verbraucherzentrale
Bundesverband

Defendo IT GmbH | Mauerweg 7 | 66133 Saarbrücken

REPORT ON THE ARCHITECTURE OF THE EUDI-WALLET

File number 2024-0393

22. November 2024

Prepared on behalf of the

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

Rudi-Dutschke-Straße 17
10969 Berlin

Gefördert durch:

Bundesministerium
für Umwelt, Naturschutz, nukleare Sicherheit
und Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

With the revision of the eIDAS regulation in 2024, the European Union has laid the groundwork for the development and deployment of European Digital Identity (EUDI-)Wallets. These software-based credential storages shall be usable across the EU in order to securely and reliably identify online and offline. Users of EUDI-Wallets shall be able to authenticate each other and login to public as well as private services.

As with all new technology, EUDI-Wallets are not free of concerns. The regulation leaves room for different models of provision, introduces new rules for liability and aims to achieve interoperability across all EU Member States; all while satisfying user expectations, fulfilling security properties and preserving the privacy of wallet users.

This report aims to give an overview of the current state of the specification and development of EUDI-Wallets, particularly in the context of Germany. It provides background information and answers to 42 concrete questions which concern the protection of consumer's rights and interests. The major findings and conclusions of the report can be summarized as follows:

A combination of public and private developers is likely to achieve the best quality of EUDI-Wallet implementations. This is the path Germany is currently following.

Competition between actors within the EUDI-Wallet ecosystem needs to be carefully monitored and controlled within the boundaries set by the eIDAS regulation. The creation and stabilisation of monopolies poses a significant threat to consumer's rights and interests.

Failure to comply with contractual or legal obligations results in liability for any party participating in the EUDI-Wallet ecosystem. No liability loopholes can be identified at this point.

Interoperability is a fundamental principle of the specification and development process. The standards currently in development are able to provide the necessary standardisation, so that interoperability can be achieved.

The principles of data security and privacy have been incorporated into the specification and development process. However, the current specification falls short on its potential for both security and the preservation of privacy. It needs to undergo a major revision before all desired properties can be achieved.

The supervision and enforcement of compliance to data protection and IT security legislation is governed by designated authorities. Their performance, the success of their cooperation and the ability to adequately protect consumer's interests and rights can only be evaluated in practice and once the deployment of EUDI-Wallets is complete.

Despite valid criticism, the EUDI-Wallet has the potential to greatly enhance comfort and security in the digital world.

2. THE AUTHORS

This report has been prepared by the Defendo IT GmbH on behalf of the Verbraucherzentrale Bundesverband e.V. The following authors have contributed to the report. The order of the authors is alphabetic by last name and no indication of the individual contribution.

Maximilian Eichacker, B.Sc., is a freelance consultant at Defendo IT and researcher at the Saarbrücken Research Centre for Law and Digitalization (Saarbrücker Zentrum für Recht und Digitalisierung – ZRD Saar). He holds a B.Sc. in business economics and has recently completed his Master's degree.

Ajla Hajric, B.Sc., is a freelance consultant at Defendo IT and researcher at the Saarbrücken Research Centre for Law and Digitalization. She holds a B.Sc. in economics and law has recently completed the first state exam in law.

Dipl.-Jur. Theresa Moll is a freelance consultant at Defendo IT and researcher at the Saarbrücken Research Centre for Law and Digitalization. She has recently passed the second state exam in law.

Dr. rer. nat. Frederik Möllers, LL.M., is the founder and CEO of Defendo IT. He is also the Deputy CEO of the Saarbrücken Research Centre for Law and Digitalization. He holds a Ph.D. in computer science as well as an LL.M. in IT & Law from Saarland University.

Dr. jur. Stephanie Vogelgesang, LL.M., is a freelance consultant at Defendo IT and the CEO of the Saarbrücken Research Centre for Law and Digitalization. She holds a Ph.D. in law and an LL.M. in IT & Law from Saarland University.

3. BACKGROUND AND INTRODUCTION

The digitalization of our daily lives and of society as a whole is constantly growing. Electronic devices have long found their permanent place in everyday tasks and their assistance has become so natural that many interactions or processes are unimaginable without their help. Accessing bank accounts, registering for services and ordering goods happens mostly online and often without any physical interaction between the involved parties.

The usage and presentation of official documents such as IDs, drivers' licences or certificates has lagged behind this trend for several years. This created a discrepancy between the rising use of online services and the missing possibilities of thorough authentication and (identity) verification. This discrepancy – though not alone – facilitated the rise of online fraud, identity theft and other abuses.

In 2010, the German government introduced the electronic identity card, an official identification document which can be scanned electronically, and which supports the authentication of its owner using a computer or phone. The card also supports the creation of Qualified Electronic Signatures (QESs) – digital signatures which are legally equivalent to their hand-written counterparts. The technology however never found wide acceptance in the private economic sector and as of today is used and accepted by only few service providers.

With the revision of the eIDAS directive in 2024 (also known as "eIDAS 2.0") the EU launched an initiative to close this discrepancy and to offer its citizens a unified, usable and modern possibility for authentication. The European Digital Identity Wallet (EUDI-Wallet) is intended to have the same comfort as existing solutions from the private sector – such as credit cards stored and available on mobile phones or smartwatches – while offering the same level of reliability and legal acceptance as official (previously mostly paper- or card-based) documents.

3.1. WHAT IS THE EUDI-WALLET?

The EUDI-Wallet is a secure storage for official documents, certificates and similar data.[30] According to the current state of specification, it will take the form of a smartphone app and will offer functionalities, among others, for the following use cases [4]:

- Present Personal Identification Data (PID), e.g. at border controls or to other users of a wallet
- Present Electronic Attestations of Attributes (EAAs), e.g. a diploma or a driver's license
- Sign documents in a legally binding manner by applying a QES
- Login to online services while presenting certain data/attributes to the provider, similar to "Login with Apple/Microsoft/Google/…"

A full list of features offered by the EUDI-Wallet can be found in Art. 5a Par. 4 eIDAS.

The German government has recently decided to provide a reference implementation but to allow private actors to develop and publish their own implementations following the necessary standards.[5] The goal is to have multiple options for consumers to choose from.

3.2. WHAT IS THE RELEVANCE FOR GERMAN CONSUMERS?

According to Art. 5a Par. 15 eIDAS, the EUDI-Wallet is optional for consumers. In consequence, the introduction does not impose a change in behaviour on the consumers. However, an increase in usability compared to traditional methods of identification and authentication is likely to result in a wide adoption of this new technology. If the implementation meets the expectations of the initiators and of the general public, the EUDI-Wallet has the potential to significantly change the way identification data is exchanged and verified. Aside from these advantages in usability and speed, there are also risks. These are described in the following sections.

3.3. ORGANISATIONAL REMARKS

This report aims to answer a catalogue of questions regarding risks and opportunities for consumers with respect the EUDI-Wallet. The questions have been proposed by the Verbraucherzentrale Bundesverband and have been answered to the best of the authors' knowledge. The state of information used for the report is the 22 November 2024. URLs referenced in this report have been checked on this date as well.

While an assessment of the regulation, the specification and the corresponding technology is inherently subjective, the authors have worked towards a neutral point of view with a focus on consumer's perspectives and consumer protection. The authors have not been involved in the development or specification of the EUDI-Wallet ecosystem.

The report follows the common citation style for German legislation. This is different from the way legislation is cited e.g. within eIDAS. However, it allows for a common style across the complete report, regardless of whether a reference points to German or EU legislation.

The authors would like to thank the German Informatics Society (Gesellschaft für Informatik e.V. – GI) for facilitating the exchange with experts. Quotes from experts of the GI have been incorporated in the report and have been visually highlighted.

3.4. TIMELINE TOWARDS THE EUDI-WALLET

Figure 1 illustrates the timeline towards the deployment of the EUDI-Wallet and highlights major milestones and important dates along the path.

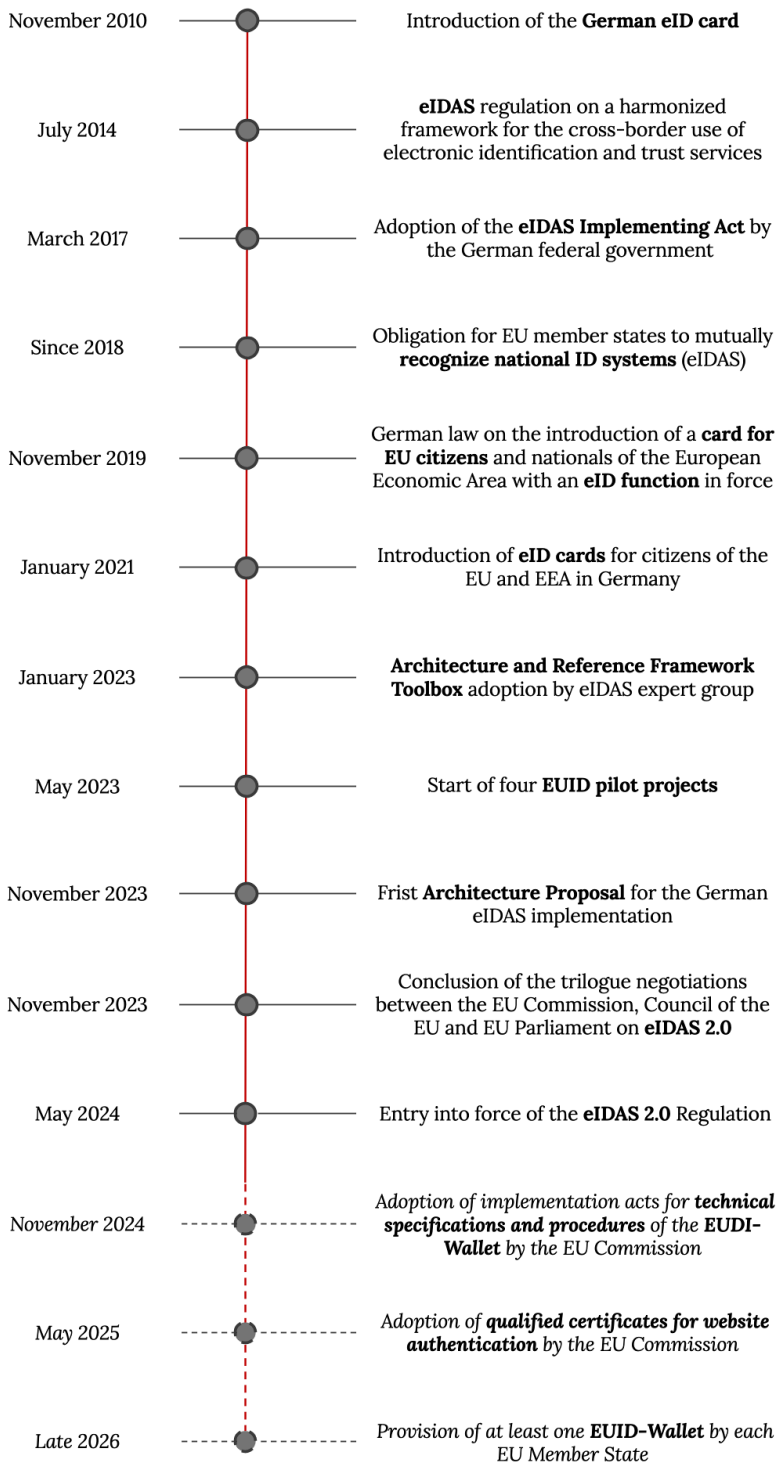

Figure 1: Important dates and milestones on the path towards the deployment of the EUDI-Wallet.

3.5. LIST OF ABBREVIATIONS FOR LEGISLATION

Throughout this report, different European and German legislation is referenced. For the sake of readability, the following abbreviations have been used instead of the full names. Unless explicitly stated otherwise, the names always reference the latest available version of the legislation.

Abbreviation	Full Name
BDSG	German Federal Data Protection Act (“Bundesdatenschutzgesetz”)
BGB	German Civil Code (“Bürgerliches Gesetzbuch”)
DA	“Data Act”: Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)
DGA	“Data Governance Act”: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)
EHDS	“European Health Data Space”: Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, published on 3 May 2022
eIDAS	“eIDAS regulation”: 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; most recently amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
ePD	“ePrivacy Directive”: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); most recently amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
GDPR	“General Data Protection Regulation”: Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection if natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC most recently corrected by corrigendum to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
NIS2	“NIS2 Directive”: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a

	high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 most recently corrected by corrigendum to Directive (EU) 2022/2555 of the European parliament and of the Council of 14 December 2022 of measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
SDGR	"Single Digital Gateway Regulation": Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012; most recently amended by Regulation (EU) 2024/1735 of the European Parliament and of the Council of 13 June 2024 on establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ecosystem and amending Regulation (EU) 2018/1724
VDG	German Trust Services Act ("Vertrauensdienstegesetz")
VwVfG	German Administration Processing Act ("Verwaltungsverfahrensgesetz")

Table 1: Abbreviations for legislation used in this report

4.ISSUER/PUBLISHER OF THE WALLET

4.1. PILOTING THE EUDI-WALLET

Pilot projects are already looking at different options for the implementation of the EUDI-Wallet. The respective consortia are taking different approaches and offering different functionalities within the wallet. One example is the “EU Digital Identity Wallet Consortium”. The focus of this project is to provide digital travel documents as an initial use case, with the aim of providing citizens of EU member states with a digital ID when traveling within the EU. Another goal is to expand the application to include payment options, on one hand in the form of NFC payments with mobile devices, and on the other hand through the authentication of payments made. The consortium consists of different partners from several EU member states, partners from non-EU countries, and includes stakeholders from both private and public sectors.[1]

Another pilot project is the Digital Identity Wallet. Here, too, the consortium named “Potential” consists of representatives from 19 EU member states and over 140 public and private partners. The focus is on six use cases that are designed to enable digital authentication for users for various services. These include the use of e-government services, the cross-border opening of bank accounts, the registration of SIM cards and the creation of Electronic Signatures. In addition, a valid digital driver's license shall be retrievable in the application and pan-European access to medication prescriptions shall be enabled.[2]

The “DC4EU” (Digital Credentials for European Union) project is also working on the piloting of initial approaches to an EUDI-Wallet. In this context, the areas of digital educational certificates for school-based and post-school qualifications as well as aspects related to social security are being considered first. The focus here is on testing the interoperability of the system with individual government applications and processes as well as cross-border cooperation. The consortium consists of various organizations from 19 EU member states together with Norway, the Ukraine and Switzerland.[3]

4.2. VERIMI – AN EXISTING GERMAN APPROACH

In Germany, too, digital wallets are already available. One example is the “Verimi ID-Wallet”. Verimi is a payment institution supervised by the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) and licensed under the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz, ZAG). With this application, citizens who are in possession of an eID (“Personalausweis”, “Aufenthaltstitel” etc.) can store various forms of proof of identity, including their driver's license and passport, in the app and use them for identification and authentication with various partners using the online ID function. However, the focus here is on identification for private-sector companies that require proof of identity for the use of the corresponding services, such as car rental, the conclusion of mobile phone contracts or banking transactions.[4]

[1] https://eudiwalletconsortium.org/

[2] https://www.digital-identity-wallet.eu/

[3] https://www.dc4eu.eu/

[4] https://www.personalausweisportal.de/SharedDocs/anwendungen/Webs/PA/DE/Unternehmen/verimi_wallet.html

4.3. EXISTING WALLET SOLUTIONS WITHIN THE EU

Question: What variants exist in other member states?

4.3.1. Estonia

Within the EU, Estonia takes a leading role in the digitalisation of its administration. Every Estonian citizen receives a digital identity, the eID, which enables them to reliably identify themselves to various private and public providers. The eID offers the possibility of identification using a chip within a regular ID card. In addition, there is the so-called Mobile ID, for which a specific SIM card can be requested from the respective mobile phone operator. The SIM card, in combination with private keys stored on it, can act as an authentication medium. The third option is the Smart ID, which, similar to the Mobile ID, can be used on a smartphone. For the Smart ID, authentication is not done via the SIM card but via the use of an app. Estonian citizens can use these various digital authentication options for a range of purposes, including traveling, as a health insurance card (e.g. for e-prescriptions or viewing medical records), for banking transactions, for the electronic voting system or for tax matters.[5] The infrastructure behind this is the result of collaboration between government agencies and private-sector issuers such as Cybernetica, Raul Walter, and SK ID Solutions.

