LEGAL BASES FOR THE USE AND OPERATION OF EUROPEAN DIGITAL IDENTITY WALLETS

By Niko Tsakalakis, Alessandro Ortalda

Contents

1 Introduction

eIDAS 2.0 introduces the concept of European Digital Identity (EUDI) Wallets as an additional means of performing electronic identifications when EU digital services require it. Since electronic identification is a form of processing of personal (identification) data, lawful processing must comply with the obligations under the GDPR. Digital services requesting electronic identification will justify their processing by the legal basis that is most appropriate for their processing purpose, e.g. a legal obligation for public-sector services or performance of a contract for private-sector services. However, this is distinct from the processing performed by the EUDI Wallet itself. Since the use of EUDI Wallets is optional, in addition to existing traditional and electronic identification means, their use will likely depend on the consent of the Wallet owner (i.e. the data subject). Consent, as the agreement of the data subject of the processing of their personal data, is therefore of paramount importance for the use of EUDI Wallets. At the same time, consent appears in eIDAS 2.0 and related documents to also signify user confirmation functions for security and transparency requirements. The two concepts are different, and they should be clearly distinguished into data subject consent and user confirmation requirements.

2 Processing of (personal) data in the eIDAS ecosystem

Electronic identities (eIDs) offer an alternative in cases where services require the verification of the identity of the service recipient, a process that traditionally was performed through physical inspection of identity documents. The aim of the identification process is, in essence, to verify that the recipient is entitled to the provided service. For example, that the recipient of a student discount is an active student in a participating institution; or, that the recipient of a jobseeker's allowance is currently unemployed. In the EU, several Member States have authorised eID schemes which are able to verify electronic attestations of individuals. Although there are variations in the architecture of eID schemes, typically a scheme will accept either a software eID means (i.e. a username/password combination, B.1.1 in Figure 1) or a hardware eID means (i.e. a token in an eID card, B.1.2 in Figure 1). Digital services that require verification of an attribute will request access to the eID means, via the browser in the user's personal device or through a physical terminal.

eIDAS 2.0 introduces an additional way to use eID means. The addition of the EUDI wallet (B.2 in Figure 1) combines elements of hub-and-spoke systems[1] (with the EUDI wallet mediating communications between eID schemes and relying parties) and elements of the self-sovereign identity movement[2] (with the EUDI wallet conferring more control of the eIDs to the user).

[1] See for example the architecture of UK's 'Gov.UK Verify' system: Identity Assurance Team, Identity Assurance Documentation: Release (2015) available at: <http://docplayer.net/21642604-Identity-assurance-documentation.html> accessed 24 May 2022, pp. 7–9.

[2] See Andrew Tobin and Drummond Reed, The Inevitable Rise of Self-Sovereign Identity (whitepaper, updated 28th March 2017) available at: <https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf> accessed 23 May 2022, pp. 8 – 10.

