Identity Assurance in the UK: technical implementation and legal implications under the eIDAS Regulation

Niko Tsakalakis[*]
Web and Internet Science
University of Southampton
SO17 1BJ, UK
N.Tsakalakis@southampton.ac.uk

Kieron O’Hara
Web and Internet Science
University of Southampton
SO17 1BJ, UK
kmo@ecs.soton.ac.uk

Sophie Stalla-Bourdillon
Institute for Law and the Web
University of Southampton
SO17 1BJ, UK
S.Stalla-Bourdillon@soton.ac.uk

ABSTRACT

The UK Government has been designing a new Electronic Identity Management (eIDM) system that, once rolled–out, will take over how citizens authenticate against online public services. This system, Gov.UK Verify, has been promoted as a state–of–the–art privacy–preserving system, tailored to meet the requirements of UK citizens and is the first eIDM interoperability in which the government does not act as an identity provider itself, delegating the provision of identity to competing third parties. According to the recently enacted EU eIDAS Regulation, member states can allow their citizens to transact with foreign services by notifying their national eID scheme. Once a scheme is notified, all other member states are obligated to incorporate it into their electronic identification procedures. The UK Government is contemplating at the moment whether it would be beneficial to notify. This article examines Gov.UK Verify ’s compliance with the requirements set forth by the Regulation and the impact on privacy and data protection. It then explores potential interoperability issues with other national eID schemes, using the German nPA, an eIDM based on national identity cards, as a reference point. The article highlights areas of attention, should the UK decide to notify Gov.UK Verify. It also contributes to relevant literature of privacy–preserving eID management by offering policy and technical recommendations for compliance with the new Regulation and an evaluation of interoperability under eIDAS between systems of different architecture.

CCS Concepts

•**Security and privacy → Pseudonymity, anonymity and untraceability; Privacy protections;** *Graphical / visual passwords; Privacy-preserving protocols;* Biometrics; Multi-factor authentication; •**Social and professional topics → Governmental regulations;** *Privacy policies;* •**Applied computing → Law;**

Keywords

eID, eIDM, electronic identity, trust services, Gov.UK Verify, German nPA, eIDAS

1. INTRODUCTION

As online services increasingly complement or substitute traditional ones, public and private sectors are expressing an interest in electronic identity management systems (eIDM). eIDM offers to the public sector a trusted equivalent of physical identification of citizens, a necessary requirement for many eGovernment services. At the same time, private services may also benefit from online trustworthy civil identities (e.g. banks, public transport services). In the European Union (EU), the Regulation on Electronic Identification and Trust Services (eIDAS) was adopted recently, as part of the Digital Economy agenda.[1] It establishes a common framework for interoperation of eIDM across all member states. Interoperation is not mandatory. Instead, national eIDMs that are to be used across borders have to follow a notification process. Though the scope of the Regulation concerns public services, the Commission hopes that it will inform private sector initiatives.[2]

eIDM systems allow identification and authentication of users to online services by the use of software (username/password) or hardware (cards, mobile devices) tokens.[3] Tra-

[*] http://orcid.org/0000-0003-2654-0825

[1] 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

[2] *See* goals of eIDAS Task Force, the legislating team behind eIDAS: https://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond

[3] *Authentication* is the process by which a person proves a claim to an entity. For example, A proves to B that A is an adult. *Identification* is a subset of authentication. Identification connects a person to an identity, i.e. A proves to B that they are A. An identity normally includes multiple claims (e.g. name, date of birth, address), enough to unambiguously verify an individual.

ditional eIDM architectures involved a central entity that served as an Identity Provider (IdP) to multiple Service Providers (SP). Later systems consider central storage of eIDs as a privacy risk and employ federated architectures to distribute users' personal data across multiple IdP/storage locations [22]. Modern deployment attempts to re–introduce elements of control of the electronic identity (eID) back to the users [18].

Most member states in the EU have already deployed, or are currently deploying, national eIDM systems. Implementations vary across the Union, from centralised architectures (such as in Estonia), where the Government serves as a central IdP, to user–centric deployments with users acting as their own IdPs (such as in Germany). National eIDMs are qualitatively different from private eIDMs, as they offer eIDs that are validated against official identity records.

The UK Government has recently introduced its eIDM system, currently in public beta. The UK system, named *Gov.UK Verify* aims to create an eID market: users authenticate to online public SPs through private entities that act as IdPs. The UK, therefore, reverses existing national eID paradigms as, instead of renting validated eIDs to the private sector, it rents (officially) validated eIDs from the private sector. The innovative architecture promises complete separation of eIDs from SPs or the state. The goal is to prohibit linkability of the different uses of an eID across services, which may lead to unwanted profiling of the user.

The goal of this article is to provide a comprehensive analysis of Gov.UK Verify against the requirements set forth by the EU eIDAS Regulation. Although the UK has not yet announced intentions to notify its scheme, allowing UK eIDs to be used across borders in all European governmental services could add immense value to the aforementioned eID marketplace. To succeed though, consequences of notification should be carefully considered. The paper is organised as follows: Section 2 details the methodology used and related work on the field. Section 3 provides an overview of Gov.UK Verify. An analysis of the Regulation is provided in section 4. Finally, section 5.1 examines compliance with eIDAS and the impact on privacy and data protection.[4] Section 5.2 looks upon potential issues of interoperability with other European systems, using the German eIDM as a reference point. Suggested interoperabilitys and policy measures are offered at the end of both sections.

2. METHODOLOGY AND RELATED WORK

This paper draws upon empirical data and findings from prior research on eIDM systems, and in particular on various European projects and the limited research out there on Gov.UK Verify. It then relates the findings to relevant law, by following legal research methodologies. Doctrinal research is used to screen legislation and case law and discover the scope and aim behind legal descriptions [16]. Law is referred to in this article as a synthesis of hard (national and European legislation) and soft law (quasi-legal instruments such as codes of conduct, EU guidelines and communication). The paper uses this synthesised framework to highlight inconsistencies of the system in question (Gov.UK Verify) with the regulation and propose suggestions to mitigate them.