4.3.2. Sweden

Sweden offers the BankID system to its citizens. To use this digital authentication option, users need a Swedish personal identification number and must be a customer of one of the ten banks offering the service. After receiving a BankID, users are able to register with a wide range of providers and use their services. The functionalities are not limited to state affairs. BankID is also offered for the private use of websites as a replacement for login data and enables the digital signing of documents. An implementation of the ID function using the BankID app is planned. The aim is to be able to access the driver's license and ID card digitally. However, among other things, the release by the responsible police authorities is still awaited, as they still have to agree to this possibility.[6] The example of Sweden also shows that public authorities are working closely with private-sector providers to implement a reliable and trustworthy identification and authentication process, with the public authorities providing the platform for this and the private-sector providers also integrating their own services into the processes.

4.3.3. Belgium

The widely used app for digital identification in Belgium is “itsme”. This is a system offered purely by the private sector which can be used by any Belgian with an eID or a Belgian bank account. Belgian Mobile ID, a consortium of banks and mobile network providers, is the issuer of this system. On one hand, the use of “itsme” enables a central login with private providers using an individual PIN and eliminates the need to enter account access information.[7] On the other hand, “itsme” can also be used for authentication to digital government services. The underlying procedure remains the same. Many official activities which require identity verification offer the option

[5] https://e-estonia.com/solutions/

[6] https://www.bankid.com/en/

[7] https://www.itsme-id.com/de-DE

of registering in the government portal using the “itsme app” and thus identifying themselves in advance.[27]

4.3.4. Italy

In Italy, SPID – the Public System of Digital Identity – can be used for identification by both government agencies and private-sector providers. Italian ID documents are used for this purpose, by means of which users can register with a private-sector “digital identity manager”. Different identification providers also use different software tools for different end devices. The user is then verified and can use the service. It is also possible to identify and activate SPID at public administration offices.[8] SPID can then be used as an access key for both participating companies and public administration services. It is further possible to link SPID to health and social insurance services.[14] A three-tier security system is used, which, depending on the type of identification to be carried out, must meet various security requirements regarding the authentication.[27]

4.3.5. Other countries and publishers

Hemesath and Gerrits have performed a comparison of electronic identification solutions across different countries in 2023.[14]

Country	Publisher
Belgium (itsme)	Private Sector
Estonia (Smart ID, Mobile ID, eID)	Public- and Private Sector
Netherlands (DigID)	Public- and Private Sector
Italy (SPID)	Public- and Private Sector
Sweden (BankID)	Public- and Private Sector
France (France Connect)	Public Sector
Germany (eID Card)	Public Sector
Austria (Mobile Signature)	Public Sector
Poland (Profil Zaufany)	Public Sector

Table 2: Countries using eID systems and mode of operation for those systems

Conclusion: Wallet solutions with different functionalities and different issuer structures are already in use in various European countries. In some cases – particularly those with a high level of acceptance and use among the population – public and private institutions are working together. In such cases, state actors often provide the basis for the wallet, using official proof in combination with a framework of regulations, while downstream processes and specific processing are located in the private sector.

4.4. ISSUER OF THE WALLET

Question: Who should provide the wallet: the state, private actors, or the state and private actors in cooperation?

[8] https://www.spid.gov.it/en/

Conclusion: In principle, there is no blueprint for the implementation of a cross-border digital wallet that also offers a variety of identification and authentication options. As a result, a range of solutions with different focuses and diversified publisher and operator constellations are currently being piloted, tested or have already been in use for some time. All of the current approaches have advantages and disadvantages. However, the option of state and private actors working together to tackle publication, pooling their respective skills and experiences, offers the most promising results. This can also be seen in the successfully operating cooperative publishing structures in Estonia and Sweden.

Question: What are the advantages and disadvantages of each option?

4.4.1. Private Sector

Purely private-sector solutions for digital ID wallets have not yet been able to achieve widespread acceptance. When it comes to the monetary specifications for an EUDI-wallet, namely that private users in a private context should be able to access such an application free of charge (cf. Art. 5a Par. 13 eIDAS), this trend could possibly continue with a wallet released purely by the private sector. One potential reason is that the possible revenues for companies do not outweigh the regulatory and organizational effort and the associated costs. Alternative financing options, such as charging fees to participating companies, will only become profitable once the product is established on the market and user demand for such a possibility encourages companies to cooperate with wallet providers. It remains to be seen whether the necessary market acceptance can be achieved by a private-sector wallet and whether it will remain sustainable. Nevertheless, such a solution can represent a considerable saving of resources for participating companies by eliminating time-consuming customer identification processes, particularly in the banking and insurance sectors.[21]

Another obstacle is the security levels prescribed in the eIDAS. A distinction is made here between three different “Levels of Assurance” – low, substantial and high. Although it is possible for companies to create proofs of identity for users, in order to achieve the level “high”, an official public eID is generally required in Germany. This raises the question of which security level is required for which use cases. If, due to regulatory requirements, “high” security levels are always required for a large number of use cases, the implementation costs could outweigh the benefits for the private sector. In countries such as Norway or Italy, however, privately issued identities are also permitted for official use cases.[12] At the same time, aspects such as data protection or data security are very important, especially for German citizens (cf. Sections 8 and 9). It is therefore questionable whether citizens' trust in private companies is sufficient to use the services of such a digital wallet in all areas of life, as planned.

4.4.2. Public Sector

In a scenario with an EUDI-Wallet purely developed by a public actor, the question arises as to whether all functionalities requested and desired by the users can be implemented. In addition, similar to other EU states, interfaces to often private-sector actors need to be established and maintained. A common perception is that public digitalisation projects are often subject to over-regulation and do not meet expectations on usability. Private-sector actors are can often provide more experience and expertise and are therefore more likely to meet customer expectations.[9]

[9] https://www.gi-de.com/en/spotlight/trends-insights/eu-digital-id-wallet-10-things-to-know#c96359

Past examples show that public projects have often fallen short of expectations.[14] For example, the barriers for embedding the German eID into the authentication process of a web application have been too high for it to gain widespread use. The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), however, has recently launched a project to lower these barriers and to encourage use of the eID.[10] State-provided wallets used throughout everyday life are also likely to suffer in part from citizen's fear of state surveillance. While this might limit acceptance, substantial concerns have not yet been raised in this regard.

> In the BSI project, separate login apps need to be installed for each of the relevant systems. These login apps use the eID technology but lead to a proliferation of login apps for each individual service, while the concept of eID should support reducing the separate logins.
>
> *GI Fachgruppe Management von Informationssicherheit*

4.4.3.Public- and Private Sector

Due to the complexity of the project and the multitude of tasks, such as ensuring data protection and data security, user-friendliness and interoperability at both the federal and EU level, a collaboration between the state and the private sector in the creation and publication of the application is conceivable. In the event of a government initiative, it is necessary that the state directly involves the private sector and the free market in the process in order to dispel concerns regarding state surveillance or overregulation. Simultaneously, concerns regarding corporate surveillance and missing data protection need to be taken into account. Finally, the expertise of the private sector for a functional, user-friendly solution needs to be leveraged so that the digital wallet can also be sustainably deployed in the population.[11] Particularly Estonia and Sweden, with their cooperative solution, show how the interaction can work and how the strengths of both approaches can be combined. This requires an overarching governance model, which the state provides. In doing so, technical and regulatory interoperability at the national and European level is ensured. At the same time, the focus must be on the applicability and usability of the functions. This can only be achieved if, from the very beginning, widely available and relevant use cases are included that are aimed at the needs of users and enable individual use of data management and authorization.[28] As described in printed matter 20/13075[12], an uncertified preliminary version of a digital wallet is to be released first, which is limited to the identification of natural persons. The full range of functions, such as the storage of driving licenses, university certificates or signatures, is only to be achieved in the next steps and after the eIDAS implementing acts have entered into force. It can be concluded from this that a wallet issued purely by the state is initially being considered. It remains to be seen whether, how and at what point private actors will be brought into play here. A corresponding certification process has not yet been determined.

[10] https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Online-Ausweisfunktion/eID-Login/eID-Login_node.html

[11] https://www.egovernment.de/die-digitalisierung-der-brieftasche-identity-wallets-a-2bc230905ad349986d962e09524c22cb/

[12] https://dserver.bundestag.de/btd/20/130/2013075.pdf

Conclusion: In the context of a publication that is initiated purely by the private sector, the respective companies are faced with possible problems regarding profitability. In addition, there are concerns from consumers with regard to data security and data protection. From a consumer perspective, monopolization or expansion of already existing monopoly positions of larger companies (cf. Section 5) is to be avoided. The state as the sole issuer offers the most trustworthy option with regard to the issuance and the fulfillment of all requirements for an EUDI-Wallet. However, past experiences show that public digitalisation projects often fall short of their actual potential. This holds especially if there are no incentives for the private sector to integrate services. The described disadvantages could be offset by involving the private sector at an early stage.

5. COMPETITION

5.1. PRIVATE-SECTOR DEVELOPMENT OF AN EUDI-WALLET

Question: Are there specific requirements for private-sector developers of an EUDI-Wallet?

In principle, the same requirements apply to private-sector developers of an EUDI-Wallet as to state providers. Legal and functional requirements must be fulfilled independently of the publisher. In some cases, however, potential private-sector publishers must pay particular attention to some of the requirements laid down in the eIDAS Regulation. These include Art. 5a Par. 14, which refers to the analogous application of Art. 45h Par. 3 to “private parties” (in accordance with Art. 5 Par. 2 lit. b and c). A functional separation between the provision of the wallet and other services provided by the provider is mandatory. This means that the provision of the EUDI-Wallet must be completely independent of previous processes, in particular with regard to the collection and processing of data. If, for example, a company already has a customer base in another field and participates in issuing the wallet, it must not be possible to draw conclusions from the existing customer base towards the users of the wallet, nor may data from the wallet be integrated into the company's own business processes.

NIS2 sets out measures to ensure a high common level of security of network and information systems across the European Union. It provides for “stronger cooperation between member states, as well as minimum security requirements and reporting obligations for critical infrastructures and for certain digital service providers”.[13] This also includes Trust Service Providers within the meaning of Art. 3 Nr. 19 eIDAS.

In addition to such specific regulations, the provisions of the GDPR must also be taken into account when providing an EUDI-Wallet (cf. Sections 6.1.3 and 9). The EHDS as a specific area of the EU data strategy, might also be relevant for certain use cases. EHDS builds on the GDPR and the NIS2 Directive.[14] Depending on the intended functionality, which does not exclude health insurance cards, e-prescriptions or electronic patient files, specific regulations regarding health data must be observed and implemented.

5.2. INVOLVEMENT OF LARGE CORPORATIONS

Question: Which competitive implications could arise from the fact that large corporations like Google and Apple are involved in the development process of Wallet?

It is likely that large companies such as Google or Apple will have ambitions to participate in the development process or operation of an EUDI-Wallet. For example, it is already possible to use the Apple Wallet for identification at airports in the US. Using their own existing infrastructure and systems in Europe to expand their services from providing payment options and storing customer cards to digital identification is a reasonable next step. The first concrete signs of this can be seen in Google's participation in the SPRIND innovation competition. This innovation competition offers companies the opportunity to develop prototypes for German EUDI-Wallets. Google's participation was subject to criticism. SPRIND states that “when evaluating the Google team's application,

[13] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinien/nis-richtlinie_node.html

[14] https://www.european-health-data-space.com/

the jury expressed concerns about data protection. One jury member spoke out clearly against Google due to data protection and competition concerns. Since the team met all evaluation criteria and requirements (including data protection requirements), the majority of the jury members decided to invite the team to participate in stage 1 and to reevaluate this aspect (among others) at the end of stage 1."[15]

> **Conclusion:** The crowding out of smaller wallet providers is to be seen as a fundamental competitive consequence. In view of the current lack of a direct business model with the EUDI-Wallet as the only service offered by a company, large companies find it easier to include this branch in their portfolio in a cost-covering manner. This holds true especially for companies that have already integrated a wallet into their business model. These companies are able to provide the resources for the development and operation of such a wallet and, especially in the beginning, to ensure reliable financing of operations, to cross-finance the costs incurred by other revenue streams (see section 5.3.2). Since this option is only available to large companies, the corresponding monopoly position would be cemented and the market entry barriers for smaller competitors in particular would be significantly increased.

Question: In what way could they use their dominant position to the detriment of consumers?

With regard to consumers, privacy concerns are often raised in relation to private-sector companies, especially those based outside the EU. However, these companies are also bound by the guidelines set by the EU and by the national law of the respective country. Art. 5a Par. 17 eIDAS states that the wallet must be provided in accordance with appropriate and effective data protection measures. In addition, providers have a duty to demonstrate that processing activities are in accordance with the GDPR. It is the responsibility of the respective company to implement and comply with these obligations. However, the risk of non-compliance is not limited to large companies.

One issue that is relevant for consumers, especially with regard to large companies with an already extensive customer base, is the implementation of Article 5a Par. 14 eIDAS. This states that control over the use of the wallet and the data it contains must lie solely with the users. Consequently, providers should not be able to collect information about the use of the wallet that is not necessary for the provision of the services associated with the wallet. Furthermore, no combination of personal identification data should be stored or personal data related to the use of the wallet should be linked with personal data from the services offered by the provider or from third-party services that are not necessary for the provision of the services associated with the wallet. Specifically, this means a prohibition on linking existing profiles, such as a Google account, to the EUDI-Wallet, so that a comprehensive consumer profile can be created. An exception to this is the user's explicit request to combine and use the data. It remains to be seen to what extent this exception, for example by preselecting the opt-in during initial registration in the wallet, can be exploited to the detriment of consumers.[6]

In addition, Art. 5a Par. 16 lit. b regulates the unlinkability of attribute certificates (e.g. the mere confirmation of the user's age of majority) with the identification of that user (e.g. personal data). This is to prevent, for example, the linking of individual processes in the wallet, e.g. the proof of age in combination with the use of a payment option in a tobacco shop, from being linked together. However, this unlinkability can be circumvented through the cooperation of the relying party – in this example the tobacco shop – with the issuer of the attribute certificate.[1]

[15] https://www.sprind.org/impulse/challenges/eudi-wallet-prototypes

As mentioned in the previous section, the possible crowding out of smaller wallet providers and the associated expansion of the monopoly position of large companies such as Apple and Google, who dominate the market for cell phone operating systems, a further disadvantage for consumers could arise. Should one of these companies be primarily involved in the development and publication of a corresponding EUDI-Wallet, it could induce consumers who want to use the wallet to use cell phones from a particular brand or with a particular operating system, which could restrict consumers' freedom of choice.

Conclusion: In principle, large companies that already exert a certain market power in a sector can further expand their position by participating in the publication of an EUDI-Wallet and thus exert influence on the market and, as a result, on the end user. By squeezing out smaller providers, monopoly positions can be expanded and users who want to make use of the wallet are pushed to buy or use products or services from the respective companies. Not only does this restrict the freedom of choice for users. Users can also be enticed or effectively forced to share more data with a specific company if that company's EUDI-Wallet is embedded in an ecosystem which ties several services together (such as a mobile operating system). Although, as required by eIDAS, the processing of data within the provision of the wallet may not be linked to any customer accounts held by the providers, the freedom of choice and the control over personal data might be impaired. Large companies may therefore become effective gatekeepers for EUDI-Wallets, restricting access to certain implementations by shaping the environment in which they can be used. Furthermore, collusion between companies (legal or illegal) to indirectly benefit from further data acquisition and user profiling is difficult to effectively prevent.

5.3. FUNDING

Question: Are there concrete ideas for the funding of providers of wallets, what conclusions can be drawn about them from the perspective of the consumers and which funding models are possible and which advantages and disadvantages do they offer?

