Privacy in digital identity systems: models, assessment and user adoption

Armen Khatchatourov, Maryline Laurent, Claire Levallois-Barth

Privacy in Digital Identity Systems:
Models, Assessment and User Adoption

Armen Khatchtatourov[1,4], Maryline Laurent[2,4], Claire Levallois-Barth[3,4]

[1]Télécom Ecole de Management, [2]Télécom SudParis, [3]Télécom ParisTech
[4]Chair Values and Policies of Personal Information, Institut Mines-Télécom, Paris, France

armen.khatchtatourov@telecom-em.eu

Abstract. The use of privacy protection measures is of particular importance for existing and upcoming users' digital identities. Thus, the recently adopted EU Regulation on Electronic identification and trust services (eIDAS) explicitly allows the use of pseudonyms in the context of eID systems, without specifying the way they should be implemented. The paper contributes to the discussion on pseudonyms and multiple identities, by (1) providing an original analysis grid that can be applied for privacy evaluation in any eID architecture, and (2) introducing the concept of *eID deployer* allowing to model virtually any case of the relation between the user, the eID implementation and user's digital identities. Based on these inputs, a comparative analysis of four exemplary eID architectures deployed in European countries is conducted. The paper also discusses how sensitive citizens of these countries are to the privacy argument while adopting these systems, and presents the "privacy adoption paradox".

Keywords: eID, eID deployer, pseudonymous authentication, privacy, multiple / partial identities, technology adoption, selective disclosure, privacy adoption paradox, digital identity, privacy by design, personal data, privacy impact assessment, eIDAS, e-Government

1 Introduction

The use of digital or electronic identity (eID) systems is a growing trend in on-line environments, both in public and private sectors. In public sector, the eID ecosystem is believed to be a driver for stronger e-Government adoption by citizens, while private sector (banks, travel companies, etc.) may also be interested in secured solutions strongly linked to the civil identity. In the European Union, a long term strategy has been in place for the last few years, and has resulted in a recent adoption (August 2014) of the Regulation on Electronic identification and trust services (eIDAS) [1]. This text establishes main principles that will guide implementation and use of digital identities in the Member States in the near future. While the scope of the Regulation

concerns public e-services only, the goal is clearly to set a global policy framework to boost the adoption of eID in both public and private sectors.[1]

Basically, an *electronic identity management system* (eIDMS) allows user identification and authentication to on-line services through the use of various authentication means (from login/password to smartcards). Once authenticated, the user is linked to a set of attributes (civil identity, date of birth, address, etc.) and is able to use the service. Today's eIDMS use a various approaches defining technical and organizational architectures for establishing trust relationships between the following entities: users, the Identity Provider (IDP) which is a trusted third party in charge of managing the eID of users, and Services Providers (SPs) which deliver a service to the user [2]. As the cornerstone of that architecture, the IDP has an influential role in privacy handling: it belongs to a continuum where at one extremum the IDP only manages issuance and revocation (e.g. when the eID is declared stolen or lost) and, at the other extremum, it knows all about the users' transactions as it is asked each time to assert user attributes.

In these architectures, different stakeholders (SPs, IDP) manage users' attributes, which are personal data in the sense of Data Protection Directive 95/46/EC [3]. Consequently, the use of eIDMS raises several privacy concerns. It must be emphasized here that the EU legislation deals with the notion of personal data, which is clearly distinguished from the notion of privacy [4]. However, for the sake of simplicity, this paper uses both notions without distinction.

The main privacy concerns are disproportionate data disclosure and user linkability across service providers, which may lead to the knowledge of user's behaviour by third parties, and thus to unwanted behaviour profiling [5]. If the user has to prove to be over 18 years old to access a service, there should be no disproportionate data disclosure of an exact age and/or civil identity for that purpose. If the user accesses an e-health service and a bank service, in principle there should be no possible linking of the two actions, neither by both SPs nor by IDP.

A possible way to cope with such privacy threats is to implement two measures. The first one is pseudonymous authentication which basically refers to the use of one or many pseudonyms, not unequivocally associated to the civil identity, for identification and authentication to on-line services. Only the issuing authority (IDP) has the knowledge of this association and may reveal it for legal grounds (e.g. fraud). The second one is user controlled selective attributes disclosure, which is usually implemented as a checkbox allowing the user to select which attributes are disclosed to a particular SP. Both effectiveness and user's perception of privacy protection may be quite different depending on design choices about how the pseudonymous authentication and the data flows between the different stakeholders are designed.

These privacy protection principles are recalled in the aforementioned eIDAS Regulation under Art. 5 which states that (1) processing of personal data shall be carried out in accordance with Directive 95/46/EC (that is respecting among other prin-

[1] We use the term *digital identity* in a broad sense relevant for all on-line transactions, and the term *eID* when the context is particularly relevant to the eIDAS Regulation. The findings of this paper are relevant for both cases.

ciples that the data disclosed are "adequate, relevant and not excessive in relation to the purposes for which the data are collected and/or further processed") and that (2) "the use of pseudonyms in electronic transaction shall not be prohibited". The Regulation however does not specify the way these principles should be implemented, nor does it take into account the eIDMS already deployed in several Member States. However, according to the design choices made by Member States, these eIDMS lead to different privacy protection levels.

The goal of this paper is to provide a comprehensive analysis of eIDMS architectures with regard to the data protection criteria, and to generalize into an analysis grid for privacy evaluation of any existing or future eIDMS. The paper is organized as follows. Section 2 highlights the methodology of the comparative analysis and introduces the analysis grid. Section 3 motivates the selection of the four European States and provides a brief description of their eIDMS. Section 4 introduces the models of the relation between the user, the eID implementation and user's digital identities, develops the analysis grid and applies it to four European countries to describe the efficiency of privacy protection. Finally, Section 5 addresses two open questions. First, as the privacy concerns seem to grow among the population, it could be expected that more privacy preserving eIDMS would get larger user adoption. However, we underline that, as of today, there is no strong evidence of such correlation. Second, we identify some of the key factors (namely the number of services available for the user and the perceived privacy) that may influence the user adoption of eIDMS.

