HAL open science

Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?

Niko Tsakalakis, Sophie Stalla-Bourdillon, Kieron O'hara

To cite this version:

Niko Tsakalakis, Sophie Stalla-Bourdillon, Kieron O'hara. Data Protection by Design for Cross-Border Electronic Identification: Does the eIDAS Interoperability Framework Need to Be Modernised?. Eleni Kosta; Jo Pierson; Daniel Slamanig; Simone Fischer-Hübner; Stephan Krenn. Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data : 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers, AICT-547, Springer International Publishing, pp.255-274, 2019, IFIP Advances in Information and Communication Technology, 978-3-030-16743-1. 10.1007/978-3-030-16744-8_17 . hal-02271656

HAL Id: hal-02271656

https://inria.hal.science/hal-02271656v1

Submitted on 27 Aug 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Data Protection by Design for cross-border electronic identification: does the eIDAS Interoperability Framework need to be modernised?

Niko Tsakalakis[1][0000−0003−2654−0825], Sophie Stalla-Bourdillon[2], and Kieron O'Hara[1]

[1] Web and Internet Science, ECS, University of Southampton, Southampton, UK
✉N.Tsakalakis@soton.ac.uk kmo@soton.ac.uk
[2] Institute for Law and the Web, University of Southampton, Southampton, UK
S.Stalla-Bourdillon@soton.ac.uk

Abstract. This paper contributes to the discussion on privacy preservation methods in the context of electronic identification (eID) across borders through interdisciplinary research. In particular, we evaluate how the GDPR principle of 'Data Protection by Design' applies to the processing of personal data undertaken for identification and authentication purposes, suggesting that, in some cases, unlinkable eIDs should be a key requirement in order to facilitate data minimisation and purpose limitation. We argue that in an attempt to welcome diverse types of architectures, the Interoperability Framework could have the effect of reducing the data protection level reached by some national eID schemes, when transacting with services that do not require unique identification. We consequently propose that data minimisation and purpose limitation principles should be facilitated through the implementation of two methods, pseudonymisation and selective disclosure, through an addition to eIDAS' technical specifications.

Keywords: electronic identification · eIDAS · GDPR · privacy by design · data protection by design · unlinkability · selective disclosure · pseudonymisation

1 Introduction

Electronic identification aims at revolutionising the way users interact with online services. In the EU, electronic identification of citizens is at the discretion of the Member States. A handful of Member States have developed national schemes for electronic identification (eID) provision to their citizens, with their architectures varying to a large extend [9].[3] As a result, national systems differ not only in the amount of citizen data they process but also in the level of data protection they offer to these data.

[3] See also country profiles in http://ec.europa.eu/idabc/en/document/6484.html.

Regulation 910/2014 on electronic identification and trust services (hereinafter eIDAS),[4] which came into force on 1 July 2016, enables cross-border interoperability of the diverse national eID schemes. eIDAS aims to create *"a common foundation for secure electronic interaction between citizens, businesses and public authorities"*[5] in order to *"remove existing barriers to the cross-border use of electronic identification means."*[6] Chapter II *"Electronic Identification"* defines the principles required for cross-border eID use across EU Member States by specifying a common denominator in architecture and policies for national schemes to become interoperable. The eID scheme of Germany is the first that has become accessible by all Member States since 29 September 2018.

Meanwhile, the EU's personal data protection framework has been updated by the General Data Protection Regulation (GDPR),[7] which introduced a risk-based approach to data protection and became directly applicable on 25 May 2018. The GDPR aims to facilitate the *"free movement of personal data within the Union"*,[8] in particular in a cross-border context,[9] while ensuring that the data subjects' rights (and in particular their right to the protection of their personal data) are not violated.[10]

Article 25 of the GDPR introduces a new requirement of Data Protection by Design. The term is linked to Privacy by Design, a principle stemming from modern privacy engineering. Privacy by Design[11] is advocating for privacy considerations that are embedded in the technology itself, from the design stage throughout the life-cycle of a system [11], rather than imposed only through soft policy measures.[12] The Privacy by Design Resolution, adopted in 2010 by the International Conference of Data Protection and Privacy Commissioners, stresses that Privacy by Design is a *"holistic concept that may be applied to operations throughout an organization, end-to-end"* [1].

Although Privacy by Design is increasingly explored in literature, the effect of the new requirement of the GDPR on design and architectural choices of online services, such as eID provision, remains partially uncertain. This is especially

[4] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

[5] eIDAS Rec. 2.

[6] eIDAS Rec. 12.

[7] 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 (General Data Protection Regulation) (Text with EEA relevance), OJ L119/1.

[8] GDPR Art. 1(3).

[9] GDPR Rec. 5 *"The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data."*

[10] GDPR Art. 1(2).

[11] A term first coined by Ann Cavoukian [10, 11] but referring to concepts that started to emerge in privacy literature since the 1970s; see, for example, [12, 13, 30].

[12] Which are considered less effective, *"an afterthought"* [40].

true since Data Protection by Design befalls data controllers and processors but not system designers, creating therefore inconsistencies as to how the obligation will be translated into system design. Neither eIDAS nor the GDPR offer specific guidance on the means to achieve Data Protection by Design, allowing room for interpretation by the data controllers. However, although eIDAS is technology-neutral,[13] its provisions and accompanying Implementing Acts define a set of requirements for national schemes. Consequently, there is a need to assess the extent and the means by which Data Protection by Design can be effected in the eIDAS Interoperability Framework. This becomes particularly important when considering that, even though eIDAS primarily targets public-sector online services, voluntary use of the eIDAS framework by private-sector services is actively encouraged.[14] In contrast to public-sector services, whose data dissemination practices are often regulated by national legislation, the private sector remains relatively free to decide how to comply with the data protection requirements of the GDPR.

One key question, therefore, is to assess the implications of Data Protection by Design upon the eIDAS Interoperability Framework, and determine whether the Interoperability Framework could be extended to maintain a high level of data protection in cross-border transactions with both public- and private-sector services.

In order to tackle this question, this paper employs an interdisciplinary approach through the use of three different methods: Desk research on Privacy by Design and its application for eID schemes, a synthesised assessment of the general guidance on Data Protection by Design and Data Protection Impact Assessments, and qualitative data collection through a series of interviews with experts in the field of eID. The desk research is used to identify the goals and methods of Data Protection by Design, and in particular how these goals are met in the context of eID. To fully identify its effects in the context of eID, Article 25 of the GDPR should be read in conjunction with Article 35 on Data Protection Impact Assessments, which are meant to provide a process through which the engineering of data protection principles and security measures shall be assessed [37]. Finally, the interviews, which followed a semi-structured format, were used to confirm the findings of the assessment and gave the opportunity to eID experts to express their opinion on Data Protection by Design for eID and the expected impact of eIDAS' Interoperability Framework on participating schemes.

