Prepared for the eGovernment Unit
DG Information Society and Media
European Commission

Modinis
Study on Identity Management in eGovernment

Modinis*IDM*
A conceptual framework for European IDM systems

Report Date: 18 September 2006

Table of contents

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

1. Modinis^{IDM} Project Scope

The eEurope 2005 Action Plan stressed that eGovernment identity management in the EU should be advanced by addressing interoperability issues as well as future needs, without ignoring differences in legal and cultural practices and the EU framework for data protection.

The aim of the Modinis^{IDM} Study on Identity Management in eGovernment is to build on expertise and initiatives in the EU Member States to progress towards a coherent approach in electronic identity management in eGovernment in the European Union, and

- To assess the impact of such initiatives on the policies supporting cross-border and cross-sector eGovernment services, e.g., to ease company registration, procurement, and citizen mobility;
- To provide a prospective analysis of possible initiatives and solutions at the European level;
- To provide information on identity technologies, related market developments and technical requirements;
- To propose a methodology to feed the framework described in the Good Practices Framework (Lot 1) with actual use cases of good practices in identity management and with their analysis.

The study is 100% EU funded and started 1 January 2005. It covers 26 months ending 28 February 2007.

The results of the study will be communicated to the Member States and the European Commission with

- Five workshops organized in Brussels (Commission premises) or Leuven (Belgium),
- Identity management reports,
- An eGovernment identity management working group.

2. Background of the underlying document

The conceptual framework described in this document is one of the building blocks identified in the pan-European eIDM roadmap for eGovernment services that was prepared in collaboration between the Modinis*IDM* Study Team and RAND Europe.

Before the first steps towards any kind of implementation activities can be taken, it is important to have a clear view and a substantial consensus regarding the general organisation and basic principles governing a pan-European eIDM infrastructure. This phase precedes the answering of more practical implementation-oriented questions such as the technical choices to be made and the identification of parties to take responsibility of the creation and management of the infrastructure.

Such an infrastructure would need to be based on a federated model, using (at least) *n* identity portals for *n* Member States, and possibly more, depending on national administrative organisation and task division. As indicated in the Signpost[1] Paper, this would "require a framework and policies which respect current national infrastructures and permit the mutual recognition of national eIdentities between countries. The authentication requirements for a particular eService in one Member State would accept as equivalent the levels of security provided by the equivalent authentication requirements and mechanisms of another Member State, and for those services and authentication levels for which each Member State is prepared to cooperate. These policies do not require any specific EU-level infrastructure to be established."

The conceptual framework constitutes a high-level model of the infrastructure envisaged for the realisation of this eIDM infrastructure. Building on the terminological framework, the conceptual framework will indicate the basic principles of the infrastructure. After completion of this conceptual framework, a consensus should exist on the high-level requirements of the eIDM infrastructure, even if technical, organisation and legal questions regarding the exact implementation still remain. Without such a consensus, no meaningful implementation work can be achieved.

The authors of this document welcome any comments and input for this document. Comments and input can be sent directly to the Modinis*IDM* Study Team at modinis-idm@esat.kuleuven.be.

[1] http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf

3. Intended Audience

3.1 Target audience

The reader of this document is supposed to be a member of the:

- Public sector,
- Suppliers of eGovernment systems and eGovernment IDM solutions,
- eGovernment decision makers who deal with IDM systems.

3.2 Required background knowledge of the reader

This document is not an introductory document to eGovernment or Identity Management. It is also not intended as a reference manual or reference document. This document, however, is intended to assist the reader to extend his eGovernment-related knowledge.

A prerequisite to reading this paper is to have a basic understanding of identity management terminology. Therefore we point the reader to our paper on a "Common Terminological Framework for Interoperable Electronic Identity Management":

https://www.cosic.esat.kuleuven.be/modinis-idm/glossary/

3.3 Benefits for the reader

The reader of this document learns:

- What eGovernment IDM is all about;
- What the basic functionality of an eGovernment IDM system should consist of;
- How the reader's system can be integrated in a cross-border and multi-level eGovernment environment.

4. Introduction and Basic Concepts

4.1 Limited Scope

The goal of this document is to specify a framework that is compatible with all Member States' vision on eGovernment identity management, by providing a rigorous set of basic concepts and ideas that help to reason about the domain. The scope of this conceptual framework is limited to electronic identity management in the sense that an attempt is made to create a link between the paper world and the electronic world, without 'rethinking' the whole identity management problem because non-electronic identity management is already in place as we can all be identified within government contexts. When used the term identity management (IDM) refers to electronic identity management or eIDM.

