Discussion Paper

An Inexpensive Privacy Protection Strategy for eID Cards

version: 0.2, 30-3-2007

Bud P. Bruegger <bud@comune.grosseto.it>, Comune di Grosseto, Italy

Martin Meints <meints@datenschutzzentrum.de>, Independent Centre for Privacy Protection Schleswig-Holstein, Germany

Marit Hansen <marit.hansen@datenschutzzentrum.de>, Independent Centre for Privacy Protection Schleswig-Holstein, Germany

Amir Hayat <amir.hayat@iaik.tugraz.at>, Technical University of Graz, Austria

Koen Simoens <koen.simoens@esat.kuleuven.be>, KU Leuven, Belgium

Xavier Huysmans <xavier.huysmans@law.kuleuven.be>, KU Leuven, Belgium

Purpose

This paper attempts to contain the minimum useful content to launch a discussion on what is possibly easiest to implement approach to eID privacy protection. The scope of the contribution is to find a best practice and solution that is compatible with the currently issued eIDs, much rather than proposing a next generation of eID that breaks with the major commitments and assumptions of the current roll-outs and evolving standards.

Acknowledgments

Some of the work on this privacy protection approach has been conducted in the eForum's PPP eID Working Group that discussed best practices in this area and how to combine them.

Objectives of Privacy Enhancement

While there may be many privacy issues around eID cards, the one focused on in this discussion is solely the unlinkability of personal data in regard of authentication with eIDs. In particular, it is to avoid that the authentication mechanism encourages different, unrelated service providers to use identical person identifiers that make linking of transactions and related data across sectors of use very easy.

This issue of unlinkability becomes increasingly important once government-issued (partial) identities (in the form of eIDs) will be used to access private sector services at a large scale. It may be very difficult to address privacy at a later time once a single unique identifier for every citizen is introduced as keys in data bases across all sectors. For this reason, we try to launch a discussion on this issue now.

Current eID Privacy Strategies

The most sophisticated privacy enhancement strategy in the current eID domain has been implemented by Austria. The use of different identifiers in different sectors has been an integral part of the design and is implemented both legally and in the technical solution.

The core concept of the Austrian solution foresees the dynamic derivation of a potentially unlimited number of sector- or purpose-specific person identifiers from a single government issued source identifier. This approach is much more cost-effective than the issuance of separate static identifiers for different sectors. Its applicability to an arbitrary number of sectors promises a much more far reaching privacy protection than a necessarily limited number of static identifiers could ever achieve.

We believe that the Austrian approach comes with two significant barriers to adoption: (i) cost of operations and (ii) incompatibility with major standards.

(i) The Austrian approach requires government-operated third parties to derive the sector-specific identifiers. This is enforced by law through the requirement that only government approved applications can get access to the source identifier. The approach thus requires the government to put up and maintain the necessary trusted third party that is necessary for all accesses to services—also in the private sector. This can become a significant cost factor and asks for a specific business model that can guarantee long term sustainability. Also, the concentration of the enabling infrastructure solely in the hands of government may raise privacy issues in itself.

(ii) In order to protect the confidentiality of the source identifier, the Austrian solution refrains from using X.509 certificates that are instead substituted with a proprietary approach called *Identity Link*. Considering that the large majority of countries who issue eID cards today and all the relevant standards in the domain (CEN TS 15480 “European Citizen Card” [xx ref], American PIV [xxx ref]) have strongly committed to the use of X.509, a direct use of the Austrian approach can be expected to be rather problematic in many countries.

In the domain of X.509-based eID cards, two countries in particular have come up with interesting approaches in support of unlinkability of personal data.

One of them is Belgium. While their X.509 authentication certificate contains the nationally unique person identifier, legislation forbids its storage in databases. This means that the unique identifier is used only for a short period of time during service access; its absence in databases eliminates a majority of opportunities for malicious linking. This legal approach is thus a rather solid protection against linkability that covers the majority of possible attacks.

It is interesting to note that the Belgian approach seems to imply the need for a dynamic derivation of local, sector- or purpose-specific identifiers that are suitable to be used as keys in databases. The rational behind this claim is that the alternative approach of statically assigned local identifiers requires lookup tables that store exaclty what is prohibited by the same law. Also technically, such lookup tables would obviously be at very high risk of attacks.

In the Belgian approach, this derivation of local identifiers is under the responsibility of each service provider. While it is true that this legal requirement can be disregarded, an adequate strategy of auditing and prosecution promises to largely limit the number of violations and thus effectively prevent large-scale linking of personal data.