[13] eIDAS Rec. 27: *"This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met."*

[14] See eIDAS Rec. 17: *"Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions."* See also [44], p. 2: *"the Commission will further promote interoperability actions, including through issuing principles and guidance on eID interoperability at the latest by 2017. The aim will be to encourage online platforms to recognise other eID means – in particular those notified under the eIDAS Regulation (EC) 910/2014 – that offer the same reassurance as their own."*

Through thematic analysis, the transcripts established the current practices in eID schemes and the state-of-the-art in regards to Data Protection by Design. We refer to national eID schemes to illustrate how a state-of-the-art system will be impacted by the Interoperability Framework.

The paper is structured as follows: Section 2 provides an overview of the Interoperability Framework as defined by eIDAS and its Implementing Acts. We explain the link to the GDPR in section 3 and examine the domain and effect of Data Protection by Design, through seven 'data-protection goals' as proposed by the German Standard Data Protection Model [15]. In section 4 we examine how the Interoperability Framework meets the data protection goals and note that the goal of unlinkability is only partially met. We focus, thus, on unlinkability and analyse what unlinkability entails for eID schemes. We explain how the Interoperability Framework might in certain cases result in constrains on the level of unlinkability that can be supported in cross-border transactions in section 5 and consequently propose a practical way to assure the Interoperability Framework can be extended to support a higher level of unlinkability in section 6. A summary of our findings and concluding remarks can be found in section 7.

2 The eIDAS Interoperability Framework

The cross-border communication of national eID schemes takes place through a set of nodes and related specifications that eIDAS names *'Interoperability Framework'*.[15] Communication between national eID schemes and service providers happens through *'eIDAS nodes'*.[16] eIDAS names the Member State whose notified eID scheme is used as the *'sending Member State'* [17] and the Member State where the service provider resides as the *'receiving Member State'* [17]. Two configurations are supported: The sending Member State can operate an eIDAS node domestically, which will relay authentication requests and assertions between the service providers of the the receiving Member State and the national eID scheme (proxy configuration) [17]. Alternatively, the sending Member State provides an instance of their national eID scheme as an eIDAS node which is deployed to each receiving Member State (middleware configuration). The middleware is operated by operators at the receiving Member State [17].

eIDAS defines a set of *'person identification data'*[17] to be transmitted in cross-border identifications. Participating schemes need to satisfy a *'Minimum Dataset'*, which contains four mandatory and four optional attributes.[18] Mandatory attributes are the (a) first and (b) last names of the person, (c) their date of birth and (d) a unique identifier *"as persistent as possible in time."*[19] In addition, the Minimum Dataset may contain (a) the first and last name(s) at

[15] eIDAS Art. 12.
[16] eIDAS Art. 8(3) and [22].
[17] eIDAS Art. 3(3): *"a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established"*.
[18] IR 2015/1501 ANNEX 1.
[19] IR 2015/1501 ANNEX 1(d).

birth, (b) the place of birth, (c) the current address and (d) the gender.[20] The Minimum Dataset is required in every cross-border identification.

eIDAS recognises that eID services have to perform data processing for the needs of electronic identification. Accordingly, Article 5(1) establishes that all processing should be carried out *"in accordance with Directive 95/46/EC"*, which has since been repealed by the GDPR.[21] Consequently the benchmark for data protection compliance under eIDAS is the GDPR. Interestingly, eIDAS seems to have anticipated the GDPR. Article 12(3)(c) of eIDAS mandates that the Interoperability Framework shall *"facilitat*[e] *the implementation of the principle of Privacy by Design;"* and Article 5(2) provides that *"the use of pseudonyms in electronic transactions shall not be prohibited."* In addition, the explanatory recital in the preamble refers to the principle of data minimisation.[22] However, even if eIDAS seems to acknowledge the importance of Data Protection by Design, it is arguable whether the way the Interoperability Framework has been set up can really facilitate the level of data protection guaranteed by some national eID schemes in cases where full identification of a natural person is not necessary.

In order to derive the potential impact of the GDPR on eIDAS it is necessary to analyse the domain and effects of GDPR Article 25. Such an analysis needs to be coupled with an analysis of GDPR Article 35, which offers a process to contextually derive the requirements of Data Protection by Design.

3 Data Protection by Design

Data Protection by Design, under Article 25 of the GDPR, stems from the literature and practice of Privacy by Design approaches in system engineering. Privacy by Design models have extended and refined the protection goals from the field of computer security (confidentiality, integrity and availability, i.e. the 'CIA' model [7,36]), following the model developed by [52] and [28] and which formed the basis of the German Standard Data Protection Model [15]. Four privacy specific goals have been added to the CIA model, to form seven data protection goals: *confidentiality*, *integrity*, *availability*, *transparency*, *intervenability unlinkability* and *data minimisation* [6, 14, 15, 28, 29, 41, 52].

Article 25 of the GDPR obliges data controllers to *"implement appropriate technical and organisational measures"* in order to effectively adhere to data protection principles.[23] Data processors are indirectly captured by GDPR Article 25[24] and system producers are *"encouraged* [...] *with due regard to the state of*

[20] ibid.

[21] GDPR Art. 94(2): *"References to the repealed Directive shall be construed as references to this Regulation."*

[22] eIDAS Rec. 11: *"authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online."*

[23] GDPR Art. 25(1).

