JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.2 (2013)

Governance Models for Interoperable Electronic Identities

Tobias Mahler[1]

Abstract: Current implementations of electronic identity in Europe are rather diverse; they include state-driven identity management frameworks as well as private sector frameworks and different forms of public-private collaborations. This diversity may represent a major challenge for the deployment of information society services addressed towards the European internal market. This raises the question: How can we achieve interoperability of electronic identities across Europe, and potentially beyond Europe's borders? This paper argues that the interoperability of electronic identity could be governed by a multi-stakeholder governance framework that brings together different parties with interests in the provision and use of electronic identities. Such a governance framework could, for example, consist in designing and operating a portal with common functionalities that allows interoperable authentication across multiple domains and contexts. Inspiration for the governance of such a portal could come both from existing successful implementations of electronic identity and from multi-stakeholder institutions that have proven useful in Internet governance.

Introduction

Interoperable electronic identity (eID) is often considered a necessary ingredient of cross-border interactions and transactions over the Internet. Anyone building a framework for interoperable eIDs needs to address a wide array of issues, including the choice of a technical framework, the context for which eIDs shall be used (e.g., eGovernment, eBusiness, or both) and the selection or development of a suitable legal framework. Many of these issues are, in practice, dependent on and intertwined with the institutional arrangements put in place to govern the eID framework. For example, amongst the interesting legal issues is the liability of actors involved in the provision and use of eIDs. [2] The liability of parties to an eID framework depends evidently, in part, on the roles of the collaborators and their legal status. Similarly, the provision and use of eIDs needs to comply with legal requirements—for example, under data protection law—and ensuring compliance may have to be organised across a network of collaborating parties.

Identity management[3] systems are currently implemented in a variety of governance structures and models in Europe. This spans from primarily state-driven eIDs to different degrees of public-private collaborations and private sector solutions. The private sector's involvement is not necessarily surprising, because both private and public entities might, in principle, play a role in the provision and use of eIDs. Besides, the key role of the private sector in eID innovation is beyond question. While the variety of implementations and governance models in Europe may be seen as a challenge for interoperability, it

[1] Norwegian Research Center for Computers and Law (NRCCL), the Faculty of Law,University of Oslo, tobias.mahler@jus.uio.no. Thanks are due to the European Commission's Joint Research Centre, Institute for Prospective Technological Studies (IPTS), for the invitation to present this paper at the workshop "Electronic Identity for Europe" in Cyprus. Thanks go also to Lee Bygrave, Emily Weitzenboeck, and Kevin McGillivray, who have provided valuable comments to an earlier draft and to Robert Queck for discussing with me the status of identity services in the electronic communications framework. However, any errors or omissions are entirely mine. Financial support for this work is gratefully acknowledged from the Research Council of Norway and NORID under the Igov2 project.

[2] See, e.g., Georg Borges, "Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis: Ein Gutachten für das Bundesministerium des Innern," (2010). Regarding liability issues in the context of digital certificates see, e.g., Rolf Riisnæs, *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar: en tillitsorientert tilnærming til sertifikatutstederens villedningsansvar* (Bergen: Fagbokforlaget, 2007).

[3] For an introduction to identity management see Roger Clarke, "Identity Management," (Xamax Consultancy, 2004).

could also be viewed as an illustration of some of the breadth of available options and solutions for the future governance of eID in Europe and beyond. This paper discusses a few basic models for the governance of eID and exemplifies these based on selected examples of existing European eID implementations.

The structure of this paper is as follows: Section 1 introduces the concept of eID and the roles involved in issuing and using interoperable eIDs. This paper focuses primarily on interoperable eID in a European context. Therefore, Section 2 provides a very brief outline of the European legal framework for eID. However, the main interest of this paper does not centre on the legal issues as such, but on the governance of interoperable eIDs. Therefore, Section 3 introduces the concept of governance; Section 4 discusses the governance of other identifiers—such as domain names, and Section 5 explains how interoperable eID can be framed as a governance challenge. The paper then turns towards the core of eID governance. In this context we can make a rough distinction between eID provision and use. The subsequent Sections (6, 7 and 8) focus on eID provision and describe three basic models of eID provision, respectively based on public, private and public-private governance structures. When eIDs are offered based on very dissimilar governance structures, this may result in a rather heterogeneous picture, which may be challenging in terms of interoperability. Therefore, Section 9 focuses on the governance of interoperability itself. One solution to the problems of inconsistent and diverging eIDs may be to create an intermediary agency (an authentication authority) that is able to handle interoperability problems directly. This approach, as well as its governance challenges, is explained based on a concrete example of an eID portal. The concluding Section 10 argues that the latter model could potentially be employed to address eID interoperability not only at the European level, but also in a wider context.