The second country with an interesting privacy protection approach is Italy that refrains from including any personal data in the authentication certificate of their CIE card. This approach is very comparable to the use of opaque handles in the Liberty Alliance approach where all personal data is provided on an as-needed basis and with explicit user consent (XXX is this true? XXX).

While some countries (such as Belgium) split up personal data into multiple files[1] in order to support selective disclosure of personal information, the minimally disclosed data is always the one

[1] The personal information of the Belgian eID card is contained in the certificate, and general data file, and a file containing the postal address. The information contained in the certificate is always disclosed in any case to the service provider, while there is a choice of whether to disclose the data contained in the other files.

contained in the certificate; it is impossible to authenticate without disclosing this data. Italy's approach is unique by allowing a zero minimal disclosure.

Proposed Privacy Approach

We propose to combine and evolve the best practices of these three countries in order to find a relatively simple and cost-effective strategy to privacy protection. It is hoped to be attractive also to countries who committed to the use of the X.509 standard.

The basic idea is to combine the Italian approach of zero disclosure authentication certificates, the Belgium concept of legally requiring service providers to derive local identifiers, and the proven Austrian approach of deriving local identifiers from a single source identifier.

The major components of the solution are described in more detail in the following:

Autentication Certificate with Opaque Source Identifier

The first component is an X.509 authentication certificate that lacks any personal data and contains solely an opaque identifier for the person. This identifier shall be call “source identifier” in the sequel.

There are several characteristics that this source identifier has to possess in order to be used efficiently in the overall strategy. They include the following:

- The source identifier must not be linkable to the person via already existing identifiers or other personal data. This obviously prohibits the use of unique national identifiers (such as social security or tax numbers) that are already in common use . and thus easy to link to their owner.
- To support efficient derivation of local identifiers without the need of a secret, the source identifier further needs to have a high degree of entropy (i.e., not be systematic or predictable) and ideally have the properties of a random number.

While source identifiers could be created as purely random numbers, the approach taken by Austria to derive them from a commonly used unique person identifier is very attractive. In this case, the source identifier is derived[2] from a known unique identifier with the use of a closely guarded secret key. In the case of Austria, this derivation is done by the Privacy Commission. It is important to note that the secret is necessary to effectively break the linkability between the commonly used unique identifier and the source identifier.

It is important to understand that the proposed privacy strategy does not require confidentiality of the source identifiers as a such. Much rather, it requires that the source identifier be never used together with any other personal data. This means that full publication of authentication certificates (e.g., in a national LDAP server) is completely compatible with the proposed approach.

Static Sets of Personal Data

All personal data is managed solely under the citizen's control. Data sets must also contain the source identifier in order to link the data to the authentication certificate. All these data sets are signed either by the issuing authority or another trusted third party. Users, as data owners, are the only subjects authorized to store personal data together with their source identifiers. The data sets can be either stored on the eID card itself (which is assumed to be more secure) or on any other

[2] suitable derivation algorithms include encryption (that can be reversed by the owner of the secret key (e.g., a privacy commission) or an HMAC.

storage media such as local file system or removable storage media (such as a USB stick). In any case, some access control mechanism (like a PIN or Password) should enforce that only the data owner has access to the data.

The requirement of minimal disclosure of personal data requires the availability of a very large number of combinations of data elements; including both, selections of base data elements and data that is functionally derived from the base data. For example, a data set could contain the base-data element of citizenship and the fact that the person is above 20 that is derived from the date of birth.

While the separation of personal data into multiple data sets is surely a step in the direction of more user-controlled data disclosure, it necessarily falls far short of the requirement of disclosing only the minimal necessary personal data.

For this purpose and as a possible evolution of a countrie's eID strategy over time, it is possible for trusted third parties to derive the required data sets from a certified set of base data. This is discussed in more detail in the following section.

Derivation of Personal Data Sets by Trusted Third Parties

Trusted third parties (TTPs) are required if one is to support the creation of derived data sets with lower information content following an as-needed strategy.

The base functionality of such a TTP is to receive a full set of personal data together with a specification of what derived data content is necessary. The TTP then verifies the signature of the full data set, derives the requested data, and certifies the derived data with a digital signature.

Such TTPs can be run either by governments or by other organizations that a user may trust more to protect her privacy in non-governmental sectors. To the authors, a viable choice of TTPs seems to be a pre-requisite for privacy in itself.

There are two ways in which a data set can be derived: (i) in a reusable way or (ii) for one time use.

(i) In order to make derived data re-usable, the data set needs to contain the person's source identifier. This enables the citizen to store the data set and reuse it in different contexts, possibly in different sectors, and for multiple service providers. This option is relatively inexpensive since a single derivation can be used many times.

