Privacy-friendly Identity Management in eGovernment

Xavier Huysmans

K.U.Leuven ICRI, Sint-Michielsstraat 6 B-3000 LEUVEN - BELGIUM
xavier.huysmans@law.kuleuven.be

There are apparently very few incentives for government managers to implement Privacy-Enhanced Identity Management Systems *on a large scale* in an eGovernment architecture.

In this paper we explain why this is understandable to some extent and introduce a less far-going alternative – provisionally – called Privacy-Friendly Identity Management. We conclude with a brief analysis of one important driver to choose for "Privacy-Friendly Identity Management Systems": *risk management.*

1 Identity Management in eGovernment

There are probably as many definitions of the term eGovernment as there are people working in that field. The definition used in Belgian federal eGovernment runs as follows: *"eGovernment is the continuous optimization of service delivery and governance by transforming internal and external relationships through technology, internet and new media"*.[1].

This optimization relies on a number of important principles, inter alia, treating information as a strategic resource for all government activities and the integration of backoffices. [2]

From a technical perspective the integration of back-offices is typically looked for through a (cross-border) "*Service Oriented Architecture*"(SOA).

In practice, identity management components are often integrated as basic service components of such a SOA in eGovernment. These services are then compiled with other services to so-called value-added services.[3]

Depending on the goals of the eGovernment project, it is usually good to start with a risk assessment of the organization's activity.

[1] DEPREST AND ROBBEN 2003, p. 6.

[2] For more information, see DEPREST AND ROBBEN 2003, DE BOT 2005 p. 4-13, the federal portal http://www.belgium.be on the page 'about eGovernment', ROBBEN 2006a. and DEPREST AND STRICKX 2005.

[3] ROBBEN 2006b, slide 13.

Such an assessment usually starts with the evaluation of the need for identity management mechanisms to protect information, applications and the infrastructure of the organization.

These mechanisms can be understood in terms of a lifecycle: create an identity of an entity, authenticate the identity, grant the appropriate permissions to that entity, monitor and incorporate accountability mechanisms, and finally audit and assess the IDM processes.[4]

In order to perform this lifecycle, we typically need components of an IDM system, such as registration, identification, authentication, authorization and access control, user management, accountability, auditing, and data storage and communication.

It is obvious that not all IDM systems contain all these components. It is also important to realize that, since they are all part of the mentioned lifecycle, they are also strongly interconnected.

2 Privacy and data protection in identity management for eGovernment

2.1 The problem

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

There are a number of good reasons why this is problematic, especially in eGovernment. One of them is that the usage of ICT in governmental processes creates new, substantial risks, which should be adequately answered *to maintain the power balance between the citizen and the state with regard to personal data.*

Indeed, one should not forget that the fundamental right to privacy[6] protects the fundamental political value of a *democratic constitutional state.*

This means that it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards for example - their sexuality, health, personality building, social appearance and behavior, and so on.

[4] SLONE 2004, p. 24 ff.

[5] X (2005) Report on Privacy Enhancing Technologies.

[6] which was codified, inter alia, in article 8 of the European Convention on Human Rights and article 22 of the Belgian Constitution

With other words, privacy guarantees each person's uniqueness, including alternative behavior and the resistance to power at a time when it clashes with other interests or with the public interest. It therefore plays an essential role in *regulating the power balance* between governments and their citizens in regard to a very important government' resource: information.[7]

When privacy and data protection requirements are left out from the IDM architecture, the latter typically includes *user identification*, and data exchange is typically based on the common usage of *globally unique* identification keys.[8]

This creates important risks: when personal data from one context can be linked to personal data from another context (internal or external to the government sphere), it *can* result in detailed profiles about natural persons and a significant lack of privacy. Even though such interconnections can be unauthorized or illegal, it is not excluded that they will take place anyway.

The key question we have to ask ourselves is therefore whether – to protect the fundamental right to privacy and to make sure the European data protection principles are being respected – it suffices to rely on procedures to be applied by the administrative staff, if, at the other hand, massive data aggregation and linkage of databases is at least being facilitated through the unrestrained usage of ICT in eGovernment.