1. eID and interoperability

The need for eID arises in part from the fact that the Internet is designed to be somewhat agnostic to the identity of its users. Domain names and IP numbers are machine identifiers, rather than identifiers of persons, even though personal identification may be possible.[4] Therefore, we use identifiers such as e-mail addresses or user names to identify a person. An eID can be the basis for different functions, in particular authentication and signature.[5] We are here particularly interested in eIDs that can be used for authentication purposes. A relying party can *authenticate* a claimed identity by examining one or more authenticators (such as passwords or other credentials) to verify the legitimate use of an identifier (e.g., a user name).[6] Different eIDs may vary in their level of assurance, depending on certain security aspects of the authenticator(s).

The notion of eID is here not used as a precisely defined technical concept; the IT literature usually applies a more specific taxonomy.[7] However, it can be based on the technical notion of "identity" in the sense of "any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons".[8] The use of eIDs in identity management systems can be distinguished from directory services that provide some information connected to an identifier. Directory services are not designed to facilitate either authentication or signature. An example of a directory service is the WHOIS service, which provides information about the technical and administrative points of contact administering domain names.[9] Mueller and Chango have described the WHOIS service as a

---

[4] See, e.g., P. Lundevall-Unger and T. Tranvik, "IP Addresses–Just a Number?," *International Journal of Law and Information Technology* 19, no. 1 (2011). Moreover, it may be possible to use a URL as an identifier of an eID, as foreseen in the W3C specification "WebID 1.0: Web Identification and Discovery", W3C Editor's Draft, 17 October 2011, available at http://www.w3.org/2005/Incubator/webid/spec/ (last visited 10 November 2011).

[5] Regarding electronic signatures, see Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p. 12 (e-Signatures Directive).

[6] Clarke, "Identity Management," 3. Authentication is closely related to, but needs to be distinguished from, *authorization*, i.e., the decision about an authenticated user's privileges.

[7] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," (version v0.34, 2010).

[8] See ibid., 30.

[9] Cf., e.g., Article 16 (1) of Regulation (EC) No. 874/2004. See further D.I. Cojocarasu, "Legal Issues Regarding WHOIS Databases," (Oslo: Senter for rettsinformatikk, 2009).

"surrogate identity system:" [10] The data in the WHOIS record is as close as the Internet gets to an identity card.[11] The WHOIS service is not aimed at authentication, even though it may play a central role for the creation of trust on the Internet, particularly when combined with adequate security mechanisms.[12]

Despite this potential similarity in function, the primary focus of this paper is not on directory services, but on eIDs.[13] At the same time, we cannot delve into the details of eID technologies, because the centre of attention is on the governance of eIDs. We are particularly interested in eIDs that allow an identity holder to use an interoperable eID in an identity management framework spanning across multiple contexts, such as those of eBusiness and eGovernment. This use and re-use of eIDs within different contexts requires some degree of interoperability, both in the sense of technical standardisation[14] and in terms of organisational collaboration.[15] Strongly simplified, technical interoperability implies, for example, that an eID issued by one actor (e.g., the identity provider) can be understood and used by another actor (e.g., a relying party). This is usually embedded in some kind of identity management framework, which may require quite complex organizational collaboration. For example, the issuing of an eID may involve collaboration between a registration authority (enrolling the eID holder), an identity provider (who may issue the eID itself, or on whose behalf the eID is issued) and an agency that distributes the eID (for example, on a smart card). Similarly, the use of an eID could involve not only relying parties, but also authentication authorities[16] and perhaps even further intermediaries and service providers.

The governance framework has to address both the provision and the use of interoperable eIDs:[17] First, one needs to ensure that eIDs are created and issued through a collaboration of registration authorities, identity providers, and possible distributors. This corresponds to the eID *registration phase*. Second, there are governance issues related to the use of eIDs during the *authentication phase*. Interoperability is of particular importance for the latter phase. There may be many ways to ensure interoperability, but this paper will focus on institutional solutions involving an intermediary, in particular an authentication authority (see Section 9).

2. The European legal framework for eID

Any framework for eID has to be related to, and comply with, the applicable legal framework. This section will briefly note a few European legal instruments that may be at least partly relevant to the provision and use of interoperable eIDs. In principle, interoperability of eIDs is not only a European issue; it can indeed be seen as a global challenge. Nevertheless, within the European discourse about eID it may be prudent to focus on a European solution initially, because an interoperable eID in Europe would be a particularly useful facilitator for the European internal market and for eGovernment in Europe. Indeed, interoperability of eIDs has been identified as a key challenge for eGovernment and for some aspects of eBusiness in Europe.[18] One of the elements in that discussion is whether Europe currently lacks

