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

Niko Tsakalakis[1], Sophie Stalla-Bourdillon[2] and Kieron O'Hara[3]

[1] *Web and Internet Science, University of Southampton, N.Tsakalakis@southampton.ac.uk, http://orcid.org/0000-0003-2654-0825,*

[2] *Institute for Law and the Web, University of Southampton, S.Stalla-Bourdillon@soton.ac.uk*

[3] *Web and Internet Science, University of Southampton, kmo@ecs.soton.ac.uk*

ABSTRACT

Gov.UK Verify, the new Electronic Identity (eID) Management system of the UK Government, has been promoted as a state-of-the-art privacy-preserving system, designed around demands for better privacy and control, and is the first eID system in which the government delegates the provision of identity to competing private third parties. Under the EU eIDAS, Member States can allow their citizens to transact with foreign services by notifying their national eID systems. Once a system is notified, all other Member States are obligated to incorporate it into their electronic identification procedures. The paper offers a discussion of Gov.UK Verify's compliance with eIDAS as well as Gov.UK Verify's potential legal equivalence to EU systems under eIDAS as a third-country legal framework after Brexit. To this end it examines the requirements set forth by eIDAS for national eID systems, classifies these requirements in relation to their *ratio legis* and organises them into five sets. The paper proposes a more thorough framework than the current regime to decide on legal equivalence and attempts a first application in the case of Gov.UK Verify. It then assesses Gov.UK Verify's compliance against the aforementioned set of requirements and the impact of the system's design on privacy and data protection. The article 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. It is also, to our knowledge, the first exploration of the future of eID management in the UK after a potential exit from the European Union.

Keywords: eIDAS, Gov.UK Verify, Brexit, eID, eIDM, electronic identity, trust services, electronic identification, internal market

ISSN 2332-4031; DOI 10.1561/106.00000010

1 Introduction

As online services increasingly complement or substitute traditional ones, public and private sectors are expressing an interest in electronic identity (eID) management systems. eID systems offer 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)[1] establishes a common framework for interoperation of eID systems across all Member States. National eID systems 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]

eID systems allow identification and authentication of users[3] to online services by the use of software (username/password) or hardware (cards, mobile devices) tokens. A distinction between authentication in general and electronic identification as scoped in eIDAS should be made: *Authentication*, in general, is the

[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, adopted on 23 July 2014.

[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] Strictly speaking these functions can serve both natural and arbitrary persons (i.e. legal persons). For the purpose of this paper, the analysis will focus on natural persons, but it should be applicable *mutatis mutandis* also to legal persons (*see* eIDAS above footnote 1 Art. 3(1) and 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 (Text with EEA relevance) [2015] OJ L235 (hereinafter *IR2015/1501*) ANNEX (2)).

process by which a person proves a claim to an entity. For example, A proves to B that A is an adult (Fiat and Shamir, 1987). Electronic *identification*, on the other hand, as defined in eIDAS can be viewed as a subset of authentication. Identification refers to "the process of using person identification data in electronic form uniquely representing either a natural or legal person".[4] An identity normally includes multiple claim identifiers (e.g. name, date of birth, address),[5] enough to unambiguously verify an individual. Though identification is a sub-section of authentication, it entails the creation of a unique link to a specific user, preventing 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 sense, eIDAS' identification is more restrictive than authentication from a privacy standpoint, as it not only validates claims of the person but also connects them to a (unique) identity.[6] National eID systems have served both functions, but as eID technology evolves a tendency to favour authentication over unique identification can be observed, in an effort to address privacy considerations. The difference between them relates to two aspects of the identification process: the amount of identifiers transmitted and the location where identifiers are stored.

The number of identifiers transmitted can be associated with two principles of privacy-enhancing eID architectures: *data minimisation* and *selective disclosure*. Data minimisation refers to the limitation of data gathering to the minimum information necessary to accomplish a specific purpose (Cooper *et al.*, 2013). Selective disclosure, which can be viewed as a complimentary principle, refers to the disclosure of only the minimum necessary data for the stated purpose (Cavoukian, 2006; Pfitzmann and Hansen, 2010).[7] Similarly, storage locations affect the risk of data breaches (Hörbe and Hötzendorfer, 2015). Traditionally, eID architectures revolved around a central entity that served as an Identity Provider to multiple Service Providers. The Identity Provider would serve as a central location for eID storage, thereby constituting a single point of attack. Newer systems consider central storage of eIDs as a privacy risk and employ federated architectures to distribute users' personal data across multiple Identity Provider/storage locations (Maler and Reed, 2008). Modern deployment attempts to re-introduce elements of control of the eID back to the users (Hansen, 2008).

To effect the varying eID architectures, the relevant policies that regulate eID systems have also evolved. Moving away from traditional detailed rules of processes, rights and obligations, recent policy regulation favours more relaxed provisions that specify the desired outcomes (or principles) but leave the decisions on how to achieve them up to the parties (Black, 2008). The benefit of principle-based regulation is that it allows for a pluralism of implementation, therefore ensuring the regulation will stay relevant throughout the rapid change of technology (Whitley, 2016) (which is why these regulations are also referred to as 'technology-neutral'). At the same time, though, principle-based technology-neutral regulations might create compliance issues: Different levels of abstraction employed in principle-based regulation do not always guarantee absolute compatibility between concrete norms and principles, as will be shown further along this paper.

National eID systems have already been deployed, or are currently being deployed, across many Member States in the EU. Implementation varies across the Union, from centralised architectures (such as in Estonia (Martens, 2010)), where the Government serves as a central Identity Provider, to user-centric deployments without Identity Providers (such as in Germany (Federal Office for Information Security [BSI], 2011)).[8]

The UK eID system, named *Gov.UK Verify*, is based on a principle-based policy that centres around certain privacy principles.[9] The system is envisaged to allow participation of diverse private entities acting as Identity Providers, regardless of the technical infrastructure these entities choose to adopt. Its aim is to create an eID market: users authenticate to online public Service Providers through a private Identity Provider of their choice. 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 Service Providers or the state. The goal is to prohibit the latter to link different uses of an eID across services, which might lead to unwanted profiling of the user.

On 23rd June 2016 the EU Referendum took place in the UK. The result of the referendum was for the UK to leave the

[4] eIDAS Art. 3(1); subsequently 'authentication' under eIDAS is defined as the "process that enables the electronic identification of a natural or legal person" (Art. 3(5)).

[5] Identifiers can also be referred to in the literature as *attributes*. In that case, an implicit distinction is being made between attributes that contain potentially identifying information (e.g. a name) and attributes that do not (e.g. an age). Since identifiable information is context related (as will be shown in section 5.1.2) and highly dependent on the overall privacy features of the system, we regard the term *identifiers* as more appropriate for the purposes of this paper.

[6] *See* footnote 42 below and related discussion.

[7] It appears, thus, the subtle difference between the two is that selective disclosure is concerned only at the point of disclosing information for the purposes of an authentication/identification, whereas data minimisation is applicable on all stages, from data gathering, to data storage, data disclosure and data erasure (Pfitzmann and Hansen, 2010, p. 18). This seems in line with the definition included for the first time in 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 Art. 5(1)(c): "[processed personal data shall be] adequate, relevant and limited to what is necessary".

[8] Strictly speaking a governmental Identity Provider exists in Germany. It is used though to certify the identities of the Service Providers, to ensure only authorised entities have the right to read a user's eID, rather than provide eID to the users – which is provided by their personal eID card.

[9] Or, as referred to by Gov.UK, 'Identity Assurance Principles': https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf [accessed 10 October 2015, preserved at: https://perma.cc/5K2W-8BVK].