The exact financing structure of existing wallet solutions is not publicly available. However, based on the requirement that use must be free of charge for private use (Art. 5a Par. 13 eIDAS), financing options can be derived from existing approaches. When considering possible types of financing in the context of an eIDAS-compliant EUDI- Wallet, there are four options that can be used on their own or in combination.

One option is for the Member States to subsidize (in part or completely) the development and provision of EUDI-Wallets under their mandate. This is especially relevant if the respective Member State aims to provide a single solution for its citizens.

If the wallets are issued partly by private actors, it is up to them, (possibly in addition to a state subsidy), to raise the corresponding funds for the development. Three types of financing are conceivable here.

5.3.1. Commercial Users

On the one hand, commercial users can be called upon to finance the activities. Although it should be noted that eIDAS explicitly allows the private use of the EUDI-Wallet as free of charge, commercial use is excluded from this regulation. Legal entities should also be able to identify themselves to other or official bodies using the EUDI-Wallet (Art. 3 Par. 3 eIDAS). Recital 20 eIDAS explicitly excludes commercial use – in this case related to electronic signatures, but also transferable to other functionalities – from the free-of-charge requirement: "The use of a qualified electronic signature should be free of charge for all natural persons for non-professional purposes. It should be possible for Member States to introduce measures to prevent the free use of qualified electronic signatures by natural persons for professional purposes, while ensuring that such measures are proportionate to the risks identified and justified." It is therefore conceivable that a

fee may be charged to the respective user for the identification of legal entities and the use of the wallet (e.g. for tax matters, storing the business license, etc.).

5.3.2. Cross-Financing

The second possibility is to cross-finance the development and operation of the wallet through existing products or services. However, such a financing option is usually only open to companies that are already established and successful in the market and have been active in other or similar business models. One incentive here could be to drive users to demand more mobile phones from that brand – using Apple as an example – and thus to make use of other services provided by the company. Should the acceptance and willingness to use the corresponding wallet be high enough, this approach could provide the funds necessary for the operation of the wallet. This approach suffers from the disadvantages described in Section 5.2.

5.3.3. Fees for Relying Parties

The third and possibly the most feasible option is to finance the operation through fees imposed on cooperating companies and Relying Parties, similar to the Swedish BankID. Since the choice of wallet used is left to consumers and the relying parties have no influence on which and how many wallets are used by them for identification or authentication, subscription models or licenses for interfacing individual EUDI-Wallet implementations are unlikely to be an option due to the unpredictable costs. Rather, depending on the process and use of the wallet, a fee can be charged per query, which, similar to the fees for electronic payment transactions, is invoiced by the wallet provider for providing the infrastructure. However, there are currently no explicit guidelines for an appropriate pricing of data queries. According to current legislation, Relying Parties must allow any type of certified EUDI-Wallet without discrimination. This could lead to significant differences in the pricing of wallet providers, with rates being demanded that are disproportionate. Consequently, large platforms would be disproportionately affected (cf. Art. 5f Par. 3 eIDAS), since they are obliged to accept EUDI-Wallets. In conclusion, a regulatory standardization of prices per transaction is necessary.

> **Conclusion:** In principle, the choice of a financing option depends on user demand, which in turn is linked to available use cases of the wallet. If only limited functionalities are initially available within the application, the aforementioned options are difficult to scale in order to expand them to a stand-alone operation. In this case, it might be necessary to resort to state subsidies at the beginning. However, if demand, including from companies, for cooperation and integration into the services provided by the wallet is high, the solutions ranging from charging commercial use, cross-financing or charging relying parties, offer a valid and cost-covering financing option.

6. LIABILITY

6.1. LIABLE PARTIES

According to Art. 5a Par. 2 lit. a eIDAS, the German state is free to decide whether it implements a digital identity wallet in the form of a state EUDI-Wallet, a private organization commissioned to do so or a private wallet as an EUDI-Wallet by this Member State.

It is likely that the current approach of providing a publicly developed EUDI-Wallet concurrently with the certification of privately-developed EUDI-Wallets will be followed. However, in this section, all three variants are examined in terms of their scope of liability and possible liability gaps and the respective responsibilities are identified.

Questions about applicable law are non-trivial to answer. As the data stored in the EUDI-Wallet is almost exclusively personal data, at least the GDPR must be applied alongside the eIDAS and its implementing regulation. The FDPA as well as the CSA and the SDGR could also come into consideration.

Question: Who is liable and for what? Which regulations are applicable?

The question of liability can only reasonably be answered with respect to specific aspects of the EUDI-Wallet, such as malfunctions during use, damage cause by the inability to use the wallet or damage caused by data misuse and cyber-attacks.

The following legal regulations come into consideration:

- eIDAS
- GDPR
- Data Act
- Data Governance Act
- National law, such as:
    - BDSG
    - VDG
    - Other relevant national civil or public law

6.1.1. eIDAS

eIDAS is a regulation issued in accordance with Art. 288 of the Treaty on the Functioning of the European Union (TFEU) and is therefore directly applicable and legally binding for the German state in all its parts. No further act of transposition into national law is required. However, in the event of any conflicts with national law, it is assumed that the Union law provision takes precedence. The question of the extent to which German national laws may nevertheless require adaptation, such as those relating to digitalization, is not addressed here.[31]

The scope of application is defined in Art. 2 Par. 1 eIDAS, according to which it applies to electronic identification schemes notified by a Member State, to European Digital Identity Wallets provided by a Member State and to Trusted Service Providers established in the Union. However, Art. 2 Par. 3 eIDAS does not affect Union or national law relating to the conclusion and validity of contracts or legal or procedural obligations relating to sector-specific requirements. Furthermore, it does not affect the GDPR.

Art. 9 Par. 1 lit. b eIDAS requires notification of the applicable supervisory system and information on the liability rules relating to the party involved in the electronic identification means and the party carrying out the authentication procedure. According to Art. 11 Par. 4 eIDAS, these liability provisions are in line with national liability provisions and do not affect them as far as, for example, relevant procedural provisions, the concept of damage or rules on the burden of proof are concerned[16].

According to Art. 11 Par. 1 eIDAS, the respective Member State is liable in the event of a breach of its obligations under Art. 7 lit. d–f eIDAS in a cross-border transaction for all damage caused intentionally or negligently to the natural or legal person.

Furthermore, the liability under Art. 11 Par. 2 includes damage caused intentionally or negligently to natural persons by the party issuing the electronic means of identification as a result of non-compliance with Art. 7 lit. e eIDAS. The obligations under Art. 7 lit. e eIDAS are to ensure that the electronic identification means are assigned in accordance with the technical specifications, standards and procedures for the relevant level of assurance.

Liability for damage caused intentionally or negligently to natural or legal persons and attributable to incorrect authentication in accordance with Art. 7 lit. f eIDAS in a cross-border transaction is defined in Art. 11 Par. 3 eIDAS. Art. 7 lit. f eIDAS ensures the provision of online authentication.

Art. 11 Par. I–III eIDAS only apply to a cross-border transaction. Additionally, they are applied in accordance with the national provisions on liability (cf. Art. 11 Par. 4 eIDAS) and do not affect the liability of the parties to a transaction in which electronic means of identification subject to an electronic identification system notified in accordance with Art. 9 Par. 1 eIDAS were used. The notification of the Member State under Art. 9 eIDAS includes

- The description of the electronic identification scheme including the level of security (lit. a),
- The applicable supervision system and information on the liability regime in relation to the party issuing the electronic identification means and the party carrying out the authentication procedure (lit. b),
- The authorities responsible for the electronic identification procedure (lit. c),
- Information on the institutions that manage the registration of the unique personal identification data (lit. d),
- A description of the requirements for the definition of technical specifications, standards and procedures with minimum requirements (lit. e),
- The description of authentication in accordance with Art. 7 lit. f, i.e. the provision of online authentication (lit. f) and
- Rules on the suspension or revocation of the notifying electronic identification scheme, the authentication or the affected parts (lit. g).

[16] Cf. Recital 18 eIDAS

Insofar as electronic means of identification have been used, the national liability regulations are not affected by Art. 11 Par. 1–3 of the eIDAS Regulation. There are also further liability provisions in Art. 14, which is discussed in Section 6.2.3.

6.1.2.VDG

The VDG was enacted by the federal government to create an effective implementation of the "eIDAS 1.0" regulation (in the version of 2014) in the area of electronic Trust Services.

According to § 1 VDG, the scope of application of the VDG is opened insofar as it concerns the effective implementation of the provisions of the eIDAS Regulation, i.e. identification and Trust Services for electronic transactions in the internal market. This does not affect legal provisions which regulate the use of certain Trust Services and the products used for this purpose in accordance with § 1 Par. 2 VDG.

According to § 6 VDG, a Trust Service provider is liable for commissioned third parties that it entrusts with tasks in accordance with the eIDAS, the VDG and the statutory ordinance (§ 20 VDG), as it is for its own actions. The exclusion of liability for damages pursuant to § 831 Par. 1 cl. 2 BGB is also declared inapplicable.

6.1.3.GDPR

The GDPR applies insofar as the material and territorial scope of application is opened. Pursuant to Art. 2 GDPR, the material scope of application is opened insofar as fully, or partially automated (or non-automated) processing of personal data takes place that is stored or is to be stored in a file system. The territorial scope of application is opened according to Art. 3 GDPR if the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union. However, this scope of application is extended in Art. 3 Par. 2 and 3 GDPR to processing by a controller not authorized in the Union if the data processing is carried out in connection with the offering of goods or services or the monitoring of behaviour within the Union.

The geographical scope of application can be assumed to be unproblematic for the EUDI-Wallet, which is to be used particularly within the EU.

According to Art. 4 No. 1 GDPR, 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.

The eIDAS regulation references the GDPR's definition of personal data, which opens up the material scope of the latter. Among other things, the tax identification number, ID card and driving license are to be stored in this digital wallet. This is information that makes the respective holder of the documents directly identifiable and indicates special characteristics. Such special characteristics are, for example, the address, which can be found on the identity card, and the driving license class. Even though the tax identification number itself does not contain any information about the person concerned, it is used for identification in administrative procedures and is stored by the Federal Central Tax Office together with the name, date of birth and the responsible tax authority and date of the last administrative contact[17].

[17] https://www.bzst.de/DE/Privatpersonen/SteuerlicheIdentifikationsnummer/steuerlicheidentifikationsnummer_node.html#js-toc-entry3

According to Art. 4 No. 7 GDPR, the controller may not only be a natural or legal person, but also a public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data. According to Art. 4 No. 8 GDPR, a processor is an entity that processes personal data on behalf of the controller.

An example of such a controller-processor situation is the scenario where the state contracts a company to provide the EUDI-Wallet and perform the necessary processing of personal data.

6.1.4. BDSG

In principle, the provisions of the GDPR take precedence over the BDSG. However, there are opening and special clauses in the GDPR, which is why the provisions of the BDSG must be consulted in addition.

According to § 1 BDSG, the scope of application is only opened if a public body of the federal government or the federal states carries out the data processing. According to § 1 Par. 4 No. 1 BDSG, the law also applies to non-public bodies if the controller or processor processes data in Germany, if the processing of personal data is carried out as part of the activities of a domestic branch or at least falls within the scope of the GDPR.

The scope of liability follows from § 83 BDSG.

6.1.5.DGA

The DGA is intended to supplement existing Union law to promote the interests of consumers and ensure a high level of consumer protection. This shall facilitate the use of protected administrative data, regulate the role of data intermediary services as neutral actors in the exchange of data between companies and strengthen trust in the use of data. Art. 1 DGA specifies that the GDPR and the ePD remain unaffected and that the DGA does not create any new legal bases for the processing of personal data or further rights and obligations to protect privacy. Liability regulations are not included, which is why the DGA is only listed here for the sake of completeness. Recital 33 DGA clarifies that liability issues for all material and immaterial damage resulting from the conduct of the data processing service provider can be agreed in corresponding contracts on the basis of national liability regulations. Sanctions for violations of the Regulation and its implementation should be determined by the Member States, cf. Art. 34 and Recital 55 DGA.

On 17 October 2024, the Federal Government discussed the draft law “on the implementation of the EU Regulation on European data governance”, an implementing act for the DGA, for the first time.

6.1.6.DA

The DA serves to improve the use of data and the EU’s digital strategy to create more value through greater use of data. However, it only provides for the use of personal data in cases of exceptional necessity (cf. Recital 18 DA).

6.1.7.National Law

In principle, the GDPR is exhaustive and therefore supersedes the applicability of national law. According to Recital 146 cl. 4 GDPR, Art. 82 GDPR is effective without prejudice to other claims for damages. Parallel claims can therefore be based on all national bases for claims.

However, a distinction must be made between the different perspectives. On the one hand, there are liability regulations between the users of the wallet (i.e. citizens) and the respective wallet provider. However, if the wallet provider is a public law entity and has possibly also commissioned a (private) third-party company to design the wallet, the liability modalities shift.

Therefore, all claims between the contracting parties come into consideration, in particular contractual and tortious liability, according to §§ 280 ff BGB and §§ 823 ff BGB. Insofar as the state acts as the issuer of the wallet, claims arising from the public law contract pursuant to § 54 VwVfG and official liability may be considered.

Conclusion: The respective liability depends on the damage arisen. This can be divided into two groups. On the one hand, the failure of the wallet can lead to a breach of duty resulting in damage. On the other hand, misuse can result in such a breach.
A failure of use can be assumed if, in a particular case, the EUDI-Wallet cannot be used successfully or only with a time delay. Such a lack of availability may result in losses. A distinction must also be made here as to whose side is responsible for the incorrect access. For example, the user may have forgotten their PIN or not carried out other necessary steps. Depending on the design, there may also be a (technical) fault or even a block on the part of the wallet provider. If a trust service provider is already interposed, this may also cause malfunctions.
Misuse can be assumed if the EUDI-Wallet has been used inappropriately and this has resulted in damage. This can occur on the part of the user due to inadequate protection of the PIN or the securing of access by unauthorized persons. On the part of the wallet issuer or trust service provider, a lack of measures for IT security (cf. Section 8) can lead to misuse.
If the scope of the breach has been specified, the further scope of liability can be inferred.

6.2. LIABILITY FOR FAILURE

In the event of a failure, it is important to identify the *risk sphere* in which the failure happened and the party to which this risk sphere belongs. This depends on the respective legal relationship under which the failed process was to be performed.

6.2.1. Scope of Liability of the User

The user shall be liable in relation to both the Wallet Provider and a Trust Service Provider in accordance with §§ 280 ff BGB, unless otherwise stipulated in the contract. However, to be subject to liability, the user must have breached an obligation under this contract that results in damage. If the act is not based on a contractual breach of duty, tortious liability may still follow.

No specific legal obligation to use the EUDI-Wallet has yet been provided for and therefore no tortious liability can apply. No such liability arises either from eIDAS or from the GDPR.[3]

Conclusion: Liability of the user can only arise from contractual obligations, such as terms of use for the given EUDI-Wallet.

6.2.2. Scope of Liability of the Trust Service Provider / Member State / EUDI-Wallet Provider

A possible scenario is that a user is unable to obtain credentials or attestations from a Trust Service Provider and is consequently unable to use their EUDI-Wallet. This may be the responsibility of the Trust Service Provider.

Art. 13 Par. 1 governs the liability of Trust Service Providers. They are generally liable for damages caused by negligent or intentional failure to comply with obligations. Such obligations include, for example, taking appropriate technical and organisational measures to control security risks, cf. Art. 19 Par. 1 eIDAS. The employment of specialised personnel (at least for Qualified Trust Service Providers), the use of trustworthy systems for, among other things, the storage of data (cf. Art. 24 eIDAS), are also required. Appropriate measures must also be taken against forgery and theft of data.

Qualified and non-qualified Trust Service Providers are treated differently with respect to the burden of proof regarding the intention or negligence, but this does not affect the liability in general.

If the Trust Service Provider is in part operated by a Member State, a distribution of liability can take place in the internal relationship.