[10] Milton Mueller and Mawaki Chango, "Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy," *Journal of Information Technology & Politics* 5, no. 3 (2008): 304.
[11] Ibid., 310.
[12] An example of such security mechanisms are Domain Name System Security Extensions (DNSSEC), based on specifications for securing certain kinds of information provided by the Domain Name System. See, e.g., https://www.iana.org/dnssec/.
[13] However, such directory services can be a useful basis for comparing governance models, as shown below in Section 4.
[14] See generally on interoperability Laura DeNardis, *Opening standards: the global politics of interoperability*, The information society series (Cambridge, Mass.: MIT Press, 2011).
[15] See, e.g., Thomas Olsen and Tobias Mahler, "Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust'," *Computer Law & Security Report* 23, no. 4+5 (2007).
[16] On authentication providers see R. Leenes et al., "D.2.2 — Report on Legal Interoperability," (Stork eID Consortium, 2009), 23-27.
[17] Ibid., 24-25.
[18] N. N. G. de Andrade, "Towards a European eID regulatory framework. The Legal Gaps, Barriers and Challenges of Constructing a Legal Framework for the Protection and Management of Electronic Identities," in *European Data Protection: In Good Health?*, ed. S. Gutwirth, et al. (Springer, 2012 - forthcoming).

an adequate regulatory framework for eID.[19] What may be called "the legal framework" consists of a patchwork of partly relevant rules in several legal instruments, including at least the EU electronic signature directive[20] and the data protection directives.[21] Thus, all identity management systems must comply with the applicable data protection laws.[22] In complex identity management systems consisting of several collaborating parties, this requires a number of potentially difficult assessments, such as who is acting as a data *controller* and who is a data *processor*.[23] For example, in a series of cases before the Norwegian Data Protection Agency, the latter body questioned a number of operational details in a Norwegian eID system utilized in the eGovernment context.[24] The agency's criticism related not only to insufficiently clarified roles of participants, but also to whether there existed sufficient legal basis for all aspects of the processing of personal data. It is beyond the scope of this paper to discuss these issues in any detail.

However, it may be in order to highlight one minor aspect of the legal framework that is usually omitted from legal discussions about eIDs—perhaps for a good reason. This relates to the fact that the EU regulatory framework for electronic communications was in 2009 extended with explicit rules about "identity services" related to electronic communications. These rules may not be directly applicable to eIDs used for eBusiness or eGovernment services (as shown below), because the rules focus on the underlying communications network, rather than on the services. However, these rules are nevertheless of interest here, if only to illustrate the possibility of focusing on competition in the eID context. Readers without specific interest in the EU legal framework may consider skipping the remainder of this section and continuing directly with Section 3 below.

In order to understand "identity services" related to electronic communications, we need to briefly outline their legal context. In 2009, the "Better Regulation" Directive[25] introduced the notion of "associated services" into the electronic communications Framework Directive.[26] According to Article 2 (ea) of the amended Framework Directive, associated services include, *inter alia*, "*identity*, location and presence service" (emphasis added). Identity services are not defined in the Directive or elsewhere in the electronic communications framework, but "identity" is in the electronic communications context

---

[19] The lack of "an appropriate regulation regarding eID on a European level" was ascertained by T. Myhr, "Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution:: or I am 621216-1318, but I am also 161262-43774.1 Do you know who I am?," *Information Security Technical Report* 13, no. 2 (2008): 77. Concurring with this view de Andrade, "Towards a European eID regulatory framework. The Legal Gaps, Barriers and Challenges of Constructing a Legal Framework for the Protection and Management of Electronic Identities," Section I.4.5.

[20] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p. 12 (e-Signatures Directive).

[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), L 281 , 23/11/1995, p. 0031 – 0050; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002-07-31, L 201, pp. 37 – 47, as amended.

[22] See further Olsen and Mahler, "Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust'."; Thomas Olsen, "Personvernøkende identitetsforvaltning" (University of Oslo, 2010).

[23] According to the Data Protection Directive 95/46/EC (above, note21), Article 2 (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law. According to Article 2 (e) of the same Directive, 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

[24] The Norwegian Data Protection Agency (Datatilsynet), control reports 08/00291and 08/00297; decisions "Altinn sentralforvaltning" (2008) and "Skattedirektoratet og Altinn (2008). For an overview of these cases see Olsen, "Personvernøkende identitetsforvaltning," 165 et seq.

[25] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337/37.

[26] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, OJ L 108 of 24.4.2002.

sometimes used in the context of caller identification, which is perhaps closest to a directory service as described above. In general, the concept of "associated services" is relevant because it triggers the authority and obligation of national regulatory authorities to promote competition in the provision of electronic communications services and associated services.[27] Moreover, pursuant to the Access Directive, operators with significant market power may be required to provide access to associated services, including identity services.[28]

However, despite the initial similarity of terminology, it is not certain that these rules will apply to the typical eID services used in eGovernment and eBusiness, because these would typically qualify as so-called information society services.[29] This is important because, in order to qualify as an associated service under the Framework Directive, the service has to be associated with an *electronic communications service*—i.e., it needs to be related to the conveyance of signals on electronic communications networks, which explicitly excludes information society services such as eBusiness and eGovernment.[30] Thus, the provisions on "identity services" in the electronic communications context would probably not be directly applicable to the context of eIDs in eBusiness and eGovernment. eIDs are usually offered by actors involved in either eBusiness or eGovernment, with no particular role in the conveyance of signals on electronic communications networks. It remains to be seen how these rules will be applied to identity management systems operated by, e.g., telecoms operators.