We believe it isn't. We are convinced that if such a substantial erosion of privacy is made possible through eGovernment, governments should definitely take the necessary measures, including technical ones. We come back to this below.

2.2 Current research on privacy and IDM

There are several valid approaches to tackle this privacy erosion, varying from blunt acceptance ("you have zero privacy, get over it"[9]), to legal constructs

[7] Hildebrandt 2005 p. 18, DE BOT 2001 on page 186 (especially the definition of privacy by prof. Rigaux and the authors cited in footnote 14) and DE BOT 2005 32-33.

[8] This is for example the case in Belgium, where data exchange mainly relies on the usage of the National Registry Number of the person to whom the exchanged data relates. Since decades, a unique identifier is being assigned to Belgian citizens at their first registration in the National Registry. Since the advent of Belgian eGovernment, this identifier has become *globally* unique because it is now used to refer to that person *across several government contexts.* It is thus not limited to one or more particular spheres of government' activity. Other "relevant" entities (such as enterprises, foreigners etc.) hold a similar, globally unique identifier.

[9] Famous words spoken by SUN's CEO Scott McNealy in January 1999 (http://www.wired.com/politics/law/news/1999/01/17538). They illustrate an interesting approach to deal with the mentioned erosion that focuses on transparency

(e.g., qualifying privacy as a sort of intellectual property right which can be negotiated and traded) and technical measures.

It is this third approach we are interested in. As Mr. Lessig explained in his book "Code version 2.0", *code* can be used to implement privacy features.[10]

Current research on the topic of identity management and privacy, such as the EU funded PRIME project[11], usually suggests to implement code in the identity management (IDM) architecture in a *privacy enhanced* way, which means that the IDM architecture is (1) user centric and (2) focuses on context-dependent role and pseudonym management.

A privacy-enhanced application design then supports both "user-controlled data release" as well as "user-controlled data linkage".[12]

Discussions we've had with government managers seem to indicate that this type of privacy enhancements may be over-ambitious for eGovernment. They do not see enough 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, *given the relativeness of the right to privacy*[13]., the existing of competing interests in eGovernment and the (apparent) general lack of incentives for governments to restrain their technical capabilities on the personal data they are processing.

Tasks government entities carry out in the public interest undoubtedly justify to some extent limitations of the right to privacy and the foreseen exceptions of the general data protection rules.

It is self-evident that these exceptions and limitations also effect the privacy components of a data and identity management architecture used in eGovernment.

and accountability: don't put too much energy in keeping your personal information unknown to the world – make sure instead that you can verify what is being done with it (transparency) and hold people accountable if needed). See WEITZNER 2006

[10] LESSIG 2006

[11] PRIME develops a *privacy enhanced identity management system* (PE-IMS), which means that via the PRIME tools, the user is empowered to decide on the release of data and on the degree of linkage to his or her personal data within the boundaries of legal regulations. More information on the PRIME project can be found at http://www.prime-project.eu

[12] PFITZMANN 2006 on p. 23, footnote 68

[13] Not one single aspect of privacy takes absolute precedence over other rights and interests. Never does an individual have absolute control over an aspect of his/her privacy. Privacy can thus be restricted when balanced against other interests (rights of others, law enforcement, public health, etc.) and under a number of conditions (such as, the legality of the restriction, the link with a pressing social need and the proportionality between the restriction and these needs). HILDEBRANDT 2005, p. 19 and BUCHTA 2005, p. 5

Concretely, this means that a privacy-enhanced (or maximised) identity management architecture which implements *user-controlled context-dependent role and pseudonym management* will often not be a realistic option in eGovernment, where privacy coexists with a number of strong other interests and exceptions.

2.3 Privacy-friendly Identity Management

The relativeness of the right to privacy does not mean that nothing can or should be done to counter the mentioned privacy erosion in eGovernment. The underlying idea – which is not further developed here[14]– is that is possible to outline and fully describe the requirements of:

- an organizational IDM system
- that especially addresses the interest of natural persons to control, or at least significantly influence the processing of data about him/her-self, and
- incorporates at least some degree of privacy and data protection requirements in the basic IDM architecture design.