2 Methodology

To conduct the comparative analysis, we adopt a particular methodology, articulated around three points.

First, the paper aims to propose a relevant level of description of privacy protection measures, mainly related to pseudonymity. The literature often provides either too high-level description in terms of models of trust [6,7], or too detailed technical description in terms of data flows. While both are necessary in their own contexts, we are looking for an approach able to catch at the same time the functional relations between parties, and relevant aspects of actual, existing systems, while not being lost with low-level details. We believe that such a "big picture" can benefit to the discussion in the context where people from different viewpoints (engineers, policy makers, service providers, lawyers, civil society) are brought to discuss these important issues.

Second, our analysis considers only already deployed architectures, and not well-known theoretical models (such as central, federated or user-centric), nor EU research and development projects. Indeed, existing systems are known to exhibit notable differences with theoretical models. For example, Austrian eID architecture is a complex mixture of central, federated and user-centric models [8]. Similarly, German eID does not fit to any of existing theoretical models or "pure" architectures such as SAML, OAuth, etc, and to their privacy characteristics such as described in [9]. We wish our analysis to be very much practical and realistic.

Third, we identify three interrelated design axes (illustrated **Fig. 1**) that help evaluating the privacy protection level in a real system. Axis 1 concerns the relation between eID carriers, *eID deployers* (the concept we introduce on this occasion, see Section 4 for details) and multiple pseudonyms; we also mention public policy on multiple pseudonyms and user initiative related to the presence of pseudonymous authentication. Axis 2 deals with the management of user attributes. Axis 3 concerns the way the authentication scheme and the functional relations between parties are implemented. The 3 axes are interrelated from the privacy protection point of view, and the inter-axis analysis is provided in sub-section 4.4, leading to a full analysis grid applicable to any country.

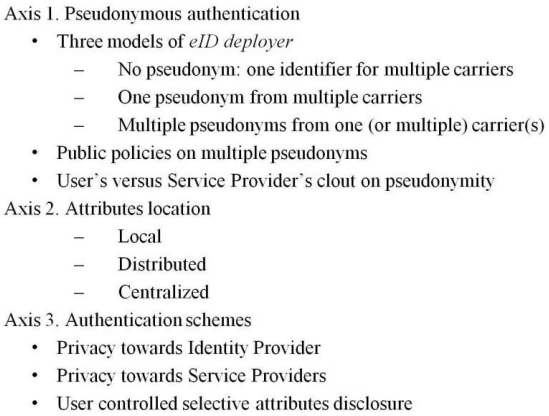

Fig. 1. Analysis grid. Bullet items are sub-axes, dash items are design options (if relevant).

3 Choice of countries

For the purposes of our analysis, we identified four countries. While small, this sample is rather representative of the diversity of solutions: from a basic non pseudonymized solution to complex privacy protection oriented ones. All the systems offer electronic authentication and electronic signature (this feature is not directly addressed here). The available service providers cover a large range of public (e-Government, social security) and private (banking, insurance, travel) services.

Estonian eID. Launched as early as 2002 and often described as a success story, the Estonian eID can be supported by various carriers (chip card, mobile) and allows the user to authenticate to on-line services. The main compulsory eID card serves also as National ID document in off-line identification. The user is identified by a unique Personal Identification Code, considered as non-confidential in Estonia and based on Population Register. The main privacy protection mechanism is related to the management of user's attributes [10,11].

Austrian Citizen Card (CC). Massively rolled-out since 2006, Austrian eID is a flexible approach based on particular technology called Citizen Card concept (CC). The eID can be supported by various carriers such as mobile phone or chip cards (e.g. Social Security e-card). The CC and its carriers are not National ID documents, but are the official eID. As in Estonia, there is a central database called Central Residents Register. However, the Austrian legislation prohibits the use of these identifiers by service providers. The main privacy protecting mechanism is the use of sector-specific pseudonymous authentication [12,13].

German eID. Launched in 2010, German credit-card format carrier fulfils two functions: eID, and machine-readable travel document and National Identity card (or "nPA" which stands for "neue Personalausweis, i.e. new passport). Here, national legislation does not allow central database of identifiers. The main privacy preserving mechanisms are: pseudonymous authentication, user controlled disclosure of attributes, no knowledge of user's activities by IDP, and mutual authentication between the user and the SP (the SP's validity is systematically verified) [14,15,16].

SuisseID. Launched in 2010 as mostly private-sector initiative, SuisseID is used only for on-line authentication, and is not an ID document. Different form-factors (smartcard, usb-stick and mobile) are available. The privacy protection mechanisms are optional pseudonymous authentication and selective disclosure [17,18].

4 Analysis grid and its application to eID management systems

In this section, several design choices for privacy protection in the four selected countries are described following the analysis grid illustrated in **Fig. 1**. In the following, we use the terms identifier (when unequivocally linked to civil identity) and pseudonym (when not) to refer to the way a Service Provider (SP) identifies the user. The same user may be represented by different pseudonyms for different SPs.

