Privacy-friendly Identity Management for eGovernment

Xavier Huysmans, K.U.Leuven ICRI

13 September 2006

Abstract

This position paper briefly introduces ongoing research on the topic of privacy-friendly identity management for eGovernment. It focuses on the incorporation of a certain level of privacy and data protection requirements in identity management architectures used in eGovernment. Privacy policy negotiation is a crucial component to achieve this.

1 An introduction to identity management for eGovernment

There are several strong drivers to implement Identity Management (IDM) in an organization's activity from a service provider perspective, such as cost reduction, risk reduction, trust enhancement, increased functionality etc.

These properties are very welcome in eGovernment, which main drivers are to cut costs and to provide more efficient and more effective services to the customer (citizens, businesses etc.)

One crucial aspect of eGovernment is that it treats information as a *strategic resource for all government activities.* This leads to a number of measures and requirements.

On the Belgian Federal government level this means for example that:

- Data has to be modeled in a flexible way that maximally takes into accounts the users' needs.
- Data should be collected only once and maximally reused via *authentic sources*, based on a functional task sharing division. This division results from an agreement (or a legally binding decision) about which government entity stores which data in authentic form.
- Data should be managed efficiently during its whole life-cycle.
- Data should be exchanged electronically where possible, based on a functional and technical interoperability framework.
- Data should be processed in accordance with privacy and data protection regulation, and, more in general, be consistent and properly embedded in the law.

2 Privacy and data protection in identity management for eGovernment

The implementation of IDM in eGovernment can, but does not necessarily take into account privacy and/or data protection requirements.

A recent field study performed in assignment of the Danish government on the usage of privacy enhancing technologies shows that across Europe, today's governmental processes only include limited privacy protecting functionality.

Also, where governmental processes are being re-engineered to eGovernment services, these new developments seem to follow this trend by not rating privacy principles high in their basic architecture design.

There are a number of good reasons why this is problematic. One of them is because without privacy and data protection requirements, the IDM architecture typically includes user identification, and data exchange is based on unique identifiers of the natural person to whom the data relates.

This creates important risks: when personal data from one context can be linked to personal data from another context, it results in detailed profiles about natural persons and a lack of privacy. Even though such interconnections are not *authorized* or illegal, it is not excluded that they will take place anyway.

Research that aims at incorporating privacy and data-protection rules in the IDM architecture usually focuses on *maximum privacy.* The enhancement from a privacy perspective mainly lays in the fact that its protection is put in the hands of the person the user trusts most: *himself.*

A privacy enhanced IDM system (PE-IMS) empowers the user to decide on the release of personal data and on the degree of linkage to his or her personal data within the boundaries of legal regulation.

Notwithstanding its unquestioned qualities in a number of contexts, also in eGovernment, discussions with government managers indicate that there are very few incentives to implement such an IDM system *on a large scale*, for systematic exchange of personal data in eGovernment.

This is understandable to some extent, since *privacy is not an absolute right*, and there are other (valuable) interests which may limit the right to privacy, especially in a governmental context.

Still, even though there might indeed be a lack of business models to implement a PE-IMS on a large scale in eGovernment as defined above, there are also other, very good reasons to incorporate privacy and data protection requirements in the basic architecture design, such as:

- from the service provider perspective: e.g. reduction of the operational risk of the organization's activity, increased trust by the users, auditability of compliance with the regulation etc.
- from the user's perspective: e.g. enforcement of their privacy and data protection rights, increased transparency and increased trust, etc.

The question we currently investigate a.o. through legal and technical research, is what the requirements are of an IDM system that is suitable for a large scale implementation in eGovernment, if it also incorporates *privacy and data protection requirements in the basic architecture design.*

Additional complexity is added due to the fact that there exists not yet a measure to express the degree of privacy enhancement of an IDM system.

This lack of vocabulary makes it very difficult to express what can be expected from an IDM system that is not maximally privacy-enhanced.

Also, the research objective is obviously not only to be compliant with privacy and data protection regulation, but where possible also go one or more steps beyond - even though it does not include *user-controlled context-dependent role and pseudonym management.*

Explained in terms of the categorization of IDM systems set out in deliverable 3.1 of the FIDIS project, we would like to investigate privacy enhancements of a type 1 IDM system, instead of putting the focus on a type 3 IDM system.

We've provisionally defined this type of IDM architecture as a "privacy-friendly" one.

3 Alternatives to user-controlled identity management

Besides IDM systems that implement a user-controlled context-dependent role and pseudonym management (type 3 IDM systems), there are clearly also other *legally admissible* ways to incorporate privacy and data protection requirements in an IDM architecture used in eGovernment.

One could for example mention the IDM system used in the Belgian Social Security sphere, which goes much more in the direction of organizational IDM (type 1), a.o. used for account and resource provisioning.

Data management is here realized by the combination of a number of principles, some of which we mentioned above and other mechanisms, such as a clearing house which makes use of a reference directory.

Crucial thereby is that data is only made accessible and exchanged with thereto *authorized entities*, based on formal authorizations by (a subcommittee of) the Belgian privacy commission. This model of course heavily relies on IDM components.

To sum up, compliance with privacy and data protection regulation in such an alternative model is not gained via user control, but via control by a trusted third party.

Additional complexity is added to the model when government entities from different administrative levels need or want to exchange data with each other.

This would typically be solved via a federation between these entities (and federated IDM), which on its turn creates a number of additional legal and technical challenges.

4 Privacy negotiation in eGovernment

Even though eGovernment that is based on data control by a trusted third party seems an interesting alternative to one that puts focus on user control and user-controlled data linkage, *very annoying issues still remain when privacy and data protection requirements are not incorporated in the IDM architecture*, namely:

- lack of privacy, since the natural person to whom the data relates looses control over his personal data;
- lack of transparency, since it is not necessarily clear what happens to which personal data;
- lack of auditability of the system;
- lack of enforceability of privacy and data protection rights;
- etc.

5 Contribution to the discussion of the workshop

The author, who has a legal background, believes that joining the discussion at the W3C Ispra workshop would be of mutual benefit.

At the one hand the presented research can serve as a use case that demonstrates a real life application field for privacy policy languages, and at the other hand it also helps to formulate the requirements he and his colleagues are working on.

We believe that both in a “regular” eGovernment environment, as in a federated one, one of the important ways to attain privacy and data protection enhancement of the IDM system is via *privacy policy negotiations*.

More precisely, we are thinking in the direction of data handling policies to enforce the mentioned authorizations of the above mentioned trusted third party.

Information that should be included in the policies might for example be:

- what data are collected,
- the identity of the controller,
- for what purposes the data are processed,
- based on which legitimacy ground,
- what the data recipients are
- what the retention period is,
- what the rights of the data subject are with regard to the data, and finally,
- what the modalities of the data processing would be, e.g. authorization to process the personal data via a reference directory or not.

Such data release policies could also be used to complement the system with user preferences.