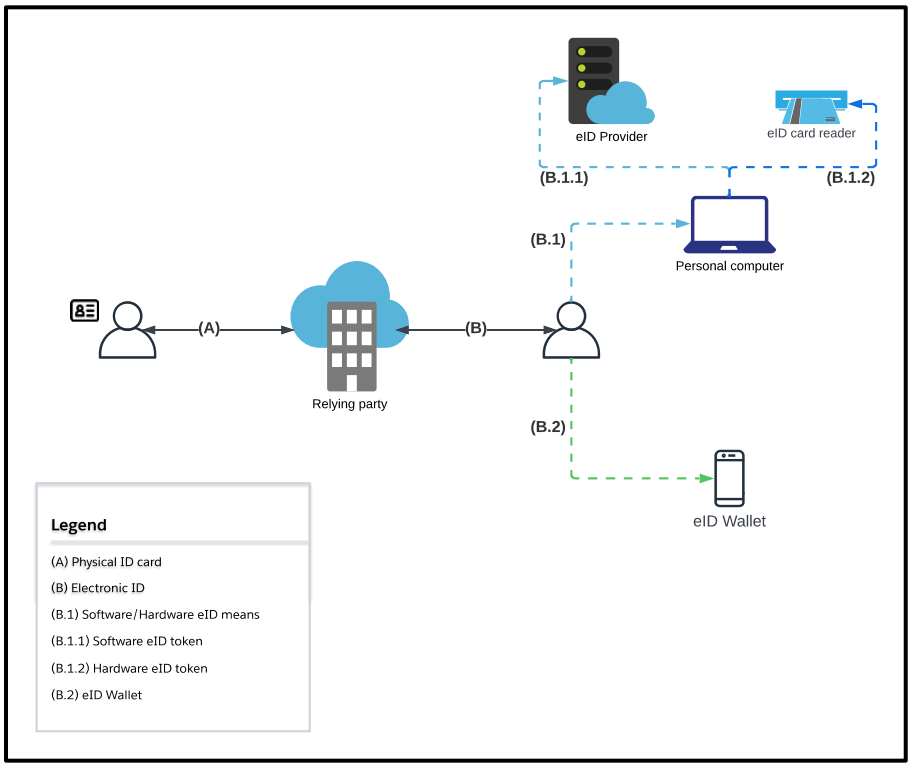

Figure 1: Identification options

Although several components are involved in a browser-based, a card-reader-based or a wallet-based electronic identification, this analysis focuses only on the processing of identification data. In the EUDI Wallet, these data are represented by the pink circle in Figure 2, but equivalent also exist in browser-based or card-reader based eID means.[3] (Person) identification data are "a set of data enabling the identity of a natural or legal person [...] to be established".[4] Evidently, identification data about a natural person are personal data, under GDPR Article 4(1).[5] As a result, services that wish to perform any type of electronic identification will have to comply with the obligations under the GDPR and especially the conditions for lawful processing of personal data. As eIDAS and eIDAS 2.0 are silent about the lawfulness of processing, the answer should be sought through consideration of the processing purposes and the legal bases available within the eIDAS ecosystem.

[3] See A.1 in ANNEX A.

[4] 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 [2014] OJ L257/73 (hereinafter eIDAS) art 3(3).

[5] GDPR art 4(1): *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

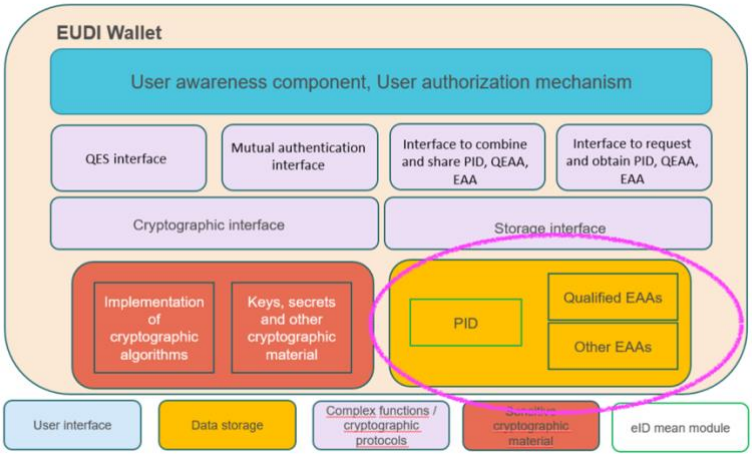

Figure 2: The components of the EUDI Wallet

3 Lawfulness of personal data processing

Lawful processing of personal data can be justified only against one of the six legal bases of Article 6(1) of the GDPR.[6] Data controllers will also have to adhere to the purpose limitation principle and process data only for "*specified, explicit and legitimate purposes*",[7] unless processing is permissible under a compatible purpose that satisfies the test of GDPR Article 6(4).

In an electronic identification, several stakeholders are expected to process identification data either as a data controller or a data processor. The main actors typically processing identification data in their role as a data controller are parties that issue and operate the eID means, as well as the relying parties offering the digital services which require electronic identification.[8]

Legal bases and processing purposes will differ, depending on the role of the stakeholder in the electronic identification process. The processing purpose of the relying parties will relate to their services: the public-sector body responsible to grant jobseeker's allowances will require an electronic identification to verify that applicants are enrolled as unemployed and have not exceeded any maximum terms for eligibility; a private-sector body offering social media services will require an electronic identification to verify that the applicant is an actual human and to personalise their experience in the platform. Compatible purposes, other than the main purpose, may relate to necessary performance metrics for troubleshooting or usage statistics for resource allocation planning.

Choosing the appropriate legal basis will depend on the processing purpose. Conversely, the provision of unemployment benefits will likely determine as appropriate legal basis the compliance with a legal obligation, whereas the provision of personalised social media services will likely rely on user consent or the performance of a contract. Evidently certain caveats exist when choosing an appropriate legal basis: it is unlikely that a public authority or a controller in a position of power

[6] In summary: consent; performance of a contract; compliance with a legal obligation; vital interests of the data subject; performance of a task carried out in the public interest; legitimate interests of the controller.
[7] GDPR art 5(1)(b).
[8] For a list of all possible stakeholders see A.2 in ANNEX A.

will be able to justify processing based on user consent for the provision of a public service,[9] but may be able to justify consent for optional personalisation features or usage analytics.