(ii) A more expensive modus of derivation that has a higher degree of privacy protection is the derivation for one time use. In this case instead of using the citizen's source identifier, the service provider's local identifier is included in the data set. Note that this requires that the local identifier is predictable by the user (and TTP). This is clearly the case in the Austrian approach where the sector-identifier fully determines the derivation of the local identifier.

The existence of multiple levels of sophistication in the privacy protection provided by TTPs again suggests that a country's privacy protection strategy can evolve over time. For example, in an initial roll out, TTPs may not be in place at all and granularity of disclosure could be solely determined by the separation of personal data into several data sets on the eID card. As private-sector use increases, the first TTPs may be set up in order to counter the increased potential for linkability with a more sophisticated protection.

Accompanying Legislation

The proposed privacy strategy fails to guarantee unlinkability with technical means but instead uses a legal approach that requires service providers and other involved parties to take adequate steps for privacy protection that prevent linkability.

The key legal requirement is that only the citizen is allowed to store his or her personal data together with the source identifier. All other subjects must not store source identifiers and instead need to derive a local identifier that can be used as a key for the data in the database.

Optionally, the legal requirement that specifies the derivation algorithms to be used may have the purpose of achieving a secure and non-invertible derivation (one-way-function). Together with a clear regulation of how to chose sector- and purpose-identifiers, it also paves the way to using TTPs that derive data sets for one time use.

Algorithms for the Derivation of Local Identifiers

Austria has already specified algorithms suitable to derive local identifiers. This work is directly usable for the proposed approach.

In essence, the algorithms are cryptographic one-way functions (so called digest functions or hashes). They use a concatenation of the source identifier and a sector-/purpose-identifier as input. If the source identifier has enough entropy and has random properties, inversely computing the source identifier from the local identifier is practically impossible.

A big advantage of the Austrian approach is that the derivation does not require any secret key. Any secret would both, prohibit one-time-use derivation of personal data sets, as well as inflict significant cost should it be necessary to replace a compromized secret.

Minimal Requirements for Starting

Rolling out a full-fledged privacy infrastructure from the very beginning is probably excessively ambitious for most national eID projects. A more gradual introduction that adds privacy protection mechanisms step by step with increasing use and spread into new sectors may be much more realistic.

For this purpose, it is interesting to understand what the minimum requirements are to keep the road laid out in this discussion open. Closely related to this is the queston on how the transition from a current eID-scheme based on unique identifiers to the describes approach could be carried out. A first attempt to address these questions is given in the remainder of this section.

One possible transition strategy is as follows:

- initially, the authentication certificate contains both, a unique identifier and other personal data.
- in a first transition step, a source identifier is being added to the certificate and legislation is released that forbids the storage of this identifier together with other personal data by anyone but the concerned citizen herself. At this point, any publication of the source identifier together with other data must be forbidden. For example, it is no longer possible for LDAP servers to publish these certificates that now contain the source identifier together with other personal data.
- Once all initial eID cards have expired and consequently, all valid cards contain a source identifier, legislation can mandate a transition period that requires all stored personal data to add a derived local identifier to the data sets. All data owners who lack a specific need for using the nationally unique number must remove it from their data sets by the end of the transition period.
- At the end of this transition period, the link between authenticated users and stored data is always possible based on the derived local identifier. At this point of time, it is possible to start issuing certificates containing only the source identifier .

The biggest weakness in the described transition is the possibility that someone can illegally store source identifiers together with other personal data (such as the unique national identifier). This would allow to derive all possible local identifiers for a selected person using the sector- or purpose-identifiers (that are usually public). Legal enforcement against keeping such data may prove very difficult.

But even if there was a limited number of offenders of privacy regulations, the approach still improves the overall privacy situation by making large-scale linking significantly more difficult and generic linking, that does not start with a selected person with known source identifier, impossible.

There may be transition strategies that are more successful and avoid the security pitfalls of the one described above. This is left for future research.

Limitations and Future Work

The proposed privacy protection strategy for eIDs focuses purely on authentication. In contrast, many services need non-repudiation together with authentication. For example, a prerequisite to the use of a given service may be to agree with certain rules of conduct or to agree to pay for the service. In these cases, there must be an easy way of finding the equivalence between the identifier used for non-repudiation and that used for authentication.

To out knowledge there is much less prior experience on the use of sector-specific identifiers in the area of non-repudiation. An effective use of the proposed approach would mandate that a compatible strategy be used in this area. Otherwise there is a high risk that either services that need both authentication and non-repudiation become impracticable or that unlinkability is lost at the first time an electronic signature is required.