We suggest to (provisionally) call an IDM system that complies with these requirements "privacy-friendly", as opposed to the above mentioned "privacy-enhanced" ones.

3 Why privacy friendly IDM in the basic architecture used in eGovernment?

Even though there might be a lack of drivers to implement a IDM system that focuses on maximum privacy on a large scale in eGovernment (PE-IMS, as described above), there are very good reasons to incorporate at least some degree of privacy and data protection requirements in the basic data architecture design used in eGovernment. These drivers are, for example:

- the reduction of the operational risk of the organization's activity due to data protection and privacy requirements,
- an increased trust in the eGovernment project, since users get more transparency and a way to enforce their privacy and data protection rights,
- the auditability of compliance with the regulation and/or authorizations received to exchange a particular set of data.

We believe these and other drivers need to be made explicit via research, to be convincing enough for government managers to change some of their priorities on privacy and data protection in eGovernment.

[14] It is work being done in Work Package 16 of the FIDIS project.

For the purposes of this paper, we believe it is useful to say a few words on the first driver we've pointed out: *risk management.*

Organizations that manage their industry and operational risks assess what the loss might be if something goes wrong, and whether they can absorb that loss if it indeed goes wrong. These decisions are typically based on information provided by trusted third parties (audits etc.). Risk assessment is the process of identifying and evaluating such risks.[15]

Managing risks thus leads to concrete actions, for example subscribing insurances, the provisioning of sufficient financial means or accepting risks and communicating these decisions to the stakeholders.

If we accept that the unrestrained usage of ICT in eGovernment at least potentially creates a substantial risk of privacy erosion for the persons to whom the data relates, this is an operational risk that needs to be identified, and which should result in a concrete *risk decision.*

A risk assessment of an eGovernment project could for example result in the decision to accept the risks related to a potential eGovernment "privacy-gate scandal" and the negative publicity, court cases, loss of electorate, burning decisions of the privacy commission etc. that goes with it.

We do not think it would be a wise decision to just accept that risk, because of the *objective liability provision* contained in the data protection regulation. Before we go any further, we need to explain 3 legal rules:

1. *Objective risk liability:* Article 23 of the European Data Protection Directive, as transposed in article 15bis of the Belgian Data Protection Act[16] states that *the data controller* – this is the entity that alone or jointly with others determines the goals and the means of the processing of personal data – *is in principle liable for the damages caused to the data subject as a result of a processing or any act that is not compatible with the Data Protection legislation.* He may only be exempted from this liability, if he proves that is not responsible for the event that gave rise to the damages.
   The mentioned article is an "obective" liability provision, because there is no need to prove the fault of the data controller to hold him/her accountable for a certain action: the mere fact that he/she infringed the data protection law leads to liability, of course only if there is a causal link between the damages and this infringement of the law.[17]

[15] IDA Authentication 2004, p. 9 and 19 ff. and HUYGHENS 2005

[16] Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, Belgian State Gazette 18 March 1993, as modified by the law of 11 December 1998 implementing Directive 95/46/EC, Belgian State Gazette 3 February 1999, and the law of 26 February 2003, Belgian State Gazette 26 June 2003.

[17] This is an exception to the normal liability rules, following which, to hold someone accountable, one has to prove the existence of a fault, damages and a causal link between them (art. 1382 of the Belgian Civil Code).

2. *Privacy in the data protection law:* Article 2 of the Belgian Data Protection law introduces a subjective right for natural persons to *respect for their private life* (read: privacy) *with regard to the processing of personal data that concern him/her.*
   Similarly, article 1 of the Data Protection Directive states that *Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.*[18].
   Concretely, based on this article, one can say that the obligation to respect the right to privacy is also applicable to data controllers. We will come back to this below.