4.1 The *eID deployer* concept

To model virtually any case of the relation between the user, the eID implementation and user's digital identities (pseudonymized or not), we introduce here the concept of *eID deployer*. Namely, the digital identities are deployed by the *eID deployer* which is an abstract functionality to establish the link between the physical form-factor of the authentication mean (called *carrier*) and the identifier or pseudonym. Several *carriers* may instantiate the same *eID deployer* if they fulfill the same function and disclose the same identifier/pseudonym and/or attributes. For example, two *carriers* belonging to the same user (e. g. a smartcard and a smartphone) may deploy the same *pseudonym* or a set of *pseudonyms* representing this user. Alternatively, the user can possess several carriers, each of which deploying its own eID, i.e. its own identifier or pseudonym. That is, multiple pseudonyms can be achieved in two manners: either by generating one pseudonym by *eID deployer* and providing the user with many *eID de-*

ployers, or by generating multiple pseudonyms from one *eID deployer*. From the user's point of view, this mechanism allows to manage partial [19,20] digital identities in the sense that user's actions in one usage context are not known in the other one (the user is cross-domain unlinkable).

In the rest of this section, we analyze the level of privacy protection according to 3 design axis: pseudonymous authentication, attributes' location, and authentication schemes.

4.2 Pseudonymous authentication

Three models of eID deployer. This sub-section describes the three models relative to the *eID deployer* implementation.

No pseudonym: one identifier from multiple carriers. There can be no pseudonymity, in which case the user is always identified with a unique identifier unequivocally linked to the civil identity (typically, the unique citizen identification number from population register). It must be noted that in this case, because of the static nature of the link between unique identifier and civil identity, the latter can be regarded as a part of the former, and not as a distinct attribute. The *eID deployer*'s function is simply to disclose the same identifier to different SPs. This is the case in Estonian eID where civil identity (i.e. name and date of birth) and unique identifier are stored directly in the electronic certificate and disclosed at each authentication session. In Estonia, the *eID deployer* is implemented on several carriers: mandatory National ID with eID based on smartcard, optional DigiID based on smartcard and which allows the same actions as the main eID without being a National ID document, and optional smartphone based Mobile-ID. In digital environments, all theses *carriers* act in the same manner and fulfill the same function to uniquely represent the user.

One pseudonym from multiple carriers. The simplest way to implement pseudonymity is to envisage an *eID deployer* which discloses one pseudonym instead of civil identity. In this case, the civil identity is known only by the eID issuing authority (IDP). The SP knows the user only as the pseudonym, and if civil identity is disclosed to the SP, it is an attribute of the pseudonym. Again, there can be multiple carriers on which the same *eID deployer* is implemented, disclosing the same pseudonym. This approach is implemented in SuisseID, where the user can purchase a smartcard based or usb-stick based carrier, and can opt for a complementary mobile phone based carrier, all deploying the same eID. With this solution, if the user wishes to use multiple pseudonyms, he has to purchase as many carriers with corresponding eID deployers as the number of pseudonyms he wishes. Typically, one may want to have a non-pseudonymized eID and one or several pseudonymized eID for different usage contexts (see below the sub-section *User's versus Service Provider's clout on pseudonymous authentication* for details).

Multiple pseudonyms from one (or multiple) carrier(s). A more sophisticated mechanism is used in Austria and Germany. The *eID deployer* can generate software de-

fined sector-specific pseudonyms, each of which is used in corresponding sector. In Austria for example, there are 26 distinct sectors, from social security to banking. It seems that there is no technical difficulty to increase the granularity from sectors- to service-specific pseudonyms. The SP identifies the user only as the pseudonym specific to the sector so that no cross-sector linkability is possible. In this approach, there is no "root" pseudonym or identifier. Indeed, German legislation prohibits central registry of citizen and unique identification numbers in general. Austrian eID system does rely on the Central Registry of Residents (CRR), but there are additional one-way hash mechanisms implemented at two stages: first to prevent to track back from sector-specific pseudonym to the sourcePIN stored in a separate container on the eID carrier, and second to prevent to track farther back from sourcePIN to the CRR. Here also, all the *carriers* (social security smartcard, bank smartcard, mobile phone, etc.) represent the same *eID deployer*, because all *carriers* fulfill the same functional role to generate sector-specific pseudonyms in the same manner. In Austria, it is not possible to hold more than one *eID deployer*: whatever the carrier is, the same user will be represented by the same pseudonym in the same sector. In Germany, only one carrier and thus one *eID deployer* is allowed for the moment which is a smartcard combining eID, national ID and machine readable travel document. There are however plans to implement mobile *carriers* as well, as in Austria.

The three models are depicted **Fig. 2**

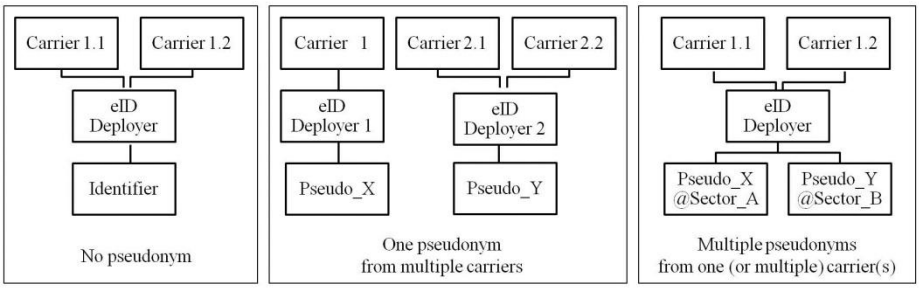

Fig. 2. Three models of *eID deployer*, implemented in Estonian eID; SuisseID; Austrian Citizen Card and German eID respectively (from left to right).

Public policies on multiple pseudonyms. Different States present different public policies with regard to the use of multiple pseudonyms and to the enrolment procedure. It is interesting to note that the strength of enrolment is not directly related to the presence of pseudonymity. Estonia and Germany exhibit rather strict procedures involving the Ministry of Interior, while they do have opposite policies as to the use of pseudonyms. Austria and especially Switzerland have lighter procedures, with possibly remote activation, via Internet or post.