[24] GDPR Art. 28(1): "[data controllers] *shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures"*.

the art, to make sure that controllers and processors are able to fulfil their data protection obligations."[25] Of note, eIDAS' requirement to facilitate Privacy by Design could be seen as going further than the GDPR in that it does not expressly target only data controllers. The measures envisioned by Article 25 have to be in place *"both at the time of the determination of the means for processing and at the time of processing itself"*.[26] In other words, technological and policy support for the privacy of data subjects has to be implemented from the design phase and throughout the processing operations. A failure to comply with this requirement might trigger an administrative fine of up to €10.000.000 or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[27] The controller shall justify the selected measures against a list of contextual factors: *"the cost of implementation and the nature, scope, context and purposes of processing as well as the risks* [...] *posed by the processing"*.[28]

The seven data protection goals align with the data protection principles of Article 5 GDPR.[29] An overarching principle, explicitly mentioned in Article 25, is data minimisation. Data minimisation requires the processing (including the collection) of only the data *"limited to what is necessary"*[30] to accomplish a certain purpose. In tandem, under the purpose limitation principle, processing purposes must be specified, explicit and legitimate;[31] in other words purposes should already be defined before data collection. Therefore, not only collection of data must be limited, but collected data must be strictly necessary to a predefined relevant purpose. Confidentiality refers to non-disclosure of certain aspects in an IT system. In a privacy context it can be translated as the need to ensure that information is accessible only by authorised users. Integrity protects the modification, authenticity and correctness of data. It relates, therefore, to safeguards for the accuracy and completeness of the data and their processing methods. Availability concerns the availability, comprehensibility and processability of data. Transparency relates to 'soft' privacy – the relevant policies, reporting and auditing mechanisms in place. Intervenability ensures that parties to the data processing can intervene in the processing when necessary. Finally, unlinkability regards the inability of an attacker to know if any two points of a system are related (for example, an eID and its owner).[32] Of note, this definition as explained

[25] GDPR Rec. 78.
[26] GDPR Art. 25(1).
[27] GDPR Art. 83(4)(a).
[28] GDPR Art. 25(1); the qualification will be determined, among others, through a data protection impact assessment.
[29] Confidentiality under GDPR Art. 5(1)(f); integrity under Art. 5(1)(f); availability under Art. 32(b) in relation to Art. 5(1)(f); transparency under Art. 5(1)(a); intervenability under Art. 5(1)(d) and (e) in relation to Arts. 15–22; unlinkability under Art. 5(1)(c) and (e); data minimisation under Art. 5(1)(c).
[30] GDPR Art. 5(1)(c).
[31] GDPR Art. 5(1)(b).
[32] "[Unlinkability] *ensures that a user may make multiple uses of resources or services without others being able to link these uses together* [...] *Unlinkability requires that*

below is only partial as it focuses upon external actors only. Yet, we argue that in a data protection context, unlinkability should also take into account internal actors.

The data protection goals systematize the obligations put forth by the GDPR, to assist when performing a Data Protection Impact Assessment [15]. Data Protection Impact Assessments are meant as a tool to effect the engineering of data protection principles in a system and, thus, Data Protection by Design. Examining the Interoperability Framework, therefore, in the light of the data protection goals is a useful way to determine the level of Data Protection by Design afforded by eIDAS.

4 The goal of unlinkability for eID schemes

Looking at the Interoperability Framework through the prism of data protection goals, it is clear that those goals have guided the action of the EU legislature. Although most data protection goals have been taken into account by eIDAS and its Implementing Acts,[33] facilitation of the level of unlinkability might be further extended, especially in cases where the service provider is a private-sector entity.

Data minimisation in eIDAS is dealt with through the definition of the Minimum Dataset. The premise is that the Minimum Dataset represents the absolute minimum of attributes necessary to *"uniquely represe*[nt] *a natural or legal person"*.[34] *Confidentiality* is guarding against unauthorised access and disclosure of data. The Implementing Acts define a series of *"implement*[ed] *security controls"*,[35] following a risk-based approach depending on the applicable Level of Assurance, that aim to secure that access and disclosure happens only against authorised actors. The Levels of Assurance ('Low' – 'Substantial' – 'High')[36] also guarantee that technical controls are in place to effect the *integrity* of the claimed identity and its data.[37] *Availability*, which is an explicit goal of eIDAS Article 7(f), is served through legal[38] and technical controls.[39] *Transparency* is addressed by way of published notices and user information about the service providers and the national schemes.[40] Even though eIDAS does not strictly require service providers to display their identity to the users, it allows service providers to do so if they wish [18]. *Intervenability*, which relates to the user rights about rectification, revocation and erasure of their data, is left to the

users and/or subjects are unable to determine whether the same user caused certain specific operations in the system" [35].

[33] For a detailed analysis of how the Interoperability Framework meets the data protection goals, see [47].

[34] eIDAS Art. 12(4)(d).

[35] Commission Implementing Regulation (EU) 2015/1501 Art. 6(2).

[36] Commission Implementing Regulation (EU) 2015/1502 ANNEX 2.3.1.

[37] ibid, ANNEX 2.4.6.

[38] eIDAS Art. 11(1) and 11(3).

[39] Commission Implementing Regulation (EU) 2015/1502 ANNEX 2.4.4 and 2.4.6.

[40] ibid, ANNEX 2.4.2.

responsibility of the national eID schemes, since eIDAS is only meant to relay eID data.

Unlinkability appears to be one of the most challenging goals to meet in the context of the Interoperability Framework. Unlinkability aims to serve data minimisation and purpose limitation. In general unlinkability is used to express the impossibility of linking an action performed inside a system (for example, sending a message) to a particular process or agent of the system (in this example, the sender), or the possibility to infer from an outside standpoint that two different sessions in the system (for example two different messages) are performed by the same agent (have, for example, the same originator).[41] However, in a data protection context, unlinkability refers to the risk of linking personal information to its data subject. Therefore, the goal of unlinkability is to eliminate risks of data misuse by minimising risks of profiling [52]. Unlinkability is a key requirement for eID schemes. Indicated in the literature, and confirmed in the expert interviews,[42] a primary goal of *privacy-enhancing* eID schemes is to prevent different pieces of information to be linked together [28, 29, 49].

The GDPR elevates unlinkability into a performance standard through the data minimisation and purpose limitation principles. Privacy discourse has identified mechanisms for unlinkability, such as data avoidance, separation of contexts through federated distribution, encryption, access control, anonymisation, data destruction etc. [20]. However, the GDPR refrains from providing design standards to realise purpose limitation and data minimisation. Article 25 and its relevant Recital 78 only provide pseudonymisation as an example. In this paper we limit the focus to two specific measures, pseudonymisation and selective disclosure, since both have been identified in electronic identification literature as of particular importance for unlinkability [16, 39, 41, 52]. Pseudonymisation is explicitly mentioned in the GDPR.[43] Based on the definition of pseudonymisation,[44] it must be assumed that a pseudonymised eID dataset can only exist coupled with selective disclosure, i.e. when no other identifying attributes are present in the dataset.[45]

Data minimisation could be seen as having three dimensions: minimisation of content, where the amount of information collected should be the minimum necessary;[46] temporal minimisation, where information should be stored only for the minimum amount of time necessary for the specific processing;[47] and

[41] See [3] where the authors define the two as "*strong*" and "*weak*" unlinkability.