If a Member State fails to represent a user, to ensure the technical specifications, standards and procedures for the relevant level of security (Art. 7 lit. d eIDAS) or to provide online authentication (Art. 7 lit. f), that Member State is liable for damage caused.

The liability of the EUDI-Wallet provider – who can be either a Member State or a private actor (possibly under a mandate from a Member State) – not specified in the eIDAS regulation but left to national legislation. According to Art. 11 Par. 1 eIDAS, liability of a Member State is limited to the obligations arising from the operation of identification schemes, online authentication and cross-border authentication (cf. Art. 7 lit. d and f eIDAS, and consequently not to obligations arising from the provision of an EUDI-Wallet.

Liability under Art. 82 GDPR must also be considered and can apply to the EUDI-Wallet provider. As already discussed in Section 6.1.3, the GDPR is applicable in parallel. The liability provision of Art. 82 Par. 2 GDPR clarifies that every controller is liable for damage caused by improper processing. This also applies to EUDI-Wallet providers who process data of their users. It is irrelevant whether the processing out of which the liability arises is related to the provision of the EUDI-Wallet or whether it is a separate business process.

With respect to national law, the liability of a private Trust Service Provider or private EUDI-Wallet provider is governed by civil law. If the provider is responsible for a breach of duty, claims for damages according to § 280ff BGB come into consideration.

If the provider is a public body and unless there is an overriding contractual liability, public liability according to § 839 BGB in conjunction with Art. 34 GG is applicable. This is relevant if unlawful behaviour by the state leads to damage.

If the breach of duty is also a breach of contract by a public official under a public-law contract to which the general law on the impairment of performance applies, public liability is generally excluded.[17]

6.2.3.Scope of Liability in the Event of Misuse

If an EUDI-Wallet is misused, damage might incur for either or any combination of the involved parties:

- User
- EUDI-Wallet Provider
- Trust Service Provider (i.e. issuer of credentials or attestations)
- Relying Party

User liability towards the other parties arises from the contractual relationships. There is no liability arising from the eIDAS or GDPR. It is possible that so-called duties of care have been contractually agreed, which have been violated by improper handling. The user has a duty carefully store their sensitive data and to secure their data systems.[3]

In individual cases, however, it must always be examined whether such a breach of duty has occurred. A deceptive disclosure of data does not always constitute a breach of duty. This is e.g. the case if the user has breached a duty of care, the fulfilment of which would have prevented the deception. This duty includes, for example, not to follow an unusual request that is contrary to the agreed procedure.[16] Clicking on links in obviously forged emails is regarded as such a breach of the duty of care, if the user could have recognised the deception.[2]

In addition to contractual liability, tortious liability pursuant to § 823 BGB may also be considered. The aforementioned duties of care can be applied here. Furthermore, there must be an infringement of the legal interests specified in § 823 Par. 1 BGB. In particular, the property of third parties could be infringed, but this must be examined on a case-by-case basis.

Regarding misuse, the obligations of Trust Service Providers and EUDI-Wallet providers previously mentioned apply. Particular attention should be given to Art. 5a Par. 14 eIDAS, which states the obligation of the EUDI-Wallet provider to keep their data logically separate from other processes.

> **Conclusion:** If the user breaches certain contractual duties of care, they might be liable according to §§ 823 ff BGB. In practice, however, the breach of contractual duties is seldomly attributed to the user.
> There is liability under the eIDAS regulation and the GDPR for the EUDI-Wallet provider and for Trust Service Providers with an impact on national liability law. In particular, liability under the GDPR covers a large number of practical cases.

Question: Are there liability gaps?

> **Conclusion:** Due to the liability standards of the eIDAS, which refer to the national regulations of liability law, no obvious liability gaps are recognisable. Nevertheless, for special individual cases that are not yet foreseeable, a liability gap may arise. Depending on the constellation, closing such a gap may be achieved in national law.

Question: How are the responsibilities organised and how can roles and responsibilities be presented transparently in a responsibility model?

> **Conclusion:** The responsibilities are divided between three classes of actors: The Member States, the EUDI-Wallet providers and the Trust Service Providers.
> The Trust Service Providers are liable for damages caused by non-compliance with the eIDAS regulation.
> The EUDI-Wallet provider must fulfil relevant security measures in accordance with the eIDAS Regulation and, if it is offers services beyond the EUDI-Wallet, must logically separate its data. It must take precautions to prevent data misuse and implement suitable security measures.
> The responsibility of a Member State follows from Art. 11 eIDAS. The Member State is liable for a breach of the obligations under Art. 7 lit. d and lit. f eIDAS. According to Art. 7 lit. d eIDAS, the Member State must ensure that the relevant specifications, standards and procedures are in place for the implemented Electronic Identification Scheme. The obligation under Art. 7 lit. f eIDAS requires the Member State to provide online authentication which can be used by any Relying Party within the EU.
> If the Member State takes on the role of an EUDI-Wallet provider or Trust Service Provider, the respective scope of liability applies.

7. INTEROPERABILITY AND TECHNICAL STANDARDS

The landscape of regulations and standards which are relevant for the implementation and consequently for the interoperability of the EUDI-Wallet is complex. The following regulations and standards have direct influence on the implementations and are therefore considered for the remainder of this section.

- **eIDAS regulation**
  The revision of the eIDAS regulation ("eIDAS 2.0") introduces the concept of the EUDI-Wallet and sets the high-level goals and requirements for the EUDI-Wallet ecosystem. However, the eIDAS Regulation does not immediately mandate technical standards or formats for data storage and exchange.

- **Commission Recommendation (EU) 2021/946** of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework
  The EU Commission published a recommendation for its Member States to work towards a common "Toolbox". While the term "Toolbox" is not clearly defined and thus does not immediately imply a format (as opposed to e.g. "Implementing Acts" or European Standards/Euronorms), the Recommendation states what the Toolbox should contain. Among others, the Architecture and Reference Framework (cf. the next item) is part of the proposed contents.

- **NIS2 Directive**
  The NIS2 Directive aims to harmonize and increase cybersecurity and resilience across the EU. The NIS2 Directive affects the eIDAS regulation and specifies additional requirements for institutions in sectors of high criticality. Among others, this includes trust service providers.

- **Architecture and Reference Framework (ARF)**, currently available in version 1.4.1
  The ARF has been proposed by the European Commission (cf. the previous item). The Member States contribute to the ARF by means of the eIDAS Expert Group, which consists of representatives for each Member State. Technically, the ARF itself is not legally binding, as it is merely a joint document created by the Member States through the eIDAS Expert Group. However, the ARF will *de facto* bind the Member States' EUDI-Wallet implementations: The contents of the ARF will serve as the basis for the eIDAS Implementing Acts, which will then hold legal value.[18]

7.1. INTEROPERABILITY ON A NATIONAL LEVEL (GERMANY)

The declared goal of the German implementation of the EUDI-Wallet is to be interoperable both on a European as well as a national level.[4]

Question: What needs to be considered to make sure the Wallet is interoperable on a national level (Germany)?

The eIDAS directive 2.0 clearly specifies a mandatory set of features which is required to be supported by all EUDI-Wallet implementations of EU member states. The list is not exclusive, so

[18] "The contents of the ARF are being used to refine the Toolbox and will ultimately inform the content of the Implementing acts – outlining the exact specifications required for the wallet – that will be adopted later on and will be legally mandatory for every Member State." [10]

there is no limit on optional, additional features which member states may include in their respective implementations of the Wallet. However, interoperability can feasibly only be assured for mandatory features or for features that have become a quasi-standard due to their widespread availability and usage. Since the implementation of EUDI-Wallets by member states is still in progress, there are no well-established, quasi-standard features yet. Consequently, interoperability can only pertain to mandatory features at this time. Furthermore, interoperability inherently only pertains to features which interact – directly or indirectly – with external components (e.g. hard- or software). Of the features listed in Art. 5a Par. 4 and 5 of the eIDAS 2.0 directive, these are:

- Requesting and obtaining identification data, attribute attestations and certificates from authorities (Par. 4 lit. a)
- Sharing/presenting credentials to other EUDI-Wallets and verifying the credentials of other EUDI-Wallets (Par. 4 lit. a and c)
    - Note that the two interfacing Wallets might use different implementations and might contain credentials from different countries.
- Reporting alleged data protection violations (Par. 4 lit. d no. iii and Par. 5 lit. a no. x)
- Requesting removal of data according to Art. 17 GDPR from service providers (Par. 4 lit. d no. ii and Par. 5 lit. a no. ix)
- Signing documents, i.e. applying a Qualified Electronic Signature (Par. 4 lit. e)
- Authenticating to online services (Par. 5 lit. a no. ii and iii)

In essence, these features can be broken down into a number of interfaces, which we investigate individually in the following sections.

7.1.1. Receiving Identification Data, Attribute Attestations and Certificates to Store in the Wallet

For a device- and implementation-independent transfer of credentials[19], the data needs to adhere to a common format. This way, parties implementing their own EUDI-Wallet or related services can assure compatibility with this common format alone and be compatible with all other EUDI-Wallets and services.

> It is not only important that the data is available in a common format, but also that there are standardised interaction patterns across different use cases in terms of user experience.
>
> *Max Sauer, GI Fachgruppe Usable Safety & Security*

The data format for credentials is not specified in the eIDAS Regulation itself or any related legal act. Instead, the decision on formats was left for the eIDAS expert group to publish in the ARF. At

[19] In this section, the term “credentials” is used to refer to Personal Identification Data, Electronic Attestations of Attributes and certificates.

the current state, the ARF references two existing data formats suitable for the representation (and, consequently, for the storage and exchange) of cryptographically signed credentials:

- **ISO/IEC 18013-5:2021**, a standard for mobile Driving Licenses (mDLs)
  ISO/IEC 18013 itself references RFCs 7049 and 8949, defining the "Concise Binary Object Representation" (CBOR). ISO/IEC 18013 defines a structure and mandatory attributes for mobile Driving Licenses, but the approach can be adopted for generic credentials and attestations. It has been used as the basis for vaccination certificates and for generic eID systems in ISO/IEC 23220.[13]

- **JSON Web Tokens** supporting selective disclosure of attributes
  JSON Web Tokens (JWTs) are defined in RFC 7519. The support of selective disclosure is in the process of being standardized via the IETF draft "Selective Disclosure for JWTs (SD-JWT)". JWTs themselves are again based on the JavaScript Object Notation (JSON) format defined in RFC 8259.

The ARF also specifies a set of mandatory attributes for specific use cases in its annexes. At the current time, these use cases are Person Identification Data (PID, the EUDI-Wallet equivalent of an ID card) and mDLs, specified in Annex 3 of the ARF. It is likely that more datasets will be fixed in the ARF or elsewhere for documents which are standardized across the EU and that the Member States will individually standardize datasets for national documents such as diplomas.

The choice over the exact data format is not left to the Member States: According to the ARF, PIDs must be issued in both formats. Since the list of mandatory attributes applies to both formats, though, implementations can convert between the two. This means that in practice, EUDI-Wallet implementations do not have to store both representations. However, it is likely they must be able to present either of the two formats upon request from another device or service provider. mDLs must only be issued in ISO/IEC 18013 format (CBOR).

EUDI-Wallet implementations must also be able to request these credentials from the respective authorities. The ARF specifies that the "OpenID for Verifiable Credential Issuance" [22] (OpenID4VCI) interface is to be used for the process. The parameters (such as server addresses and issuing authorities) will be subject to existing national infrastructure and individual Member State's choices. Consequently, EUDI-Wallet implementations must accommodate for each Member State's national infrastructure if they are to support that particular country's credentials and attestations.

The OpenID4VCI specification requires credentials to be served via a web interface, where they can be downloaded into the EUDI-Wallet. Authentication data and addresses for this interface could be distributed via regular mail or via QR codes, to be scanned with the device which has the EUDI-Wallet installed. The ARF specifies the general procedure on a high level in Annex 4.03.

7.1.2. Sharing and Presenting Credentials and Attestations for Other EUDI-Wallets or for Verification by Service Providers and Authorities (e.g. for Authenticating to Online Services)

Annex 4 of the ARF contains high-level flowcharts for the process of presenting and validating the contents of an EUDI-Wallet. The details of how to exchange the necessary information are not specified in the ARF itself; instead, Section 4.2.1 references

- the "OpenID for Verifiable Presentations" protocol [29] (OpenID4VP) for the "remote" presentation, e.g. when logging into websites using the EUDI-Wallet and

- the standard ISO/IEC 18013-5 for the "proximity presentation", i.e. the presentation of PID or mDL data during border or traffic controls and possibly to other EUDI-Wallet users who are physically present

The OpenID4VP protocol allows for both SD-JWT formatted and ISO mdoc (ISO/IEC 18013-5) formatted credentials to be exchanged. The ISO/IEC 18013-5 presentation mechanism only considers mdoc credentials. The reference implementation of a booking service, provided by the European Commission, implements the request and verification of both formats.[20]

Since the ARF defines a complete list of mandatory and optional attributes to be included in PID or mDL datasets, the transfer and verification are essentially country-independent. The only difference in this regard between Member States will be the chains of trust which verify the respective credentials and attribute attestations, such as the issuing authorities or addresses for certificate revocation lists. The necessary information is contained in the datasets themselves, so EUDI-Wallet implementations can be developed to be able to handle information from any EU Member State.

7.1.3. Reporting Data Protection Violations and Requesting Data Removal According to the GDPR

In Annex 2.3.50, the ARF specifies high-level requirements for the reporting of alleged data protection violations by Relying Parties. Among others, it requires EUDI-Wallets to offer an interface for the preparation of a complaint and the logging of submitted complaints. It does not specify concrete mechanisms for requesting the removal of personally identifying data according to Art. 17 GDPR.

There is currently no standardized reporting mechanism and most data protection authorities merely publish mail and email addresses for reporting violations. It is therefore unlikely that the EUDI-Wallet specifications and implementations will offer functionality beyond preparing an email to the respective authority.

A minimal solution within the EUDI-Wallet app could be to provide a contact form with notes on how to report a violation. This way, the users could fill out the form and submit it within the app. The app could then log the contents for review by the user later. Additional assistance could be offered, e.g. by showing a structured form.

7.1.4. Signing Documents by Applying a Qualified Electronic Signature

Qualified electronic signatures have been specified in the first version of the eIDAS regulation and have since been implemented by numerous providers. The German eID card technically supports the creation of these signatures, if a suitable certificate is acquired and stored on the card. However, due to missing demand, all providers of these certificates have seized issuing them.[26] The current available method for generating qualified electronic signatures is by means of a qualified trust service provider, who authenticates the user and remotely generates the signature on their behalf. One example of such a provider is the service “sign-me”, offered by the Bundesdruckerei.

The eIDAS 2.0 regulation states that EUDI-Wallet implementations must support the creation of qualified electronic signatures. It does, however, not state whether an “offline” generation like that previously available with the German eID card is to be supported or whether “remote signatures” by means of qualified trust service providers are sufficient. The Architecture Proposal for the German eIDAS Implementation [4] provides for the implementation of remote signatures. Since remote signatures are already available, the existing infrastructure can (and will likely) be used to assure interoperability.

[20] https://github.com/eu-digital-identity-wallet/eudi-web-booking-service-demo

7.1.5.Conclusion: Interoperability on a National Level (Germany)

The essential technical protocols for the interoperability of EUDI-Wallet implementations have been fixed in the ARF. The OpenID4VCI and OpenID4VP are based on the OAuth 2.0 protocol, which is already widely used in online platforms. This facilitates implementation of the issuing process and the adoption of EUDI-Wallets into the authentication procedures of online services. The ISO 18013-5 presentation mechanism is well-established and has been evaluated for other use cases, such as vaccination certificates. Qualified electronic signatures have been standardized and implemented as well, with several trust service providers offering APIs for the creation of remote signatures.

> **Conclusion:** If EUDI-Wallet implementations adhere to these standards, a high level of interoperability can be achieved regardless of how data is handled internally by the respective application.