This can be explained by the fact that policy strategies are based not on the presence of pseudonyms per se, but on the articulation between the national ID document and the *eID deployer*. Indeed, in countries with strictest enrolment procedures where at least one of the carriers fulfils the traditional physical identity card purpose, only

one *eID deployer* is allowed. In countries with lightest enrolment procedure where there is no direct link with the traditional ID purpose (SuisseID), there are no restrictions on the number of *eID deployers*. Austria falls in between: while not being a National ID, the eID is official for on-line transactions; thus, multiple *eID deployers* are not allowed.

User's versus Service Provider's clout on pseudonymity. When pseudonymity is implemented, the user may be granted or not the initiative of its use. The pseudonymity can be called automatic when all authentications make use of pseudonym, as in Germany and Austria, and user-defined when the user has the initiative to use or not the pseudonym, as with SuisseID. In the particular case of SuisseID however, for unknown reasons, it is not possible to have both pseudonym and real name in the *eID deployer* so that the user's choice at issuance is definitive.

It has to be noted however that whatever the design choice is, specific SP such as tax office may require to disclose civil identity. In automatic pseudonymisation this situation may be handled by eID deployer and does not prevent the use of the service. In user-defined pseudonymisation, at least in the particular case of SuisseID, this may prevent the use of service if the pseudonymisation has been chosen at issuance. In other words, the SP may have the last word on the use of pseudonyms, possibly by preventing the use of the service.

4.3 Location of user's attributes

While pseudonymous authentication is certainly the main factor to preserve user's privacy, the way the eIDMS manages users' attributes that are personal data from the legal point of view, has a significant influence as well. The scope of this sub-section is limited to the attributes at issuance (those stored on the carrier and those known by IDP) and does not include dynamic attributes collected by particular SP during online transactions which may be used for profiling. We distinguish three situations.

Localized attributes. This first extremum depicts the case when the attributes such as personal address (i. e. data other than those strictly necessary for authentication) are stored locally on the carrier, and are not continuously stored by IDP or SP, thus reducing the degree to which personal data can be accessed by third parties. This scheme is implemented in German eID where the carrier bears attributes such as family and given names; artistic name and doctoral degree; date and place of birth; address and community ID; expiration date and optional fingerprints.

Distributed attributes. The opposite option is to store only minimum attributes on the carrier itself (e.g. name, date of birth and nationality). In this case, the different SPs manage the attributes relative to their services, such as the personal address for example. This option has certain advantages: the IDP does not have any additional information about user's attributes, and a given SP normally cannot access attributes stored by other SPs. This option is implemented in Estonian eID. Here however, these ad-

vantages are enforced by legal requirements only, as the use of unique personal identifier across public and private SPs makes the cross-service correlation of attributes technically possible. In Austrian Citizen Card, few attributes are present in the eID deployer (namely name and date of birth).

Centralized attributes. In this intermediate option, the *eID deployer* itself contains fewer personal data than the set managed by the issuing IDP. The role of IDP is complex as it deals both with the knowledge of attributes themselves, and with their assertion and disclosure to the SP: in some cases, IDP could disclose all attributes that it stores, while in other cases only a sub-set of attributes. The centralized design option is implemented in SuisseID, where the only mandatory attributes on the carrier are the SuisseID number and the name or the pseudonym. However, despite this minimal mandatory design, SuisseID carrier can also carry optional attributes, such as affiliation, e-mail, etc., if the user decides so. In addition, SuisseID introduces "auxiliary identity providers" distinct from the IDP involved into the issuing of SuisseID. They are similar to what is classically called Attribute Providers: while the main IDP manages only basic personal data, these providers manage extended attributes (e.g. professional data such as lawyer, moral person, etc.). There can be an arbitrary number of Attribute Providers, allowing further development of the usages. The design decisions implemented in SuisseID confer a central role to the IDP and to Attribute Providers and require a great amount of trust in them.[2]

4.4 Authentication schemes

The authentication scheme determines the roles of IDP and SPs, and the attributes' flow between them during the authentication. Also, in relation to the scheme, an eventual user controlled selective attributes disclosure can be implemented, which is typically done via a dashboard or a checkbox. In the following, we describe 4 schemes of high-level functional relations (and not the low-level data flow) between the parties.

Offline scheme (A). In this scheme, illustrated **Fig. 3**, the IDP is normally not aware of the flow of user attributes which are managed directly by SPs. After the enrolment, IDP manages only revocation lists and verification of card's status by SPs. Along with distributed attributes management described above, this scheme is intended to prevent establishing a central data holder. However, when implemented together with unique identifier, it does not prevent cross-SP linkability.

In the particular case of Estonia, where this scheme is implemented, the user has no a priori control on attributes' management. This lack is partially compensated by a posteriori user access, as there are legal dispositions allowing the user to monitor

[2] Note that the 4 countries studied here have actually limited differences on *location* criterion: the most localized solutions add only address, age, doctoral degree and optional fingerprints (Germany) to the basic set present on the most distributed ones. However, other countries or future eIDMS could give a different picture, by including attributes such as tax number or profession. This is why we think it is important to include this criterion in the discussion.

which attributes are accessed or stored by each SP. However, it is unclear to which extent this obligation is respected, and several reports[3] [21] and users' comments [22] seem to doubt about the system's transparency.

Federation without user control (B). In the scheme illustrated **Fig. 4**, implemented in Austrian Citizen Card, the federal IDP plays a central role. This scheme requires that SP sends an authentication request to IDP in a systematic manner.

As already mentioned, the ²wards SPs is guaranteed by the use of sector specific pseudonyms generated by IDP. There is no selective disclosure, and it seems that the personal data transmitted to SPs may on some occasions contain more than strictly needed for the authentication (e.g. the name and the date of birth) [23]. The privacy towards IDP is not ensured as IDP knows all the services accessed by the user. Overall, this scheme requires high level of trust into the IDP.