[42] Excerpts from the interviews are not included in this paper due to space constraints. For a transcript of the experts' opinions, see section 8 and the appendix in [47].

[43] GDPR Art. 4(5).

[44] *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;"* [emphasis given].

[45] For a thorough explanation of this argument, see [48].

[46] GDPR Art. 5(1)(c): *"limited to what is necessary in relation to the purposes"*.

[47] GDPR Art. 5(1)(e): *"for no longer than is necessary for the purposes for which the*

minimisation of scope, where data should be used only for the purposes collected.[48] Selective disclosure addresses data minimisation in the strict sense of Article 5(1)(c) – content minimisation. As a means to effect content minimisation, selective disclosure refers to the ability to granularly release information for a specific purpose. Selective-disclosure-capable systems have the ability to accept and transmit only a subset of the available attributes, depending on the processing at hand [38]. An advanced example of selective disclosure can be seen in figure 1, where the system only transmits an inferred claim calculated from the user's age instead of transmitting the user's date of birth.

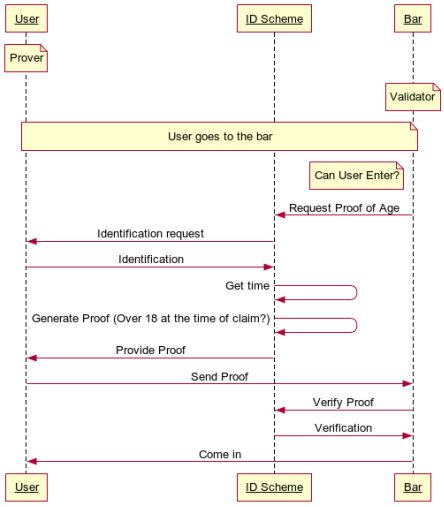

Fig. 1: Simplified Verifiable Claim using Selective Disclosure

Pseudonymisation as a means of unlinkability refers to the substitution of direct identifiers with constructed attributes so that the link with the original identifying dataset weakens. There are several degrees of pseudonymisation, with the main impacting factors being the frequency of use of a certain pseudonym and the amount of remaining identifying information in the set. In cases where pseudonyms change across uses ('unidirectional pseudonyms'), linkability between datasets is greatly reduced. On the contrary, where the same pseydonym is deployed regardless of use (an 'omnidirectional' pseudonym) there is a risk of linkability as the pseudonym can act in the form of a *de facto* unique identifier. In eID architectures unidirectional pseudonyms have so far been deployed in two ways: in 'pairwise persistent' configurations, different pseudonyms are constructed

personal data are processed".

[48] GDPR Art. 5(1)(b): *"not further processed in a manner that is incompatible with those purposes"*.

for every pair of pseudonym–user, but remain the same for the specific pair. This way no two service providers receive the same pseudonym, and therefore, service providers cannot easily infer that the pseudonyms refer to the same user. However, since the pseudonym is persistent for that specific user–service pair, it is technically possible for the service to monitor how the pseudonym is used in its system (even if the real identity of the user is not yet known).[49] In contrast, in deployments where the pseudonyms change in between uses even of the same service ('transient pseudonyms') a service provider is not able to distinguish that two uses concern the same user [50]. Although this resolves the issue of linkability it makes it difficult for services to recognise recurring users. For this reason pairwise persistent pseudonyms are preferred in practice.[50]

An illustrative example of how unlinkability has been addressed can be given through the case of the German "*neuer Personalauswess*" (*nPA*). The nPA is a federated eID scheme, based around a national eID card that is provided to every citizen. The scheme was built around Privacy by Design principles, supporting advanced privacy controls for the users.[51] The implementation does not depend on an Identity Provider,[52] identification of the user happens through the eID card and a user-controlled middleware software [42].

The nPA incorporates data minimisation through selective disclosure and pseudonymisation. The card has a pre-defined set of attributes stored inside a local RFID chip (refer to table 1). When performing an electronic identification, the service provider requests the attributes necessary for the identification. The user can then select which of the requested identifiers they wish to disclose to the service provider (selective disclosure). Additionally the nPA employs pairwise-persistent pseudonyms in lieu of an identifier, which are different for every pair of user–service [23,24]. Notably, if a service decided to sub-let their eID infrastructure to other services, all services under the same infrastructure would receive the same pseudonym, therefore increasing the potential to infer the associated identity of the user by combining data. To eliminate this risk, Germany has put policies in place (soft privacy) that forbid linking of data.[53]

[49] This is an issue with 'pairwise persistent' pseudonyms. In a case where two or more services merge together, pairwise persistent pseudonyms can potentially allow linkability depending on the existence of other common identifiers in the dataset.

[50] Privacy-aware eID schemes have started to deploy alternative architectures to sidestep the privacy concerns of pairwise-persistent pseudonyms. See, for example, the implementation of Gov.UK Verify, where a hub in between the Identity and Service Provider mediates all communication in order to obscure the one from the other [27] (cf. though [46] on potential risks); in contrast, the approach taken by the German nPA scheme is to generate pseudonyms locally in the user's eID token.

[51] The basic premise behind the system's design is that the identifying set of information, referred to as a *"sovereign data set"*, has greater value after validation as trustworthy by an official source and therefore deserves greater protection.

[52] Although strictly speaking there is a central Identity Provider operated under the Federal Ministry of the Interior; however its role is to authenticate the service providers, not the users.

[53] German law is rich in privacy-enhancing principles. At the core is the *'right to*

The nPA also supports advanced calculations, providing a Yes/No answer about a user's age or location eligibility – without disclosing therefore the user's date of birth or address [24].

On 22 August 2017 Germany pre-notified the nPA under the process of eIDAS Article 9 [25], with the notification published on 26 September 2017.[54] Since the nPA is the first notified scheme, it is an excellent example to highlight potential issues with unlinkability within the eIDAS framework. Of note, the nPA is not the only national scheme to feature unlinkability for privacy protection: the Austrian and the UK's schemes also feature a form of pairwise persistent pseudonymisation, whereas Austria plans to also introduce a form of selective disclosure.[55] The Belgian scheme is also exploring pseudonymisation solutions.[56] Effectively, one third of the schemes currently undergoing a notification procedure for eIDAS is deploying some level of unlinkability.[57] However, this paper will largely refer to the German scheme since it has already undergone the notification process.