It is important to note that different stakeholders in the same transaction will operate under different processing purposes and legal bases. For example, where a user selects one of multiple eID providers to access an age-restricted casino, the casino may be required to verify that the user is of legal age under a legal obligation, but the operator of the eID scheme will process data for the performance of a contract between the operator and the user. A full list of processing purposes and legal bases can be found in ANNEX B. This distinction is important in cases where multiple roles are conflated, like in the EUDI Wallet. The use of the EUDI Wallet as an eID means should be distinguished from the use of the eIDs that are stored in it. Although the use of an eID as a precondition to access a service might rely on a legal obligation, the use of the EUDI Wallet as a means to access the eID in question shall rely on consent. This seems likely since the EUDI Wallet is but one available option in performing the necessary identification. In other words, the use of the EUDI Wallet is – and should remain – optional, since the necessary precondition, aka the identification, could be performed in a browser or via physical presence.

4 Potential issues of the current approach

Two issues are arising by the current drafts of eIDAS 2.0 and the European Digital Identity Architecture and Reference Framework (ARF).[10] As it has already been mentioned, eIDAS 2.0 is silent as to any potential legal bases, including consent. Presumably this is intentional to allow freedom to the respective relying parties and eID services when determining which legal basis most closely reflects the true nature of their relationship with the individual.

One has to do with the formulation of consent. The ARF does contain references to user consent when discussing aspects of the EUDI Wallets. However, the ARF seems to prescribe a different meaning to the notion to that of informed consent under the GDPR.[11] Whereas consent under the GDPR has a very specific formulation[12] and can justify processing of personal data where no other legal basis obviously applies,[13] the ARF refers to consent in the context of the user awareness and the user authorization components.[14] In fact, the use of consent in the ARF more closely resembles the concept of 'user confirmation'. The ARF conditions the successful occurrence of certain processes to an explicit indication by the user that they wish for this process to be carried out.[15] This is different to an individual consenting to the processing of certain data for a specific purpose

[9] See EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, v 1.1, adopted on 4 May 2020, p. 8.
[10] European Digital Identity Architecture and Reference Framework – Outline, (22 February 2022).
[11] GDPR art 7.
[12] "*freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*" GDPR art 4(11).
[13] Or where special categories of data are to be processed, where explicit consent is required: see GDPR art 9(2)(a).
[14] ARF ss 4.6.1 and 4.6.2.
[15] See ARF fn. 29: "*the informed willingness of the user to carry on an operation, such as performing an electronic identification, performing a qualified electronic signature, sharing attributes*".

and more akin to the checks that the security of the system has not been compromised, e.g. by man-in-the-middle attacks. User confirmation is an important security check,[16] but also strengthens the transparency information provided to the individual. User empowerment through transparency notifications is, after all, one of the tenets of the user-centric systems[17] that would later evolve to the concept of 'self-sovereign identity'. The provision of specific requirements for user confirmation is, therefore, welcome but it is unfortunate that this term is not separated from the term of consent as a legitimising legal basis for lawful processing under the GDPR. It would be useful if the term 'user confirmation' was instead used, making it clear where the requirement is for a confirmation dialog for security or transparency purposes.

The second issue, which is related, has to do with the silence in both eIDAS 2.0 and the ARF precisely on consent as a legal basis. As explained, the use of the EUDI Wallets will be optional, and in addition to physical identification processes and pre-existing eID processes. EUDI Wallets will likely depend on data subject consent to download, store, combine and transmit eID data. The consent must satisfy the requirements under the GDPR, i.e. to be free, specific, informed and unambiguously given. Clear instructions about valid consent are currently absent. Article 6a, which hints at user consent for compatible purposes, limits the requirement to an express request of the user. The ARF echoes the same wording, in its functional and non-functional requirements.[18] Both run the danger to allow data controllers to bury user consent inside the general terms and conditions, rendering the control that the user is supposed to exert meaningless. Instead, consent should be viewed as an integral part for GDPR compliance. eIDAS 2.0 should include an explicit mention to the requirement of a positive, active action by the user to a specific, informed, and unambiguous consent prompt. Similar changes should be mirrored to the wording of the ARF.