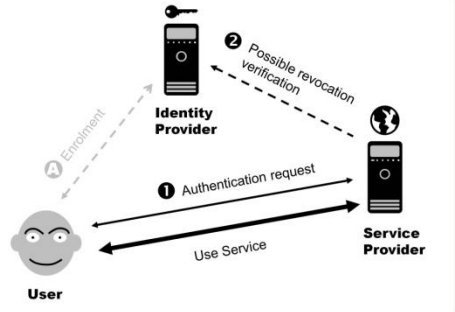

Fig. 3. Off-line (A)

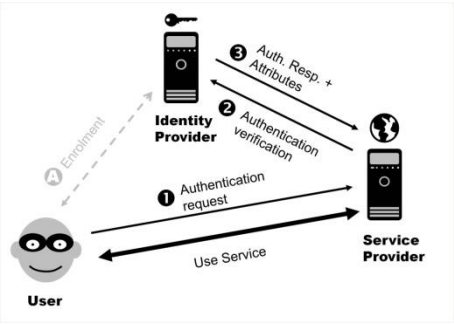

Fig. 4. :Federation without user control (B)

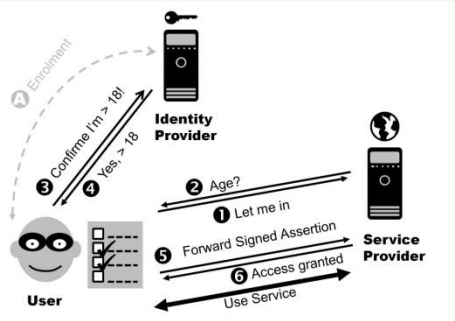

Fig. 5. Federation with user control (C)

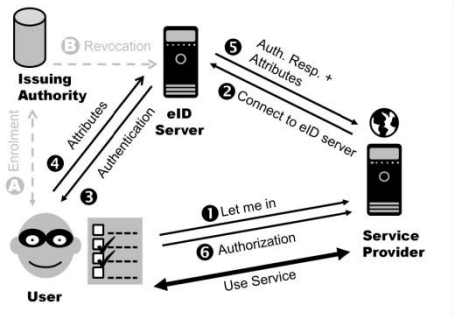

Fig. 6. Mediation with user control (D)

[3] The Estonian Data Protection Inspectorate Annual Report 2012 mentions that (i) misuse of the Population Register is the most common reason of misdemeanor proceedings (30 of 43 completed proceedings); (ii) only 2 of 66 companies monitored were publishing private debt data on their websites in full compliance with the Estonian Personal Data Protection Act.

Federation with user control (C). The scheme illustrated **Fig. 5** is implemented in SuisseID. This scheme is guided mainly by the wish to allow more user control. To enable this, all authentication requests are redirected to the user which controls, via a checkbox-style interface, which attributes he agrees to disclose to the SP.

To guarantee the privacy towards SPs, both basic and extended attributes follow this selective disclosure procedure. As multiple *eID deployers* are allowed, when the same user has several (pseudonymized) SuisseID, the linking across SPs is more difficult. As for the privacy towards IDP, the IDP still holds a central role and is able to link the identifier and pseudonyms across different SPs that the user access to.

Mediation with user control (D). The last scheme illustrated **Fig. 6**, implemented in Germany, is guided by extended security and privacy requirements. Mutual authentication between the user and the SP is used to provide access control, so that only authorized, white-listed SPs can access to the user attributes. To this end, an additional element called eID Server is implemented at the SP side to support communications with the eID client. The eID Server regularly receives, from the authorization certificates authority, updated authorization certificates for the SPs and revocation lists for eID cards. The role of eID Server is quite different from the IDP's in its classical acceptance as it is not a centralized federation operator. The SP can develop its own eID Server according to publically available specification. Alternatively, 4 eID servers are certified by the German Federal Office for Information Security and made available for SPs to establish connection to.

Once the connection between the eID deployer and the SP is established through the eID Server, the attribute disclosure is controlled by the user via a checkbox.

To avoid that SPs uniquely identifies the user, an additional mechanism is implemented. The same authentication key is placed on a batch of carriers belonging to different users. Thus, the SP knows only that it is communicating to an authentic *eID deployer* but ignores to which one amongst the batch.

4.5 Interdependencies between design axes

We can now draw conclusions on the design interdependencies between the 3 design axes we are interested in, which are pseudonymity, attributes location and authentication schemes. Three main aspects are addressed here: privacy towards IDP (knowledge of user's actions and attributes), privacy towards SPs (cross-SP linkability of the identifier or pseudonym, and cross-SP linkability of attributes) and selective attributes disclosure to SPs.

In both cases of *No pseudonym* and *One pseudonym*, there is no a priori necessity to grant a central role to the IDP.

In *No pseudonym* design option, most of the time, the IDP is not informed about user's transactions and attributes. The IDP is informed only when the SP needs to check revocation state of a certificate, as it can be seen in the authentication scheme (A). Distributed attributes is a possible way to achieve some privacy protection against cross-SP attributes linkability, even if cross-SP identifier linkability is not addressed, as in Estonian eID. As few attributes are present on the *eID deployer*, there

is little interest to implement selective disclosure of attributes, although it could be technically possible.

In *One pseudonym* approach such a global scheme could also be implemented. However, if additional Attribute Providers are envisaged, the IDP and Attribute Providers are playing a more central role, both in terms of knowledge of centralized attributes and their assertion to SPs. To partially prevent excessive knowledge of attributes by SPs and thus cross-SP attributes linkability, the selective disclosure can be implemented. The simplest and "natural" way is to handle it at the level of IDP which asserts user attributes at each transaction, as illustrated by the authentication scheme (C). These measures, implemented in SuisseID, do not address cross-SP linkability of the pseudonym (unless the user has many *eID deployers*), neither the knowledge of user's actions by IDP.