EU.[10] The exit process, as mandated by the Lisbon Treaty,[11] can take up to two years. Article 50 of the Lisbon Treaty was triggered on 29 March 2017 but the exit process is still under negotiation and it is currently uncertain whether the UK will attempt to remain as part of the European Economic Area (EEA)[12] or seek alternatives to trade with the single market.

The outcome of the British exit from the EU will significantly shape its collective legislation in general and how eID management is regulated in particular. EEA legislation is subject to the primary legislation of the EU[13] at the time of signing of the EEA Agreement and on certain secondary legislation with EEA relevance (regulations, directives and decisions).[14] Although not directly subject to CJEU rulings,[15] the EEA is subject to the equivalent EFTA court.

If the UK, after leaving the Union, acquires an EEA membership the framework surrounding eID should remain, for the most part, the same.[16] In the event that the UK, though, exits the EU without acquiring EEA membership it will become a 'third country' from the EU perspective. The UK Government has proposed a bill to incorporate current EU legislation into UK law so it can be amended at will.[17] When enacted, the UK will have to decide carefully on which aspects of eIDAS should be preserved.[18] If the UK wishes access to the EU online public-sector services (for example to allow for an EU citizen to authenticate against a UK public authority, or for a UK citizen to access EU public administration services online) it will have to ensure interoperability of its eID services with the ones in the Union. Assessing legal equivalence becomes, therefore, crucial.

The goal of this article is to provide a comprehensive analysis of Gov.UK Verify against the requirements set forth by the eIDAS and offer a preliminary examination of how an exit from the Union might impact on Gov.UK Verify. The paper is organised as follows: Section 2 details the methodology used and related work on the field. Section 3.1 describes the current eID policy in the UK and section 3.2 provides an overview of Gov.UK Verify. An analysis of the European legal framework for eID is provided in section 4 and its requirements are classified into our proposed framework of sets of requirements in section 4.2. Section 4.3 discusses eIDAS' provisions on legal equivalence of foreign (third-country) eID systems. Finally, section 5 examines Gov.UK Verify's compliance with eIDAS and the impact on data protection,and its potential compliance with eIDAS if the UK becomes a third country. Further work about eID legal equivalence is highlighted in section 6.

2 Methodology and Related Work

This paper draws upon empirical data and findings from prior research on eID 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 formulations (Duncan and Hutchinson, 2012). 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 Gov.UK Verify with eIDAS and propose means to mitigate them. The paper also suggests a framework for classification of legal requirements applicable to eID systems. After extracting the various requirements applicable to eID systems from eIDAS and relevant legislation, each of these requirements is expanded and analysed according to its *ratio legis*[19] to identify the desired effect it should produce in an eID system. Requirements are

[10] The UK has voted to leave the EU by 52%: http://www.bbc.co.uk/news/politics/eu_referendum/results [accessed on: 17 October 2016].

[11] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 [2007] OJ C 306 Art. 50.

[12] EEA is currently comprised of 31 states, all EU Member States and Iceland, Liechtenstein and Norway, as constituted by the Agreement on the European Economic Area - Final Act - Joint Declarations - Declarations by the Governments of the Member States of the Community and the EFTA States - Arrangements - Agreed Minutes - Declarations by one or several of the Contracting Parties of the Agreement on the European Economic Area [1994] OJ L 001 . For more *see* Barnard, 2013.

[13] Treaty Establishing the European Economic Community [1957] 298 U.N.T.S. 11 ("Treaty of Rome"); Primary sources of EU law are the founding Treaties (as amended now contained in Lisbon Treaty under Arts. 1 and 2 about the Treaty to the European Union and the Treaty on the Functioning of the European Union) along with their Protocols and Annexes and the Charter of Fundamental Rights of the EU..

[14] There is debate around the transposition of secondary legislation in EEA: In Judgement of 26 September 2013, *United Kingdom v Council (EEA)* C-431/11, EU:C:2013:589 the Court held that Art. 7(a) EEA Agreement is to be understood to not require any implementing measures for an act to be made part of the internal legal order (at para. 54). However that is in contrast with current practice, whereby EEA States are implementing EU secondary legislation by transposing it into national law: *See* EFTA Court. The EEA and the EFTA Court: Decentred Integration. Hart Publishing, 1 edition, 2015 pp. 263–266.

[15] Art. 6 EEA Agreement subjects the EFTA Court to follow CJEU case law up until the signature of the EEA Agreement (2 May 1992) and Art. 3(2) of the "Agreement on the establishment of a Surveillance Authority and a Court of Justice" ([1994] OJ L344/3) obliges the EFTA Court to pay 'due account' to the case law laid down by CJEU..

[16] See section 4 for an overview of the applicable framework. eIDAS, as secondary legislation with EEA relevance creates an obligation of EEA countries to transpose it into national law. Its current status in EEA law is "under scrutiny for incorporation into the EEA Agreement", a process that started on 29/8/2014: http://www.efta.int/eea-lex/32014R0910 [accessed on: 28 October 2016]. EEA states are already subject to the Data Protection Directive (EEA Agreement footnote 12 above ANNEX XI) and the superseding GDPR (footnote 7) will have to be incorporated to the Annexes (Its current status in EEA is "under scrutiny for incorporation into the EEA Agreement", started on 4/5/2016: http://www.efta.int/eea-lex/32016R0679 [accessed on: 28 October 2016]).

[17] Institute for Government, 'The Repeal Bill' (7 July 2017) https://www.instituteforgovernment.org.uk/brexit-explained/repeal-bill [accessed 3 August 2017].

[18] The UK has already incorporated eIDAS in its national legislation by the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 which came into force on 22nd July 2016.

[19] '*Ratio legis*' refers to the underlying reason or purpose that a specific norm, rule or tribunal decision aims to serve. *Ratio legis* is a valuable instrument in legal scholarship, as it is used to interpret

grouped together based on the desired effect. The proposed classification is then being used to highlight potential conflicts when assessing legal equivalence of international eID systems.

For a review of different architectural models for eIDs *see* Jøsang *et al.*, 2005; Windley, 2005; Strauß and Aichholzer, 2010, where the benefits and drawbacks between standalone and federated systems is explored. In Strauß and Aichholzer, 2010, p. 15 the authors discuss the privacy challenges of federated systems that are based around a Unique Identifier for each eID, therefore endangering linkability of the eID accross uses and services.

A comparison of past European projects about interoperability of eIDs can be found in Roßnagel *et al.*, 2012. 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 Honcharova and Eryomenko, 2014. 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.[20] 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 gateway for foreign eIDs. Roßnagel et al. in (Zwingelberg and Hansen, 2012) 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 (Cavoukian, 2006). Details of what should be the minimum dataset necessary for identification according to case of use are provided in (Zwingelberg, 2011).

Jøsang in Jøsang, 2015 offers a breakdown of different user authentication systems, finding that Assurance Levels are overall harmonized across national and international systems. The paper concludes, though, that the assurance offered only works one way, as in most systems users have no ability to verify back the service they transact with.

For the legal treatment of electronic identities in the UK, *see* Sullivan and Stalla-Bourdillon, 2015 where it is proposed that borrowing identity rights from civil law jurisdictions could alleviate the shortcomings of eID protection in the UK legal system.