A comparison of past European projects about interoperability of eIDs can be found in [27]. Analysis of 'Secure Identity across Borders Linked' (STORK), a large scale pan–European pilot aiming to test an interoperability infrastructure across Europe can be found in [19]. The project defined 4 security levels of identification (Quality Authentication Assurance or QAA). QAA were based on level of certainty of the identification, with the highest level being equivalent to a traditional physical identification. Three of them were later used as a reference point in eIDAS Levels of Assurance.[5] It also successfully implemented two different architectural designs, a middleware to communicate with foreign identification services and a Pan–European Proxy Service (PEPS) which acted as a getaway for foreign eIDs. Roßnagel et al. in [33] examine the new criteria set by Privacy by Design principles, namely *unlinkability, transparency* and *intervenability* which will be mentioned in the analysis of Gov.UK Verify below. Privacy by Design derives from Cavoukian's work on the Laws of Identity [11]. Details of what should be the minimum dataset necessary for identification according to case of use are provided in [32].

[23] explore the concept of eIDAS Assurance Levels in two international standards. After analysing Level 1 (the provided identity is a valid identity and it is possible it belongs to the user) and 2 (the provided identity fully identifies the person it relates to and it is probable it belongs to the user), the authors propose that a new intermediate level would be most appropriate for the majority of business cases, in terms of cost and technology investments required. Jøsang in [21] offers a breakdown of different user authentication schemes, finding that Assurance Levels are overall harmonized across national and international schemes. The paper concludes, though, that the assurance offered only works one way, as in most schemes users have no ability to verify back the service they transact with.

For the legal treatment of electronic identities in the UK, *see* [30] where it is proposed that inadequate protection of electronic identities should be supplemented by borrowing identity rights from civil law.

3. GOV.UK VERIFY

3.1 eID Policy in the UK

Contrary to the majority of countries in the EU, United Kingdom does not have a national identity card scheme in place. Citizens prove their identity by alternative identification documents, such as passports and driving licenses. This is largely attributed to the bad connotations centrally issued ID cards still have: the UK had introduced national identity card schemes twice before, during the two World Wars, where the ID cards were used for conscription purposes. Since this use was against the principles the schemes were created on, national ID cards were regarded as a means to monitor population activity [2].

Perhaps unsurprisingly, later attempts to introduce mandatory ID cards failed: 2010 saw the deprecation of the Identity

[4] It must be noted that personal data are clearly distinguished from the notion of privacy, which is wider. eIDAS only addresses eIDs in terms of personal data protection. This paper touches upon privacy when discussing aspects of the system architecture but references to the Regulation are focused on personal data.

[5] *See* table 1 below.

Cards Act,[6] that never got implemented due to strong opposition. The Act provided for a mandatory ID card roll–out in two stages, first to non–EU residents and at a later date to all. The card would contain an identifying set (full name, address, date of birth) as well as biometric data including a head and shoulders photograph as per the ePassport specifications. The biometrics along with an electronic representation of the identifiers would be stored in an electronic chip that would make them available for identification, authorization an electronic signing. Each card had a unique serial number, which along with the rest of information would be stored in a central government database, the National Identity Register. A simple biometric scan, or request from the serial number, would retrieve the information from the database. The register, and especially its unique serial number, was considered means of potential mass–surveillance and a hit to privacy and was destroyed in 2010, with the Identity Documents Act.[7] Consequent interoperabilitys for an eID focused on software tokens instead of physical cards and examined approaches where eIDs would not be under sole central control of the Government — which was hoped to be more in accord with the spirit of common law tradition.

Central role in the design of the new eID scheme is played by the Data Protection Act 1998 (DPA) that transposes the EU Data Protection Directive to English law. The DPA regulates the processing of all personal data and introduces to the legal landscape important concepts about data minimization, purpose limitations and data subjects consent. This is an important inclusion, since concepts of privacy protection have been traditionally absent from UK common law.[8] The DPA does not include all provisions of the EU Directive and many passages have been kept purposefully vague. As with many UK policies, it focuses on a goal oriented approach to data protection rather than details on how to achieve them [31]; instead the Act gets supplemented by explanations on practical applications from the Information Commissioner.

In 2013, the Government published its new Digital Strategy.[9] Part of it was a 'Digital by default' plan, according to which all central government services should focus on online operation first, aiming to drive most citizens' interactions with the state online. As more services would be transferred online, creation of a scheme that could verify the identity and claims of citizens became imperative. Towards that end, and having in mind people's attitudes towards Governmental identification schemes, the Government Digital Service (the department in charge of digital strategies) set up an advisory group that would explore and inform Government Digital Service about the principles that the system should be designed on.[10]

The Privacy Consumer Advisory Group came up with 9 Identity Assurance Principles (IdAP) that the system should be built upon, data minimization and user control among them. The principles form the bare minimum of how the system should operate. It should be noted that the principles are again target goals; they do not address legality or enforcement of policies — instead they specify technological interoperabilitys that would serve these principles by design. The model is based around server hub and spoke authentication using username/password software tokens. Instead of electronic identity management, design moved towards identity assurance: the system should offer different levels of certainty about one's identity. It would be organized around risk–based assessment of identity assurance.[11] Identity Assurance is considered to be more consumer–led in focus, with no need of central databases, extensive data sharing or data consolidation [13].

Reversing the aims of the deprecated Identity Cards Act, where the Government would be the only IdP, the new scheme aimed to create a private market of IdPs, with the aspiration that consumers would be able to choose which entity they trust more to handle their identification. It would also allow users to manage multiple electronic identities, having different accounts with separate providers. This way a user can choose where to deploy each identity and for which use.

Multiple IdPs also assists against data aggregation: identity data get split across different small databases of each IdP, mitigating the risk of a single point of failure.

Finally, design was kept in line with the general technology–agnostic principle of the 'Digital by Default' strategy: the specification does not constrain the providers in the technology they wish to implement, as long as a translation layer exists, specified by the Government Digital Service, to allow inter–communication.

3.2 Overview of the system

3.2.1 *System components*

To avoid privacy concerns of a centrally operated system, Gov.UK Verify moves to a federated approach of handling digital identities. There is no single Unique Identifier for users. It is instead comprised of four different elements that operate separately from each other:

(1) **Central Hub:** An online central hub (**CH**) mediates all interactions across the different components and the users. The hub acts as a broker to ensure that identification and authentication exchanges are sealed from the parties, offering higher security, privacy and usability.