However, these rules can serve here at least to illustrate the competition aspect of eIDs. Competition in a market for eIDs is indeed one of the relevant governance issues related to interoperable eIDs.

3. Governance

The problems of interoperability and competition in the eID context are here portrayed as governance challenges. The aim of this section is to briefly introduce the concept of governance, particularly in an Internet context.

Governance can be defined as a process of steering.[31] Its etymological origins include the ancient Greek word *kybernan* and the Latin *gubernare*, 'to steer' as well as *kybernetes*, "pilot" or "helmsman." Thus, the double nature of both (i) the act of governing and (ii) the role of a governor are relevant to understand the concept. However, while governance may involve an authority relationship, this is not necessary by definition. Governance can take many forms, it can be carried out alone or collaboratively, top-down or bottom-up, and may exists across levels of social organization, e.g. at intra-organizational, national, European or global levels.

Of particular relevance for the eID context is Internet Governance. This can be defined based on the following working definition, drafted by the UN-appointed Working Group on Internet Governance and included in the Tunis Agenda adopted by the World Summit on Information Society:

> "Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules,

[27] See Article 8 (2) of Directive 2002/21/EC (note 26 above). In any case, a NRA has in practice to balance several aims, including, for example, consumer protection and competition. Thus, this provision may not in itself be sufficient to require NRAs to prioritize competition.

[28] See Article 12 (1) (j) Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), as amended by Directive 2009/140/EC (note 25 above).

[29] Information society services are defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" in Article 1 of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998, laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, OJ L 24, 21.7.1998, p. 37.

[30] See Article 2 (c) of Directive 2002/21/EC (note 26 above).

[31] This definition, its historical origins and connotations are based on William J. Drake, "Introduction: The Distributed Architecture of Network Global Governance," in *Governing global electronic networks: International perspectives on policy and power*, ed. William J. Drake and Ernest J. Wilson (Cambridge, Mass.: MIT Press, 2008), 7 et seq.

> decision-making procedures, and programmes that shape the evolution and use of the Internet."[32]

Central for this definition is the focus on the role of multiple stakeholders, including governments, the private sector and civil society. This multi-stakeholder focus is of particular relevance to the Internet, which has historically evolved with very limited involvement by states. While the discussion about multi-stakeholderism is still continuing in international fora, many of the key elements of the Internet are at the time of writing governed by an institutional ecosystem that facilitates a high degree of influence for different stakeholders.[33] For the purposes of the present paper, it is particularly interesting to note that Internet governance focuses, inter alia, on governing identifiers.

4. Governance mechanisms for identifiers

Amongst the basic functions of an eID is to identify a person. This identification function is interesting when we compare it to other identifiers, such as domain names and telephone numbers. My conjecture is that the spectrum of governance models in use for other identifiers might illustrate some of the available policy choices when designing an eID framework. Before we address the specific problems related to eID, we should therefore take a brief look at governance mechanisms used for other interoperable identifiers.

The governance of domain name addresses and IP (Internet Protocol) numbers is amongst the key issues in global Internet governance. Both of these identifiers are governed by a dedicated institutional framework that is administrated primarily by the Internet Corporation for Assigned Names and Numbers (ICANN) and its supporting organizations.[34] The most striking characteristic of this institutional framework is the substantial private sector influence, which is built into ICANN's decision-making procedures. At the same time, the ICANN model illustrates the difficulties with agreeing on a global framework for identity-related services, i.e., the contact information available in the WHOIS directory service. At the time of writing ICANN is still struggling with a reform of the WHOIS system that adequately addresses issues such as data protection and law enforcement.[35]

In addition, there are other identifiers of international relevance, such as radio frequency identification (RFID) tags which are administered by the private sector[36] and telephone numbers which are administered in part at national level—with substantial involvement of both national regulatory agencies and telecom operators—and in part at the international level under the auspices of the International Telecommunications Union—also with significant industry participation.

In summary, the governance of other interoperable identifiers is carried out in a number of different institutional models. While many identifiers are governed by stakeholders from the private sector alone (e.g. RFIDs), other governance models involve some degree of collaboration between stakeholders. In some cases, such as telephone numbers, this involves collaboration between stakeholders from the private sector with governmental authorities. Such public-private cooperation may not be sufficient to justify the label "multi-stakeholder governance", but there are also examples of the latter, where additional stakeholders such as end-users and civil society have some measure of influence. My argument in this

---

[32] Tunis Agenda for the Information Society, World Summit on the Information Society, 18 November 2005, paragraph 34.

[33] See, e.g., Lee A. Bygrave and Jon Bing, *Internet Governance: Infrastructure and Institutions* (Oxford: Oxford University Press, 2009).