Opt.[a]	**eIDAS MDS**	**German eID**
M	Uniqueness identifier	Pseudonym[b]
M	Current family name(s)	Family name
M	Current first name(s)	First name
M	Date of birth	Date of birth
O	First name(s) and family name(s) at birth	Birth name (if present on the eID card)
O	Place of birth	Place of birth
O	Current Address	Address
O	Gender	N/A

[a] *M = Mandatory attribute, O = Optional attribute*

[b] The pseudonym of the German eID scheme is specific to each eID card and each receiving Member State (for public-sector bodies) or each service provider (for private-sector bodies).

Table 1: Minimum Data Set provided by the German eID scheme [26]

information self-determination' which is a German inception. It confers the right to decide when and within what limits information about one's self should be communicated to others [31]. The right stemmed from a decision of the German Constitutional Court: Volkszählungsurteil 1 BvR 209/83, BVerfGE 65 E 40 1ff. The Court further prohibited any future creation of a persistent unique identifier, ibid s 1. Public authorities operate under a *'separation of informational powers'* – they are not allowed to collate data, as the state should not operate as a single entity, and all data transfers have to be justified against the principles of 'purpose specification' and 'proportionality' [8].

[54] CEF Digital, Overview of pre-notified and notified schemes under eIDAS (2018) https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

[55] See for more [47] pp. 48–64.

[56] ibid, Appendix.

[57] For the full list of national schemes undergoing notification, see https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

5 Unlinkability in the Interoperability Framework

The aspiration of eIDAS to set up a *"technology-neutral"* Interoperability Framework should indicate that advanced privacy designs are supported. This is supported by the explicit mention that the Interoperability Framework will facilitate Privacy-by-Design[58] and eIDAS will not prejudice against the use of pseudonyms.[59] At the very least, it should denote that where national systems support such features, they can be integrated in the Interoperability Framework. However, it appears that the necessity of a common denominator, which is considered essential for transactions with public-sector services, hampers the extend to which Privacy by Design can be used. The main obstacle is the Minimum Dataset and its mandatory attributes.[60]

The Minimum Dataset was devised in order to ensure that public-sector service providers, who are obliged to accept other EU Member State's notified eIDs, will have enough information to uniquely identify a foreign citizen. The Minimum Dataset, in other words, is based on the assumption that public-sector services are dependent on successful unique identification of a person in order to provide a service. This is true for a lot of public-sector services eIDAS targets: filing taxes, proving residence status, using student services, opening bank accounts.[61] In addition, some e-government services depend upon a degree of linkability, that the Minimum Dataset provides, in order to satisfy the *'once-only principle'*.[62] However, not all services benefit from a degree of linkability: this is certainly true for providers of the private-sector who rarely require identification in order to provide a service, such as for example online social platforms, but also for a number of public-sector providers who either operate services where identification is not necessary (i.e. where age verification suffices) or operate sensitive services, like national health services (i.e. drug rehabilitation services). In such cases, linkability could damage the reliability of the provided service, increasing the risk of profiling or data misuse.

Looking back at Germany's notification, the adaptation of the nPA's characteristics in order to conform to eIDAS' requirements already excludes its full

[58] eIDAS Art. 12(3)(c).

[59] eIDAS Art. 5(2).

[60] This is also the position of the ABC4Trust project in [2], which was published before the GDPR, and hence before Data Protection by Design was elevated to a requirement.

[61] The four use cases are indicative examples about the benefits of eIDAS by the eGovernment and Trust team: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid.

[62] An e-government concept that citizens and businesses provide diverse data only once in contact with public administrations, while public administration bodies take actions to internally share and reuse these data. The *'once-only principle'* was one of the targets of the EU's 'eGovernment Action Plan 2016-2018' [21] and the reason behind the EU's 'Single Digital Gateway': http://www.europarl.europa.eu/news/en/headlines/economy/20180911STO13153/single-digital-gateway-a-one-stop-shop-for-all-your-online-paperwork.

pseudonymisation and selective disclosure capabilities. Germany will be deploying the nPA as middleware instances – an instance located at and operated by each receiving Member State. They have also provided a mapping against the attributes required by eIDAS (table 1). The optional attribute of the gender is not present in the nPA dataset; the optional attribute of name at birth can be provided but only where the attribute has been included in the eID card. All mandatory attributes, nonetheless, are supported. Since eIDAS mandates that the mandatory part of the Minimum Dataset shall in any case be transmitted, and, depending on the receiving service, might be enriched by optional attributes, a user of the nPA will not be able to (de)select attributes for transmission without resulting in an unsuccessful authentication.

In addition, in absence of unique identifiers in Germany[63] the nPA will substitute the mandatory *'Uniqueness identifier'* with a pseudonym. As explained above, the card is capable of producing a persistent unique pseudonym for each pair of user–service, which provides a basic protection against linkability of data between services. However, in cross-border authentications, all of the public-sector services of the receiving Member State will be considered as one service. The receiving Member State will be assigned a pseudonym unique for the pair user–Member State, which will function as the Minimum Dataset's *'uniqueness identifier'* [26].[64] As a result, all public-sector services of the receiving Member State will be receiving the same unique identifier (along with at least the remaining mandatory attributes) thereby raising the question of how linkability of data and uses within a receiving Member State can be prevented. Note that, as abovementioned,[65] under the GDPR in order for a dataset to be considered pseudonymised all other attributes aside from the pseudonyms have to be such that identification of the data subject is not possible. That would be the case, for example, when the only attributes in a dataset are a pseudonym and a date of birth. Seeing as, even when a pseudonym is used in place of a unique identifier, it will always be accompanied by identifying information (the rest of the mandatory Minimum Dataset attributes) it is unlikely that an eIDAS dataset will ever meet the definition of GDPR's pseudonymisation.[66] In this sense, there can be no pseudonymisation in eIDAS without selective disclosure. Thus, use of pseudonyms in eIDAS might not be *'prohibited'* per se, but it certainly is restricted.

With selective disclosure and pseudonymisation restricted, *'facilitation'* of Privacy by Design is constrained. In the spirit of the GDPR, the measures afforded by a system should be proportionate to the levels of risk involved in the data processing [4]. Cross-border eID provision should be expected to involve

[63] See prohibition of the German Constitutional Court above fn. 53.