Finally, in relation to legal equivalence between EU law and third-countries' legal frameworks, for an analysis of the influence of EU law, and EU data protection legislation, outside of the EU's territorial boundaries, *see* Kuner in Kuner, 2017 dealing with the global reach of EU Law in areas of Internet governance, international agreements, private international law and data protection. Svantesson defines a model in Svantesson, 2013 to investigate when EU instruments (in this case the Data Protection Directive) affect third countries' legislation and constructed for this purpose different layers of protection. The model uses three groups, or layers, of data protection provisions according to the objective of protection they offer. Svantesson opines that an effective data protection framework should adjust its expectations and subsequent requirements depending on the nature of each international data transfer, what he calls 'degree of contact'.[21] The author draws upon that test so as to classify data protection requirements according to the different degrees of substantial, continuous and systematic contact of the third party (e.g. the third country) with the forum of the rules (i.e. the State whose data protection rules apply). He formulates three layers: the 'abuse-prevention layer', that dealt with provision about unauthorised or unreasonable disclosure, the 'rights layer' that contained rules about data subjects' rights and the 'administrative layer' with provisions about procedural safeguards.

3 Electronic Identification in the UK

3.1 eID Policy in the UK

Contrary to the majority of countries in the EU, the UK does not have a national identity card system 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 systems twice before, during the two World Wars, where the ID cards were used for conscription purposes. Since this use was against the principles the systems were created on, national ID cards were regarded as a means to monitor population activity (Beynon-Davies, 2011).

Later attempts to introduce mandatory ID cards failed: 2010 saw the deprecation of the Identity Cards Act,[22] due to strong opposition. The Act provided for a mandatory ID card roll-out. The card would contain an identifying set of attributes (full name, address, date of birth) as well as biometric data including a head and shoulders photograph as per the ePassport specifications (ICAO, 2017, p. 7). 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 and electronic signing. Each card had a unique serial number, which along with the rest of the information would be stored in a central governmental 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 a means of potential mass-surveillance and a hit to privacy and was destroyed in 2010, with the Identity Documents Act.[23] Consequent plans 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.

the intent behind the letter of the law. For reference, *see* Barak, 2007.

[20] *See* table 1 below.

[21] He borrows that concept from the 'minimum contact test', formulated in *International Shoe Co. v Washington* [1945] 326 U.S. 310 para. 316: "... in order to subject a defendant to a judgement [...] he [must] have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice'...".

[22] 2006 c 15.

[23] 2010 c 40.

Central role in the design of the new eID system 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.[24] The DPA does not include all provisions of the EU Data Protection Directive and many passages have been kept purposefully vague. As with many UK policies, it is a principle-based policy, focusing on a goal oriented approach to data protection rather than details on how to achieve it (Whitley, 2016); instead the Act gets supplemented by explanations on practical applications from the Information Commissioner.

In 2013, the Government published its Digital Strategy.[25] Part of it was the '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 system that could verify the identity and claims of citizens became imperative. The system would improve on the 'Government Gateway', the existing online platform to access Governmental services, by offering better assurance of identification and authentication.[26] Having in mind people's attitude towards Governmental identification systems, the Government Digital Service (the department in charge of digital strategies, part of the Cabinet Office) set up an advisory group that would explore and inform the Government Digital Service about the principles that the system should be designed on.[27]

The Privacy Consumer Advisory Group came up with 9 Identity Assurance Principles that the system should be built upon, data minimization and user control among them. It should be noted that the principles are again target goals; they do not address legality or enforcement of policies — instead they form a principle-based policy that allows for variation in technological implementation. The model is based around server hub and spoke authentication using username/password software tokens. Instead of electronic identity management, design moved towards a risk-based assessment of identity assurance.[28] Identity Assurance is considered to be more consumer-led in focus, with no need of central databases, extensive data sharing or data consolidation (Crosby, 2008).

Instead of a central governmental Identity Provider, the new system aims to create a private market of Identity Providers, with the aspiration that consumers will be able to choose which entity they trust more to handle their identification. It also allows users to manage multiple eIDs, having different accounts with separate providers. This way users can choose where to deploy each eID and for which use.

Multiple Identity Providers also assist against data aggregation: eID data are split across different small databases of each Identity Provider, mitigating the risk of a single point of failure.

Finally, design was kept in line with the general principle-based technology-agnostic '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 intercommunication.

3.2 Gov.UK Verify

3.2.1 System components

To avoid privacy concerns of centrally operated systems, Gov.UK Verify moves to a federated approach of handling eIDs. There are no central databases or single Unique Identifiers used for eIDs. The system is 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 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 (Chatfield, 2014).

(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.

(5) **Document Checking Service:** a supplementary service designed and operated by the Government Digital Service (GDS), whose role is to check the official documents provided by the user against authoritative

[24] 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* Lloyd, 2009.

[25] 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].

[26] Government Gateway is still used for several services: http://www.gateway.gov.uk/Help/Help.aspx?content=help_government_services_online.htm.

[27] Above footnote 9.

[28] 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) – *see* section 1 on the difference of identification – authentication.

sources.[29] The Document Checking Service is not engaged in every eID transaction; instead it is only needed for the registration of a new user with an Identity Provider.

3.2.2 Authentication process and protocols

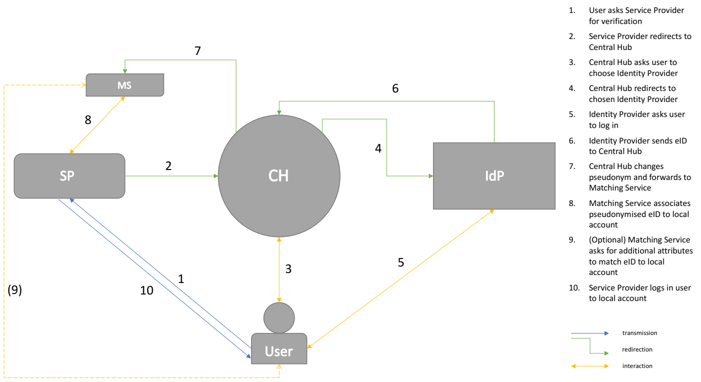
MS
SP
CH
IdP
User
1
2
3
4
5
6
7
8
(9)
10
1. User asks Service Provider for verification
2. Service Provider redirects to Central Hub
3. Central Hub asks user to choose Identity Provider
4. Central Hub redirects to chosen Identity Provider
5. Identity Provider asks user to log in
6. Identity Provider sends eID to Central Hub
7. Central Hub changes pseudonym and forwards to Matching Service
8. Matching Service associates pseudonymised eID to local account
9. (Optional) Matching Service asks for additional attributes to match eID to local account
10. Service Provider logs in user to 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 authentication 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 the 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[30] and any additional attributes. The minimum dataset is then sent to the CH under a pseudonym. In future verification requests after the initial creation of an eID 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 transmits the minimum dataset under a pseudonym to the CH. Each pseudonym for a particular user is persistent across each CH (and there is no premise to assume there are more than one CH). The SP needs to have a local translator (MS) set up that will associate the pseudonymised account received to a local account on the SP's service. 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, containing the minimum dataset. It then assigns a new pseudonym to this pseudonymised record in order to make the record unique for each SP (edge-unlinkability). The MS tries to match the received record 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 minimum dataset to search for a matching local record. If found, it stores the association between the pseudonym and the local record's identifier to a persistent table.[31] If not, the next cycles widen the search criteria to the point of asking the user of additional information.[32] The table is used for subsequent verifications — if an association between the pseudonym received and a local record is already found, the matching cycles do not take place (dubbed *cycle 0*). All assertions are facilitated through SAML 2.0, an XML-based protocol that facilitates authentication through a web-browser (Cabinet Office, 2013). 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 system satisfies stricter security and privacy criteria.[33]

4 eID Policy in the EU

Even though eID management remains at the remit of each EU Member State, legislation at the EU level aims to create a European framework that will allow the cross-border use of national eID systems. This initiative 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.[34] Electronic identification at the EU level is governed by eIDAS, although other legislative work should also be taken into account, mainly in the field of data protection.