[34] See, e.g., A.M. Froomkin, "Habermas@discourse.net: Toward a critical theory of cyberspace," *Harvard Law Review* 116, no. 3 (2003); Milton Mueller, *Ruling the root: Internet governance and the taming of cyberspace* (Cambridge, Mass.: MIT Press, 2002).

[35] See http://gnso.icann.org/issues/whois/policies. For the historical background see Mueller and Chango, "Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy."

[36] See further http://www.gs1.org/epcglobal (last visited 20 September 2011). The discussion of RFID governance falls outside the scope of this paper. For a multi-stakeholder governance model for RFID see http://www.rfid-in-action.eu/public/results/rfid-stakeholder-model (last visited 20 September 2011). The latter was created to achieve a structured model of all stakeholder groups that are relevant for the development, deployment and operation of RFID systems.

paper is that some of these governance models could be usefully applied to govern the development and use of interoperable eIDs. We might learn from successful governance models developed in other contexts and apply the lessons learned there to address some of the challenges with eID interoperability.

5. Interoperable eID as a governance challenge

If the interoperability of eIDs is recast as a governance challenge, it can be analysed in terms of the influence exercised by different stakeholders. A multi-stakeholder governance framework for eIDs would require that we first identify relevant stakeholders.

Who are the stakeholders related to the issuing and use of an interoperable eID? The answer to this question may depend to some degree on the specific context, so this must here be addressed in the abstract. The starting point can be the above-mentioned roles typically related to an eID, i.e., identity holders, registration authorities, identity providers, authentication authorities, relying parties, and other possible intermediaries and service providers.[37] Of particular interest are the roles of identity providers, registration authorities and authorization authorities, because these actors arguably have the greatest influence on the governance of an eID framework. At the same time, relying parties and identity holders should not be forgotten, as these two stakeholder groups are the primary "users" of eID. Moreover, a governance model should also include intermediaries with a core focus on interoperability, who might be able to address and manage some of the existing inconsistencies between different eID implementations (see further Section 9).

Any of these roles can, in theory, be filled by a person from the public or private sector. Moreover, also end-users and civil society hold stakes in an eID system, and their interests should be represented in a full multi-stakeholder framework. However, in order to limit the scope of this paper, we shall here concentrate primarily on the roles of business and the public sector.

We may roughly distinguish three very basic models of eID governance, namely:

- public eID governance,
- private eID governance, and
- governance by public-private partnerships.

Each sector brings with it the typical governance mechanisms. This is particularly evident when we focus on governance through legally binding rules. While private sector governance is limited to contractual governance, the public sector may in addition also employ legislative rule-making. Where the public and the private sectors collaborate on an equal footing, this usually implies some element of contractual governance. Of course, regardless of the specific governance model, any eID framework will obviously need to be operated within the context of the applicable laws. Thus, issues such as compliance with data protection law arise regardless of the chosen eID governance model.

As mentioned above,[38] we may distinguish between the governance of eID provision (the registration phase) and the governance of eID use (authentication phase), during which interoperability is essential. Any of the above three models could theoretically be applied to governance issues of both phases, as illustrated in Table 1.

Table 1: eID provision and use within the three governance models

eID provision and use:	**Public**	**Private**	**Public-private**
eID provision (registration phase)	Section 6	Section 7	Section 8
eID use (authentication phase)	Section 9		

[37] See Section 1.
[38] See Section 1.

The following sections (6-8) present and exemplify the three above mentioned governance models based on selected aspects of eID provision in several European countries. These sections focus primarily on the institutional framework in place to govern the issuance of eIDs. Thereafter, Section 9 is dedicated to the governance of the authentication phase, with a particular focus on how interoperability of eIDs can be facilitated.

6. Public eID provision

The ideal type[39] of public eID provision is a setting in which an eID is issued and administered by organs of a state. The classical example of this model is the role of a state issuing a passport or a citizen card. In this case, a public authority functions as a registration authority and the organ issuing the passport is the "identity provider". This model can, to some extent, be transposed into the Internet context.

The German eID framework serves here as an example of an eID provided and governed by the public sector. In Germany, an eID can be included in the citizen card, which is at the same time an identification document in the off-line context.[40] Thus, one of the eID's functions is to resemble the identification in the off-line world, traditionally based on official documents such as passports. Just like the latter, the German eID could in principle be used both in a governmental context and for all other contexts where identification is needed. However, while anyone can read the physical ID card, not everyone can access the eID stored on it. Relying parties in eBusiness or eGovernment need a specific certificate, called an access certificate, to access the eID on the card. The access certificate also specifies what kinds of information may be communicated, such as the identity holder's address or age. This eID framework does not seem to include any authentication authorities, as the authentication is either directly carried out by the relying party or outsourced to other parties.[41]

The German eID governance framework is primarily of a public sector nature. The use of these eID is governed by the German act on personal identification cards and electronic identification.[42] The card itself is issued by the authorities and produced by the Federal Printing Office "Bundesdruckerei".