3. *Obligation to take the appropriate technical and organizational measures:* Article 16 of the Belgian Data Protection Law and article 17.1 of the Data Protection Directive contain an obligation to take *appropriate technical and organizational measures* to protect the processed personal data against:
   - accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and
   - *against all other unlawful forms of processing.*

   Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the *state of the art* and the cost of their implementation.

By jointly reading these 3 legal rules, it becomes clear that, (1) if the unrestrained ICT usage in eGovernment at least potentially creates a substantial risk of privacy erosion for the persons to whom the data relates and (2) if a government wants to avoid the mentioned liability risk, all adequate organizational and technical measures should be taken to avoid unlawful forms of data processing (including privacy infringements).

Also, as explained in the third bullet point, the "adequateness" of such measures is evaluated by having regard to the state of the art. The latter could, *given the maturity of the research on privacy and identity management*, refer to the incorporation of at least some degree of privacy and data protection in the basic eGovernment architecture design.

Whether a concrete IDM architecture is adequate or not, is not easy to evaluate. Nevertheless, it is clear that the usage of privacy enhancing *technologies* are increasingly being perceived – also on the political level – as a suitable way

[18] The main difference between both texts is that only the Belgian article creates a concrete (subjective) right for natural persons which is usable in court to tackle infringements committed by other natural persons. This is the so-called horizontal action of the right to privacy. Both texts apply, however, also to vertical relations between governments and the natural persons that fall under their jurisdiction.

to enhance the level of privacy and data protection in an organization's activity.[19]

In sum, to answer the question mentioned supra, we believe it is definitely not sufficient to only rely on procedures to be applied by the administrative staff to protect the fundamental right to privacy and to make sure the European data protection principles are being respected in eGovernment.

4 Conclusion

The starting points of this paper are, that the unrestrained usage of ICT in eGovernment creates a substantial privacy erosion and that privacy principles are often not rated very high in a basic eGovernment architecture design.

The question we've asked ourselves is whether – to protect the right to privacy and to make sure the European data protection principles are being respected – it suffices to rely on procedures to be applied by the administrative staff, if, at the other hand, massive data aggregation and linkage of databases is at least being facilitated through the unrestrained usage of ICT in eGovernment.

In this paper we've explained why we believe the answer is no. After a general introduction on eGovernment and identity management, we made clear that there are several approaches to tackle this privacy erosion and that research on privacy and identity management that wants to implement privacy and data protection *via code*, usually focuses on *maximum privacy*, and includes *user-controlled data release and user-controlled data linkage via context-dependent role and pseudonym management.*

We explained that this might be a tad too much for eGovernment, and suggested to follow another approach to implement privacy and data protection requirements in the basic eGovernment architecture design.

In the last section of the paper we've identified a number of reasons to implement a so-called "privacy-friendly identity management system". One of these reasons is *operational risk management.* Our general conclusion is that it would definitely be a too large risk to take, to only rely on procedures to be applied by the administrative staff to protect privacy and to make sure the European data protection principles are being respected in eGovernment.

[19] See for instance, the recent communication of the European Commission on the Promoting Data Protection by Privacy Enhancing Technologies (PETs) on this topic: *"To pursue the objective of enhancing the level of privacy and data protection in the Community, the Commission intends to clearly identify the need and technological requirements of PETs and further promote the development of these technologies* [...] *and their use by industry and public authorities, involving a vast array of actors, including its own services, national authorities, industry and consumers."*(EC Communication of 2 May 2007 available at: http://europa.eu/rapid/).