[64] The decision might be related to how services in Germany are authorised to access the eID data: services have to file an application with the Federal Office of Administration, listing all the attributes they wish to have access to along with how the attributes relate to the processing purposes [51]. The decision to treat all public-sector services of a Member State as one, and therefore request a combined authorisation, might be in an attempt to make the process easier for the receiving Member State's authorities.

[65] In fn. 44 and related discussion.

[66] See further analysis in [48].

high-risks of processing before any mitigating controls are put in place, in light of the guidance on Data Protection Impact Assessments [5].[67] It can be argued therefore that, by limiting the amount of unlinkability afforded by national systems, service providers that do not require all the attributes of the Minimum Dataset will face problems justifying its processing. Obviously this assertion is contextual. The capabilities of the national scheme providing the electronic identification have a clear impact, as not all systems support selective disclosure and pseudonymisation. However, at least when supported by the national system, the eIDAS Interoperability Framework should be able to support a higher level of unlinkability.

Acting otherwise can prove highly problematic for national schemes that support a high level of unlinkability, as these national schemes will not be able to guarantee such a level for cross-border transactions. In light of eIDAS Article 8, the description of the Levels of Assurance and their governing data protection goals, i.e. integrity, the Member States that offer a high degree of unlinkability would not be in a position to negotiate attributes with service providers that do not require the full Minimum Dataset. As a result, there is an argument that eIDAS Article 12(c) would not be met in the sense that the Interoperability Framework would undermine rather than facilitate Privacy by Design. Going further, national data controllers enabling and operating eID and authentication cross-border would be prevented from offering to their users a high level of data protection in cases where the services requesting eID do not need the complete Minimum Dataset. This could have implications in terms of liability as eIDAS Article 11 should be read in combination with GDPR Articles 82 and 83.

6 Reinforcing the level of Data Protection by Design in eIDAS

Better incorporation of selective disclosure and pseudonymisation into the Interoperability Framework could reinforce Data Protection by Design in the eIDAS Interoperability Framework. It is true that modifying the Framework to accept different capabilities depending on the features of every national system might be impossible, as it would require an upfront insight into the design of all EU systems – whose participation in the Framework is after all voluntary and, hence, not guaranteed. A potential practical way out however would be through an extension of the supported SAML exchanges.[68] Currently the SAML profile specifies that *"at least all attributes defined as mandatory within this minimum data set MUST be requested. At least one minimum data set MUST be requested in*

[67] Among others: processing that affects a significant proportion of the population, using data items in high volumes or on a wide scale, with a significant processing duration and in a large geographical extent.

[68] The national systems, the deployed eIDAS nodes and the service providers communicate through defined queries and answers in Security Assertion Markup Language (SAML) [18].

each `<saml2p:AuthnRequest>`*"* [19].[69] The SAML exchanges could be enriched to be able to distinguish and accept requests for a smaller amount of attributes than the ones present in the Minimum Dataset, depending on the requirements of the service provider. The extension would be similar to the proposed scenario in [32]. In this scenario, the service provider would have to specify the required attributes in its request for authentication (see Listing 1 in [32]). The Minimum Dataset would still be sent to the eIDAS node, so as to satisfy the design of systems that do not natively support selective disclosure or pseudonymisation. However, the eIDAS node would then be able to extract only the attributes specified in the request, repackage them into a set under a different pseudonym in place of a unique identifier and transmit them back to the service provider. A similar architecture has been proposed in [43], when the FutureID broker acts in a *'claims transformer mode'*. However, the eIDAS node would not perform the authentication itself (at least when functioning in a proxy mode) but it would simply transform the SAML assertion received by the national eID scheme. Such a functionality is supported, for example, by the eID component (based on [34]) in the FutureTrust project currently under way [33].

If the notified scheme is deployed in a proxy mode [17], and therefore operated by the sending Member State, a solution like that would ensure that no excessive personal data leave the territory of the notified scheme. In cases where the national system is deployed in and operated by the receiving Member State in a middleware configuration, the transmitting Member State has significantly less control over the amount of attributes used. In a middleware configuration it seems likely that the Minimum Dataset will always have to be transmitted to the receiving Member State. However, instead of forwarding the whole Minimum Dataset to the service provider, the eIDAS node could then be able to selectively transmit attributes. The ability to select which attributes to disclose and package them under different pseudonyms would strengthen the level of privacy by reducing the amount of information service providers receive and, effectively, the risk of data collusion. Additionally, selective disclosure at the receiving Member State level would guarantee that in a case of dispute, i.e. in cases of fraud or a law enforcement investigation, the receiving Member State would be able to backtrack the pseudonymisation to identify the affected citizens. This extension of eIDAS constitutes an easy, low cost solution since it requires neither the alteration of eIDAS nor the modification of the architecture. Instead, it can be effected through the issuance of a Regulatory Technical Standard that will provided the added SAML elements to the current eIDAS SAML profile.

7 Conclusion

The risk-based approach of the GDPR in principle allows data controllers to tailor the protection of personal data in their systems as determined by the nature of

[69] See 6.2 SAML AuthnRequest in [19]. Of note, the equivalent SAML profile of the STORK 2.0 project, which formed the basis of eIDAS, was capable of selective disclosure (see 4.1.4.8.1 in [45]).

data processing. The GDPR supports this relative freedom by refraining from specifying an explicit list of appropriate compliance measures. However in practice this might lead to protection that is sub-par to what technology can currently support. Such a case can be observed in relation to eIDAS and its requirement for a Minimum Dataset of mandatory attributes.

Modern electronic identity technology recognises that the amount of information needed for successful authentication varies depending on the service. It also accepts that for better protection of personal data, linkability of datasets should be prevented as far as possible. This paper argues that, on par with the GDPR's risk-based approach, data minimisation should vary subject to the needs of the accessed service and the implemented technical and organisational measures in the Interoperability Framework should provide the same level of data protection guaranteed by the Member States.

The adequate level of data protection should be judged based upon the data-protection goals, which systematise the obligations put forth by the GDPR. eIDAS has been diligent in satisfying most of these protection goals, through its provisions and related Implementing Acts and technical specifications. However, in an effort to define a common denominator for interoperability, the existence of the Minimum Dataset and its unique identifier put constrains into the degree of unlinkability that can be afforded by eIDAS' Interoperability Framework.

This is problematic for participating national schemes that provide a high degree of unlinkability through advanced selective disclosure and pseudonymisation. These schemes will be forced, when participating in eIDAS, to lower the level of protection they provide to their citizens.