In *Multiple pseudonyms*, the main gain is the absence of cross-sector or cross-SP linkability. The simplest way to achieve it is to involve the IDP as the trusted third party in pseudonyms' generation and confirmation to SPs, as illustrated by authentication scheme (B). The obvious drawback is that IDP may gain central role. Intrinsically, IDP's knowledge of services visited by the user is difficult to avoid in this authentication scheme. To limit at least the knowledge of users' attributes by IDP, *distributed* approach to attributes management can be implemented as a complementary measure, as in Austrian eID.

To mitigate theses issues and to preserve privacy against both IDP and SPs simultaneously, a much more complex global scheme is needed. Along with already discussed selective disclosure, two additional steps can be performed: the batching of authentication keys so that SP cannot attribute a unique identifier to or even track the user, and direct connection between the user and SP, so that no central IDP knows which service is visited by the user. Altogether, these design decisions implemented in German eID, give more technical complexity (in terms of interconnections) but allow strong privacy protection.

To conclude, from strictly technical point of view, German eID solution offers the best level of privacy protection, at the price of relatively complex and expensive architecture. SuisseID offers an elegant and flexible solution with reasonable technical com-plexity and cost, but does not address the IDP knowledge of user's activities.

5 Do privacy protection measures influence the adoption rate?

One could suppose that better privacy protecting solutions will get larger adoption by the public. In the present section, we put the levels of privacy protection described above into correspondence with the effective use of the eID systems by target populations, and analyze some of the factors that may influence the adoption rate.

5.1 Privacy adoption paradox

To assess the extent of usage, different parameters can be taken into account: the number of services available to eID authentication, the roll-out, and the usage rate (i.e. percentage of population which effectively use the eID services). We believe that

only the last parameter is suitable to assess the real adoption rate. Indeed, the roll-out rate and to a lesser extent the number of available services may result from a voluntaristic policy without triggering the real usage by the population.

One methodological problem is that it is difficult to compare different eID solutions at a given point of time because they have different age. To compensate this, we will compare the usage rate with respect to the number of years of existence. The fact that social and technical context pushes users to adopt digital solutions in 2013 faster than in 2002 cannot be taken into account with the publically available data. Another limitation is that data sources use different procedure: for Germany and Austria the evaluation is based on a representative sample, for Estonia on estimation by involved actors, for Switzerland on sales and estimations (see the footnote below). Finally, it should be emphasized that extensive, correct and yearly updated data on the subject is extremely difficult to find, probably because of their sensible political nature.

The **Table 1** shows the roll-out and usage rates (as of 2013 for Estonia and Switzerland, as of 2014 for Germany and Austria). The **Fig. 7** shows graphical representation by country and outlines the rate of adoption which is the relative speed with which the innovation is adopted. More complete data set could determine if indeed all the countries follow the same logistic s-curve [24,25] which is classically used to study the rate of adoption.

Table 1. Roll-out and usage rate

	Nb years old	Roll-out	Usage rate
Estonia [26,27] [4]	11	98% (compulsory)	37%
Austria [28,29]	8	21% (opt- in)	21%
Germany [29]	4	10,5% (opt-in)	10,5%
Switzerland [30,31] [5]	3	5,2% (opt-in)	5,2%

[4] [26] estimates the usage rate at 40%, and [27] at 37% (at least once usage occurrence in last 12 months). The middle point at year 6 is from an official presentation of Estonian executives at that time.

[5] In 2010, the number of SuisseID sold equals to 4,2% of Switzerland's active population. There is no reliable data on the 2nd and 3rd years but + 0,5% per year seems a reasonable conservative estimation. Besides, in 2013, 6% of business representatives use the SuisseID for professional purposes, and 3% of them use it for personal purposes as well. These figures indicate that SuisseID usage is driven by professional context.

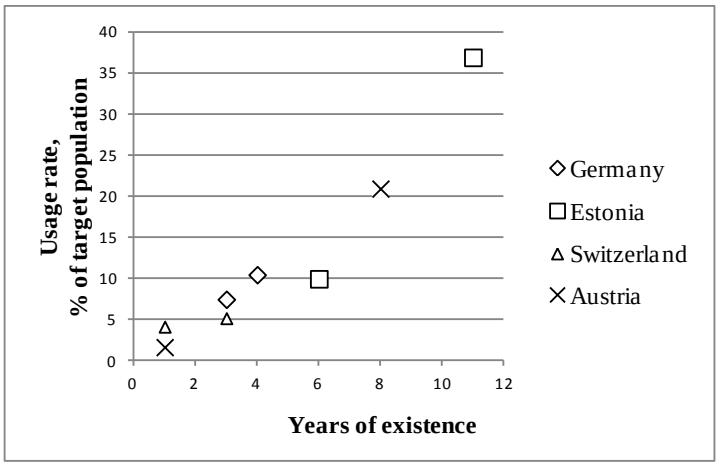

Fig. 7. Rate of adoption in 4 countries

As the data suggest, we assist to what could be called "privacy adoption paradox": there is no evidence that higher level of privacy protection leads to higher rate of adoption. It can then be hypothesized that the advantages offered by extended privacy protection solutions do not trigger an a priori increase in the rate of adoption, or are counterbalanced by other factors. The fact that the eID functionality follows an opt-out strategy (in Estonia, all the compulsory eID cards are delivered as active) or an opt-in strategy (in the other countries, the holder has to activate the eID functionality) does not seem to have a decisive influence on the adoption rate. These questions are discussed in the next sub-section.

5.2 Factors of low adoption rate

A large number of factors influence the adoption of eID solutions; for example, [32] identifies no less than 20 of them. We will limit the discussion to two factors in the context of the most privacy protecting solution identified in the previous sections, the German eID. What may limit the adoption in the case where the eIDMS objectively offers a good level of privacy protection?