It is not apparent that other stakeholders, such as the private sector or end-users, are directly participating in the governance of this eID. However, it is noteworthy that the German constitution was recently amended to introduce a collaborative framework involving both the federal government and the respective state governments (Länder) in the context of IT systems.[43] This was the basis for establishing an IT planning council, which also includes representation from municipalities and the data protection authorities.[44] Thus, there is collaboration between several stakeholders, but only from the public sector. While civil society and business interests are not formally represented, it follows from the strategy of the IT council that the involvement of these stakeholders should be increased.[45] This could become relevant when the IT council will develop an eID strategy in the near future.[46]

7. Private eID provision

There are many examples of eIDs that are issued by the private sector. At the time of writing many companies rely on user-names and passwords that can only be used for internal purposes. Yet there is an

---

[39] An ideal type is an analytical construct that can be used to highlight specific features of real cases.
[40] See, e.g., G. Hornung and A. Roßnagel, "An ID card for the Internet-The new German ID card with 'electronic proof of identity'," *Computer Law & Security Review* 26, no. 2 (2010).
[41] See also Leenes et al., "D.2.2 — Report on Legal Interoperability," 81 et seq. On authentication authorities see further below, Section 9.
[42] Gesetz über Personalausweise und den elektronischen Identitätsnachweis, 18.06.2009.
[43] See Article 91c of the German Constitution (Grundgesetz).
[44] For a general overview of the IT Planning Council see www.it-planungsrat.de (last visited 10 November 2011).
[45] National E-Government Strategy, IT Planning Council decision of 24 September 2010, goal 12, page 12. The strategy is available from the Council's website http://www.it-planungsrat.de (last visited 10 November 2011).
[46] IT Planning Council, decision 2011/18. Interestingly the planning council notes explicitly that the eID strategy should involve the authorities at federal, state and municipal level, but makes no mention of civil society or business users of eID.

increasing use of interoperable private-sector eIDs, such as the option to authenticate a user based on credentials used in social networks like Facebook.[47] The fact that Facebook at the same time relies on eIDs issued under the open standard OpenID[48] illustrates that interoperability of private sector eIDs may go both ways. In other words, the identity provider for one eID may at the same time be a relying party accepting another eID, and both eIDs could be used interchangeably to authenticate users for certain contexts. Of particular interest for the present paper is the possibility to use such private sector eIDs in an eGovernment context.[49]

In addition, in some European countries there is also a market for interoperable private-sector eIDs that offer a high level of security. Such eIDs can be offered, for example, on a smart card, and they may fulfil the security requirements for eGovernment in some countries. Such use raises, of course, specific governance issues related to the authentication phase, which will be further addressed below in Section 9.

8. Public-private eID provision

The third basic type of eID provision is based on different types of public-private partnerships. This approach was chosen for the provision of eIDs in several European countries, including Denmark and Austria. The Danish eID is offered by a public-private partnership based on consortium agreement amongst the collaborating parties and a contract with the end-user.[50]

By comparison, the Austrian eID is based on the Austrian eID act and is provided with significant involvement of the Austrian government as well as the private sector. The details of this collaboration cannot be exhaustively presented here, but a brief and simplified summary may illustrate the essentials.[51] It is perhaps best to describe this collaboration by following the life-cycle of an eID. This starts with the registration phase, where a "certification service provider" is responsible for verifying the citizen's identity as part of the registration procedure. This entity also as requests a digital signature called an "identity link" from the register authority (public sector). While the identity provider is lastly the Austrian register authority, the issuers of the "Citizen Card" can be both private and public parties. Interestingly, the identity provider is consulted only during the issuance of the Citizen Card. During use of a Citizen Card, no identity provider is consulted, because only the identity link is used.

9. Governance of eID interoperability

So far we have focused primarily on the issuance of interoperable eIDs. We should now turn our attention to the governance of eID interoperability itself. The starting point for this is a situation where there is a multiplicity of available eIDs, as well as many potential relying parties. An example is the variety of eIDs currently available in Europe, which potentially could be used in eBusiness and eGovernment across Europe, but which currently cannot be used due to lacking interoperability. This lack of interoperability can have technical, organizational and legal dimensions, and it may to some degree be influenced by relying parties' insufficient knowledge about existing eIDs and lack of trust for ID providers and other parties involved in issuing an eID. This raises the question whether it would be possible to design

---

[47] See Omer Tene, "Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services" in this issue.

[48] See Luke Shepard, "Facebook Supports OpenID for Automatic Login", Developer Blog, May 18, 2009, http://developers.facebook.com/blog/post/246/. OpenID is is a Web registration and single sign-on protocol that lets users register and login to OpenID-enabled websites using their own choice of OpenID identifier. It is offered by the OpenID Foundation, an international non-profit organization. See further www.openid.net.