The reporting of alleged data protection violations via the EUDI-Wallet will likely suffer from a missing standardized process.

> **Conclusion:** As there is no common format for violation reports, EUDI-Wallet implementations will likely offer no assistance beyond references to contact addresses. Consequently, the burden of collecting the necessary information, preparing and submitting the report will be left to the users.

7.2. ARCHITECTURE AND REFERENCE FRAMEWORK (ARF)

The Architecture and Reference Framework constitutes the most concrete technical specification which directly stems from the legislative process.

Question: Is the ARF (legally) binding?

As stated in the preamble of Section 7, the ARF itself is not legally binding. It will, however, form the basis of the eIDAS implementing acts. It is therefore possible that these acts will reference the ARF and require adherence to its specifications. Furthermore, EUDI-Wallet pilots and preliminary services currently being developed apply the specifications from the ARF, forming a landscape of ARF-compliant implementations which will in turn influence the development of further software.

> **Conclusion:** While the current legislation does not strictly require the adherence to the ARF, this is likely to follow with the eIDAS implementing acts. In any case, the ARF constitutes a *de facto* standard as of now. Interoperability with other EUDI-Wallet implementations and related services can only reasonably be assured by adhering to the ARF.

7.2.1.Legally Binding Technical Specifications

Question: Are there legally binding, technical specifications, which Member States must adhere to when developing EUDI-Wallets?

As with most technical or digitalization-related legislation, the eIDAS regulation itself does not reference concrete, technical standards or specifications. The general idea behind this is that changes in legislation are usually much slower than technological advancements. In order to avoid having to revise legislation whenever technical advancements bring significant change, most legislation requires adherence to the technical “state of the art”. This means that the implementation must make use of currently available technology and must be updated whenever the technological circumstances change. As an example, the use of obsolete, insecure encryption algorithms can compromise the confidentiality of transferred data when a user authenticates to an online service.

For a qualified trust service provider, this would pose a violation of Art. 24 Par. 2 lit. e of eIDAS, which requires the use of “suitable cryptographic techniques”.[21]

The legislation does, however, indirectly require the adherence to specifications and standards. One example is the ARF, as described previously, which itself references standards like ISO/IEC 18013-5, JD-SWT or the OpenID interfaces/protocols OpenID4VCI and OpenID4VP. Furthermore, the eIDAS regulation requires the development and provision of EUDI-Wallets to implement

- the principle of “security by design” (Art. 5a Par. 5 lit. f), which can be achieved by adhering to standards such as the “BSI Grundschutz”, the ISO/IEC 27000 series or ETSI TS 103 645,
- the principle of accessibility (Art. 5a Par. 21), which can be achieved by adhering to standards such as EN 301 549,

> The AusweisApp2 has already shown how important a sufficient level of user experience is for the solution to be accepted and used by users. Also with regard to the Barrierefreiheitsstärkungsgesetz (BFSG).
> Important points regarding user experience are
> - Consistent interaction patterns across use cases
> - No use of overly technical terms
> - Explanation of functionality based on experience, e.g. skippable introductory tutorial
> - Sufficient assistance during use
> - Considering any accessibility requirements, e.g. red-green weakness, visual impairments, physical impairments, etc.
>
> *Max Sauer, GI Fachgruppe Usable Safety & Security*

- the certification by a national conformity assessment body (Art. 5c Par. 1), and
- “administrative and management procedures which correspond to European or international standards” (Art. 24 Par. 2 lit. b in conjunction with Art. 5a Par. 20)

Additionally, the GDPR applies to the processing of personal data and thus to the operation of EUDI-Wallets. Art. 5a Par. 17 eIDAS requires that the compliance to the GDPR is explicitly demonstrated.

A noteworthy exception is that developers and providers of EUDI-Wallets do not fall under the provisions of the NIS2 directive unless they also provide trust services (e.g. the issuing or verification of credentials) and thus act as a trust service provider (qualified or unqualified).

Conclusion: Current legislation does not immediately specify technical standards and specifications. However, a number of specifications such as the ARF, the standards referenced

[21] Note that the developer or publisher of an EUDI-Wallet is not necessarily required to be a Qualified Trust Service Provider.

therein, as well as standards pertaining to accessibility, data protection and IT security will be required de facto by developers and providers of EUDI-Wallets.

7.2.2. Creative Leeway for Member States

Question: What creative leeway do Member States have for the development of EUDI-Wallets?

As described in Section 3.5, Member States can individually decide on a model for the provision of EUDI-Wallet implementations. Art. 5a Par. 2 eIDAS specifies that Member States may provide any combination of wallet implementations that have been publicly or privately developed as long as at least one such implementation is officially supported ("recognized") by that country.

According to Art. 5a Par. 7 eIDAS, Member States may also choose to support additional functionalities in their respective implementation of the EUDI-Wallet. This is useful e.g. for diplomas or certificates which are only valid and applicable in that particular country. Examples for such features are certificates for German apprenticeships ("Ausbildungsnachweis"), tax-related information or public transportation tickets.

The responsibility for the certification of EUDI-Wallet implementations, trust service providers, QES creation devices etc. is largely left to the Member States. They may choose the authorities which are responsible for the certification and therefore have a degree of control over the prevalence of wallet implementations, trust service providers and other related entities. Member States can also control the requirements for these certifications to some degree: Art. 20 Par. 4 eIDAS states that auditing requirements will be established by the EU commission. However, the list will likely not be exhaustive, so Member States may refine the requirements and thus shape the landscape of services in their jurisdiction. Depending on the final list, a Member State could theoretically, for example, only allow publicly developed EUDI-Wallets and non-commercial trust services. Nevertheless, this Member State would still have to accept EUDI-Wallet implementations certified in other Member States and provide interoperability with them.

No changes are made to the decision over which public services require which kind of authentication. Member States are free to choose whether to require e.g. the provision of names (as opposed to pseudonyms), addresses or birthdates to access a particular service and they are free to define the use cases for qualified electronic signatures and seals.

According to Art. 28 Par. 5 eIDAS, Member States may lay down national rules governing the temporary suspension of certificates for qualified electronic signatures (and seals, cf. Art. 38 Par. 5). This allows Member States to define if and when citizens and institutions are temporarily prevented from electronically signing documents using a QES.

The ARF specifies further possibilities for Member States to shape the use of EUDI-Wallets. In Annex 3.1, Section 2.2.2, the option to specify "domestic PID namespaces" is defined. This allows Member States to provide arbitrary additional attributes in the PID datasets which are only applicable in the national context. As an example, the German PID datasets could contain the Tax ID number. This allows Wallets and services in the national context to use and rely on this information without affecting the implementations in other Member States. The same holds for mobile Driving Licenses, as mentioned in Annex 3.2, Section 2.1.

Conclusion: Member States have a high degree of control over how national EUDI-Wallet implementations are developed and certified. They can influence the deployment of trust services, qualified electronic signatures and seals by means of provider certification and the choice over where these mechanisms are required or allowed. Furthermore, Member States may define additional, domestic functionalities in their respective EUDI-Wallet implementations, and they may choose to add additional, domestic data to the credentials (PID datasets and mobile Driving Licenses) stored in the wallet.

7.3. EU-WIDE STANDARDIZATION OF QUALITY

Question: How can a common level of quality be assured for the implementation of trust anchors?

Trust anchors are collected and published in so-called “Trusted Lists”, which are governed by the Member States. The inclusion in these Trusted Lists is only open to qualified trust service providers, who are bound to adhere to the requirements of the eIDAS regulation, particularly those in Art. 24. However, as stated in the previous section, Member States do have significant freedom when it comes to the certification of qualified trust service providers. While the generic requirements are harmonized across the EU, details may be subject to interpretation by the relevant certification authorities, who are in turn designated by the respective Member State.

Some harmonization of the requirements is implemented by the eIDAS regulation itself. Art. 24 governs the process of identifying users as well as the notification of authorities in the case of a security incident. It also states high level requirements such as the use of “trustworthy systems” and the employment of staff who has “received appropriate training regarding security and personal data protection rules”. Further requirements are specified in the NIS2 directive, which applies to all kinds of trust service providers (unless they fall under the definition of small enterprises). According to Art. 20 Par. 1 eIDAS, qualified trust service providers must adhere to Art. 21 NIS2, regardless of their size.

> **Conclusion:** The minimum level of quality with respect to security and data protection for the implementation of EUDI-Wallets is defined by the harmonized EU legislation, most notably the eIDAS regulation, the NIS2 directive and the GDPR. Member States may influence the level of quality by refining the requirements for certification, but this only applies to EUDI-Wallets developed and trust services offered in that particular country. The overall level of security and privacy for cross-border use and the protection against identification fraud is expected to be the figurative “lowest common denominator” between all EU Member States. The overall level of security and privacy for a Member State’s citizens is determined by that Member State’s security measures and by the service providers used by the citizens.

Question: Which standards need to be implemented?

> **Conclusion:** Similar to how EUDI-Wallet developers and publishers are governed (cf. Section 7.2.1, the regulation does not dictate a concrete set of standards for the operation of qualified trust service providers. It does, however, require the providers to adhere to the NIS2 directive, which effectively mandates the adherence to common IT security standards such as the ISO/IEC 27000 series or the “BSI Grundschutz”. Qualified trust service providers have to be audited and have to repeat the audit periodically (every 2 years), the details of which can be influenced by the Member States.

Question: Which procedures can be applied by Member States to periodically check the quality of the implementation?

In addition to the previously mentioned audits for qualified trust service providers, the eIDAS regulation also defines a peer review process in Art. 12 Par. 5. Member States are thereby required to carry out peer reviews for each other’s electronic identification schemes, i.e. the mechanisms to electronically identify natural and legal persons. These electronic identification schemes comprise, for example, which attributes of natural and legal persons are stored by the public administration and which combination of attributes is used to uniquely identify each such person.

The exact process for these peer reviews is not yet specified and will be the topic of implementing acts which are due to be established by 18 March 2025, according to Art. 12 Par. 6 eIDAS.

Aside from the peer reviews and the audits for EUDI-Wallet providers and trust services in their own jurisdictions, Member States have little to no opportunity to check or influence the quality of the implementation in other Member States. In particular, the revocation of compromised EUDI-Wallet implementations and qualified trust services is left to the Member State responsible for the

certification in the first place. While Member States are legally obliged to revoke the certification of compromised services, the eIDAS regulation does not specify a mechanism by which other Member States may initiate and audit or a revocation.

> **Conclusion:** Member States may designate authorities responsible for performing audits and thus certifying EUDI-Wallet providers and qualified trust services. They may likely influence the certification procedure, subject to the regulation to be established by the EU commission. Furthermore, Member States can and must perform peer reviews of each other's electronic identification schemes.

8. SECURITY

The security of EUDI-Wallet implementations is a central aspect of the development process and of utmost importance for both the acceptance within the population and the continuous operation of the infrastructure. In a 2024 survey, 66% of the participants expressed concern about the theft of their private identity.[25] The legislation on the EUDI-Wallet tries to account for this by specifying requirements for all relevant parties of the EUDI-Wallet ecosystem, e.g. wallet providers, credential issuers, trust service providers, supervision authorities and Member States.

8.1. USER AUTHENTICATION

The authentication of the user by the EUDI-Wallet application is a fundamental prerequisite to prevent identity theft and misuse of identification data. The data stored in the wallet and the functionalities for authenticating online presenting credentials and attestations etc. must therefore be protected against unauthorized access.

In Annex 2.3.9, the ARF specifies high-level requirements, which include the authentication of users before providing cryptographic services (by the Wallet Secure Cryptographic Application, according to requirement WTE_02) and before providing any other functionality (by the Wallet Instance, according to requirement WTE_03). Effectively, any interaction with the wallet requires the authentication of the user.

> It is therefore all the more important that security mechanisms can be used in a user-friendly way (Usable Security). Even the strongest security mechanisms are useless if they are not used correctly.
>
> *Max Sauer, GI Fachgruppe Usable Safety & Security*

The Wallet Secure Cryptographic Application is further required (requirement WTE_28) to verify the authentication factors of a user in accordance with Commission Implementing Regulation (EU) 2015/1502 (CIR 2015/1502) Section 2.2.1, which states that for means of electronic identification, two authentication factors from different categories (possession-based, knowledge-based, physical-attribute-based) need to be used. The ARF does not further specify the authentication factors and exact procedure. This is done by the Architecture Proposal for the German eIDAS Implementation [4]. It lists 3 mechanisms “to securely bind the PID to the user as identity holder”. The mechanisms differ significantly in how cryptographic information is transferred and stored. A comparison with respect to security and privacy properties is also provided in the Proposal.[22] All configurations require the presentation of the eID card during the issuing process for the PID. From a purely visual perspective and with respect to user authentication during the PID presentation, however, the only difference between the approaches is the verification of the authentication factor.

- **eID Card:** The eID PIN for the card (together with the card itself) is requested every time the PID is presented.

[22] https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/functions/00-pid-issuance-and-presentation/#preliminary-assessment-and-comparison-of-pid-design-options

- **Cloud Support:** The user configures a PIN with the PID provider, which is requested every time the PID is presented.
- **Secure Element in Smartphone:** The user configures a PIN with the EUDI-Wallet app, which is requested every time the PID is presented.

The use of a PIN for authentication is problematic: The Architecture Proposal states that the wallet application itself must be unlocked by a device-specific method (such as FaceID, fingerprints or similar) whenever it is used. It does, however, also explicitly mention the possibility of using a PIN or swipe pattern. This enables users to unlock access to their stored PID by means of two knowledge-based authentication factors, e.g. two PINs, which is in clear violation of the legal requirements for EUDI-Wallets.

> **Conclusion:** It is therefore necessary for EUDI-Wallet developers and providers to prevent users from configuring the device and the wallet in a way that violates the requirement for proper 2-Factor-Authentication.

The Proposal argues that regardless of whether 2 PINs are used, access to the stored PID always requires a possession-based second factor: the smartphone. Since the data is only available from the EUDI-Wallet, physical access to the smartphone is necessary. This interpretation is however not convincing. The authentication is performed by the EUDI-Wallet application on the smartphone itself. The context for the authentication is therefore already limited to the physical vicinity of the phone. A requirement for 2-Factor-Authentication in this physically limited context must therefore be interpreted as requiring 2 factors which are independent of this context.

The authentication approach based on the eID card does not suffer from this issue. Since the card and its PIN are required for every PID presentation, the conditions for 2-Factor-Authentication are always satisfied.

> From a pure security point of view, eID cards seem like a good idea, but requiring a card in addition to the smartphone to use the wallet seems quite impractical for many use cases.
>
> *GI Fachgruppe Management von Informationssicherheit*

Question: What are advantages and disadvantages of biometric authentication mechanisms from the perspective of the consumer?

Advantages and disadvantages of biometric authentication mechanisms in general have been thoroughly discussed in literature.[15, 20, 24] In the context of the EUDI-Wallet, the relevant advantages and disadvantages can be summarized as follows:

Advantages	Disadvantages
Usability benefits (e.g. not having to enter a PIN or password)	Lower acceptance
Smaller chance of loss	Imperfect confidence for authentication (possibility of errors)
Possibility for continuous acquisition (e.g. continuous scanning of face throughout app usage)	Compromise (or loss) is usually permanent

Cannot easily be copied for delegation of access	Not available to everyone (e.g. people with disabilities)
	Harder to protect against unauthorized copying (e.g. faces or fingerprints from public photos)
	Verification is harder to implement (powerful sensors, more complex algorithms)
	Require high amount of trust in storage (provider)

Table 3: Advantages and disadvantages of using biometric features for authentication

A clear recommendation for or against the use of biometrics cannot be made in this context. Whether the benefits outweigh the disadvantages depends on multiple factors, including the personal preference and behaviour of the respective user. A possible way to account for this situation is to offer multiple different authentication configurations, one of which does not require the use of biometrics.