4.1 eIDAS

eIDAS[35] was adopted by the Parliament and the Council on 23 July 2014 and came into force on the 1st of July 2016. It aims

[29] At the moment checks are performed against the HM Passport Office or the Driver and Vehicle Licensing Agency. GDS has announced its intention to expand on the sources used for the Document Checking Service, but further information has not yet been published: https://identityassurance.blog.gov.uk/2014/12/01/data-sources/.

[30] or Matching Dataset, comprised of full name, date of birth, gender, current and previous address (Cabinet Office, 2013).

[31] The correlation between pseudonym and local record is referred to as 'optional', even though it appears necessary for recurring users: http://alphagov.github.io/rp-onboarding-tech-docs/pages/ms/msCua.html#ms-cua-diagram.

[32] If no match is found after the first 2 cycles, the system employs input from the user to help determine a match: http://alphagov.github.io/rp-onboarding-tech-docs/pages/ms/msWorks.html. Cycle 2 is not currently supported by the system. 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; similarly each SP is free to choose if they will use some or all the attributes of the minimum dataset: http://alphagov.github.io/rp-onboarding-tech-docs/pages/ms/msBuild.html#ms-strat [accessed 23 January 2017].

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

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

[35] Footnote 1 above.

to offer a comprehensive legal framework that will boost mutual recognition and interoperation of cross-border eID management, trust services and certificates. eIDAS is divided into three main parts: Chapter I containing general provisions, Chapter II on '*Electronic Identification*', setting up common interoperability requirements for national electronic identification systems and Chapter III, titled '*Trust Services*', expanding the framework introduced by Directive 1999/93/EC (eSignature Directive)[36] to include electronic seals, time stamps, certificates for website authentication and electronic documents and delivery, laying down rules for the provision of such services by Trust Service Providers. eIDAS follows a technology-neutral principle-based approach to perform its objectives.[37] Chapter II defines the interoperability framework for national eID systems. Minimum specifications are not defined by the Regulation, but are included in subsequent implementation acts.[38] Member States that wish to allow their systems to be used cross-border need to notify their eID systems to the Commission. Notification is not obligatory and can only happen for national systems (either public sector systems or private systems officially recognised by the state) that are used to identify citizens at at least one public service.[39] Successful notification comes after a lengthy deliberation process where Member States make (non-binding) suggestions on the eID system in question.[40] Upon acceptance of the notified system, all other Member States are obliged to incorporate it into their authentication services.[41]

eIDAS focuses on identification in expense of authentication; it specifies that the goal is 'unique representation' of a person.[42] IR 2015/1501 clarifies this further in the design of the interoperation framework.[43] Under IR 2015/1501, persons are unambiguously identified by transmission of a minimum dataset, which should include a Persistent Unique Identifier.[44] In this respect, eIDAS has been criticised for offering less privacy than what is technically possible (Massacci and Gadyatskaya, 2013). eIDAS further specifies a common reference of identity assurance levels that notified systems should adhere to. Using the STORK project as a reference point,[45] eIDAS defines named levels of assurance (LoA), low – substantial – high (table 1). Definition of the levels comes with the Implementing Regulation 2015/1502[46] 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 systems access to services of a higher assurance level than the system.[47] Finally, eIDAS specifies that all systems must comply with the Data Protection Directive.[48] The Data Protection Directive has since been superseded by the General Data Protection Regulation (GDPR)[49] and data protection compliance should now be sought with the GDPR, which becomes applicable from 25 May 2018, as the most recent EU regulatory framework. However, an analysis of all of the GDPR's requirements is beyond the scope of this paper.

	eIDAS LoA	**STORK 2.0** QAA	**Gov.UK Verify**	**German nPA**	Example
Levels of Assurance	N/A	N/A	N/A	N/A	Anonymous submission of a form.
	N/A	1	1 (not currently supported)	0	Opening an e–mail account. The account only verifies that an email address exists.
	'Low'	2	2	1	Online account with an electricity provider. The account only verifies that it relates to an actual electricity meter.
	'Substantial'	3	3 (not currently supported)	2	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.
	'High'	4	4 (not currently supported)	3	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

Notified systems are expected to interoperate inside an EU 'Interoperability Framework'. Anticipating that notified systems will differ in architecture, the eIDAS Task Force produced IR 2015/1501.[50] IR 2015/1501 recitals 2 and 3 point at two options for deployment: notified systems can either be deployed as redirection servers (proxies) or as individual instances (middleware).

As a proxy, the system can be deployed at and operated by the notifying Member State, or it can be based at and operated by the foreign Member State. Foreign Member States subsequently send authentication requests to that server, who then redirects to the notified eID system to perform the identification. The notified system sends the server the result of the identification that is then redirected to the foreign Member State's service.

Alternatively the notifying Member State can create standalone instances of its system which will be based and operated by the receiving Member State at the same level as the local

[36] Council Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [1999] OJ L013/0012.

[37] Note that under rec. 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".

[38] The implementing acts, though, appear to point towards specific implementations, creating thus de facto standards (*see* for example Annex in IR 2015/1501 footnote 3).

[39] eIDAS Arts. 7 and 9.

[40] Note that the Member State is free to disregard all comments and that the Commission has no real power to deny notification of a system, unless the application is *obviously* fraudulent or faulty.

[41] eIDAS Art. 6.

[42] eIDAS Art. 3(1); Previous drafts defined the goal as "unambiguously representing a natural or legal person": *see Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market* (Text with EEA relevance) (COM(2012) 238 final, Brussels, 4 June 2012) p.19; the adopted version changed the phrasing to "uniquely representing", though it is doubtful that resulted in any material change.

[43] Footnote 3, ANNEX 1, pp. 1–6.

[44] *See* Art. 11(1) and ANNEX 1 footnote 43 above.

[45] STORK defined 4 assurance levels, with 1 being "no assurance" and 4 "high assurance" (Hulsebosch *et al.*, 2009).

[46] 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.

[47] eIDAS Art. 6(1)(c).

[48] eIDAS Art. 5(1).

[49] Footnote 7 above.

[50] Footnote 3 above.

eID system. When the receiving Member State needs to identify a foreign user, the identification will go through the standalone middleware 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 system 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.[51] A (simplified) representation from (eIDAS Technical Sub-group, 2015) of all possible configurations can be found in figure 2.

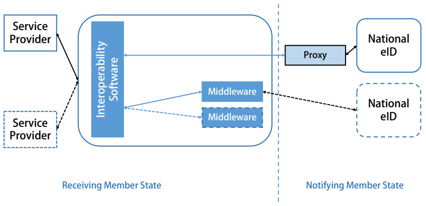

Figure 2: Configuration options for interoperable systems

4.2 The sets of requirements

We can identify five groups — or sets — of requirements, each group pursuing a specific objective within a complex relational system:

(i) ***Quality* requirements**, which place constraints on the way operations necessary for the purposes of identification and authentication shall be conducted:[52] While eID systems are meant to make electronic identification possible[53] electronic identification means of natural and legal persons falling under a notified identification system should perform an authentication function[54] Nevertheless eIDAS distinguishes between different levels of assurance and in this sense eligible systems should (*a*) comply with at least one of the three LoA that should be (*b*) equal or higher than the LoA of the service they are attempting to access.[55] They should be (*c*) available online and (*d*) transmit the Minimum DataSet to identify natural and legal persons.[56] The interoperability framework shall (*e*) be technology neutral[57] and (*f*) allow for Privacy-by-design principles.[58] (*g*) Data protection compliance of all components is also a requirement.

(ii) ***Governance* requirements**, relating to the number and roles of actors involved in the process of eID provision to end users: Eligible systems should (*a*) identify citizens against at least one public sector service and be either (*b*) issued by the Member State, (*c*) issued by a third party under mandate from the Member State or (*d*) issued under mandate of a third party but recognised by the Member State.[59] They should also be (*e*) included in the Notification list of Art. 9 and (*f*) be supervised by a national body.