(2) **Service Providers (SP):** Service providers are the different services that could request identification of

[6] 2006 c 15

[7] 2010 c 40

[8] UK law does not include a positive right to privacy. Data protection differs significantly to privacy: Privacy refers to every kind of possession of information whereas data protection is only concerned with the disclosure of that information. As a result, there is no effective redress in a case of a breach of privacy, such as injunctions or adequate compensation. Lately, the courts have started to protect private information by joining the tort of breach of confidence with the provisions of arts 8 and 10 ECHR to compensate. For more *see* I. Lloyd, "Anonymity and the Law in the United Kingdom", in Lessons From the Identity Trail: Anonymity, Privacy and Identity in A Networked Society, I. Kerr, C. Lucock, and V. Steeves, Editors. 2009, Oxford University Press.

[9] Cabinet Office, "Government Digital Strategy: December 2013". 2013, available from: https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy [accessed 14 October 2015]

[10] https://www.gov.uk/government/consultations/draft-identity-assurance-principles/privacy-and-consumer-advisory-group-draft-identity-assurance-principles

[11] Not all transactions require the same level of certainty about somebody's identity. Some only require authentication of an attribute (i.e. that a person is above 18 years old to access age–restricted content).

users to allow them further access. SPs are not part of the system, strictly speaking; instead they are contractors who lease the use of the system for their services. At the moment, SPs are solely governmental departments [12].

(3) **Identity Providers (IdP):** IdPs are commercial companies, that users contract with, who verify a user's information against various authoritative sources (at the moment the National Passports Office and Driving Licensing Authority (DVLA)) and set up accounts on their databases of persistent digital identities of their users.

(4) **Matching Service (MS):** the MS is a middleware between the SP and IdP. The MS is operated by the SP and is built with an adapter provided by the Government Digital Service. Its goal is to match up the persistent digital identity of the user, sent by the IdP, to a local account in the SP's database.

3.2.2 *Authentication process and protocols*

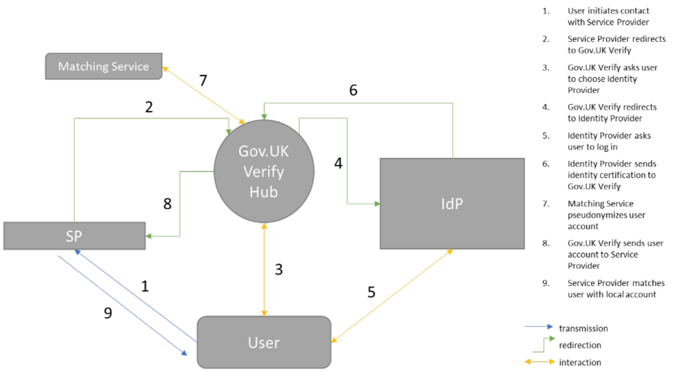
Matching Service
Gov.UK Verify Hub
IdP
SP
User
1
2
3
4
5
6
7
8
9
1. User initiates contact with Service Provider
2. Service Provider redirects to Gov.UK Verify
3. Gov.UK Verify asks user to choose Identity Provider
4. Gov.UK Verify redirects to Identity Provider
5. Identity Provider asks user to log in
6. Identity Provider sends identity certification to Gov.UK Verify
7. Matching Service pseudonymizes user account
8. Gov.UK Verify sends user account to Service Provider
9. Service Provider matches user with local account
transmission
redirection
interaction

Figure 1: Identification transaction in Gov.UK Verify

Whenever a user wishes to log in to a service, the SP contacts the CH asking for verification of the user provided information. The CH redirects to the user's browser with a list of IdPs. After selection, the CH relays the request to the chosen IdP, withholding any information about the SP. If this is a new user, the IdP checks the information they provided against Passport Office or DVLA. An intermediary service, called 'Document Checking Service', assures that the IdP has access to only the necessary information — IdPs receive a strictly Yes/No answer from governmental departments, without having to share information directly. If the information provided is correct, the IdP creates an eID containing a minimum dataset (MDS)[12] and any additional attributes. The MDS is then sent to the CH. The CH creates a pseudonymized record that it then sends to the SP. The SP needs to have a local translator (MS) set–up that will associate the pseudonymized account received to a local account on the SP's service. All assertions are facilitated through SAML 2.0, an XML–based protocol that facilitates authentication through a web–browser [10]. Figure 1 shows the process diagrammatically.

The interference of the CH between the SPs and IdPs, satisfies the privacy principles about minimisation of data transfers, allowing data processing inside silos without leakage of data from SPs to IdPs or vice–versa. Compared to federated approaches implemented in other countries, where the central hub communicates directly with the SPs and IdPs without a matching service, the programme satisfies stricter security and privacy criteria.[13]

4. THE EIDAS REGULATION

In 2012 a draft Regulation was proposed to revise the previous eSignatures Directive. The proposed Regulation was adopted by the Parliament and the Council in 2014. eIDAS[14] aims to offer a comprehensive legal framework that will boost mutual recognition and inter–operation of cross–border eID management, trust services and certificates. The Regulation is part of a series of reforms in line with the Commission's 'Digital Agenda' which pushes for a unified internal market across all member states.[15] Though the main aim of the Regulation is to manage electronic seals, time stamps, certificate services for website authentication and electronic documents and their delivery, eID management had to be addressed first as it would allow authentication to all other services. eIDAS defines an interoperability framework of national eIDMs. Minimum specifications are not defined by the Regulation, but are included in subsequent implementation acts.[16] Member states that wish to operate cross-border transactions through their schemes need to notify their national eID interoperability to the Commission. Notification is not obligatory and can only happen for national schemes (either public sector schemes or private schemes officially recognised by the state) that are used to identify citizens at at least one public service.[17] Successful notification comes after a lengthy deliberation process where member states make (non–binding) suggestions on the eID scheme in question.[18] Upon acceptance of the notified scheme, all other member states are obliged to incorporate it into their authentication services.[19]

4.1 eID Requirements under eIDAS and implementation acts

In terms of requirements, eIDAS specifies that all schemes must adhere to the Data Protection Directive (DPD).[20] A

[12] or Matching Dataset, comprised of full name, date of birth, gender, current and previous address [10].

[13] For example, see US's FCCX, where the MS component is absent: https://gcn.com/articles/2013/08/22/usps-fccx.aspx

[14] Footnote 1 above.