> Users must be able to choose authentication configurations according to their needs, so that security does not have a negative impact on the user experience.
>
> *Max Sauer, GI Fachgruppe Usable Safety & Security*

Conclusion: The advantages of biometrics are a relatively clear gain in usability and a higher protection against certain attacks such as the deliberate transfer of access by the wallet user. The disadvantages include the fact that biometrics cannot be changed once compromised (or lost) and offer lower protection against advanced, targeted attacks such as the extraction of face and fingerprint data from publicly available photos.

The authentication factor category of inherent physical attributes does not only include biometrics. Approaches have been developed e.g. to measure the behaviour of users for continuous authentication in the context of IoT devices.[18] Implementing such mechanisms for the EUDI-Wallet, however, is infeasible: A core idea of the wallet specifications is that the user spends little time in the EUDI-Wallet app. In order to acquire enough data for continuous authentication, the approach would have to start the authentication process minutes or hours ahead of a potential access of data. This presents challenges to privacy (data is processed even though it is not clear whether it is needed) as well as the implementation (the EUDI-Wallet app might not be running by the time the authentication process needs to start).

Question: Are there alternatives to biometric authentication as a second (or first) factor and what are their advantages and disadvantages from a user perspective?

There are several possibilities to implement the authentication process while offering proper 2-Factor-Authentication.

1. The authentication process may rely on knowledge- and possession-based authentication factors. This is given e.g. by the envisaged use of the eID-Card. Usage of the card requires physical possession of the card and knowledge of the PIN. In fact, since the usage of the eID card already requires the entry of its PIN, there is no need for an additional authentication factor. Theoretically, the wallet could be unlocked with the eID PIN

and the card could be presented for access to the PID without having to enter it again. One issue with this approach is that the planned widespread use of the wallet implies that access to (cryptographic) wallet functionalities happens relatively often. In practice, users are therefore likely to keep their eID card close to their smartphone. This effectively decreases the benefit of the second factor, as loss or theft of the smartphone likely go along with loss or theft of the card.
With the rise of wearable devices, it is possible that these can pose as a second factor. For example, smartwatches already serve as electronic wallets for proprietary payment schemes. Technically, they could also be used as a possession-based authentication factor for the EUDI-Wallet.

2. Approaches using e.g. behaviour-based authentication could be applied instead of biometric features to offer an authentication factor from the same category without some of the disadvantages inherent to biometrics. However, they suffer from significant disadvantages, as stated above.

Conclusion: Biometrics can be removed from the authentication process if the authentication is based solely on knowledge- and possession-based factors. This can be achieved using existing technology and complies with the requirements set out in the eIDAS regulation and in CIR 2015/1502. Other alternatives to biometrics such as behaviour-based authentication are not feasible at this time, as the disadvantages outweigh potential benefits.

Question: Which variant of the PIN verification as a second factor is to be preferred and what are the consequences for security and usability?

As stated before, there is no mechanism which is preferable in all regards and all situations. The choice of the most suitable PIN verification method depends on the preferences of the user and their requirement on usability, privacy and security. Some recommendations can however be made for typical use cases.

Conclusion: The verification of the PIN by the Secure Element of the smartphone has a significant privacy advantage over the other methods. Since all data necessary for the presentation of the PID is saved on the Secure Element, no communication with the PID provider is necessary during the presentation process. This prevents the disclosure of usage patterns to the provider[23] and offers the practical benefit of requiring less data transfer. The downside of the approach is that in addition to the eID card and PIN, which are necessary for the issuance of PIDs, the user has to configure and remember another PIN. Furthermore, the compromise of the Secure Element (e.g. by theft of the smartphone together with a disclosure of the PINs) enables an adversary to present the PID without any further parties involved. The revocation of the credentials or the wallet altogether becomes harder in this case.
The use of the eID card in conjunction with the PIN for user authentication has the benefit of building on already established technology with strong security properties. The user only has to have their eID card ready and only has to remember a single PIN, which might provide a minor usability benefit.
The use of cloud-backed authentication requires less hardware on the user's end. For the presentation of the PID, neither an NFC-capable smartphone, nor a Secure Element capable of storing the PID is necessary.
If the hardware requirements are satisfied, the use of the Secure Element for user authentication is likely to be the best option in terms of usability, security and privacy for most users.

[23] Note that for the other mechanisms, the PID provider by default does not learn *where* the credentials are used. They only learn *when* credentials are requested.

9. DATA PROTECTION

Privacy and data protection play a fundamental role in the EU. The right to privacy is declared in the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union and forms the basis for the General Data Protection Regulation.[23] The eIDAS regulation tries to account for this by requiring that users have full control over their data, according to Art. 5a Par. 1 eIDAS. It further refines the requirements, e.g. by stating that trust service providers must be prevented from learning about the use of attribute attestations by users (Art. 5a Par. 5 lit. b eIDAS).

However, the data protection features of the EUDI-Wallet, specifically those defined in the ARF, are not undisputed. An online discussion has been initiated on how well the proposed architecture preserves the users' privacy and whether alternative cryptographic protocols may enhance the situation.[24] A group of cryptographers has expressed their concern that the current specification is falling short on the expectations on privacy preservation and has proposed the application of alternative approaches in order to strengthen the data protection features.[1] While the feedback was taken into consideration, the propositions have not been implemented in full by the authors of the ARF.

9.1. GUIDING PRINCIPLES

Question: Which guiding principles can be defined for the design of the EUDI-Wallet to ensure that the processing of personal data within the EUDI-Wallet ecosystem complies with legal requirements and with the expectations of the data subjects?

Legal requirements related to the protection of personal data within the EUDI-Wallet ecosystem are mostly defined in the GDPR and the eIDAS regulation. From the consumers' perspective, two principles from these regulations are most important:

On one hand, service providers (including trust service and EUDI-Wallet providers) must only request, collect and process personal data that is absolutely necessary for the provision of the respective service. This principle of data minimisation is implemented in Art. 5 Par. 1 lit. c GDPR.

On the other hand, consumers (i.e. data subjects) must be able to decide where and when to provide their personal data. In Art. 6 Par. 1 GDPR, consent is only one of 6 lawful grounds under which processing of data may be legal. The eIDAS regulation, however, specifies in Art. 5a Par. 4 lit. a that the sharing of person identification data (PID) must be under the sole control of the user. This means that regardless of the lawful grounds for data processing according to Art. 6 Par. 1 GDPR, data from the EUDI-Wallet can practically only be acquired by a service provider if the user has explicitly approved of the data transmission. Note that, however, an approval does not automatically express consent: For the fulfilment of e.g. a contract, a person might be obliged to provide their PID and may choose to do so using their EUDI-Wallet. The processing of data by the contracting party could still be based on Art. 6 Par. 1 lit. b GDPR (performance of the contract) and failure to provide the data may render the user liable under national civil law.

A third principle is that the situation of EUDI-Wallet users should not be worse – with respect to privacy and data protection – than it would be if they did not use the wallet. This principle is not explicitly stated in the regulations but is likely to be a decisive factor for the uptake of the EUDI-Wallet among the population.

[24] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/192

Conclusion: The guiding principles for ensuring that the processing of personal data within the EUDI-Wallet ecosystem complies with legal requirements and user expectations are:

- Compliance with existing data protection legislation, most notably the GDPR
- Particularly, the minimisation of data, i.e. limiting the processing to data which is required for the provision of a given service
- Compliance with legislation on the EUDI-Wallet ecosystem, most notably the eIDAS regulation
- Particularly, ensuring that the user always is in complete control over the sharing of their personal identification data
- Ensuring that the EUDI-Wallet does not have negative consequences for the privacy of its users

The supervision of these principles is inherent to the respective regulations.

Question: How can compliance to these principles be effectively supervised?

Compliance to data protection legislation is already supervised by the national and European data protection authorities. Despite criticism [9] and internal dispute [11], there is no feasible alternative to the supervision by the existing authorities.

For the supervision of eIDAS compliance, the regulation itself provides for the nomination of responsible authorities. Each Member State must designate authorities for the supervision of compliance and must regulate the certification of providers. The suitability of this approach cannot be assessed at this time, since it has not been practically evaluated.

The eIDAS regulation specifies guidelines for penalties in Art. 16 eIDAS. Upper limits on monetary fines are outlines in Art. 16 Par. 2 eIDAS, but only apply to trust service providers. The concrete specification of fines is left for Member States to regulate in implementing acts. While liability is regulated as described in Section 6, abstract fines for general non-compliance can constitute a more significant incentive for providers to adhere to the regulations. This is commonly perceived as a major achievement of the GDPR. Similar data-protection-related fines, the eIDAS regulation specifies that fines are to be imposed directly or indirectly by the supervision authorities.

Ultimately, the citizens of the EU will decide whether the implemented Wallets and services satisfy their expectations. As the example of the German eID card shows, failure to fulfil the expectations of users will likely result in a low adoption rate. Since the EUDI-Wallet is optional, citizens are unlikely to use it if it does not provide adequate and perceptible protection of their privacy.

Conclusion: The existing and specified authorities from the GDPR and eIDAS regulation are suitable for the supervision of compliance by parties involved in the EUDI-Wallet ecosystem. The users themselves will also play a major role in the evaluation of privacy and data protection, as the general acceptance of this technology is fundamental to its success. Aside from the optimization of the current supervision regime for data protection legislation, the specification of concrete fines for non-compliance to the eIDAS regulation by Member States may provide further incentives for adequate consumer protection.

9.2. DATA UPDATES

As specified in Art. 5a Par. 14 eIDA, the PID cannot be requested from the EUDI-Wallet without approval by the user. This means that for data to be updated at a service provider (public or private) from the EUDI-Wallet, user interaction is always required.

Question: Can a Relying Party demand an update of data from an EUDI-Wallet?

There are potential scenarios in which an EUDI-Wallet user is legally obliged to update their data with another party. The eIDAS regulation itself does not specify under which circumstances a data update is required or can be demanded.

In German civil law, however, it is not uncommon to require a contract party to notify the other upon updates to relevant personal data. One such example is a work contract, where the employer needs to know the address, bank account, and additional details such as the marital status or details on the driving license in order to fulfil their own contractual and legal obligations. The parties can agree on a means to communicate these updates and if they choose to use the EUDI-Wallet, updates will effectively be required.

Under public law, it is also possible that updates to e.g. the address, the employment status, or educational qualifications are required to be communicated to an authority. In the case of public authorities, some updates can be requested from repositories other than the EUDI-Wallet and can then be performed without approvement by the respective person.

Sanctions for not performing the required updates are specified in the respective legal frameworks. For civil law, failure to fulfil contractual obligations usually results in liability. Sanctions in public law are specified in schedules of penalties or similar legislation.

Conclusion: In certain scenarios, updates of personal data can be mandatory for users of an EUDI-Wallet. However, the users are usually not required to use the wallet to perform the update. Traditional methods are still valid under the eIDAS regulation, unless e.g. a contractual agreement has been made. In any case, there is no designated scenario in which an update of data from an EUDI-Wallet can be performed without the approval of its user. Any request for data strictly involves a confirmation screen, where the user must authenticate before the data is shared.

Question: Is an update required for the sake of up-to-date information?

Technically, updating data is within the EUDI-Wallet equivalent to deleting the existing data and retrieving a new set of data from the issuer. This can happen for 3 possible reasons:

- The validity of the existing data has expired. At least for the PID, the specification of a validity period is mandatory. Every PID therefore expires after a given time and has to be renewed.
- The data has been explicitly revoked by the issuer. This can happen either on request of the user (e.g. if the smartphone containing the data has been lost or stolen) or be initiated by the issuer (e.g. if the data is known to be compromised or out-of-date). Data is revoked by publishing a reference to the dataset in a revocation list, which is publicly available or can be queried through an interface such as OCSP[25]. When a Relying Party or the EUDI-Wallet itself notices that the data has been revoked, the user can request a new dataset to be issued.
- The data is found to be out-of-date by the user. The user can then notify the issuer about the actual data. The issuer can then revoke the old dataset and provide a new one for the user to store in their EUDI-Wallet.

Conclusion: It is usually not necessary for the EUDI-Wallet or its user to periodically check for the validity of the stored data. Data is revoked “silently” only if there has been a compromise of the data itself, the issuer or the EUDI-Wallet provider. This can be detected by checking publicly available revocation lists. In scenarios where data can suddenly become obsolete and therefore be revoked, periodic checks can be useful.

[25] Note that the use of OCSP itself is discouraged in the context of PID and attribute attestation presentation, as it enables traceability of the user. OCSP however forms the basis for OCSP stapling, which solves the problem of traceability in certain constellations.

9.3. TRACKING

Question: Which risks exist for which actors within the EUDI-Wallet ecosystem? How can the by mitigated?

A list of possible risks can be structured by highlighting the different actors within the EUDI-Wallet ecosystem.

9.3.1. EUDI-Wallet Developer/Provider

The developer or provider of the EUDI-Wallet controls the implementation. They are able to modify the wallet app arbitrarily. Art. 5a Par. 3 eIDAS states that the source code – particularly of the software components installed on user devices – must be open source licensed. The goal is to enable users or neutral third parties to check whether undesired features e.g. for tracking user behaviour have been added to the implementation. However, this does not immediately enable users to check whether the software installed on their mobile device actually matches the published source code. Reproducible builds [19], a measure to verify this property, are not required by the eIDAS regulation.

> **“Lack of unobservability of wallet uses:** There are no safeguards that prevent the governments, which actually provide the wallet, from exercising surveillance over everything its users do with it. As the wallet may be used in all areas of life (e.g. health, transport, finance, etc.) the related information may cover all these areas and give a very complete view on what people do with the wallet. Last-minute changes in Recital 11c [in the final version Recital 32] oblige the wallet provider to "**ensure unobservability** by not collecting data and not having *insight* into the transactions of the users of the Wallet. This means that the providers should not be able to see the *details* of the transactions made by the user." Again this provision is only given in the recitals, and its technical implementation is essential.” [8]
>
> *Prof. Dr. Kai Rannenberg, GI Arbeitskreis Datenschutz und IT-Sicherheit*

Conclusion: The EUDI-Wallet developer or provider can (deliberately or due to a compromise) modify the app to include tracking functionality. Legislation forbids this and requires the source code to be available, but matching the installed application to the published source code is non-trivial.

9.3.2. Issuer of Credentials and Attestations

As described in Section 8.1, depending on the implementation of the EUDI-Wallet – particularly the user authentication – the issuer of credentials is contacted every time these credentials are presented. They also learn which attributes are presented. By default, the issuer does not learn information about the Relying Party and the EUDI-Wallet may be able to spoof requests in order to obfuscate the actual usage patterns. By employing the Secure Element of the user’s smartphone, the necessity to contact the issuer can be removed.

If issuers collude with the Relying Party or Parties, however, they can identify where and when credentials are presented and can therefore build behaviour profiles. This property of the technical specification has been criticized [1, 8], but not revised as of yet. The users have no way of detecting this collusion and there is no technical mechanism to effectively prevent it. The only safeguards against this behaviour are legislative.

Conclusion: Issuers may be able to gain limited information on usage patterns in the default implementation of the EUDI-Wallet. If issuers collude with Relying Parties, they can completely trace credential and attestation usage, effectively profiling the user. Technical countermeasures have been proposed, but not yet incorporated into the specification.

9.3.3. Relying Parties

For Relying Parties, the situation is similar to that of issuers. The specification does not mandate whether credentials are short-lived – i.e. a new credential is requested and issued for every presentation – or whether the same credential is to be used for multiple presentations. Depending on the implementation, Relying Parties might therefore be able to match subsequent authentications of the same user, even though this user did not intend to be re-identifiable. By colluding with issuers, Relying Parties are able to build extensive user profiles.

Conclusion: Depending on the implementation, Relying Parties might be able to recognize subsequent presentations of the same attribute attestation, even if the user did not reveal a persistent identifier. Collusion with issuers allows Relying Parties to fully trace credential and attestation usage (as far as it involves the colluding parties). Technical countermeasures have been proposed, but not yet incorporated into the specification.