5 Proposed solutions to the identified issues

Text as proposed	Amendment (in **bold**)
6a.4.a (4) for the user to allow interaction with the European Digital Identity Wallet and display an "EU Digital Identity Wallet Trust Mark";	6a.4.a (4) for the user to **actively** allow interaction with the European Digital Identity Wallet and display an "EU Digital Identity Wallet Trust Mark";
6a.6 The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'. The use of the European Digital Identity	6a.6 The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'. The use of the European Digital Identity

[16] See Eric Verheul, Some observations and questions on the European Digital Identity Architecture and Reference Framework (28 February 2022), available at < https://www.cs.ru.nl/E.Verheul/papers/eIDAS/Some%20observations%20and%20questions%20on%20the%20eIDAS%20wallet%20ARF.pdf>, point 4.

[17] See Lee A Bygrave, "Hardwiring Privacy" in Roger Brownsword, Eloise Scotford, and Karen Yeung, The Oxford Handbook of the Law and Regulation of Technology (Roger Brownsword, Eloise Scotford, and Karen Yeung eds, Oxford University Press 2017), pp. 4–5.

[18] See ARF in pp. 18, 21, 25.

Wallets shall be free of charge to natural persons.	Wallets shall be optional to natural persons and provided free of charge.
6a.7 The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.	6a.7 The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly and actively requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.

Table 1: Proposed amendments to the text of eIDAS2.0

6 Conclusions

The adoption and use of EUDI wallet involve processing of personal data. As such, the adoption and use should comply with the rules set by EU law on data protection, especially the GDPR. Processing of personal data by the EUDI wallet should only be allowed for specified purposes under appropriate legal bases.

The issue of legal bases concerns two aspects. The first aspect is about the provision of the EUDI wallet to users. Such a provision is not mandatory and, as such, users can freely decide if they want to have an EUDI wallet. Thus, the provision of EUDI wallets seems conceptually tailored for the legal basis of consent. The second aspect is about the use of electronic identification. There are cases where such use cannot be justified by consent, such as in the delivery of public services.

Notwithstanding, the current draft of eIDAS 2.0 is silent on how the legal bases under the GDPR relate to the digital identity framework and, specifically, to the new concept of the EUDI wallet. The supporting ARF touches briefly on this aspect by mention of user consent. However, consent under the ARF is conceptually different to the term in the GDPR. The two aspects above should be reflected in the final version of eIDAS 2.0 to clarify compliance with the GDPR.

7 References

Andrew Tobin and Drummond Reed, The Inevitable Rise of Self-Sovereign Identity (whitepaper, updated 28th March 2017) available at: <https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf> accessed 23 May 2022

EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, v 1.1, adopted on 4 May 2020

Eric Verheul, Some observations and questions on the European Digital Identity Architecture and Reference Framework (28 February 2022), available at < https://www.cs.ru.nl/E.Verheul/papers/eIDAS/Some%20observations%20and%20questions%20on%20the%20eIDAS%20wallet%20ARF.pdf>

European Digital Identity Architecture and Reference Framework – Outline, (22 February 2022)

Identity Assurance Team, Identity Assurance Documentation: Release (2015) available at: <http://docplayer.net/21642604-Identity-assurance-documentation.html> accessed 24 May 2022

Lee A Bygrave, "Hardwiring Privacy" in Roger Brownsword, Eloise Scotford, and Karen Yeung, The Oxford Handbook of the Law and Regulation of Technology (Roger Brownsword, Eloise Scotford, and Karen Yeung eds, Oxford University Press 2017)

A ANNEX: EUDI Wallet data elements and actors

A.1 Data elements

The data elements in scope are only data that can be considered personal data under the GDPR

- PID
- Qualified attestations
- Other attestations
- Use metrics/analytics – EUDI wallets will likely need to capture some form of data to monitor operation/plan updates/troubleshoot

A.2 Actors

The actors in scope are only the stakeholders whose involvement is necessary for the provision of electronic identification and authentication

- Official ID issuers
- multiple issuers of identity information (eID providers)
- attestation provider
- wallet provider
- supervisory authority
- conformity assessment body
- relying parties

A.3 Data flows

Data flows are grouped by actor for simplicity. The distinction is necessary to determine the processing purposes and legal bases