(iii) ***Administrative* requirements**, about the internal administration and management of eID providers: Systems should (*a*) have a published description of its operation, have set (*b*) liability regimes, (*c*) arrangements for suspension and revocation procedures, (*d*) rules of procedure and (*e*) dispute resolution mechanisms, (*f*) public T&C of use for non-public-sector services and (*g*) have appointed a data registration manager.[60]

(iv) ***Security* requirements** relating to organisational and technical measures eID providers have to put in place in order to ensure the security of their services:[61] They should adhere to (*a*) EU and international standards, have set (*b*) suspension and revocation procedures (also under item (iii)) and (*c*) withdrawal procedures in case of a security breach that lasts more than 3 months.

(v) Finally, ***liability* requirements** capture requirements relating to the identification of the party liable in case of damage, allocation of liability share as well as allocation of the burden of proof:[62] Aside from (*a*) national rules of liability, the Member State is liable (*b*) for the appropriate attribution of the eIDs and (*c*) the availability of authentication online. (*d*) The party issuing the eIDs is liable for the appropriate attribution of an eID to a person and (*e*) the operator of the eID system is liable

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

[52] Note that eIDAS does not list all possible purposes; for eID services the purpose given is usually identification.

[53] "the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person": eIDAS Art. 3(1).

[54] Authentication under eIDAS means "an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed": eIDAS Art. 3(5).

[55] eIDAS Arts. 8, 6(1) and (2); as explained in section 4.1 compliance with LoAs ensures the levels of certainty any given identification should produce.

[56] IR 2015/1501 footnote 3 ANNEX I.

[57] The first drafts of the Regulation required Member States to operate systems 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, so that Art. 7(f) of eIDAS now reads: "Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication". *See* Cuijpers and Schroers, 2014, pp. 23–38.

[58] A specific mention is made to the data minimization principle, with services required to request and process only data strictly necessary for each individual authentication: eIDAS recital 11 "processing of only those identification data that are adequate, relevant and not excessive" and Art. 12 [the Interoperability Framework] "facilitates the implementation of the principle of privacy by design".

[59] eIDAs Art. 7(a) and (d).

[60] eIDAS Art. 12.

[61] eIDAS Arts. 10, 12.

[62] eIDAS Art. 11.

	quality	governance	administrative	security	liability
requirements	LoA	national system	system description	Suspension & revocation procedures	Availability of service
	Unique representation	notification list	liability regime	withdrawal procedures if security breach > 3 months	Correct allocation of eID
	Online	supervision for operator & issuer	data registration manager	EU standards	Correct operation of eID
	Minimum DataSet		Suspension & revocation arrangements		Contractual (national rules)
	Compliance with Data Protection Law		No disproportionate technical requirements		
			T&C for non-public use		
	Interoperability framework: Technology neutral & support Privacy-by-Design		Minimum technical requirements for Interoperability Framework		

Table 2: eID Sets of Requirements

for a failure to ensure the correct operation of the identification process.

It should be noted, however, that allocation of liability becomes more complex in systems where several parties perform the same role, especially after the enactment of the GDPR. Under the GDPR Article 82(4) and (5) joint controllers are always jointly and severarally liable. As a result, if a role is performed by more than one parties[63] both shall be liable unless one of them demonstrates they are free of blame.[64]

4.3 Legal equivalence under eIDAS

The concept of 'legal equivalence' determines whether eID services offered in third counties offer an equivalent level of protection to those in the EU. Legal equivalence is thus conceived as a pre-condition for attaching specific legal effects to third countries' eID. eIDAS deals with international legal equivalence in its Article 14, but equivalence is only defined in relation to (qualified) trust services and not eID systems. Article 14 posits three requirements for legal equivalence: (*a*) an agreement needs to be put in place between the EU and the third country (or an international organisation),[65] (*b*) the Trust Service Providers in the third country need to meet the requirements applicable to qualified Trust Service Providers in the EU and (*c*) the third country needs to recognise qualified trust services provided in the Union as legally equivalent to the trust services provided in the third country.

Legal equivalence for eIDs is not defined, although eID equivalence will be essential in order to access online services inside the EU.[66] The requirements presented in section 4.2 would, therefore, assist in an initial exploration of legal equivalence of eID services. A future distinction on the essential requirements for eID legal equivalence could indicate which of them could be offset by existing norms of private international law.[67] At the moment, there is no distinction in eIDAS between essential and non essential requirements, which raises the question whether all types of requirements should indeed be considered.

5 Compliance and Interoperability

Since the system is fairly recent[68] a perfect assessment of its characteristics is difficult. Instead, the discussion that follows will focus first on how decisions taken by the Government Digital Service could impact on Gov.UK Verify's compliance with some key sets of eIDAS requirements and second on its potential equivalence to EU systems after a UK exit from the EU.

5.1 Compliance with quality requirements

5.1.1 Levels of Assurance

As mentioned in section 4.1, eIDAS Levels of Assurance have been informed by the four levels specified in the STORK 2.0 project. Although some national systems, 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 by certain Service Providers; eIDAS specifies that Member States do not have to accept eIDs that satisfy lower levels,[69] and recognition of systems of LoA 'Low' is voluntary.[70] 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 system.[71] According to eIDAS, Hungary will be free to

[63] e.g. the operation of the eID scheme is performed by a public entity and a private entity.

[64] GDPR Art. 82(3).

[65] The agreement needs to be "in accordance with Article 218 TFEU": eIDAS Art. 14.

[66] It is unclear at the moment why such equivalence was omitted, especially in light of individual Member States already offering eID services with an international reach. *See*, for example, Estonia's e-residency programme: https://e-estonia.com/e-residents/about/. For a general discussion on barriers of international eID recognition, *see* ongoing work by the United Nations Commission on International Trade Law in UNCITRAL, 2016.

[67] An illustrative example can be seen in the case of qualified Trust Service Providers: Aside from eIDAS Art. 24, titled "Requirements for qualified trust service providers" , requirements should be sought in several other articles of Chapter III Section 3, in relation particularly to item (*b*) above. These requirements range from traditional private law rules (for example, to penalise unauthorised behaviour, such as the rules about the burden of proof of qualified Trust Service Providers (eIDAS Art. 13)) to rules with a public law nature (to regulate relationships of the State, for example Arts. 17 and 20 on supervision of qualified Trust Service Providers).

[68] The system went live in May 2016: https://identityassurance.blog.gov.uk/2016/05/19/gov-uk-verify-update-on-progress-were-ready-to-go-live/.

[69] eIDAS Art. 6(1)(b): [the eID shall be recognised when] "the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body...".

[70] eIDAS Art. 6(2): "*may* be recognised" [our emphasis].

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

deny access to its online tax services to UK eIDs.

Gov.UK Verify at the moment only supports LoA 'Low', Identity Assurance Level 2 (see table 1),[72] meaning that cross-border interoperation is voluntary. However, support of higher LoA and 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 around a principle-based policy, the private Identity Providers are in principle free to use any technological means they wish. LoA 3 is specified in Cabinet Office, 2014 as 'Level Identity 4'. Accommodation of biometrics, therefore, is up to the discretion of the Identity Provider. Careful consideration of how Gov.UK Verify and the Central Hub will handle biometric data is a matter of future work, if LoA 3 becomes available to the system.

5.1.2 Interoperability framework

Gov.UK Verify aims to be technology neutral, as noted in its Identity Assurance Principles.[73] It also aims to comply with Privacy-by-design and minimisation principles. Certain design choices, though, involving central components appear inconsistent with these premises.