9.3.4. Others (e.g. Qualified Trust Service Providers Offering the Creation of Qualified Electronic Signatures)

Whether other parties within in the EUDI-Wallet ecosystem are able to track users depends on how they interface with the aforementioned parties and the user. If a user e.g. authenticates to a qualified trust service provider in order to create a qualified electronic signature, it is necessary for the provider to verify the identity of the user. This means that the provider learns personal identification data about the user and is therefore able to recognize subsequent accesses to their service. As a counterexample, the sole verification of qualified electronic signatures can be done without the user providing any personal information. A provider in this case would not be able to track the user.

Conclusion: A major concern about the current state of the specification is that, depending on the implementation, Relying Parties can recognize users over the course of different presentations of attestations and that Relying Parties and Issuers may collude in secret to track users comprehensively. The mitigation of these risks requires significant changes to the underlying protocols and algorithms, so it is questionable whether they will be incorporated into the specification. Consequently, concerns about the non-compliance of the specification to the eIDAS regulation itself have been raised. In the current state, misuse is only disincentivised by the imposed fines and liabilities.

Question: What are concrete strategies and measures for the implementation of mitigations?

The authors of the paper criticizing the lack of unlinkability propose the use of *Anonymous Credentials*.[1] These offer full protection against the described tracking attacks, which means that users can request credentials and use them arbitrarily without any involved party learning usage patterns or being able to recognize subsequent presentations (unless a persistent identifier is deliberately established by the user).

If the proposed changes to the specification are not implemented, only limited protection from tracking can be achieved. By requesting batches of attestations for the same attribute, users can collect a number of single-use datasets in their EUDI-Wallet. This way, Relying Parties alone cannot distinguish between different presentations of the same user and of different users. However, the collusion of Relying Parties and issuers is still possible in this scenario.

Conclusion: The specification – i.e. the ARF and, consequently, the German Proposal – need to undergo a significant revision in order to incorporate the use of Anonymous Credentials.

This allows the implementations to achieve full unlinkability and effectively prevents any collusion between issuers and Relying Parties.
If the proposed changes are not incorporated, the use of batch requests for attestations provides a limited amount of protection against tracking. It is then even more important that the legal requirements are thoroughly enforced, so that collusion is prevented.

9.4. DATA ABUSE

Question: How can a reported abuse of data by a Relying Party be effectively forwarded to the responsible national supervision authority?

As described in Section 7.1.3, the ARF requires EUDI-Wallet implementations to escort the user through the process of reporting alleged data protection violations. There are two possible approaches to transfer this information to the responsible authority:

- The Wallet uses available information about the Relying Party to determine which data protection authority is responsible for its supervision. It then sends the entered report to this authority directly.
- The Wallet sends all reports to an intermediary, who determines from the included information where to forward them. Parts of the report might have to be encrypted, since they might contain confidential data not to be disclosed to the intermediary.

Due to the added layer of indirection, which introduces an additional loss of privacy for the users, and to other difficulties inherent to the second option, the first option is to be preferred. However, this requires the EUDI-Wallet implementation to be able to identify and contact all relevant data protection authorities across the EU. This adds complexity to the development and provision of EUDI-Wallets, as the contact information needs to be up-to-date at all time.

Conclusion: The high-level requirements specified in Annex 2.3.50 of the ARF already require EUDI-Wallets to escort the user through the complete reporting process. Since information about the Relying Party in question can be determined from publicly available information – among others, the necessary data is included in the certificate used to verify the authenticity of the Relying Party – the EUDI-Wallet can determine the responsible national data protection authority and send the report directly to it.

Question: How can an efficient and timely processing of reports be achieved?

The efficient and timely processing of reports on data protection violations is not specific to the deployment or use of the EUDI-Wallet. However, if the uptake of the wallet is high, this will constitute a major increase in electronic accesses to public and private services. Depending on, among others, the usability of the EUDI-Wallet implementations, this may lead to a strong increase in data protection violation reports. The already criticized speed and quality of processing of these reports [9] is then likely to further deteriorate.

Conclusion: The only conceivable approach to maintain or preferrably improve the speed at which reports about data protection violations are processed by authorities is to strengthen these authorities in terms of funding and staff. It is unlikely that parallel structures such as different authorities for EUDI-Wallet-related reports bring a significant improvement on the long term.

Question: How is the cooperation between supervision authorities within the EUDI-Wallet ecosystem designed with respect to reports about data protection violations by Relying Parties?

The eIDAS regulation does places only abstract high-level requirements on the cooperation between supervision authorities with respect to data protection violations. Reports about alleged violations are to be transferred immediately to the responsible data protection authorities. The supervision bodies specified in the eIDAS regulation are responsible for monitoring compliance

with the eIDAS regulation itself and most of the provisions govern the supervision of EUDI-Wallets and trust service providers. However, in Art. 46a Par. 4 lit.g eIDAS, the regulation states that supervisory bodies designated for the supervision of the regulation itself shall cooperate with data protection authorities designated according to the GDPR. In particular, eIDAS supervision authorities shall inform data protection authorities about any possible infringement or personal data breach.

Conclusion: eIDAS supervision authorities are required to forward information on possible data protection violations to the responsible data protection authorities. The extent to which this is practically relevant depends on several factors. It is, for example, theoretically possible for a Member State to assign the supervision of the eIDAS regulation (i.e. of EUDI-Wallets and trust service providers) to its data protection authorities. In this case, cooperation on both matters would be inherent to their work. In other constellations, it remains to be seen to which degree cooperation and the exchange of information is necessary at all. If most of the information regarding alleged data protection violations is immediately reported to the relevant data protection authorities, coordination between the different authorities is of less importance. This can, however, only be evaluated once the EUDI-Wallet ecosystem is operational.

9.5. UNFORGEABILITY

The current version of the Architecture Proposal for the German eIDAS Implementation describes two methods to ensure the authenticity and integrity of the PID.

- **Authenticated Channel:** Authenticity and integrity of the PID are protected using a Hashed Message Authentication Code (HMAC). The key for the HMAC is based on ephemeral data specific to the particular presentation process.
- **Signed Credentials:** The PID is signed persistently by the issuer, protecting its authenticity and integrity. For a presentation to a Relying Party, an ephemeral dataset is generated which can only be used once.

Additional details of the approaches depend on the method of user authentication as compared in Section 8.1.

Question: What are the advantages and disadvantages to the two methods from a consumer's perspective, which method is more consumer-friendly and why?

The German Proposal provides a comparison of the different approaches and highlights the main differences with respect to security and privacy goals as well as other relevant properties. A notable difference in the two approaches for PID authenticity and integrity is the property of *plausible deniability*.

When using the method based on an Authenticated Channel, the presented PID is secured using ephemeral data. This means that after the presentation session has ended, the Relying Party and the PID issuer can (and should) discard the cryptographic keys used for the HMAC. If the parties adhere to the protocol, it is then no longer possible to prove that the PID was in fact used in a presentation. It is currently not possible to implement this method in accordance with the ARF.

When using the method based on Signed Credentials, the presented PID is signed using a persistent key by the PID issuer. The wallet creates an ephemeral dataset to make sure that the same data cannot be used in two unrelated presentations. However, the persistent signature on the PID is part of the presented data. This enables the Relying Party to later prove that the PID was in fact presented by the user at some point. This method complies with the current version of the ARF.

Conclusion: From a consumer's perspective, the use of an Authenticated Channel is preferrable. This method does not allow a Relying Party (or an adversary who has gained access to the data) to later prove that the user has presented their PID. However, the method is currently

not compliant with the ARF. The ARF needs to be revised to enable the implementation of Authenticated Channels for the authenticity and integrity protection of PID.

Question: Does the choice of the approach affect the interoperability?

Answer: Yes. In the current state, Authenticated Channels cannot be implemented in compliance with the ARF. If the ARF is revised to enable the use of Authenticated Channels, their support will likely be mandatory for EUDI-Wallet implementations. In this case, interoperability would not be affected.

9.6. ZERO-KNOWLEDGE-PROOFS

The current version of the ARF does not specify the use of Zero-Knowledge-Proofs (ZKPs) for any part of the implementation. For the remainder of this Section we therefore assume that the ARF will be revised to allow or enforce the use of ZKPs.

Question: Under which circumstances must the use of Zero-Knowledge-Proofs be avoided? Why?

The goal of ZKPs is to prove the knowledge of a secret without revealing information about the secret itself. In the context of the EUDI-Wallet, ZKPs could e.g. be used for authentication systems that do not store confidential data such as passwords with the service provider. Other applications are also conceivable.

The use of ZKPs in unsuitable, however, if the confidential information is the data to be presented to the Relying Party in the first place. When identifying to a service provider, a user might be required to provide their personal details such as name, address etc. Using a ZKP would allow a proof of knowledge of these attributes without disclosing them to the provider. However, the provider needs to know and possibly save the attributes in order to operate the service. In these scenarios, ZKPs are not an appropriate protocol.

Conclusion: Zero-Knowledge-Proofs are unsuitable in scenarios where data needs to be explicitly disclosed to a Relying Party. In identification scenarios where the service provider needs to know and possibly store the identification data, the use of Zero-Knowledge-Proofs is inadequate.

Question: Which other security mechanisms can be established in these use cases to protect the users?

To protect data which needs to be disclosed to a Relying Party, common mechanisms can be applied:

- As described in Section 9.5, plausible deniability is an important property for consumers as it mitigates the risk of being tied to a specific transaction at a later time.
- The provision of on-demand data can, in some cases, remove the necessity for service providers to persistently store sensitive data in their systems. This reduces the risks of data breaches and data misuse. For service providers it adds the benefit that the provided data is always up-to-date.
- Established mechanisms for the protection of data stored with the providers such as pseudonymisation, encryption and other technical and organisational measures can reduce the risks of data breaches.

9.7. OVER-IDENTIFICATION

Question: How can over-identification be defined?

Conclusion: Over-identification can be defined as the provision of personal – usually identification – data, which is not strictly necessary for the provision of a service.[7] The provision can

be voluntary or involuntary be the user and the request for more information than necessary can be deliberate or accidental by the service provider. In any case, over-identification negatively affects the privacy of the user and introduces unnecessary risks with regard to the protection of their personal data.

Question: How can the request and verification of data be prevented if that data is requested e.g. for an ordering process, but is not legally required?

The GDPR specifies the principle of data minimisation in Art. 5 Par. 1 lit. c GDPR (cf. Section 9.1). It requires data controllers to only request and process data if that data is absolutely necessary for a particular task. The GDPR also specifies guidelines for fines if the principles are violated by controllers. This constitutes a significant incentive for service providers to not request and process data which is not necessary for the respective service.

The eIDAS regulation reinforces this idea by requiring that data from the EUDI-Wallet can only be obtained by Relying Parties if the user explicitly authorizes the transmission (cf. Art. 5a Par. 4 lit. a eIDAS). The implementation specifications in the ARF and most notably the German Architecture Proposal further refine this requirement by specifying the display of a summary of the request for data within the confirmation screen, so that the user can inspect what data is requested. They can then decide whether the request is acceptable or not.

In the confirmation screen, it is important that users are clearly shown which data is required and which can be provided voluntarily.

Max Sauer, GI Fachgruppe Usable Safety & Security

Practical experience shows that many controllers collect more information than necessary. Showing a summary of the data requested, rather than showing the data themselves and allowing fine-grained permission or rejection, is unlikely to resolve this problem.

GI Fachgruppe Management von Informationssicherheit

Conclusion: On one hand, the legal framework defines the conditions, under which data may be requested and processed. The principle of data minimisation expressed in the GDPR is abstract but can be leveraged as legal grounds for fines and lawsuits. The legal framework also specifies fines which serve as a strong incentive to adhere to the regulations.
On the other hand, ensuring that the user can always cast the ultimate decision on whether to allow or prevent a data transfer from the EUDI-Wallet enables a strong possibility for self-governance and supervision of providers by consumers themselves.

Question: Why is pseudonymisation important? Which use cases profit from pseudonymisation? Which use cases require real names?

The importance of pseudonymisation is expressed in the GDPR. In recital 28, the regulation states that “the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations”. Pseudonymisation is also explicitly mentioned as an example for technical and organisational measures in Art. 25 Par. 1 GDPR.

Corresponding to the principle of data minimisation, pseudonymisation is useful in any use case where the processing of real names is not absolutely necessary. This includes accounts on websites, as long as the user does not perform a purchase or other action which requires them to

provide a real name. This holds true e.g. for most users of social networks. In contrast, any service where the processing of real names is obligatory for the provider, the use of pseudonyms is ruled out.

> **Conclusion:** Pseudonymisation constitutes an effective technical measure to protect personal data from accidental or deliberate disclosure. It can reasonably be applied in all use cases where the processing of real names is not (legally) required. Consequently, in cases where the processing of real names is legally required, pseudonymisation cannot be used.

9.8. ANONYMISATION

Question: Are there technical measures which can be implemented with respect ot the EUDI-Wallet architecture and which make compliance with the GDPR unavoidable?

If yes, which ones? If no, why not and what measures could be taken instead?

As mentioned in Section 9.1, any transfer of data required a confirmation by and authentication of the user. While this does not automatically express the user's consent to the processing of data, it does provide a natural blueprint for the implementation of consensual data transfers. If a processing of personal data is based on the data subject's consent according to Art. 6 Par. 1 lit. a GDPR, then that consent can be expressed by approving the transfer of data from the EUDI-Wallet to the controller, i.e. the Relying Party. Furthermore, periodic refreshing of data can then be tied to continuous consent and a withdrawal of the consent automatically prevents any further acquisition of up-to-date personal data. However, this does not technically prevent continued processing of the existing data.

The option of using a pseudonym for the registration with online services or of staying completely anonymous by presenting unlinkable[26] attribute attestations using the EUDI-Wallet reduce the amount of personal data processed. By processing pseudonymised or fully anonymised data, the controller may significantly reduce the risks for its data subjects. Since the anonymisation or pseudonymisation is enforced by the EUDI-Wallet and the corresponding protocols, the controller cannot deviate by processing more data than available.

If a service provider offers registration and authentication via the EUDI-Wallet, the mechanism provides a way for users to exert the right to rectification according to Art. 16 GDPR. Upon every authentication, users can present their current PID and attribute attestations. The provider can update their records accordingly. Note that this only works if the provider knows ther user's PID or if a pseudonym is used; it does not work for anonymous registration and logins.

> **Conclusion:** The EUDI-Wallet architecture provides mechanisms to enforce the use of pseudonymisation and anonymisation (provided the architecture is revised according to the suggestions), if the respective Relying Party designs their processes accordingly. It provides the option of implemting the acquisition of user consent and in part allows users to subsequently withdraw their consent, at least pertaining to updates to their personal data. Finally, it provides a mechanism for users to update their data automatically and without intervention of the service provider.

[26] Note that in the current state of the architecture specification, unlinkability of attribute attestation presentations cannot be guaranteed, cf. Section 9.3. For this paragraph we assume that the specification will be revised to offer true unlinkability.

10. COMPLIANCE

10.1. REPORTING MECHANISMS

Question: How can an appropriate reporting system be designed for security vulnerabilities and incidents affecting the eID and the EUDI-Wallet? Does the approach offer timely notification and adequate protection for consumers?

According to Art. 5a Par. 10 eIDAS, providers of EUDI-Wallets must ensure that users can easily request technical support, report technical problems or other incidents that may have a negative impact on the use of European digital identity wallets.

The European Digital Identity Cooperation Group is responsible for coordinating cross-border cooperation (Art. 46e eIDAS). The aim is to facilitate the exchange of information in the area of Trust Services, the EUDI-Wallet, digital identity and notified electronic identification schemes. This group consists of appointed representatives of the Commission and the member states and fulfils the tasks listed in Art. 46e Par. a–d. These are primarily the examination of relevant developments in the areas of the EUDI-Wallet and eID. This also includes the exchange of best practices for the development and implementation of security breach notifications and joint measures in accordance with Art. 5 and Art. 10 eIDAS.

Additionally, each Member State must designate a national single point of contact according to Art. 46c Par. 1 eIDAS who is to be notified whenever a breach of security of an EUDI-Wallet implementation (cf. Art. 5e Par. 1 eIDAS) is detected. In contrast, Art. 10 eIDAS does not require the notification of the single point of contact if an electronic identification scheme suffers a security breach.