1. Wallet provider
    a. Wallet provider ←→ User
    b. Wallet provider ←→ Conformity assessment body
    c. Wallet provider ←→ Supervisory authority
    d. [optional] Wallet provider ←→ Cloud storage service
    e. [optional] Wallet provider ←→ Analytics/metrics analysis service
2. ID issuer
    a. ID issuer ←→ eID provider
    b. ID issuer ←→ Supervisory authority
3. eID provider
    a. eID provider ←→ User
    b. eID provider ←→ Relying party[19]
    c. eID provider ←→ Supervisory authority
    d. [optional] eID provider ←→ conformity assessment body
    e. [optional] eID provider ←→ Cloud storage service
    f. [optional] eID provider ←→ Analytics/metrics analysis service
4. Attestation provider
    a. Attestation provider ←→ User
    b. Attestation provider ←→ Relying party
    c. Attestation provider ←→ Supervisory authority
    d. [optional] Attestation provider ←→ Conformity assessment body
    e. [optional] Attestation provider ←→ Cloud service
    f. [optional] Attestation provider ←→ Analytics/metrics analysis service
5. Relying party
    a. Relying party ←→ User
    b. Relying party ←→ Supervisory authority
    c. [optional] Relying party ←→ Conformity assessment body
    d. [optional] Relying party ←→ Analytics/metrics analysis service

B ANNEX: EUDI Wallet purposes and legal bases

Each data flow identified in ANNEX A.3 must serve a distinct processing purpose and must be justified by a legal basis. Data flows can be grouped under three categories: (1) Use of EUDI Wallet; (2) Use of eID/attestation; and, (3) Performance monitoring of EUDI Wallet/eIDs

[19] "Without prejudice to the actual mechanism how the information is provided, including whether directly or indirectly" ARF p. 10.

B.1 Use of EUDI Wallets

Dataflow	Processing purpose	Legal basis	Justification
1a	Downloading the application; registering eIDs/attestations in the Wallet	Performance of a contract	Although the use of of the Wallet is voluntary, the provider will likely be in a contractual relationship with the user to offer them Wallet services
1a	Using the application	Consent	The use of the Wallet is voluntary; alternatives exist (use of eID, use of physical ID)
1d	Storing eID/attestations in the cloud	Consent	Storing in a cloud provider is likely to be voluntary; mandatory saving of eIDs in the cloud will be hard to justify since options to store locally or to not store at all can be available
5a	Receiving eID/attestations from the Wallet	Consent	The use of the Wallet to transmit eIDs is voluntary. This process should be distinguished from any mandatory obligations to authenticate against a service, since authentication can be performed through alternative means (eID scheme; physical presence)

B.2 Use of eID / attestations

Dataflow	Processing purpose	Legal basis	Justification
2a	Provision of authentic sources for creation of an eID	Compliance with legal obligation	The ID issuer of the member state will likely be under an obligation from national law to provide authentic data for the creation of an eID; ID issuer and eID provider may be the same entity in some Member States
3a; 4a	Downloading eID/attestations to the Wallet	Consent	The use of the Wallet is voluntary; therefore loading eIDs in the Wallet will have to be anchored to the user's consent
5a	Transmitting eID/attestations to relying parties	Consent OR	Several legal bases are available here; the suitability will be determined by the relying party in question (e.g. public sector relying parties are unlikely to be

		Legal obligation OR Performance of a contract	able to justify consent; legal obligation might be available if absence of alternatives (i.e. physical presence) can be justified)
3b; 4b	Transmitting eIDs/attestations to relying parties (directly from providers)	Legal obligation OR Performance of a contract	The legal basis will be determined by the national eID scheme in place. In schemes with multiple providers, performance of a contract may be used. Where there is only one provider, it will most likely fall under legal obligation. Consent cannot be justified without viable alternatives.
3e; 4e	Using cloud storage for processing	Performance of a contract	For providers that use cloud services, cloud services will be contracted as data processors under an agreement

B.3 Performance monitoring

Dataflow	Processing purpose	Legal basis	Justification
1b; 3d; 4d; 5c	Monitoring the conformity of the Wallet/scheme/eIDs	Legal obligation	The conformity bodies might need periodic access to operation data to monitor conformity; depending on details some of the data may be personal data
1c; 2b; 3c; 4c; 5b	Supervisor monitoring the operation of the Wallet/scheme/eID	Legal obligation	The supervisor will need periodic access to operation data some of which may be personal data
1e; 3f; 4f; 5d	Providers monitoring the operation of wallet/scheme/eID to troubleshoot or to plan	Legitimate interest	Providers will likely need to gather analytics for troubleshooting and planning purposes, some of which may be personal data