One of eIDAS' requirements is the *'unique representation'* of an individual.[74] In other words, each record is required to have a Unique Identifier associated with it. This Unique Identifier is expected as part of the mandatory minimum dataset for natural persons.[75]

Gov.UK Verify does not include Unique Identifiers by design. In fact, it was one of the design goals to avoid the feature that caused the attempted National Register Database to fail. Implementation of the Central Hub in between Identity Providers and Service Providers aimed 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 system.

The system does provide for a minimum dataset though. Between the Identity Provider, the Central Hub and the Matching Service, eIDs are exchanged in the form of a record with a set amount of attributes. The record contains a pseudonym and the minimum dataset. The minimum dataset, in other words, is the transaction identity (Sullivan, 2011).

Since Gov.UK Verify does not seem to support selective disclosure (Brandão *et al.*, 2015), it is safe to assume that the minimum dataset is always transferred to and from the Central Hub. On top of the original identifiers, the minimum dataset will be enriched by user provided attributes, in case of a failed attempt to match the local records.[76] In the end, the Matching Service creates an association table, storing the received pseudonyms and matching datasets to the local accounts of the Service Provider. The pseudonym assigned by the Matching Service is persistent. This is in order to avoid having to follow the same process every time: the Matching Service needs to associate the account from the Identity Provider to a local one only the first time; by keeping the pseudonyms static each subsequent time the Matching Service knows to which local account the eID refers to. But this also means that if more than one Service Providers access the same Matching Service, they will all receive the same pseudonym for each eID. Since the Matching Service is deployed at the Service Provider level, there is no telling of how many different Matching Services exist. If the same pseudonym assigned to a user is shared by more than one Service Provider, it effectively allows the pseudonym to function as a *de facto* Unique Identifier (Brandão *et al.*, 2015).

Though eIDAS mandates that a Unique Identifier is expected, definition of the Unique Identifier is up to the Member State. The 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 system — to assign as Unique Identifier the Pseudonym created by the eID card (BSI, 2016).[77]

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

In order for this function to produce consistent pseudonyms for each user every time a single Matching Service must exist between Central Hub and Service Provider (of the receiving Member State). This means that the UK will have to deploy its system to receiving Member States in the form of a proxy. A proxy would give the UK the opportunity to operate one Matching Service that could then transmit the pseudonymised minimum dataset across indefinite Service Providers.[78] Obvi-

[72] *See* note in http://alphagov.github.io/rp-onboarding-tech-docs/pages/arch/arch.html [accessed 20 February 2017].

[73] Section 3.1 and footnote 9.

[74] eIDAS Art. 3(1).

[75] According to IR 2015/1501 the minimum dataset is comprised of at least First and Last Name(s), date of birth and Unique Identifier. It is unclear whether additional attributes are mandatory: most of the translations of the IR refer to additional attributes as an optional set of which Member States *'may'* include one or more into the minimum data set. Note that there are translations that have used the workd *'must'* though (*see* for example http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015R1501&from=EN [in Greek]). The eIDAS technical specification refers to those attributes as optional depending on availability and legality under national law.

[76] The specification requires additional user consent to be given in case an attribute provider is involved to enrich the minimum dataset (*see* footnote 32), but user consent can be assumed if the user is the source of the attributes.

[77] 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 Unique Identifier is forbidden: *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].

[78] A proxy based interoperability seems logical in any case, considering that the Central Hub is a centrally deployed key part of the system. Perhaps central deployment of the Central Hub and a middleware offer of the Matching Service would be possible, but in that case each user would acquire a different pseudonym for each Matching Service.

ously this functionality is 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.

Existence of *de facto* Unique Identifier would be hard to justify as long as it remains undocumented.[79] Federated architectures were developed to function without need of global identifiers (or transfer of identifiers across organisations) (Rundle and Laurie, 2005). Perhaps the Government Digital Service intended for a different Matching Service at every Service Provider, in which case there is no risk of the described behaviour. But since in theory combination of Service Providers under a single Matching Service is possible, the system and its regulation should be updated to include this possibility (or its prevention).

The Government should update the policies that regulate the relationship between Central Hub, Identity Provider and Service Provider[80] 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 Service Provider. 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 Service Provider (or many Service Providers under one Matching Service) would allow the system to accommodate the Unique Identifier function eIDAS requires. This of course presupposes that adequate risk assessment has been undertaken beforehand.

5.1.3 Data protection

Under requirement (i)(*g*) a notified national system needs to comply with Data Protection rules. The system under Gov.UK Verify is governed by the Data Protection Act (DPA), which transposed the requirements of the Data Protection Directive. The Directive's provisions on the lawful bases for legitimate processing of personal data have been essentially preserved under the GDPR.[81]

According to the contractual agreement Gov.UK Verify signs with each Identity Provider, the Central Hub is a data controller in respect to the personal data that it processes.[82] The DPA mandates that in order for any processing to be fair and lawful, it needs to be transparent and based on a legal basis.[83] It has been accepted that in a transparent processing users should be fully informed of the kind of processing that is taking place (Article 29 Working Party, 2011). The Impact Assessment carried out for Gov.UK Verify specifies that processing is enabled by two legal bases: Processing necessary in the public interest or in exercise of official authority and processing after user consent.[84] However, between the two emphasis is given to user consent.[85] The relevant privacy policy does not enumerate the data collected in an exhaustive way[86] and contains no information on retention periods. According to the Privacy Policy, the Central Hub stores "the level of assurance, the date and time, an identifier that is used to help in the matching process and some anonymous identifiers that are used to manage the integrity of the authentication session" and "may also collect the IP address, device fingerprint and details of what device and which version of web browser was used to access the service."[87] The Policy specifies that the data are stored for monitoring and reporting and the Central Hub will not attempt to identify users from them.[88] However, this seems to contradict the Impact Assessment, which claims that even though "some data is gathered [. . .] this does not include any personal details [. . .] and is dropped at the end of the session".[89] Consequently, the Impact Assessment opines that no consent is needed for the Central Hub and therefore no information is given on users' right to revoke their consent at any time. It is certain that the Matching Service stores at least a record of received pseudonym and associated pseudonym to facilitate linking of eIDs to local accounts (Cabinet Office, 2013). It is unclear therefore what happens to the data held in the Central Hub and the Matching Service in case a user decides to close down an account with an Identity Provider.[90]

Adding to the confusion, promotional material of the system insist that no personal data are processed inside the Central Hub,[91] raising questions about the specificity of user consent to the processing, as blanket consent is not allowed under the

[79] *See* also Brandão *et al.*, 2015 where the authors conclude that persistent pseudonyms and visibility of attributes (non-selective disclosure) could lead to user impersonation by the Central Hub, should the Central Hub become compromised.

[80] including the Framework Agreement and the Identity Assurance Principles.

[81] For a detailed comparison of the differences, *see* Chapter 7 "Lawful basis for processing", in D. Gabel and T. Hickman, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law. 2016, White & Case LLP. Available from: https://www.whitecase.com/publications/article/chapter-7-lawful-basis-processing-unlocking-eu-general-data-protection [accessed on: 23 February 2017].

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

[83] DPA Sch. 2; the list is exhaustive.

[84] Section 3.4.3 in T. Stevens. Gov.UK Verify Data Protection Impact Assessment. V1.0, Government Digital Service, 18 May 2016. Available from: https://identityassurance.blog.gov.uk/wp-content/uploads/ sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf [accessed on: 25 May 2017].

[85] With Section 3.4.3 footnote 84 detailing how user consent is obtained by each component of Gov.UK Verify; user consent is also the usual basis mentioned in public communication.

[86] 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.

[87] 'What information we process' in footnote 86.

[88] Ibid.