The European Union Agency for Cybersecurity ENISA is also referenced; the single points of contact designated by the member states and the European Digital Identity Cooperation Group are to cooperate with the ENISA on matters of IT security.

> **Conclusion:** In general, the provisions of the eIDAS regulation specify a suitable regime of authorities for the coordination of IT security efforts. However, there is currently no regulation on a point of contact for users and security experts who have identified vulnerabilities with respect to the EUDI-Wallet ecosystem. It is unclear how the reporting of possible vulnerabilities will practically be implemented and whether the processes will offer a timely handling of reported issues.

Question: According to the current state of the architecture development process, who is responsible for the handling of vulnerabilities and security incidents on a national and European level? Does the approach offer timely notification and adequate protection for consumers?

According to Art. 46a eIDAS, Member States shall designate a supervisory authority for the EUDI-Wallet. They shall supervise the established providers of an EUDI-Wallet and take the necessary measures in the event of infringements of the Regulation.

Until the revision of the eIDAS regulation, the BSI has been the supervisory body for trust services in the area of creating, verifying and validating certificates for website authentication, while the Federal Network Agency has been responsible for the remaining responsibilitien. The revision of the eIDAS regulation, however, now explicitly requires the creation of a supervisory body for the EUDI-Wallet and eID. It is not yet clear how the responsibilities will be distributed and whether the approach will offer timely notification and adequate protection for consumers.

According to Art. 5a Par. 4 lit. d No. iii eIDAS, the EUDI-Wallet must be able to easily send a notification to the competent national data protection authority if an unlawful data request is considered. Users can thus contact the supervisory authority directly via the portal.

In the event of a personal data breach, the supervisory authority is notified by the supervisory authority in accordance with Art. 51 GDPR pursuant to Art. 20 Par. 2 eIDAS. This supervisory authority is established by the Member State.

A national supervisory body is very advantageous for the consumer, as there are no language barriers and the supervisory body created can offer quick and effective solutions thanks to its expertise.

Conclusion: With respect to data protection, a notification system exists and can be used to handle reports of users. However, the handling of reports of security breaches and vulnerabilities is not yet implemented. Additionally, it is unclear whether there will be a designated authority for the reception of vulnerability reports, aside from the single point of contact, who is only obliged to accept notifications by the Member State.

10.2. SUPERVISION OF DATA PROCESSING

Question: Which regulations and measures can contribute to the control and supervision of data processing in the EUDI-Wallet ecosystem?

Art. 5a Par. 1, 4 lit. a, 14 eIDAS, which gives the user sole access to their data, plays a fundamental role in the enforcement privacy preservation. The user must confirm each data transfer from the EUDI-Wallet individually and can decide whether the transmission of the requested data is acceptable for the given purpose. Furthermore, the certification of Qualified Trust Service Providers provides a strong incentive against the violation of data protection legislation.

While the supervisory bodies specified under Art. 46a eIDAS can take action against non-compliant Trust Service Providers, this practically happens once a violation has already occurred. In the event of a breach of the GDPR, the competent (data protection) authority is notified, which in turn is responsible for enforcing the principles of data economy and data minimisation. Authorities can also act preventively and offer consulting aid for relevant actors. This is common practice in the field of data protection.

Conclusion: The fact that users must authorize each transfer of data from their EUDI-Wallet ensures that they have strong control over their data. The supervision authorities specified in the eIDAS regulation and the GDPR enforce compliance to the respective regulations and penalize data abuse.

In terms of user experience, it would be relevant for users to be able to set up automated authorisation of data transfer for certain use cases or for certain data with certain levels of trust. This is because too frequent requests for authorisation can also have a negative impact on security if users find them annoying and simply confirm them over time without checking the data

Max Sauer, GI Fachgruppe Usable Safety & Security

Question: What preventive work can be done to ensure that all actors in the EUDI-Wallet ecosystem adhere to the principle of data minimisation?

A strong incentive for compliance is given by the sanctions imposed in the GDPR and the eIDAS regulation. Both catalogues of sanctions have a preventive character, although they can only be applied after a violation has taken place. The certification of Qualified Trust Service Providers and EUDI-Wallets is another measure incentivising compliance, as the process is likely to be costly for the involved parties and revocation of the status due to non-compliance therefore corresponds to a significant financial disadvantage.

Furthermore, compliance is incentivised by the fact that the users themselves control access to their data. Given the explicit illustration of which data is requested by which Relying Party and given the power to deny any transfer which is not deemed appropriate, the users themselves might constitute a regulating force for service providers.

> **Conclusion:** The main preventive mechanisms laid down by the eIDAS regulation are the certification of Qualified Trust Service Providers and EUDI-Wallets, the danger of sanctions for non-compliance and the necessary authorisation of each data transfer from the EUDI-Wallet by its user.

Question: Are Relying Parties privileged through lawful grounds?

Relying Parties are natural or legal persons who rely on an electronic identification, European Digital Identity Wallets or other means of electronic identification or a trust service.

The eIDAS regulation does not elaborate on lawful grounds for data processing as defined in Art. 6 Par. 1 GDPR. The ARF, however, states in Section 6.6.3.3. that there is no legal basis for automatic data processing.

> **Conclusion:** Even though the ARF is not legally binding, the sole fact that a party is a Relying Party according to the eIDAS regulation does not provide a lawful ground with respect to Art. 6 Par. 1 GDPR for any processing of personal data. Furthermore, the approval of a data transfer from the EUDI-Wallet by its user must not be mistaken for an expression of consent as specified in Art. 6 Par. 1 lit. a GDPR.

11. CONCLUSION

The specification and development of EUDI-Wallet implementations is already in full progress. The regulation as well as the choices taken by the relevant actors show that past successes (such as the security properties of the German eID system) have been considered just as well as past mistakes (such as the scarce adoption rate of the German eID system and of Qualified Electronic Signatures).

With the eIDAS regulation in force, questions of liability (cf. Section 6) are largely clarified. Aside from corner cases, the responsibilities and resulting liabilities are clearly defined. However, legislation both on the European as well as the national level intertwines, so careful study of the relevant regulations is necessary.

There is still significant movement in the legislative process:

Implementing acts refining the eIDAS regulation must be passed. Only then can proper interoperability be achieved and enforced (cf. Section 7).

Supervision authorities must be designated and properly supported to ensure compliance with data protection and other relevant legislation (cf. Section 10).

Finally, practical decisions must be taken to define the framework in which the EUDI-Wallet can be evaluated and assessed:

The choice of a provision model plays a major role for the potential adoption by users (cf. Section 4) and, together with provisions on fair competition, will shape the landscape of providers offering services which can be accessed using the EUDI-Wallet (cf. Section 5).

The technical specifications need to be finalized and in certain parts be revised in order to provide the desired security (cf. Section 8) and privacy (cf. Section 9) properties.

If the existing opportunities of cooperation and participation are leveraged, a consumer-friendly and universally beneficial EUDI-Wallet implementation can be achieved.

12. LIST OF REFERENCES

[1] Carsten Baum, Oliver Blazy, Jan Camenisch, Jaap-Henk Hoepman, Eysa Lee, Anja Lehmann, Ann Lysyanskaya, René Mayrhofer, Hart Montgomery, Ngoc Khanh Nguyen, Bart Preneel, Abhi Shelat, Daniel Slamanig, Stefano Tessaro, Søren Eller Thomsen, and Carmela Troncoso. 2024. *Cryptographers' Feedback on the EU Digital Identity's ARF*. Retrieved November 22, 2024 from https://files.dyne.org/eudi/cryptographers-feedback-june2024.pdf

[2] Georg Borges. 2005. Rechtsfragen des Phishing - Ein Überblick Aufsatz von Professor Dr. Georg Borges. *NJW* 2005 (2005), 3313–3376.

[3] Georg Borges. 2011. *Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis* (1. Auflage ed.). Nomos, Baden-Baden.

[4] Bundesministerium des Innern und für Heimat. 2024. Architecture Proposal for the German eIDAS Implementation. Retrieved October 8, 2024 from https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/

[5] Bundesministerium des Innern und für Heimat. 2024. Sichere digitale Identitäten: Bürgerinnen und Bürger sollen sich mit dem Smartphone ausweisen können. *Pressemitteilung vom 30.09.2024*. Retrieved October 11, 2024 from https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/09/eudi-wallet-sep.html

[6] Michael Cepic. 2023. Rechtmäßigkeit der Verarbeitung personenbezogener Daten. In *Datenschutz bei den Zivilgerichten* (1st ed.). Verlag Österreich, 71–116. https://doi.org/10.33196/9783704692795-104

[7] Pasquale Chiaro, Simone Fischer-Hübner, Thomas Groß, Stephan Krenn, Thomas Lorünser, Ana Isabel Martínez Garcí, Andrea Migliavacca, Kai Rannenberg, Daniel Slamanig, Christoph Striecks, and Alberto Zanini. 2018. Secure and Privacy-Friendly Storage and Data Processing in the Cloud. In *Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers*, Marit Hansen, Eleni Kosta, Igor Nai-Fovino and Simone Fischer-Hübner (eds.). Springer International Publishing, Cham, 153–169. https://doi.org/10.1007/978-3-319-92925-5_10

[8] Council of European Professional Informatics Societies. 2023. CEPIS suggests improvements on amendment to eIDAS regulation. Retrieved November 22, 2024 from https://cepis.org/cepis-suggests-improvements-on-amendment-to-eidas-regulation/

[9] Ingo Dachwitz and Alexander Fanta. 2023. Die fünf größten Schwächen der DSGVO. *netzpolitik.org*. Retrieved November 22, 2024 from https://netzpolitik.org/2023/5-jahre-datenschutzgrundverordnung-die-fuenf-groessten-schwaechen-der-dsgvo/

[10] European Commission. Technical Specifications – EU Digital Identity Wallet. *Technical Specifications – EU Digital Identity Wallet*. Retrieved November 22, 2024 from https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Technical+Specifications

[11] European Data Protection Board. 2023. Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR). Retrieved November 22, 2024 from https://www.edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf

[12] Arno Fiedler and Franziska Granc. 2022. Nationale und europäische Sicht auf eIDAS 2.0 – Aufwand und Nutzen. *Datenschutz Datensich* 46, 1 (January 2022), 27–31. https://doi.org/10.1007/s11623-022-1556-0

[13] Arjan Geluk, Mourad Faher, Fabrice Jogand-Coulomb, Brandon Gutierrez, Kristina Yasuda, Nuno Ponte, Martijn Haring, Anthony Nadalin, David Zeuthen, Jens Urmann, Kenichi Nakamura, Loffie Jordaan, Adam DeFranco, Jesse Dyer, Jean-Marc Desperrier,

Jeff Quarrington, David Chadwick, Xiangying Yang, Sebastian Zehetbauer, Mindy Stephens, David Bakker, Evangelos Sakkopoulos, Bas van den Berg, Matthias Schwan, Gilles Roux, David Jencel, Andrew Hughes, and Ketan Mehta. 2021. ISO/IEC 18013-5 mdoc for eHealth. Retrieved November 22, 2024 from https://github.com/18013-5/micov/blob/469f43bea62a4aee0b2c3a0ba6642726fc3e6d15/ISO_IEC_18013_5_for_eHealth.pdf

[14] Sebastian Hemesath and Lasse Gerrits. 2023. Der elektronische/digitale Personalausweis im internationalen Vergleich (E-ID). In *Handbuch Digitalisierung in Staat und Verwaltung*, Tanja Klenk, Frank Nullmeier and Göttrik Wewer (eds.). Springer Fachmedien Wiesbaden, Wiesbaden, 1–16. https://doi.org/10.1007/978-3-658-23669-4_50-2

[15] Anil Jain, Lin Hong, and Sharath Pankanti. 2000. Biometric identification. *CACM* 43, 2 (February 2000), 90–98. https://doi.org/10.1145/328236.328110

[16] I. Kaper. Sorgfaltspflichten beim Online-Banking — Der Bankkunde als Netzwerkprofi? *DuD* 30, 215–219.

[17] Ferdinand Kopp and Ulrich Ramsauer. 2023. *Verwaltungsverfahrensgesetz* (24th ed.). C.H.BECK, München.

[18] Andraž Krašovec, Daniel Pellarini, Dimitrios Geneiatakis, Gianmarco Baldini, and Veljko Pejović. 2020. Not Quite Yourself Today: Behaviour-Based Continuous Authentication in IoT Environments. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 4 (Dezember 2020), 136:1-136:29. https://doi.org/10.1145/3432206

[19] Chris Lamb and Stefano Zacchiroli. 2022. Reproducible Builds: Increasing the Integrity of Software Supply Chains. *IEEE Software* 39, 2 (March 2022), 62–70. https://doi.org/10.1109/MS.2021.3073045

[20] Chi-Wei Lien and Sudip Vhaduri. 2023. Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey. *ACM Comput. Surv.* 56, 1 (August 2023), 14:1-14:37. https://doi.org/10.1145/3603705

[21] Patrick Liptak. 2022. Ein neuer Rahmen für eine europäische digitale Identität: Änderungsvorschlag der Verordnung (EU) 910/2014 – Neue Handlungsspielräume und regulatorische Stolpersteine. *DuD* 46, 1 (January 2022), 18–21. https://doi.org/10.1007/s11623-022-1554-2

[22] Torsten Lodderstedt, Kristina Yasuda, and Tobias Looker. 2024. OpenID for Verifiable Credential Issuance. Retrieved November 22, 2024 from https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[23] Bert Lukkien, Nitesh Bharosa, and Mark De Reuver. 2023. Barriers for developing and launching digital identity wallets. In *Proceedings of the 24th Annual International Conference on Digital Government Research*, July 11, 2023. ACM, Gdańsk, Poland, 289–299. https://doi.org/10.1145/3598469.3598501

[24] Václav Matyáš and Zdeněk Říha. 2002. Biometric Authentication — Security and Usability. In *Advanced Communications and Multimedia Security: IFIP TC6 / TC11 Sixth Joint Working Conference on Communications and Multimedia Security September 26–27, 2002, Portorož, Slovenia* (*IFIP: The International Federation for Information Processing*), 2002. Springer US, Boston, MA, 227–239. https://doi.org/10.1007/978-0-387-35612-9_17

[25] Münchener Rückversicherungs-Gesellschaft. 2024. *Munich Re Global Cyber Risk and Insurance Survey 2024*. München, Germany. Retrieved November 22, 2024 from https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey-2024.html

[26] Max Muth. 2023. Eine gute Idee, die einfach nicht funktionieren will. *Süddeutsche Zeitung*. Retrieved November 22, 2024 from https://sz.de/1.6044801

[27] Floris Roelofs. Analysis and comparison of identification and authentication systems under the eIDAS regulation.

[28] Isabel Skierka. 2022. Digitale Identitäten. In *Handbuch Digitalisierung in Staat und Verwaltung*, Tanja Klenk, Frank Nullmeier and Göttrik Wewer (eds.). Springer Fachmedien Wiesbaden, Wiesbaden, 1–12. https://doi.org/10.1007/978-3-658-23669-4_66-1

[29] Oliver Terbu, Torsten Lodderstedt, Kristina Yasuda, and Tobias Looker. 2024. OpenID for Verifiable Presentations. Retrieved November 22, 2024 from https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[30] Verbraucherzentrale. 2024. EUDI-Wallet: Was Sie zur digitalen Brieftasche wissen müssen. Retrieved November 22, 2024 from https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/eudiwallet-was-sie-zur-digitalen-brieftasche-wissen-muessen-95821

[31] Wissenschaftliche Dienste des Deutschen Bundestages. 2024. *Zur Umsetzung der eIDAS-VO 2.0 und der Einführung der europäischen Brieftasche für die Digitale Identität*. Retrieved from https://www.bundestag.de/resource/blob/1016308/b70aa9c4b1068b6da73c4e406d7d6405/WD-3-073-24-pdf.pdf