References

1. BOUTONNET M (2005) Le Principe de Prcaution en Droit de la Responsabilit Civile, Librairie Gnrale de Droit et de Jurisprudence, Paris
2. DE BOT D (2005) Privacybescherming bij e-government in Belgi – Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart. Vandenbroele, Brugge
3. DE BOT D (2001) Verwerking van persoonsgegevens, Kluwer, Antwerpen
4. LESSIG L (2006) Code version 2.0. Basic Books, New York
5. BAUER M, MEINTS M, HANSEN M (eds)(2005) Fidis Deliverable 3.1., Available at: http://www.fidis.net 15 September 2005, last visited: 20 August 2006
6. BUCHTA A, DUMORTIER J and KRASEMANN H (2005), The Legal and Regulatory Framework for PRIME, in FISHER-HUEBNER S, ANDERSSON CH and HOLLEBOOM TH (eds.), PRIME D 14.1.a: Framework V1, Available at: https://www.prime-project.eu/prime$_{p}roducts/reports/fmwk/pub_{d}el_{D}14.1.a_{e}c_{w}p14.1_{V}4_{f}inal.pdf$, 13 June 2005, last visited: 13 June 2005.
7. DE HERT P (2005) Titel II De Wet 8 december 1992 met betrekking tot de verwerking van persoonsgegevens, April 2005, in P. DE HERT (ed.), Privacy en Persoonsgegevens, Politeia, Brussels
8. DEPREST J, ROBBEN F (2003) eGovernment: the approach of the Belgian federal administration. Available at: http://www.ksz.fgov.be, June 2003, last visited: 20 June 2006
9. DEPREST J, STRICKX P (2005) eGovernment initiatives. Available at: $http : //www.ibbt.be/egov/pres/9._{J}an_{D}eprest_{-}2005.10.26 -_{e} Gov_{u}pdate_{i}nitiatieven.ppt$, 26 October 2005, last visited: 20 September 2006
10. HILDEBRANDT M, GUTWIRTH S, and DE HERT P (eds.) (2005) Fidis Deliverable 7.4, Implications of profiling practices on democracy and rule of law, Available at: http://www.fidis.net, 5 September 2005, last visited: 15 September 2006.
11. HUYGHENS CH (2005) IDM in the risk universe, liability, methodology, standards, Available at: https://projects.ibbt.be/idem/uploads/media/2005.12.20.idem.workshop1.risk.pdf, 20 December 2005. last visited: 20 December 2005.
12. LEENES R, FISHER-HUEBNER S (eds.)(2006) PRIME Framework version 2. Available at: http://www.prime-project.eu, July 2006, last visited: 23 August 2006
13. PFITZMANN A, HANSEN M. (2006) Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology. Version 0.27. Available at: http://dud.inf.tu-dresden.de, February 2006, last visited: 20 February 2006
14. ROBBEN F (2006), eGovernment, presentation available at: http://www.law.kuleuven.be/icri/frobben/presentations/20060327b.ppt, 27 March 2006, last visited: 1 April 2006.
15. ROBBEN F (2006), E-government in the Belgian social sector coordinated by the Crossroads Bank for Social Security, presentation available at: http://www.law.kuleuven.be/icri/frobben/presentations/20060623nl.ppt, 23 June 2006, last visited: 22 March 2007.

16. SLONE S (2004) Identity Management. A white paper. Available at: http://www.opengroup.org, March 2004, last visited: 11 November 2004
17. WEITZNER D, ABELSON H, BERNERS-LEE T and others (2006) Transparency and End-to-End Accountability: Requirements for Web Privacy Policy Languages', A position paper for the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, available at: http://www.w3.org/2006/07/privacy-ws/papers/, October 2006, last visited: 17 October 2006.
18. X. (2005) Identity Management Systems (IMS). Identification and Comparison Study', Available at: http://www.datenschutzzentrum.de, September 2003, last visited: 7 July 2005
19. X. (2005) Report on Privacy Enhancing Technologies, performed for the Danish Ministry of Science and Innovation. Available at: http://www.vtu.dk/fsk/ITC/Rapportvedrprivacyenhancingtechlologies.pdf, 28 March 2005, last visited: 15 October 2005
20. X. (2005) Modinis IDM Terminology Paper, Available at: https://www.cosic.esat.kuleuven.be/modinis-idm/, 23 November 2005, last visited: 22 December 2005
21. X. (2004) IDA Authentication Policy. Basic policy for establishing the appropriate authentication mechanisms in sectoral networks and projects, Available at: http://ec.europa.eu/idabc/servlets/Doc?id=19281, July 2004, last visited: 20 October 2006.