[89] DPIA footnote 84 p. 10.

[90] The GDS "RECOMMENDS that service providers SHOULD provide an administrative function that allows an administrator to remove" the associated data (Cabinet Office, 2013, s. 2.2).

[91] "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/.

DPA,[92] and about conformity with the Identity Principle of Transparency in personal data processing.[93]

Clearer privacy policies on the exact processing that takes place in the Central Hub and Matching Service would be of value to strengthen user consent and specificity. In particular, privacy policies and T&C of the Central Hub, as well as the Framework Agreement between the parties should detail the processing of pseudonyms inside the Central Hub, the reasons, if any, that pseudonyms should not be considered personal data[94] and how the Central Hub handles the rest of identifiers in the minimum dataset since selective disclosure is not possible in the current system.

5.2 Compliance with liability requirements

eIDAS provisions on liability pose an interesting complexity: Even though liability for Trust Service Providers is clearly defined,[95] allocation of liability for eID systems, according to Article 11, involves not only the parties that issue and operate the eIDs but also the notifying Member State.[96] The Member State of a notified system is liable for damages caused intentionally or negligently to any natural or legal person if the system fails to uniquely identify the individual or if online authentication becomes unavailable. Private providers, they have the right to limit how their services will be used through their T&C,[97] but do not seem able to limit their liability if damage occurs out of intention or negligence. Regardless, the Member State is always liable for damages and users cannot limit their liability in case of machine malfunction or compromise (Massacci and Gadyatskaya, 2013). It could be questioned, thus, why states would notify their systems since that would expose them to responsibilities for actions beyond their control (Dumortier and Vandezande, 2012), 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 (Identity Providers, authorities, Service Providers) have limited their liability with their interparty agreements to a bare minimum apart from cases of fraud or death.[98] In domestic transactions the Government has followed the same practice in its relationship to the contracted Identity Providers and Service Providers 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 might. Additionally, in Gov.UK Verify the authentication process is performed jointly by the Central Hub (owned by the government) and private providers, which might pose difficulties under the joint liability regime introduced with the GDPR. 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.[99]

5.3 Potential legal equivalence under eIDAS

In light of the above, particular attention must be given in certain areas prior to a notification of Gov.UK Verify under eIDAS. For interoperation with EU eID services after an exit from the EU, though, several other considerations must be made.

Since eIDAS allows for participation of systems of different Levels of Assurance,[100] absence of some of the levels should not impact negatively on equivalence but it could mean denial of service against Service Providers that require higher LoA. The required Minimum DataSet is matched by Gov.UK Verify's minimum dataset which includes some extra identifiers.[101]

In terms of governance requirements assessing legal equivalence is complex. Gov.UK Verify falls under category item (ii)*(c)* of eligible systems for notification, with a mix of governmental (the Central Hub and Matching Service) and private-sector (the Identity Providers) components.[102] At the moment there is no information on its supervision regime. More importantly, whether all requirements for notification (e.g. the procedures for deliberation between the Member States before notification of a system) should be followed by third countries or can be offset, at least to some degree, by equivalent provisions in the third country is a question that should be further explored in case eIDAS extends legal equivalence to eID services.[103]

Gov.UK Verify's administrative and security requirements are governed by a large number of policies, contracts and codes of practice between the participating actors (the Central Hub and private Identity Providers)[104] that will require closer examination.

Finally, it is questionable whether liability requirements are essential for the purposes of establishing legal equivalence for eIDs. In a scenario where the objective is for Gov.UK Verify

[92] 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.

[93] 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.

[94] 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* Burton *et al.*, 2016.

[95] eIDAS Art. 13.

[96] *See* section 4.2 item (v); liability allocation becomes even more complicated taking into consideration the GDPR's provisions that, when they become applicable, will allocate joint liability to data controllers and processors (Art. 82(4)) and place upon them the burden of proof (Art. 82(3)).

[97] eIDAS Art. 24(2)(d) and Rec. 37, *see* section 4.2 item (v) and item (iii)*(f)*.

[98] *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.

[99] Omission of minimum liability is something that was criticised about the eIDAS Regulation. *See*, for example, Bitkom, 2013.

[100] eIDAS Art. 6(2).

[101] *See* section 3.2.2 and footnote 30. Note that the required Unique Identifier is absent from the minimum dataset so alternative solutions need to be sought as highlighted in section 5.1.2.

[102] *See* section 3.2.1.

[103] *See* footnote 67 and related discussion about essential / non-essential requirements.

[104] *See*, for example, footnotes 82 and 98 on the Framework Agreement and the separate T&C of the private parties.

to be interoperable with EU services, the relationship of a user (of Gov.UK Verify) and the system (Gov.UK Verify) becomes a purely internal (i.e. British) relationship. On the other hand, in the case of an individual user (of an EU Member State) and a Service Provider (in the UK) liability provisions of eIDAS could be offset by conflict-of-law rules, if they were to ensure in many cases the applicability of a Member State's national tort law integrating Article 13 of eIDAS.[105] However, note that liability will be important for legal equivalence under the GDPR, as explained in section 4.2.

6 Future Work

A more detailed and comprehensive analysis of data protection adequacy will be needed to determine to what extend data protection requirements complement eIDAS requirements. The requirements set forth in the GDPR will need to be classified into a framework similar to the one detailed in this paper, in order to assess complementary or potentially conflicting requirements to the ones already discussed. At that stage it will then be possible to draw a basic hierarchy between these different requirements and distinguish between essential and non essential requirements for equivalence between eID systems. For that analysis an interdisciplinary approach is needed that will be able to bridge legal considerations with system engineering and trust modelling. Ultimately the goal is to identify the requirements that would make interoperability between third country eID services and EU eID services possible.

7 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 eID operation across borders and highlighted potential discrepancies in policy and modus operandi should the UK wish to notify their system under eIDAS.

In particular, the way the system (and namely the Matching Service component of the Central Hub) handles pseudonymisation currently seems incompatible with the founding Identity Assurance Principles, data protection guidelines and the goal of unlinkability. In case pseudonyms as a *de facto* Unique Identifier 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 a Unique Identifier 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 Central Hub processes personal data and to establish minimum liability requirements for contracting parties of the system. 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.

Consecutively we examined issues of legal equivalence which will become relevant when UK exits the EU. We highlighted that eIDAS does not cover international interoperability of eID systems, although eIDAS caters for international trust services. By analogy with the approach taken for trust service providers, we identified five categories of requirements that could be relevant for equivalence assessment and ultimately interoperability, noting that the last set, i.e. liability requirements, appear less relevant for the purpose of ensuring interoperability between third country eID systems and EU services. Finally, we acknowledged that future work is needed in order to distinguish between essential and non essential requirements as well as to model GDPR requirements, including its adequacy framework.

Acknowledgments

This research was funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, University of Southampton, EP/L016117/1, partly supported by the SOCIAM Project, funded by the UK Engineering and Physical Sciences Research Council under grant number EP/J017728/2, and was partly funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 700542. This paper reflects only the authors' views; the Commission is not responsible for any use that may be made of the information it contains.

References

Article 29 Working Party. 2011. "Opinion 15/2011 on the definiton of consent". *adopted 13 July* No. WP 187.

Barak, A. 2007. *Purposive interpretation in law*. Princeton University Press. ISBN: 0691133743.

Barnard, C. 2013. "Competence Review: The Internal Market". Department for Business, Innovation and Skills. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/226863/bis-13-1064-competence-review-internal-market.pdf (accessed on 11/20/2016).

Beynon-Davies, P. 2011. "The UK national identity card". *Journal of Information Technology Teaching Cases*. 1(1): 12–21. DOI: 10.1057/jittc.2011.3.