This paper proposes that the way the eIDAS nodes operate should be altered so that selective disclosure and pseudonymisation can be possible for the national schemes that support them. Selective disclosure and pseudonymisation, and consequently a greater level of data minimisation, will significantly improve the amount of data that data controllers in electronic identification, residing either in the sending Member State or the receiving Member State, are processing. Thus, such a solution would reduce the associated risks, offering easier ways to demonstrate compliance with the GDPR. We demonstrate how such a solution could be achieved through alterations to the eIDAS SAML profile by way of a Regulatory Technical Standard so that its implementation causes the minimum disruption possible.

Acknowledgement This research was partly funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, University of Southampton, EP/L016117/1 and partly funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 700542. The authors would like to thank the DG CONNECT, the DG DIGIT and the eIDAS Technical sub-group for their invaluable feedback during the review process of this paper. This paper reflects only the authors' views; the Commission is not responsible for any use that may be made of the information it contains.

FutureTrust

References

1. 32nd International Conference of Data Protection and Privacy Commissioners: Resolution on privacy by design (2010)
2. ABC4Trust: Privacy-ABCs and the eID Regulation. Position paper, ABC4Trust (2014), https://abc4trust.eu/download/documents/ABC4Trust-eID-Regulation.pdf
3. Arapinis, M., Chothia, T., Ritter, E., Ryan, M.: Analysing Unlinkability and Anonymity Using the Applied Pi Calculus. In: 23rd IEEE Computer Security Foundations Symposium. pp. 107–121 (July 2010). https://doi.org/10.1109/CSF.2010.15
4. Article 29 Data Protection Working Party: Statement on the role of a risk-based approach in data protection legal frameworks. WP 218 (30 May 2014)
5. Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP 248 rev 0.1 (4 April 2017), as last revised and adopted on 4 October
6. Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M.: A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In: Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (eds.) Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings, pp. 21–37. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-44760-5_2
7. Bishop, M.: Introduction to Computer Security. Addison-Wesley Professional (2004)
8. Burkert, H.: Balancing informational power by informational power or Rereading Montesquieu in the internet age. In: Brousseau, E., Marzouki, M., Méadel, C. (eds.) Governance, Regulation and Powers on the Internet, book section 4, pp. 93–111. Cambridge University Press, Cambridge (2012)
9. Castro, D.: Explaining international leadership: Electronic identification systems. Tech. rep., ITIF (2011), http://www.itif.org/files/2011-e-id-report.pdf
10. Cavoukian, A.: 7 Laws of Identity: The Case for Privacy-embedded Laws of Identity in the Digital Age. Information and Privacy Commissioner of Ontario (2006), http://www.ontla.on.ca/library/repository/mon/15000/267376.pdf
11. Cavoukian, A.: Privacy by Design: The 7 foundational principles. Information and Privacy Commissioner of Ontario (2009), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
12. Chaum, D., Fiat, A., Naor, M.: Untraceable electronic cash. In: Goldwasser, S. (ed.) CRYPTO - Lecture Notes Computer Science, vol. 403, pp. 319–327. Springer (1988)
13. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**(2), 84–90 (Feb 1981). https://doi.org/10.1145/358549.358563
14. CNIL: Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA). Commission Nationale de l'Informatique et des Libertés (2015), https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf
15. Conference of the Independent Data Protection Authorities of the Bund and the Länder: The standard data protection model. V.1.0 – Trial version (2017), https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf
16. Dhamija, R., Dusseault, L.: The seven flaws of identity management: Usability and security challenges. IEEE Security & Privacy **6**(2), 24–29 (2008). https://doi.org/10.1109/msp.2008.49
17. eIDAS Technical Sub-group: eIDAS – Interoperability Architecture (2015), https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

18. eIDAS Technical Sub-group: eIDAS SAML Attribute Profile (20 June 2015), https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf
19. eIDAS Technical Sub-group: eIDAS Message Format. v. 11.2 (2016), https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20Message%20Format_v1.1-2.pdf?version=1&modificationDate=1497252919575&api=v2
20. ENISA: Privacy and Data Protection by Design (2015), https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design
21. European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU eGovernment Action Plan 2016-2020 – Accelerating the digital transformation of government. COM(2016) 179 final, Brussels, 19 May (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0179
22. European Commission: eIDAS-Node Integration Package Service Offering Description (2018), https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Node+integration+package?preview=/46992716/59191417/CEF_eID_eIDAS-Node_Integration_Package_Service_Offering_Description.pdf
23. Federal Office for Information Security [BSI]: Innovations for an eID Architecture in Germany (2011), http://www.personalausweisportal.de/SharedDocs/Downloads/EN/Flyers-and-Brochures/Broschuere_BSI_innovations_eID_architecture.html?nn=6852820
24. Federal Office for Information Security [BSI]: Technical Guideline TR-03127: Architecture electronic Identity Card and electronic Resident Permit (2011), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03127/BSI-TR-03127_en.pdf
25. Federal Office for Information Security [BSI]: eIDAS Notification of the German eID (February 2017), https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS/notification/eIDAS_notification_node.html
26. Federal Office for Information Security [BSI]: German eID based on Extended Access Control v2: Overview of the German eID system. version 1.0 (20 February 2017), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf?__blob=publicationFile&v=7
27. Government Digital Service: Gov.UK Verify Technical Guide: Architecture Overview (October 2014), https://alphagov.github.io/rp-onboarding-tech-docs/pages/arch/arch.html
28. Hansen, M.: Marrying transparency tools with user-controlled identity management. In: Fischer-Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (eds.) The Future of Identity in the Information Society, IFIP – The International Federation for Information Processing, vol. 262, book section 14, pp. 199–220. Springer US (2008). https://doi.org/10.1007/978-0-387-79026-8_14
29. Hansen, M., Jensen, M., Rost, M.: Protection goals for privacy engineering. In: 2015 IEEE Security and Privacy Workshops. pp. 159–166. IEEE, San Jose, CA, USA (2015). https://doi.org/10.1109/SPW.2015.13
30. Hes, R., Borking, J. (eds.): Privacy-Enhancing Technologies: The Path to Anonymity – Revised Edition. Registratiekamer (2000)
31. Hornung, G., Schnabel, C.: Data protection in Germany I: The population census decision and the right to informational self-determination. Computer Law & Security Review **25**(1), 84–88 (2009). https://doi.org/http://dx.doi.org/10.1016/j.clsr.2008.11.002, http://www.sciencedirect.com/science/article/pii/S0267364908001660