[15] European Commission, 'Annual Growth Survey' Brussels, 28112012, COM(2012) 750 final.

[16] Note that under §27 of the eIDAS preamble, it is stated that "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". In contrast, the implementing acts point towards specific implementations, creating thus de facto standards (*see* for example Annex in IR 2015/1501 OJ L 235/2015).

[17] eIDAS arts 7 and 9

[18] Note that the member state is free to disregard all comments and that the Commission has no real power to deny notification of a scheme, unless the application is *obviously* fraudulent or faulty.

[19] eIDAS art 6

[20] Directive 95/46/EC of the European Parliament and of the

Gov.UK Verify	German nPA	STORK 2.0 QAA	eIDAS LoA	Example
N/A	N/A	N/A	N/A	Anonymous submission of a form
1	0	1	N/A	Opening an e–mail account. The account only verifies that an email address exists.
2	1	2	'Low'	Online account with an electricity provider. The account only verifies that it relates to an actual electricity meter.
3	2	3	'Substantial'	Paying online. The account only verifies (a) the user holds a valid bank card and (b) the bank account associated with the card will be used.
4 (not supported currently)	3	4	'High'	Using an ePassport to enter a country. The electronic terminal verifies (a) the credentials relate to a valid identity and (b) the identity belongs to the person presenting the ePassport.

Table 1: Mapping of national assurance levels to STORK and eIDAS

specific mention is made to the data minimization principle, with services required to request and process only data strictly necessary for each individual authentication.[21] Schemes are also required to adhere to 'Privacy by Design' principles, meaning that privacy cannot be dealt with only by policy — privacy should be aided by technological means on the design of the system. Finally, system design should by technology–neutral, referring to specific technologies only when that is absolutely essential for the security of the system or the users.[22]

The Regulation focuses on identification in expense of authentication; it specifies that the goal is 'unambiguous representation' of a person[23]. Implementation act 2015/1501 clarifies this further in the design of the inter–operation framework.[24] According to it, persons are unambiguously identified by transmission of a minimal dataset, which should include a Persistent Unique Identifier (UID).[25] Though identification is a sub–section of authentication, it entails the creation of a unique link to a specific user, disallowing the use of more privacy-preserving authentication methods (e.g. age–restricted services that do not require to identify users could be satisfied by Yes/No answers to questions about legal age). In this respect, the Regulation has been criticised for offering less privacy than what is technically possible [24].

eIDAS further specifies a common reference of identity assurance levels that notified schemes should adhere to. Using the STORK project as a reference point,[26] eIDAS defines named assurance levels, low — substantial — high (table 1). Definition of the levels comes with the implementation act 2015/1502[27] where 'Low' is assigned when evidence are 'assumed' to be valid, 'Substantial' after validation of the evidence and 'High' after biometric validation. eIDAS stipulates that member states are free to deny foreign schemes access to services of a higher assurance level than the scheme.[28]

4.2 Interoperability framework under eIDAS

Anticipating that notified schemes will differ in architecture, the eIDAS Task Force produced implementing act 2015/1501 [17]. The act is a technical specification aiming to provide interoperabilitys of interoperability between all possible combinations of eIDM architectures. The specification describes two options of deploying an eIDM system to receiving member states: The system can operate either as a proxy or as middleware.

Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/0031

[21] eIDAS recital 11 and art 12

[22] The first drafts of the Regulation required member states to operate schemes that could guarantee that no extra hardware or software would be necessary in order for other member states to access them. This wording has been toned down in the final text after objections from some member states. *See* C. Cuijpers and J. Schroers, "eIDAS as guideline for the development of a pan European eID framework in FutureID", in Open Identity Summit 2014, D. Hühnlein, Editor. 2014, Bonner Köllen Verlag. p. 23-38.

[23] eIDAS art 3(1)

[24] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market OJ L 235/2015, ANNEX 1, pp. 1–6

[25] *See* art 11(1) and ANNEX 1 footnote 24 above.

[26] STORK defined 4 assurance levels, with 1 being "no assurance" and 4 "high assurance". *See* STORK. "D2.3 – Quality authenticator scheme". 2009; Available from: https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577 [Accessed: 2 January 2016]. eIDAS is using STORK levels 2 to 4.

[27] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L 235/2015, ANNEX 2, pp. 7–20.

[28] eIDAS art 6(1c)

As a proxy, the system is deployed as a central server based and operated by the notifying member state. Foreign member states will subsequently send authentication requests to that server, who then redirects to the local eIDM system to perform the identification. The local system sends the server the result of the identification that is then redirected by the server to the foreign member state.

Alternatively the notifying member state can create a standalone server which will be based and operated by the receiving member state at the same level as the local eIDM system. When the receiving member state needs to identify a foreign user, the identification will go through the standalone server and its result will be redirected back to the local system.

Regardless of choice, the proxy or middleware will relay information to the national eID scheme of the receiving member state through an interoperability software. A choice on deployment of the interoperability software is given as well. Receiving member states can install the software centrally, so that all SP requests go through the same instance of interoperability software. Obviously this works better in architectures with a centralised element, such as a central hub. Or, the member state can choose to install an instance of the software at every individual SP, if communication with a central element is absent or needs to be avoided.

All communication between the different components is facilitated by the SAML protocol.[29] A (simplified) representation from [17] of all possible configurations can be found in figure 2.

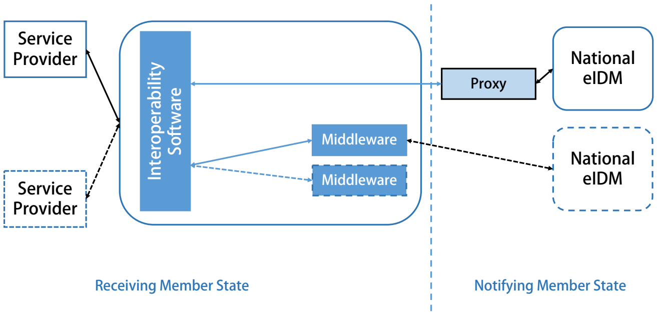

Figure 2: Configuration options for interoperable systems

5. COMPLIANCE AND INTEROPERABILITY

Since the scheme is fairly recent and its operation is still in beta, a perfect assessment of its characteristics is difficult. Instead, the discussion that follows will focus on how certain technical decisions reflect on the current regulating framework around digital identity. Where appropriate, reference is made to the German eID scheme for comparison. A brief overview of the German scheme can be found in appendix A.