Lack of applications. One factor could be the lack of useful applications limiting the adoption by users. This issue is usually presented as a classic chicken-and-egg problem [15]. The take-off can only be envisaged if a sufficient number of services are offered to the user. On the side of SPs, the incentives to offer such services are however limited by the lack of users and thus by the lack of return on investment. No pull out of the hat solution seems to be present in the countries studied here as well as in others.

Let's analyze the German example in this light. On one side, the available figures show that, as of 2013, there are 147 (40% public and 60% private) services supporting

eID authentication [33], which could cover a large scope of everyday usages; thus the lack of applications does not seem to be the main limiting factor.

On the other side, there is indeed certain general reluctance of private SPs to develop such eID-supporting services, especially when existing solutions (e.g. bank authentications) already fulfill their purpose [33]. Moreover, as of 2012, only 7% of service providers do offer privacy-preserving functionality or intend to. The remaining 93% do require full and true civil identity, while many of them do not belong to sectors where civil identity is required (e. g. banks) [34]. This reflects the specific reluctance of private SPs to offer privacy-preserving functionality.

While this specific reluctance should be addressed at the level of SPs, it is not sure that usage rate is solely limited by this issue, in particular because users' awareness on pseudonymisation is quite low as it will be shown below. We think that a broader question here is the way the articulation between e-Government and private sector is thought of. Usually, and this seems to be the rationale behind the eIDAS Regulation, the eID-supporting public services are considered as a trigger for wider user adoption of private SPs. The underlying hypothesis is that the same eID, possibly pseudonymized, will be used across all the sectors and services. The question is however, does the user want to use the same eID in such different contexts? To take a historic parallel in pre-digital age, does the user want to use the same key to gain access to his home, to his car and to his workplace? The answer is not that obvious as it may seem, and brings us to the user perception which may limit the eID adoption.

Perceived privacy. The notion of perceived privacy refers to the way the users foresee the outcome of their actions, and encompasses different factors such as trust in the technical system and organizations, reluctance to personal data disclosure, etc. A growing body of literature addresses several counter-intuitive aspects such as "control paradox" (more control over the publication of one's own personal data increases individual's willingness to publish it and decreases privacy concerns) [35] and "reverse privacy paradox" (lower privacy concerns are combined with a greater use of protection strategies) [36]. These empirical results are always different across countries and age-groups. [37]

The point here is that the perceived privacy has little to do with objective characteristics of an eIDMS. For example, [34] reports that in Germany there is a clear influence of the official nature (Identity Card) of the eID on the usage rate. Participants to this study have doubts about using an official and highly personal document to play around on the Internet, and see a "possible contradiction between being pseudonymously authenticated while using an ID card with their photo on it." Moreover, when the pseudonymous authentication mechanisms are explained, they are quickly forgotten or judged not enough usable in the light of the abovementioned issues.

That is, the usage rate of German eID depends not only on the presence of pseudonymity as available feature, but also on user's perception of the system and reluctance to use the same *eID deployer* in different contexts. While people make little use of systems with poor privacy protection, the systems with good privacy protection, even when explained to citizens, does not necessarily trigger significantly higher adoption rate if perceived privacy is low.

In this respect, an approach based on separate *eID deployers*, with distinct enrolments for each type of use (e.g. for e-Government and for e-Commerce), could be an interesting solution, allowing to dissociate usage contexts from the user's point of view. Such could be the case if multiple *eID deployers* were allowed as with SuisseID. For example, there may be a way to authorize multiple *eID deployers* in the German eID infrastructure, modulo appropriate legal dispositions for lighter enrolment depending on usage contexts. This last consideration brings us to State's global policy guiding the degree to which the civil identity is linked to electronic authentication means. This question should be taken into account in future research.

6 Conclusion

In this paper, we developed the methodology and the grid of analysis of privacy protection in existing eIDMS, allowing to analyze past and future design decisions. We introduced the concept of eID deployer and provided models for multiple digital identities.

The important structural differences in privacy protection can influence users' predisposition to adopt better solutions in everyday usages. To verify if this is the case, we compared the rate of adoption in four European countries. Paradoxically, there is no evidence for significant influence of privacy preserving characteristics on the rate of adoption of eIDMS, in the countries we studied. We discussed then the factors that may counterbalance an eventual advantage of privacy protecting solutions and limit the rate of adoption. Among those factors, perceived privacy seems of particular importance.

This analysis is of particular interest in the recent context where national legislations reinforce personal data protection measures, both at the European (with the forthcoming General Data Protection Regulation [38]) and at the international level.

Acknowledgement of Funding. This research was partially financed under the sponsorship program *Chair Values and Policies of Personal Informations, Institut Mines-Télécom, France* (www.informations-personnelles.org). The views expressed herein are those of the authors and are not necessarily those of the Funders.

7 References

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal L 257 Vol. 57, 28/08/2014, p.73-115.
2. Laurent, M., and Bouzefrane, S. (eds) 2015, *Digital identity management*, ISTE Press
3. 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. Official Journal L 281, 23/11/1995, p. 0031 - 0050.