Bitkom. 2013. *Position Paper on the Proposal for an EU Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*. URL: https://ameliaandersdotter.eu/sites/default/files/wp-content/uploads/2013/04/20130408-BITKOM-Position-on-eID-regulation1.pdf (accessed on 07/25/2015).

Black, J. 2008. "Forms and paradoxes of principles-based regulation". *Capital Markets Law Journal*. 3(4): 425–457.

[105] Even though selection of the applicable rules will vary depending on the national legal system and its choice of law rules, in general it is presumed that in actions raised by EU nationals the *lex loci delicti* will amount to a Member State's legal system, which will already have incorporated eIDAS in its national legal order.

Brandão, L., N. Christin, and G. Danezis. 2015. "Toward Mending Two Nation-Scale Brokered Identification Systems". *Proceedings on Privacy Enhancing Technologies*. 2015(2): 135. DOI: 10.1515/popets-2015-0022.

BSI. 2016. *TR-03110 eIDAS Token Specification*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile~%5C&~v=1 (accessed on 01/12/2016).

Burton, C., L. D. Boel, C. Kuner, A. Pateraki, S. Cadiot, and S. G. Hoffman. 2016. "The Final European Union General Data Protection Regulation". *BNA Privacy & Security Law Report*. 15: 153.

Cabinet Office. 2013. "Identity Assurance Hub Service SAML 2.0 Profile v1.2a". *Report*. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458610/Identity_Assurance_Hub_Service_Profile_v1.2a.pdf (accessed on 07/23/2015).

Cabinet Office. 2014. *Good Practice Guide No. 45 Identity Proofing and Verification of an Individual*. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf (accessed on 08/08/2015).

Cavoukian, A. 2006. "The Case for Privacy-embedded Laws of Identity in the Digital Age". *White Paper*. URL: https://www.ipc.on.ca/images/resources/up-7laws_whitepaper.pdf (accessed on 06/11/2015).

Chatfield, T. 2014. *Digital Government Review*. URL: http://digitalgovernmentreview.readandcomment.com/ (accessed on 06/15/2015).

Cooper, A., H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, and R. Smith. 2013. *Privacy Considerations for Internet Protocols*. URL: http://www.rfc-editor.org/info/rfc6973 (accessed on 09/06/2016).

Crosby, J. 2008. "Challenges and opportunities in identity assurance". URL: http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf (accessed on 08/16/2015).

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

Dumortier, J. and N. Vandezande. 2012. "Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market". *ICRI Research Paper*: 9. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152583 (accessed on 12/25/2016).

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

eIDAS Technical Sub-group. 2015. "eIDAS Technical Specifications". *v0.90, July*. URL: https://joinup.ec.europa.eu/sites/default/files/eidas_technical_specifications_v0_9.pdf (accessed on 11/04/2016).

Federal Office for Information Security [BSI]. 2011. *Technical Guideline TR-03127: Architecture electronic Identity Card and electronic Resident Permit*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03127/BSI-TR-03127_en.pdf (accessed on 05/23/2016).

Fiat, A. and A. Shamir. 1987. "How To Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *Advances in Cryptology – CRYPTO' 86*. Ed. by A. M. Odlyzko. Vol. 263. *Lecture Notes in Computer Science*. Springer Berlin Heidelberg. 186–194.

Hansen, M. 2008. "Marrying Transparency Tools with User-Controlled Identity Management". In: *The Future of Identity in the Information Society*. Ed. by S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci. *IFIP – The International Federation for Information Processing*. Springer US. Chap. 14. 185–206.

Honcharova, Y. and A. Eryomenko. 2014. "STORK - Promising project of european transnational electronic identification". *First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*. DOI: 10.1109/infocommst.2014.6992347.

Hörbe, R. and W. Hötzendorfer. 2015. "Privacy by Design in Federated Identity Management". In: *IEEE Security and Privacy Workshops (SPW)*. San Jose, California, USA.

Hulsebosch, B., G. Lenzini, and H. Eertink. 2009. "D2.3 – Quality authenticator scheme". *STORK deliverable, 3 March*. URL: https://perma.cc/R5SH-DQG3 (accessed on 07/29/2015).

ICAO. 2017. "Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs". *Machine Readable Travel Documents, 7th edition,* No. Doc 9303.

Jøsang, A. 2015. "Assurance Requirements for Mutual User and Service Provider Authentication". *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*: 26–44. DOI: 10.1007/978-3-319-17016-9_3.

Jøsang, A., J. Fabre, B. Hay, J. Dalziel, and S. Pope. 2005. "Trust requirements in identity management". In: *Proceedings of the 2005 Australasian workshop on Grid computing and e-research*. Ed. by R. Buyya, P. Coddington, P. Montague, R. Safavi-Naini, N. Sheppard, and A. Wendelborn. Vol. 44. Australian Computer Society, Inc. 99–108. ISBN: 1920682260.

Kuner, C. 2017. "The Internet and the Global Reach of EU Law". In: *Collected Courses of the Academy of European Law*. Ed. by L. Azoulai, N. Bhuta, and M. Cremona. Oxford: Oxford University Press. Forthcoming.

Lloyd, I. 2009. "Anonymity and the Law in the United Kingdom". In: *Lessons From the Identity Trail: Anonymity, Privacy and Identity in A Networked Society*. Ed. by I. Kerr, C. Lucock, and V. Steeves. Oxford University Press.

Maler, E. and D. Reed. 2008. "The Venn of Identity: Options and Issues in Federated Identity Management". *IEEE Security & Privacy*. 6(2): 16–23.

Martens, T. 2010. "Electronic identity management in Estonia between market and state governance". *Identity in the Information Society*. 3(1): 213–233. DOI: 10.1007/s12394-010-0044-0. URL: http://dx.doi.org/10.1007/s12394-010-0044-0.

Massacci, F. and O. Gadyatskaya. 2013. "How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results". *White Paper*. URL: http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf (accessed on 07/27/2015).

Pfitzmann, A. and M. Hansen. 2010. "Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology". *Version v0.33, April 8*. URL: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.doc (accessed on 06/12/2015).

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

Rundle, M. C. and B. Laurie. 2005. "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*. DOI: 10.2139/ssrn.881107.

Strauß, S. and G. Aichholzer. 2010. "National Electronic Identity Management: The Challenge of a Citizen-centric Approach Beyond Technical Design". *International Journal on Advances in Intelligent Systems*. 3(1).

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

Sullivan, C. and S. Stalla-Bourdillon. 2015. "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. DOI: 10.1016/j.clsr.2015.01.002.

Svantesson, D. J. B. 2013. "A "layered approach" to the extraterritoriality of data privacy laws". *International Data Privacy Law*. 3(4): 278–286. DOI: 10.1093/idpl/ipt027. URL: http://idpl.oxfordjournals.org/content/3/4/278.abstract.

UNCITRAL. 2016. *Legal Issues Related to Identity Management and Trust Services*. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/026/34/PDF/V1602634.pdf (accessed on 10/15/2016).

Whitley, E. A. 2016. "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.

Windley, P. J. 2005. *Digital Identity*. O'Reilly.

Zwingelberg, H. 2011. "Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card". In: *Privacy and Identity Management for Life*. Ed. by S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, and G. Zhang. *IFIP Advances in Information and Communication Technology*. Springer Berlin Heidelberg. ISBN: 978-3-642-20768-6. DOI: 10.1007/978-3-642-20769-3_13. URL: http://dx.doi.org/10.1007/978-3-642-20769-3_13.

Zwingelberg, H. and M. Hansen. 2012. "Privacy Protection Goals and Their Implications for eID Systems". In: *7th IFIP Advances in Information and Communication Technology*. Springer Berlin Heidelberg.