5.1 Compliance with national and European laws

5.1.1 *Pseudonymity under IdAP*

Upon request of verification of an identity from the CH, the IdP authenticates the user via username/password, associates the username with other identifiers of the same user (e.g. name or date of birth) and then derives a user pseudonym that it transmits to the CH. Each pseudonym is persistent across each CH (and there is no premise to assume there are more than one CH). The CH then assigns a new pseudonym to this pseudonymised record in order to hide from the SP the activity of the IdP (edge–unlinkability). This happens inside the MS. The MS is a middleware, provided by the Government Digital Service but operated at the SP level. The MS receives the pseudonymised record from the CH. The record, as noted previously, contains the Matching (or minimum) Dataset (MDS)[30] under a pseudonym. After assigning a new pseudonym to the MDS, the MS tries to match it with a local record of the SP. The process has three possible cycles, depending how successful initial matching is. At the lowest cycle, the MS uses the MDS to search for a matching local record. If found, it associates the record to the pseudonym on a table. If not, the next cycles widen the search criteria to the point of asking the user of additional information.[31] Since Gov.UK Verify does not seem to support selective disclosure [4], it is safe to assume that the MDS is always transferred to and from the CH. On top of the original identifiers, the MDS will get enriched by user provided attributes, in case of a failed attempt to match the local records.[32] In the end, the MS creates an association table, storing the received pseudonyms and matching datasets to the local accounts of the SP. The pseudonym assigned by the MS is persistent. This is in order to avoid having to follow the same process every time: the MS needs to associate the IdP account to a local one only the first time; by keeping the pseudonyms static each subsequent time the MS knows to which local account the eID refers to. But this also means that if more than one SP access the same MS, they will all receive the same pseudonym for each eID. Since the MS is deployed at the SP level, there is no telling of how many different MS exist. If the same pseudonym as-

[29] Implying, therefore, that since communication happens through web browser requests, the more components are involved the slower the whole process becomes.

[30] *See* footnote 12.

[31] If no match is found after the first 2 cycles, the system employs input from the user to help determine a match. In **cycle 3** the system asks the user for additional information, through the Gov.UK Verify Hub. The example given by the Government Digital Service is the ability of the user to input their Unique Taxpayer Reference when trying to access tax services. The requested information differs for every SP and is determined by the SP's policy: http://alphagov.github.io/identity-assurance-documentation/_downloads/Build_matching_service.pdf

[32] The specification requires additional user consent to be given in case an attribute provider is involved to enrich the MDS, but user consent can be assumed if the user is the source of the attributes. The CH is forbidden by the policy to store any other information than the MDS and the association of pseudonyms: Cabinet Office, "Identity Assurance Hub Service SAML 2.0 Profile v1.1a". 2013; Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458610/Identity_Assurance_Hub_Service_Profile_v1.2a.pdf [Accessed: 16 January 2016]

signed to a user is shared by more than one SP, it effectively allows the pseudonym to function as a *de facto* UID [4].

Existence of *de facto* UID would be hard to justify as long as it remains undocumented.[33] Federated architectures were developed to function without need of global identifiers (or transfer of identifiers across organisations) [28]. Perhaps the Government Digital Service intended for a different MS at every SP, in which case there is no risk of the described behaviour. But since in theory combination of SPs under a single MS is possible, the scheme and its regulation should be updated to include this possibility (or its prevention).

The Government should update the policies that regulate the relationship between CH, IdP and SP[34] to account for this use of pseudonyms as a known and intended function of the system. It should also describe in detail the definition of a SP. Detailing under which circumstances static pseudonyms are permitted would allow the system to take advantage of them in certain cases. For example, should the eIDAS interoperability software be considered an SP (or many SPs under one MS) would allow the system to accommodate the UID function eIDAS requires (see below). This of course presupposes that adequate risk assessment has been undertaken beforehand.

5.1.2 Unique Identifiers under eIDAS

One of the Regulation's requirements is the *'unambiguous representation'* of an individual.[35] In other words, each record is required to have a Unique Identifier associated with it. This UID is expected as part of the mandatory minimum dataset for natural persons.[36]

Gov.UK Verify does not include UID by design. In fact, it was one of the design goals to avoid the feature that caused the attempted National Register Database to fail (which is why the system funcion described in section 5.1.1 is in need of documentation and justification by the Government Digital Service). Implementation of the CH in between IdP and SP is to guarantee unlinkability — that a user cannot be associated with a particular eID and activities of an eID cannot be associated to each other. Unlinkability is mandated by the Assurance Principles of 'Minimisation' and 'Transparency' that form the regulating policy of the whole scheme.

The scheme does provide for a minimum dataset though. Between IdP, CH and MS, eIDs are exchanged in the form of a record with a set amount of attributes. The record contains a pseudonym and the MDS. The MDS, in other words, is the transaction identity [29].

Though the Regulation mandates that a UID is expected, definition of the UID is up to the member state. Only requirement is that it uniquely represents an individual across a period of time. This freedom of interpretation led the design team behind the nPA — the German eID scheme — to assign as UID the Pseudonym created by the eID card as described in appendix A [5].[37]

Gov.UK Verify could take advantage of the way pseudonymity works under the present design to supply the required eIDAS function. Since the CH (& the MS) has the ability to create unique pseudonyms for each user, these could be used along with the MDS to comprise eIDAS' minimum dataset.

In order for this function to produce consistent pseudonyms for each user every time a single MS must exist between CH and SP (of the receiving member state). This means that the UK will have to deploy its scheme to receiving member states in the form of a proxy. A proxy would give the UK the opportunity to operate one MS that could then transmit the pseudonymised MDS across indefinite SPs.[38] Obviously this is a interoperability based on the way the system operates in practice and does not seem to be currently in line with what the design team intended. Support of this function should, therefore, come after proper revision of the system architecture.

5.1.3 Compliance with data protection

A general obligation set forth by eIDAS is that any setup should be compliant to the Data Protection Directive.[39] Accordingly, Gov.UK Verify as a whole is required to conform to the requirements of the DPA.