4. Levallois-Barth, C. 2014. *Legal Challenges Facing Global Privacy Governance*, in Dartiguepeyrou, C. (ed.) The futures of privacy, Fondation Télécom, Paris. ISBN 978-2-915618-25-9
5. Opinion of the European Data Protection Supervisor on the Commission proposal for a Regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market, 2012. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-09-27_Electronic_Trust_Services_EN.pdf
6. Jøsang, A. Fabre, J., Hay, B., Dalziel J., and Pope, S., 2005. Trust Requirements in Identity Management. *Proceedings of the Australasian Information Security Workshop (AISW'05)*, Newcastle, Australia.
7. Benantar, M. (ed), 2006. *Access Control Systems: Security, Identity Management and Trust Models*, Springer.
8. Strauß, S., and Aichholzer, G., 2010. National Electronic Identity Management: The Challenge of a citizen-centric Approach beyond Technical Design, *International Journal on Ad-vances in Intelligent Systems*, vol 3 no 1 & 2, 2010
9. Corella, F., and Lewison, K., 2013. Privacy Postures of Authentication Technologies. *The Internet Identity Workshop (IIW)*, Mountain View, CA.
10. Martens, T., 2010. Electronic identity management in Estonia between market and state governance, in *Identity in the Information Society*, Springer 2010 3(1), 213-233.
11. AS Sertifitseerimiskeskus. The Estonian ID Card and Digital Signature Concept http://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf Accessed October 2014.
12. Leitold H., Hollosi A., and Posch R. 2000. Security Architecture of the Austrian Citizen Card Concept, in *Proceedings of ACSAC'2002*, ISBN 0-7695-1828-1, pp. 391-400.
13. Federal Act on Electronic Signatures 2001 (Signature law), *Austrian Federal Law Gazette*, part I, Nr. 190/1999, 137/2000, 32/2001
14. BSI 2014. Technical Guidelines eID-Server. Part 1: Functional Specification, BSI. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part1_pdf.pdf?__blob=publicationFile
15. Poller, A.; Waldmann, U.; Vowe, S.; Turpe, S., 2012. Electronic Identity Cards for User Authentication - Promise and Practice, *Security & Privacy, IEEE* , vol.10, no.1, pp.46,54, Jan.-Feb. 2012 doi: 10.1109/MSP.2011.148
16. BSI, 2010 Innovations for an eID Architecture in Germany. Accessed October 2014. http://www.personalausweisportal.de/SharedDocs/Downloads/EN/Flyers-and-Brochures/Broschuere_BSI_innovations_eID_architecture.pdf?__blob=publicationFile
17. Hemmer, P. 2010. *La SuisseID, qu'est-ce que c'est?* http://www.ari-web.ch/docs/ARI_2010_06_18_SUISSE_ID_020_PROJET_EXPOSE.pdf Accessed October 2014.
18. Doujak, M (ed.) 2011. SuisseID specification, eCH-0113 http://www.suisseid.ch/endkunden/suisseid/news/update_spezifikationen/
19. Pfitzmann, A., and Hansen M., 2010. *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management.* TU Dresden. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.
20. International Standard, Information technology - Security techniques - Privacy framework, ISO/IEC29100, First edition, December 2011
21. The Estonian Data Protection Inspectorate Annual Report 2012.

22. https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/#comment-3776 Accessed October 2014
23. Slamanig, D., Stranacher, K., and Zwattendorfer, B., 2014. User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure, *SACMAT '14 Proceedings of the 19th ACM symposium on Access control models and technologies*, ACM.
24. Rogers, E., *Diffusion of innovations*, 2003, Simon and Schuster.
25. Hühnlein, D., Roßnagel, H., and Zibuschka, J. 2010. Diffusion of Federated Identity Management, in Freiling, F.C., (ed) *Sicherheit*. Bonn: Köllen Druck + Verlag GmbH, pp. 25–36
26. GSMA 2013, Estonia's Mobile-ID: Driving Today's e-Services Economy. http://www.gsma.com/personaldata/wp-content/uploads/2013/07/GSMA-Mobile-Identity_Estonia_Case_Study_June-2013.pdf ; Accessed October 2014.
27. Estonian Ministry of Economic Affairs and Communications, 2014. *Digital agenda 2020 for Estonia* (source: AS Sertifitseerimiskeskus) http://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf Accessed October 2014
28. eID Interoperability for PEGS: Austrian country profile, 2009. IDABC - European eGouvernement Services, http://ec.europa.eu/idabc/en/document/6484.html Accessed October 2014.
29. Institute for Public Information Management 2014, eGovernment Monitor 2014, http://www.initiatived21.de/wp-content/uploads/2014/09/eGovMon2014_web.pdf
30. Newsletter E-Government Suisse 2011 http://www.egovernment.ch/dokumente/newsletter/Newsletter-E-Gov-02-2011-f.htm Accessed October 2014.
31. ATS 2013, Les entreprises suisses satisfaites des prestations internet des administrations (source ATS). http://www.lenouvelliste.ch/fr/societe/multimedia/les-entreprises-suisses-satisfaites-des-prestations-internet-des-administrations-476-1239889 Accessed October 2014.
32. Hofman, S., Räckers. M, Becker, J. 2012. Identifying factors of e-government acceptance – a literature review. *Thirty Third International Conference on Information Systems*, Orlando.
33. Fromm, J. Hoepner, P., Pattberg, J., Welzel, C., 2013. *3 Jahre Onlineausweisfunktion - Lessons Learned.* Fraunhofer Fokus, www.fokus.fraunhofer.de
34. Harbach, M., Fahl, S., Rieger, M., & Smith, M. 2013. On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards, in *Privacy Enhancing Technologies*, Springer Berlin Heidelberg (pp. 245-264).
35. Brandimarte, L., Acquisti, A., Loewenstein, G. 2010 Misplaced Confidences: Privacy and the Control Paradox, *Ninth Annual Workshop on the Economics of Information Security (WEIS)* June 7-8 2010 Harvard University, Cambridge, MA
36. Miltgen, C., and Peyrat-Guillard, D. 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries, *European Journal of Information Systems*, Vol 23, 103-125
37. Lusoli, W., and Miltgen, C. 2009. *Young people and emerging digital services. An explora-tory survey on motivations, perceptions and acceptance of risks*. EC JRC-IPTS Report.
38. Proposal for Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) / COM/2012/011 final -2012/0011 (COD). Accessed May 2015.