[49] D. Thibeau and R. Drummond, "Open trust frameworks for open government: Enabling citizen involvement through open identity technologies," in *White paper, OpenID Foudation and Information Card Foudation* (2009).

[50] This eID solution is called "NemID" and its governance by the Danish banking sector and the National IT and Telecom Agency is briefly mentioned in English at https://www.nemid.nu/om_nemid/about_nemid/ and further explained in Danish at https://www.nemid.nu/om_nemid/hvad_er_nemid/parterne_bag_nemid/ (both last visited 10. November 2011). The organizational framework may change in the near future, because the agency will be discontinued by the recently elected Danish government.

[51] For a more detailed account of the Austrian eID framework see Leenes et al., "D.2.2 — Report on Legal Interoperability," 49 et seq.

governance structures that could facilitate the interoperability of otherwise incompatible eIDs. Would it be possible to design a governance framework that could define policies for eID interoperability, perhaps even within a multi-stakeholder framework? Experiences with governance structures for other identifiers as well as existing models for eID interoperability indicate, in my view, that we should not necessarily disregard this possibility.

The basic structure of such a governance framework would imply that an intermediary entity—an authentication authority—facilitates interoperability between different eID providers on the one hand and relying parties on the other hand. This possibility will here be exemplified with the Norwegian eID portal ("ID-porten"). Within the Norwegian eGovernment context, this portal is a key enabler for interoperability of eIDs from the private and the public sectors. This is to say that a range of governmental service providers (i.e., relying parties) can use the ID portal to authenticate[52] their users, who may choose among several available eIDs issued by private-sector and public-sector entities.

In the following I will briefly introduce the portal model as it may be experienced from the perspective of an end-user. This description will omit most of the technical details that are necessary to make the model work and will rather focus on the overall structure and the underlying governance model. A user who wishes to authenticate herself to a governmental service provider (for example, the tax authorities) participating in this scheme may pick one of several pre-selected eIDs. In practice, all inhabitants have access to the official Norwegian government-issued ID called "MyID", and many may in addition hold eIDs issued by the private sector. Once the user chooses an eID, the ID portal handles the authentication and communicates the result of the authentication to the relying party. This is done through an "SAML token"[53] that identifies the user (based on the national identification number) and includes information on the kind of eID used, as well as the assurance level of that eID. The latter is essentially a value between 1 and 4, where level 4 denotes the highest assurance an eID can offer.[54]

The governance framework for the Norwegian ID portal is based on contracts between the portal provider (the Norwegian eGovernment agency "Difi"[55]) and two sets of stakeholders, namely relying parties and eID providers.

First, there is the contractual relationship between Difi and eGovernment service providers—i.e., the relying parties. Any eGovernment service provider (such as the tax authority) wishing to use the ID portal needs to sign a standard "collaboration agreement" with Difi. This agreement not only includes the rights and obligations of the parties, but also lays down a basic governance framework for the eID portal. Overall, the governance of the ID portal is dominated by Difi, who finances the portal, retains the overall control over the portal and holds all rights. However, there are a number of collaborative organs with representation from relying parties. The highest degree of influence is vested on the "Advisory Board", formed by representatives from relying parties (selected by Difi). This board has a central role, *inter alia*, in advising on possible changes to the collaboration agreement. In addition, all relying parties may participate in the "Users Council", an organ that deliberates on issues prior to decisions of the Advisory Board. It should be emphasised that eID providers are not represented on the Users Council, but they can be invited to its meetings. In addition, there are other governance structures, such as the "Forum for Integration and Security" and the "Forum for User Support", and both can be attended by representatives from relying parties. The institutional framework put into place by the collaboration agreement is perhaps the clearest example of a governance model for interoperable eIDs. However, in order to assess the complete picture of this framework, we also need to take into account the roles of eID providers.

A second set of contractual relations exists between Difi and eID providers participating in the portal. These contracts were not available for the research purposes, but from publicly available information it is apparent these contracts were awarded following a request for proposals addressed to several eID

[52] To my knowledge, the current ID portal facilitates authentication only, but it is intended that future versions also will allow for functionality for signature and encryption.
[53] In essence, the ID portal is uses SAML tokens using the Security Assertion Mark-up Language, an XML-based open standard for exchanging authentication and authorization data.
[54] This scale and the criteria for assurance levels regarding authentication and non-repudiation are defined in a an official guideline entitled "Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor: Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett", available at http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli.html?id=505958.
[55] The Agency for Public Management and eGovernment (Difi), www.difi.no (last visited 10 November 2011).

providers. The requirements used to select eID providers seemed to have emphasised both the eIDs' capabilities[56] and their assurance levels (on a scale from 1 to 4, as mentioned above).

Once an eID provider is granted access to the ID portal, the principle of non-discrimination applies. According to this principle, relying parties may not discriminate between eIDs that participate in the portal. In essence, relying parties may thus only select a required assurance level—based on their security needs asserted in a risk assessment—and if an eID provider fulfils these requirements, this eID provider cannot be excluded by that relying party.