According to the contractual agreement Gov.UK Verify signs with each IdP, the CH is a data controller in respect to the personal data that it processes.[40] The DPA mandates that in order for any processing to be fair and lawful, it needs to be transparent and based on a legitimate interest. Though there are other ways to ground a legitimate interest apart from user consent, it has been accepted that in a transparent processing users should be fully informed of the kind of processing that is taking place [1]. The relevant privacy policy does not enumerate the data collected in an exhaustive way[41] and contains no information on retention periods.[42] It

[33] *See* also [4] where the authors conclude that persistent pseudonyms and visibility of attributes (non–selective disclosure) could lead to user impersonation by the CH, should the CH become compromised.

[34] including the Framework Agreement and the Identity Assurance Principles

[35] eIDAS art 3§1

[36] According to IR 2015/1501 the minimum dataset is comprised of at least First and Last Name(s), date of birth and UID. It is unclear whether additional attributes are mandatory: the IR refers to additional attributes as an optional set of which member states *'must'* include one or more into the minimum data set. In contrast, the eIDAS technical specification refers to those attributes as optional depending on availability and legality under national law.

[37] The legal implications of this decision have not yet been challenged in a court. It is reminded that by ruling of the German Constitutional Court in 1983, creation of any kind of UID is forbidden: *see* footnote 56.

[38] A proxy based interoperability seems logical in any case, considering that the CH is a centrally deployed key part of the scheme. Perhaps central deployment of the CH and a middleware offer of the MS would be possible, but in that case each user would acquire a different pseudonym for each MS.

[39] eIDAS recital 11

[40] Cabinet Office "Framework Agreement and Schedules". Draft v0,9 20 December 2014, 2014. Available at: http://data.gov.uk/data/contracts-finder-archive/contract/1690273/ [accessed on: 21 August 2015]

[41] It contains the word "including", allowing for a wide interpretation of the categories of data that follow as only a subset of the collected information: https://www.signin.service.gov.uk/privacy-notice

[42] The Government–Identity Provider agreement requires information to be provided by the IdP: https://data.gov.uk/

is certain that the CH (and the MS) stores at least a record of received pseudonym and associated pseudonym to facilitate linking of eIDs to local accounts [10]. No information is given on users' right to invoke their consent at any time. It is unclear therefore what happens to the data held in the CH in the case a user decides to close down an account with an IdP.

Adding to the confusion, promotional material of the system insist that no personal data are processed inside the CH,[43] creating questions about the specificity of user consent to the processing, as blanket consent is not allowed under the DPA,[44] and about conformity with the Identity Principle of Transparency in personal data processing.[45]

Clearer privacy policies on the exact processing that takes place in the CH and MS would be of value to strengthen user consent and specificity. In particular, privacy policies and T&C of the CH, as well as the Framework Agreement between the parties should detail the processing of pseudonyms inside the CH, the reasons, if any, that pseudonyms should not be considered personal data[46] and how the CH handles the rest of identifiers in the MDS since selective disclosure is not possible in the current system.

5.2 Interoperability issues

5.2.1 Liability under eIDAS

eIDAS provisions on liability pose an interesting complexity: Even though liability for Trust Service Providers is clearly defined,[47] allocation of liability for eID schemes, according to art 11, involves not only the parties that issue and operate the eIDs but also the notifying member state. The state of a notified scheme is liable for damages caused intentionally or negligently to any natural or legal person if the scheme fails to uniquely identify the individual or if online authentication becomes unavailable. If the parties issuing the identification means and operating the authentication procedure are private providers, they have the right to limit their liability through their T&C.[48] In contrast, the member state is always liable for damages and users cannot limit their liability in case of machine malfunction or compromise [24]. In this power imbalance, there is a question of why states would notify their schemes since that would expose them to responsibilities for actions beyond their control [15], such as when the system of a private company goes offline.

In light of the above, it seems that Gov.UK Verify should revisit its relationship with participating entities. In Gov.UK Verify, all interested parties (IdPs, authorities, SPs) have limited their liability with their inter-party agreements to a bare minimum apart from cases of fraud or death.[49] In domestic transactions the Government has followed the same practice in its relationship to the contracted IdPs and SPs under the Framework Agreement. This practice is problematic, as in a cross–border transaction the government would not be able to waive its liability even though all other parties would.

The UK should consider amending its contractual obligations to the other parties by including sets of minimum liability limits for every party involved in a transaction and with every possible scenario in mind.[50]

5.2.2 Levels of Assurance

As mentioned earlier, eIDAS Levels of Assurance (LoA) have been informed by the four levels specified in the STORK 2.0 project. Although some national schemes, such as the German nPA, support the STORK QAA 1 to 4, Gov.UK Verify was designed to support up to QAA 3. Consequently, in a cross–border scenario it always runs the risk of being denied access to certain SPs; eIDAS specifies that member states with a high LoA do not have to accommodate notifying schemes that satisfy lower levels only. QAA 4 and consequent LoA 3 *'High'* require the presence of biometrics at the moment of authentication. For example, social security and tax services in Hungary require biometric authentication under the new eID card scheme.[51] According to eIDAS, Hungary will be free to deny access to its online tax services to UK eIDs.

Incorporation of biometric authentication in a modular design such as Gov.UK Verify's should be technically possible. In fact, since the system was designed to specify target goals rather than means of achieving them, the private IdP are in principle free to use any technological means they wish. LoA 3 is specified in [9] as 'Level Identity 4'. Accommodation of biometrics, therefore, is up to the discretion of the IdP. Careful consideration of how Gov.UK Verify and the CH will handle biometric data is a matter of future work, if LoA 3 becomes available to the system.

data/contracts-finder-archive/contract/1690273/

[43] "We don't keep your identity data centrally; in fact we don't keep it at all, or even get to see it ourselves: it is held by the identity providers on your behalf.": https://identityassurance.blog.gov.uk/2014/11/05/tech-arch-privacy/

[44] The Information Commissioner refers back to the DPD art 7 to define consent and its parameters: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-2.pdf

[45] Details of the processing should be made publicly available for all activities, including those regarding security of the system, according to Identity Assurance Principle #2.

