github.com/privacybydesign/pbdf-schememanager/`

between. After the Yivi server computes the credentials, which are cryptographically signed by the IdP, it sends the credentials to the Yivi app instance (I4).

Authentication The RP initiates an authentication session at the Yivi server, whereby the RP can create a ConDisCon policy by combining one or more credentials. ConDisCon means a conjunction of disjunctions of a conjunction, providing users with a possible choice on which parts of credentials to disclose. If the RP want to ensure that credentials are not revoked (for credentials that support it), the RP can request this at the Yivi server within the session request.[21] Then (A2), the Yivi server request revocation update messages from the issuer for the credential types. After unlocking the Yivi app by entering the PIN (A3) and have it verified at the keyshare server (A4), the user scans the QR code shown to establish the session between the Yivi app and the Yivi server (A5). If revocation is enabled, the numbers included in the revocation update messages are also passed along. Then, the user is shown the policy within the app so she can possibly choose which parts of her credentials to disclose. As Yivi implements partly IBM's *Idemix* specification [41] by using CL signatures [42], it supports *Zero-Knowledge Proofs* (ZKPs). With ZKPs, a user can hide attributes within a proof, while still convincing the RP to possess a valid signature, thereby supporting selective disclosure. After the user chooses which parts of credentials to disclose, the Yivi app computes and transmits the credentials (A6). If revocation is enabled by the RP, the Yivi app also includes a non-revocation proof, which is calculated based on the revocation update messages. The Yivi server then verifies the signature of each transmitted ABC based on the IdPs public key. The RP checks the status of the session at the Yivi server to either grant or reject access (A7).

B Mapping EUDI requirements to privacy properties

In this section, we map requirements of EUDI (the EUDI's requirement specification text and the requirement index), listed in annex 2 to our privacy properties (see section 3) if an requirement somehow relates to a specific property.

[21] See for a full description of Yivi's revocation protocol: `https://irma.app/docs/revocation`

Table 2: Mapping EUDI requirements to privacy properties.

Privacy property	**Relevant requirement specification**	**Requirement index**
PP1	A Wallet Unit SHALL support selective disclosure of attributes from PIDs and attestations to be released to the requesting Relying Parties.	OIA_07
PP2	A Wallet Unit SHALL enable a User to generate a Pseudonym and register it at a Relying Party. A Wallet Unit SHALL enable a User to authenticate with a Pseudonym towards a Relying Party.	PA_01, PA_02
PP3 & PP4 & PP5	A Wallet Unit SHALL support selective disclosure of attributes from PIDs and attestations to be released to the requesting Relying Parties.	OIA_07
PP6	An EUDI Wallet Instance SHALL verify and process PID or attestation presentation requests from Relying Parties in accordance with the protocols and interfaces specified in OpenID4VP for remote flows.	OIA_04
PP7	no specification found	
PP8	After verifying and processing a PID or attestation request, the Wallet Unit SHALL display to the User the identity of the requesting Relying Party and the requested attributes.	OIA_05
PP9	A Wallet Provider SHALL enable a User to access a dashboard functionality in their Wallet Unit.	DASH_01
PP10	The Wallet Provider SHALL request User consent (through the Wallet Instance) for all information and data it will process, both during activation and throughout the lifetime of the Wallet Unit	WIAM_05
PP11	A PID (personal identification data) Provider SHALL verify the identity of the EUDI Wallet User in compliance with Level of Assurance (LoA) High requirements.	ISSU_18