10. Concluding remarks

Could this example of an eID portal be used as a blueprint for governing interoperability in Europe and beyond? It may be the case that existing eIDs in Europe are too heterogeneous to be incorporated in a single hub. However, this example illustrates fairly clearly that there are alternatives to creating a single and all-encompassing European eID if one wishes to facilitate interoperability in Europe.[57] Rather than offering European citizens and others yet another eID (for European use), we should consider the alternative of governing authentication processes based on a selection of existing eIDs. Of course, the model raises many new questions, such as who might establish such a portal, and how it should be governed. In my view, a governance framework for a potential European eID portal should go beyond the participative model selected in Norway and also encompass other stakeholders, such as eID providers, other intermediaries and perhaps also end-users and their representations in civil society organizations. Moreover, if the intention is to ensure eID interoperability also for non-governmental actors, the private sector should definitely be incorporated into the governance framework. The advantage of the eID hub model is its potential openness, which could potentially be used to encompass not only European eIDs, but perhaps even allow sufficient flexibility to facilitate interoperability with other non-European eIDs in the future. At the same time it has to be acknowledged that the model also may involve new legal challenges related to, for example, compliance and liability.

References

Borges, G. "Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis: Ein Gutachten für das Bundesministerium des Innern." 2010, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/studie2_npa.pdf?__blob=publicationFile.

Bygrave, L. A., & Bing, J. *Internet governance: Infrastructure and institutions*. Oxford: Oxford University Press, 2009.

Clarke, R. "Identity management." Xamax Consultancy, 2004, http://www.rogerclarke.com/EC/IdMngt-Public.pdf.

Cojocarasu, D. I. "Legal issues regarding WHOIS databases." Oslo: Senter for rettsinformatikk, 2009.

de Andrade, N. N. G. "Towards a European eID regulatory framework. The legal gaps, barriers and challenges of constructing a legal framework for the protection and management of electronic identities." In *European data protection: In good health?*, edited by S. Gutwirth, P. De Hert, R. Leenes and Y. Poullet. Springer, 2012 - forthcoming.

DeNardis, L. *Opening standards: the global politics of interoperability*. The information society series. Cambridge, Mass.: MIT Press, 2011.

Drake, W. J. "Introduction: The distributed architecture of network global governance." In *Governing global electronic networks: international perspectives on policy and power*, edited by William J. Drake and Ernest J. Wilson. Cambridge, Mass.: MIT Press, 2008.

Froomkin, A. M. "Habermas@discourse.net: Toward a critical theory of cyberspace." *Harvard Law Review* 116, no. 3 (2003): 749-873.

Hornung, G., & Roßnagel, A. "An ID card for the Internet-The new German ID card with 'electronic proof of identity'." *Computer Law & Security Review* 26, no. 2 (2010): 151-57.

[56] One applicant—the eID solution of the banking sector, bankID—was not awarded a contract because its eID solution did not facilitate encryption as specified in the requirements.

[57] See Patrick Van Eecke's contribution in this issue.

Leenes, R., Priem, B., van de Wiel, C., & Owczynik, K. "D.2.2 — Report on legal interoperability." Stork eID Consortium, 2009.

Lundevall-Unger, P., & Tranvik, T. "IP addresses–Just a number?" *International Journal of Law and Information Technology* 19, no. 1 (2011): 53.

Mueller, M. *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, Mass.: MIT Press, 2002.

Mueller, M., & Chango, M. "Disrupting global governance: The Internet WHOIS service, ICANN, and privacy." *Journal of Information Technology & Politics* 5, no. 3 (2008/10/27 2008): 303-25.

Myhr, T. "Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution:: or I am 621216-1318, but I am also 161262-43774.1 Do you know who I am?" *Information Security Technical Report* 13, no. 2 (2008): 76-82.

Olsen, T. "Personvernøkende identitetsforvaltning." University of Oslo, 2010.

Olsen, T., & Mahler, T. "Identity management and data protection law: Risk, responsibility and compliance in 'circles of trust'." *Computer Law & Security Report* 23, no. 4+5 (2007): 342-51 & 415-26.

Pfitzmann, A., & Hansen, M. "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management." version v0.34, 2010, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

Riisnæs, R. *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar: en tillitsorientert tilnærming til sertifikatutstederens villedningsansvar*. Bergen: Fagbokforlaget, 2007.

Thibeau, D., & Drummond, R. "Open trust frameworks for open government: enabling citizen involvement through open identity technologies." In *White paper, OpenID Foundation and Information Card Foundation*, 2009, http://openid.net/docs/Open_Trust_Frameworks_for_Govts.pdf.

.* * * * *

Cite as: Mahler, Tobias. Governance Models for Interoperable Electronic Identities. *Journal of International Commercial Law and Technology*, Vol.8 No.2 (April,, 2013)