[46] It is highly doubtful that pseudonymous data could be considered non personal data, especially under the light of the new EU General Data Protection Regulation. For more, *see* C. Burton, et al., "The Final European Union General Data Protection Regulation". BNA Privacy & Security Law Report, 2016. 15: 153

[47] eIDAS art 13

[48] eIDAS art 24(2d)

[49] *See* for example Experian, T&C: https://www.experianidentityservice.co.uk/Help/Terms; Digidentity T&C: https://auth.digidentity.eu/terms_and_conditions/uk; Post-Office T&C: http://www.postoffice.co.uk/terms-of-use.

[50] Omission of minimum liability is something that was criticised about the eIDAS Regulation. *See*, for example, Bitkom "Position Paper on the Proposal for an EU Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market", 2013. Available at: https://ameliaandersdotter.eu/sites/default/files/wp-content/uploads/2013/04/20130408-BITKOM-Position-on-eID-regulation1.pdf [accessed on: 28 July 2015]

[51] As reported in http://www.planetbiometrics.com/article-details/i/3994/desc/hungary-launches-biometric-eid-card/

6. CONCLUSIONS

In this paper, we analysed Gov.UK Verify's operation according to system architecture and regulating policies. We detailed the requirements set forth by eIDAS for eIDM operation across borders, briefly related UK system's architecture to that of another member state and highlighted potential discrepancies in policy and modus operandi should the UK wish to notify their scheme under eIDAS.

In particular, the way the system (and namely the MS component of CH) handles pseudonymisation currently seems incompatible with the founding Identity Assurance Principles, data protections guidelines and the goal of unlinkability. In case pseudonyms as a *de facto* UID is declared to be an intended function instead of a practical coincidence, it should be documented exactly which needs such a function would cover and what the associated risks would be. In fact, this paper suggests an intended use of pseudonyms as UID for the purposes of eIDAS could allow Gov.UK Verify to transmit the required minimum dataset. At the same time, policy amendments are needed to clarify how the CH processes personal data and establish minimum liability requirements for contracting parties of the scheme. Future work is needed to explore how additional attributes, such as biometric information and attribute providers, should be incorporated into the existing system in order to equate it to higher international Levels of Assurance.

7. ACKNOWLEDGMENTS

This research was funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, University of Southampton. EP/L016117/1.

8. REFERENCES

[1] Article 29 Data Protection Working Party. *Opinion 15/2011 on the definition of consent.* WP187. 2011.

[2] P. Beynon-Davies. The uk national identity card. *Journal of Information Technology Teaching Cases*, 1(1):12–21, 2011.

[3] Bitkom. Position paper on the proposal for an eu regulation on electronic identification and trust services for electronic transactions in the internal market. 2013. Available at: https://ameliaandersdotter.eu/sites/default/files/wp-content/uploads/2013/04/20130408-BITKOM-Position-on-eID-regulation1.pdf?language=en [Accessed: 14 June 2015].

[4] L. Brandão, N. Christin, G. Danezis, and Anonymous. Toward mending two nation-scale brokered identification systems. *Proceedings on Privacy Enhancing Technologies*, 2015(2), 2015.

[5] BSI. Technical guideline tr-03110-1 advanced security mechanisms for machine readable travel documents part 1 v 2.20. 2015. Available at: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html [Accessed: 15 October 2015].

[6] BSI. Technical guideline tr-03127 architecture electronic identity card and electronic resident permit. 2011. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03127/BSI-TR-03127_en.pdf?__blob=publicationFile [Accessed: 15 October 2015].

[7] H. Burkert. *Balancing informational power by informational power or Rereading Montesquieu in the internet age.* Cambridge University Press, 2012.

[8] C. Burton, L. De Boel, C. Kuner, A. Pateraki, S. Cadiot, and S. G. Hoffman. The final european union general data protection regulation. *BNA Privacy & Security Law Report*, 15:153, 2016.

[9] Cabinet Office. Good practice guide no. 45 identity proofing and verification of an individual. 2014. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf [Accessed: 8 August 2015].

[10] Cabinet Office. Identity assurance hub service saml 2.0 profile v1.1a. 2013. Available at: https://www.gov.uk/government/publications/identity-assurance-hub-service-saml-20-profile [Accessed: 3 September 2015].

[11] A. Cavoukian. 7 laws of identity: The case for privacy-embedded laws of identity. 2006. Available at: https://www.gradbook.soton.ac.uk/?link=registration.php [Accessed: 14 July 2015].

[12] T. Chatfield. Digital government review. 2014. Available at: http://digitalgovernmentreview.readandcomment.com/ [Accessed: 15 June 2015].

[13] J. Crosby. Challenges and opportunities in identity assurance. London:HMSO. 2008.

[14] C. Cuijpers and J. Schroers. eIDAS as guideline for the development of a pan European eID framework in FutureID. *Open Identity Summit*, 2014(237):23–38, 2014.

[15] J. Dumortier and N. G. Vandezande. Critical observations on the proposed eu regulation for electronic identification and trust services for electronic transactions in the internal market. ICRI Research Paper 9. 2012. Available at SSRN: http://ssrn.com/abstract=2152583 [Accessed: 5 July 20154].

[16] N. Duncan and T. Hutchinson. Defining and describing what we do: Doctrinal legal research. *Deakin Law Review*, 17(1):83–119, 2012.

[17] eIDAS Technical Subgroup. eidas technical specifications v0.90. 2015. Available at: https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v090 [Accessed: 7 November 2015].

[18] M. Hansen. *Marrying Transparency Tools with User-Controlled Identity Management.* Springer US, 1 edition, 2008.

[19] Y. Honcharova and A. Eryomenko. Stork - promising project of european transnational electronic identification. *First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*, 2014.

[20] G. Hornung and C. Schnabel. 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.

[21] A. Jøsang. Assurance requirements for mutual user and service provider authentication. *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, pages 26–44, 2015.

[22] E. Maler and D. Reed. The venn of identity: Options and issues in federated identity management. *IEEE Security & Privacy Magazine*, 6(2):16–23, 2008.

[23] H. Masatoshi, F. Yuri, O. Sakura, K. Takeaki, S. Natsuhiko, and S. Hiroyuki. *A Practical Trust Framework: Assurance Levels Repackaged Through Analysis of Business Scenarios and Related Risks.* Springer International Publishing, 1 edition, 2015.

[24] F. Massacci and O. Gadyatskaya. How to get better eid and trust services by leveraging eidas legislation on eu funded research results. 2013. Available at: http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf [Accessed: 15 December 2015].