32. Horsch, M., Tuengerthal, M., Wich, T.: SAML Privacy-Enhancing Profile. In: Hühnlein, D., Roßnagel, H. (eds.) P237 - Open Identity Summit 2014. pp. 11–22. Gesellschaft für Informatik e.V., Bonn (2014)
33. Hühnlein, D., Frosch, T., Schwenk, J., Piswanger, C.M., Sel, M., Hühnlein, T., Wich, T., Nemmert, D., Lottes, R., Somorovsky, J., Mladenov, V., Condovici, C., Leitold, H., Stalla-Bourdillon, S., Tsakalakis, N., Eichholz, J., Comb, F.M., Bold, A., Wabisch, D., Dean, R., Shamah, J., Kapanadze, M., Ponte, N., Martins, J., Portela, R., Karabat, c., Stojičić, S., Nedeljkovic, S., Bouckaert, V., Defays, A., Anderson, B., Jonas, M., Hermann's, C., Schubert, T., Wegener, D., Sazonov, A.: Futuretrust - future trust services for trustworthy global transactions. In: Hühnlein, D., Roössnagel, H., Schunck, C.H., Talamo, M. (eds.) P264 - Open Identity Summit 2016. pp. 27–41. Gesellschaft für Informatik eV, Bonn (2016)
34. Hühnlein, D., Hornung, G., Kubach, M., Mladenov, V., Roßnagel, H., Sädtler, S., Schmölz, J., Wich, T.: SkIDentity – Trusted Identities for the Cloud (2015), https://www.skidentity.de/fileadmin/Ecsec-files/pub/7_SkIDentity-final.pdf
35. ISO/IEC 15408-1:2009. Information technology – security techniques – evaluation criteria for it security – part 1: Introduction and general model, International Organization for Standardization, Geneva, CH (2009)
36. ISO/IEC 27002:2013. Information technology – security techniques – code of practice for information security controls, International Organization for Standardization, Geneva, CH (2013)
37. ISO/IEC 29134:2017. Information technology – security techniques – guidelines for privacy impact assessment, International Organization for Standardization, Geneva, CH (2017)
38. Khatchatourov, A., Laurent, M., Levallois-Barth, C.: Privacy in digital identity systems: Models, assessment, and user adoption. In: Tambouris, E., Janssen, M., Scholl, H.J., Wimmer, M.A., Tarabanis, K., Gascó, M., Klievink, B., Lindgren, I., Parycek, P. (eds.) 14th International Conference on Electronic Government (EGOV), Aug 2015, Thessaloniki, Greece, vol. LNCS-9248, chap. 21, pp. 273–290. Springer International Publishing, Lecture Notes in Computer Science edn. (2015). https://doi.org/10.1007/978-3-319-22479-4_21
39. Koning, M., Korenhof, P., Alpár, G.: The abc of abc – an analysis of attribute-based credentials in the light of data protection, privacy and identity. In: Balcells, J. (ed.) Internet, Law & Politics : A decade of transformations. Proceedings of the 10th International Conference on Internet, Law & Politics, Universitat Oberta de Catalunya, Barcelona, 3-4 July, pp. 357–374. Huygens Editorial, Barcelona (2014), http://edcp.uoc.edu/proceedings_idp2014.pdf
40. Le Métayer, D.: Privacy by design: Formal framework for the analysis of architectural choices. In: Proceedings of the third ACM Conference on Data and Application Security and Privacy (CODASPY). San Antonio (2013)
41. Pfitzmann, A., Hansen, M.: Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology. Version v0.34 (10 August 2010), https://www.kantarainitiative.org/confluence/download/attachments/45059055/terminology+for+talking+about+privacy.pdf
42. Poller, A., Waldmann, U., Vowe, S., Turpe, S.: Electronic identity cards for user authentication – promise and practice. IEEE Security & Privacy **10**(1), 46–54 (2012), https://doi.org/10.1109/MSP.2011.148
43. Roßnagel, H., Camenisch, J., Fritsch, L., Houdeau, D., Hühnlein, D., Lehmann, A., Rodriguez, P.S., Shamah, J.: FutureID – Shaping the Future of Electronic Identity. In: Annual Privacy Forum 2012. Limassol, Cyprus (10-11 October 2012)

44. Servida, A.: Principles and guidance on eID interoperability for online platforms. Revised draft version of January (2018), https://ec.europa.eu/futurium/en/system/files/ged/draft_principles_eid_interoperability_and_guidance_for_online_platforms_1.pdf
45. STORK: D4.11 final version of technical specifications for the cross-border interface (2015), https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174
46. Tsakalakis, N., O'Hara, K., Stalla-Bourdillon, S.: Identity assurance in the uk: Technical implementation and legal implications under the eidas regulation. In: Proceedings of the 8th ACM Conference on Web Science. pp. 55–65. WebSci '16, ACM, New York, NY, USA (2016). https://doi.org/10.1145/2908131.2908152
47. Tsakalakis, N., Stalla-Bourdillon, S.: Documentation of the legal foundations of trust and trustworthiness. FutureTrust deliverable D2.8 v. 1.00 (29 June 2018)
48. Tsakalakis, N., Stalla-Bourdillon, S., O'hara, K.: What's in a name: the conflicting views of pseudonymisation under eidas and the general data protection regulation. In: Hühnlein, D., Roßnagel, H., Schunck, C.H., Talamo, M. (eds.) P264 - Open Identity Summit 2016. pp. 167–174. Gesellschaft für Informatik e.V., Bonn (2016)
49. Veeningen, M., de Weger, B., Zannone, N.: Data minimisation in communication protocols: a formal analysis framework and application to identity management. International Journal of Information Security **13**(6), 529–569 (2014). https://doi.org/10.1007/s10207-014-0235-z
50. Yee, G.O.M.: Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards. IGI Publishing (2011)
51. Zwingelberg, H.: Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card. In: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (eds.) Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, vol. 352, chap. 13, pp. 151–163. Springer Berlin Heidelberg (2011). https://doi.org/10.1007/978-3-642-20769-3_13
52. Zwingelberg, H., Hansen, M.: Privacy protection goals and their implications for eid systems. In: Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G. (eds.) Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, vol. 375, chap. 19, pp. 245–260. Springer Berlin Heidelberg (2012). https://doi.org/10.1007/978-3-642-31668-5_19