[25] A. Poller, U. Waldmann, S. Vowe, and S. Turpe. Electronic identity cards for user authentication - promise and practice. *IEEE Security & Privacy Magazine*, 10(1):46–54, 2012.

[26] G. L. Rosner. *Identity management policy and unlinkability: a comparative case study of the US and Germany.* PhD thesis, University of Nottingham, 2016.

[27] H. Roßnagel, J. Camenisch, L. Fritsch, D. Houdeau, D. Hühnlein, A. Lehmann, P. S. Rodriguez, and J. Shamah. Futureid - shaping the future of electronic identity. *Datenschutz und Datensicherheit*, 36(3):189–194, 2012.

[28] M. C. Rundle and B. Laurie. Identity management as a cybersecurity case study. *OII Conference on Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Research Publication No. 2006-01*, 2005.

[29] C. Sullivan. *Digital identity, an emergent legal concept: the role and legal nature of digital identity in commercial transactions.* University of Adelaide Press, 2011.

[30] C. Sullivan and S. Stalla-Bourdillon. Digital identity and french personality rights — a way forward in recognising and protecting an individual's rights in his/her digital identity. *Computer Law & Security Review*, 31(2):268–279, 2015.

[31] E. A. Whitley. On technology neutral policies for e–identity: a critical reflection based on uk identity policy. *Journal of International Commercial Law and Technology*, 8(2):134–147, 2016.

[32] H. Zwingelberg. *Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card.* IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, 2011.

[33] H. Zwingelberg and M. Hansen. *Privacy Protection Goals and Their Implications for eID Systems.* Springer Berlin Heidelberg, 2012.

APPENDIX

A. THE GERMAN nPA

In order to fully understand Gov.UK Verify's operation in a cross-border setting, we would need to look at how the system would behave when communicating with other national eIDM. This article opted to use the German eIDM as a reference point. The German eID system is based on the nPA, the national ID card. The card carries a RFID chip with an electronic version of the identifying information [25].[52] The card was made a central point of the system in order to allow for two-factor authentication that was missing from the previous username/password implementation. The system was designed around the premise that the set of information necessary to identify a person (referred to as 'sovereign data set')[53] is qualitatively more valuable once validated as trustworthy and, therefore, deserves greater protection than the rest of identity information that could potentially be voluntarily disclosed or available through commercial services.

To safeguard the sovereign dataset the system should minimize the identifiers transmitted each time by allowing creation of multiple eIDs with combinations of identifiers [26]. Security is aided further by end–to–end cryptography across all communication. The system has three main components: the user (represented by their ID card), a card–reader attached to the user's computer and the SP. There is no IdP in Germany's implementation;[54] instead the eID is provided by validation of data from the card by the reader through cryptographic protocols. The user and SP have to be mutually authenticated through certificates before any data flow.[55]

System design is based on the fundamental privacy principles existent in German policy [6]:

(a) Right to information self-determination: The concept describes a person's power to decide when and within what limits information about themselves should be communicated to others [20]. It got constituted into a right by a decision of the German Constitutional

[52] fore– and surname, address, date of birth, nationality, place of birth, post-code, municipality ID, expiry date and (optionally) fingerprints. Currently no eID application in Germany is designed to use fingerprint authentication. Additionally, serial numbers for the card and the chip and a biometric photo similar to ePassports are available to elevated governmental terminals.

[53] In other literature, and some other parts of this article, this concept is referred to as 'transaction identity'. For more *see* C. Sullivan, "Digital Identity, an Emergent Legal Concept: The Role and Legal Nature of Digital Identity in Commercial Transactions". 2010: University of Adelaide Press.

[54] The official provider of identities in the Governments, which produces the ID cards. The cards are produced offline in the federal printing facilities; no data need uploading on a network for the creation of the card. After production all data are required by law to be erased from the printing facilities and the government has no ability to track or monitor individual card usage. The cards only operate in an offline mode, meaning that all authenticating data can only be transmitted to devices in close proximity.

[55] Online communication to and form the SP happens through client software, triggered by a browser plugin. The Government has released a multi–platform free programme, called 'AusweisApp' free of charge. For more *see*: http://www.personalausweisportal.de/SharedDocs/Downloads/EN/Flyers-and-Brochures/Broschuere_BSI_innovations_eID_architecture.html?nn=6852820

Court.[56] In the German eID system it is manifested through requiring the user to affirm their actions by entering a PIN number before any transmission of eIDs takes place.

(b) Separation of informational powers refers to the idea that the state should not be allowed to gather personal data as a single entity, but instead all data transfers should be justified against clearly defined purposes for the data collection ('purpose–specification') and should be the least intrusive possible ('proportionality'). [7]. Because of separation of informational powers, SPs have to register with the Federal Office of Administration before allowed to access eIDs. Registration requires them to submit a case where they detail the specific data fields of the eIDs they wish to access and the corresponding service needs.

(c) Data minimization stems from the preconditions of a lawful processing of personal data under the DPD.[57] As a principle it means that a data controller should minimise the data collection to only what is relevant and necessary to the specific purpose of the processing. In the German system, minimization is implemented through the *selective disclosure* functions of the card: The card is capable of answering questions of whether a user is above a certain age or lives in a certain area with Yes/No answers without disclosing the actual birth of date or address. Enforcement of the minimization principle is ensured by allowing users to de–select some of the identifiers requested by the SP before each submission. De–selected fields do not get disclosed. There is no minimum dataset a user has to send over, but deselecting fields could potentially not allow the transaction to be completed. Nevertheless, this risk is at the discretion of the user.

(d) Pseudonymity refers to the ability to authenticate users without disclosing their actual identifying information. It is a concept found in various pieces of German legislation.[58] Pseudonymity is built directly into the system: for each pair eID card – SP a specific pseudonym is created by combining a cryptographic key stored at the card with one that each SP holds. As a result, pseudonyms change across different uses making it impossible to link different activities to one user.

[56] Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983, BVerfGE 65, 1, 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden [in German]. With the same decision the Court forbade any future creation of any kind of UID.

[57] DPD arts. 6§1(b, c)

[58] For example, *see* the 'telemedia act' that requires telecommunication providers to allow users to use and pay for their services pseudonymously: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179).