So the idea is not to solve the problems on a member state's level but rather to specify Member States could communicate with each other about their citizens and how citizens could communicate with different Member States. This framework should help to learn them how to talk to each other, to learn them how to share certain information in a federated model, like information related to authorization and authentication, and how to find this information. Different authentication levels are to be defined and standardized between different Member States.

Although harmonization seems to be the solution it is not as straightforward as it seems since the autonomy of the Member States has to be respected. Each of them has its own regulation, makes its own decisions. E.g., a country regulates the existence and the use of context-specific identifiers for its citizens on its territory, but it cannot forbid other Member States to have a different policy on the use of identifiers. As we will see later on one member state should consider another member state as a sector in a particular context.

There are many other issues to address. Protection of a citizen's information has to be taken into account and therefore appropriate measures, like auditing and logging, must be taken to deal with the privacy consequences of sharing personal information between Member States. The European citizen of tomorrow is mobile. Data protection regulation must be in place and Member States should act accordingly. This framework will not solve all privacy problems or provide the one solution, if any exists, but will rather indicate where problems will occur so that appropriate measures can be developed to prevent privacy violation.

Finally a consistent set of definitions is required to discuss about this matter and therefore we refer to the Modinis^{IDM} terminology paper on identity management which served as a basic input of this document. The reader, and even he who is familiar with the subject, is suggested to read it or use it as a reference document while reading this paper.

4.2 eGovernment

In the Modinis Study the identity management problem is looked at from an eGovernment perspective. The organizational structure of the public sector is very fragmented because of its many administrations often acting like separate islands. To tackle this fragmentation we will introduce the concepts of sectors and contexts later on.

These islands generally have two faces, usually called the front-office and the back-office, of which usually only the former is visible to the consumer of the eGovernment services. The citizen goes to the traditional office window or consults the virtual web-based portal covering one or more administrations. In the ideal case a citizen interacts with all administrations through one central and personalized portal or gateway.

Because of the omnipresence of the Internet web-based portals are the first driver for the mobility of European citizens. This approach could be further extended so that a centralized portal also covers administrations from other countries.

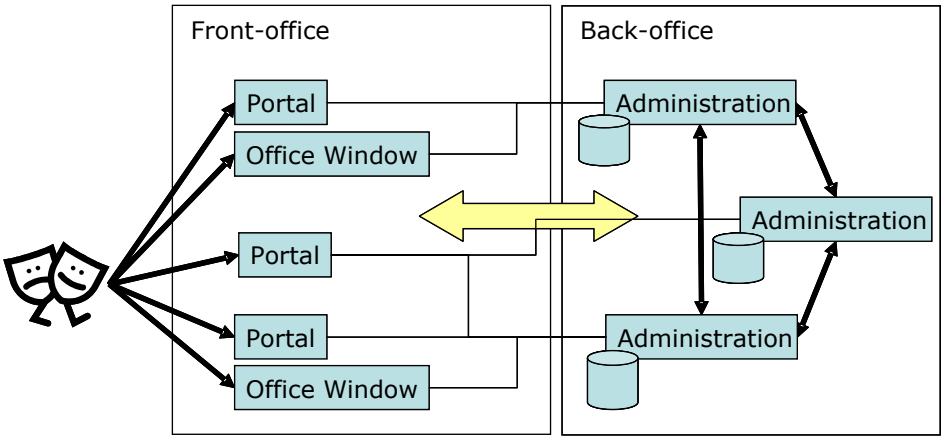

Figure 1: A top-level view on eGovernment .

4.2.1 *Authentic Data Repository*

Before introducing some basic identity management concepts we explain the idea of authentic data repositories. In eGovernment a nation offers services to its citizens and enterprises in an electronic way and therefore digitalizes information in an attempt to reduce costs and administrative burdens. Information has to be collected, stored and maintained in a reliable way so that it can easily be retrieved by those who need it and of course who are authorised to access that information.

An authentic data repository contains information, not necessarily all information, about citizens, enterprises and organisations, etc. that is believed to be correct. The information is stored for a particular purpose and only that amount of information is stored that is needed to achieve that purpose. Later on we will see that to protect a person's privacy measures have to be taken to avoid linking of personal information (profiling) when it is not allowed. An authentic data repository should provide the necessary mechanisms for auditing and access control.

In addition the information in an authentic data repository is collected only once and reused whenever possible, so that an individual does not have to enter the same information about him over and over again. This is one of the key elements eGovernment should try to achieve in order to make eGovernment services successful. Authentic data repositories are one of the basic components in an IDM infrastructure.

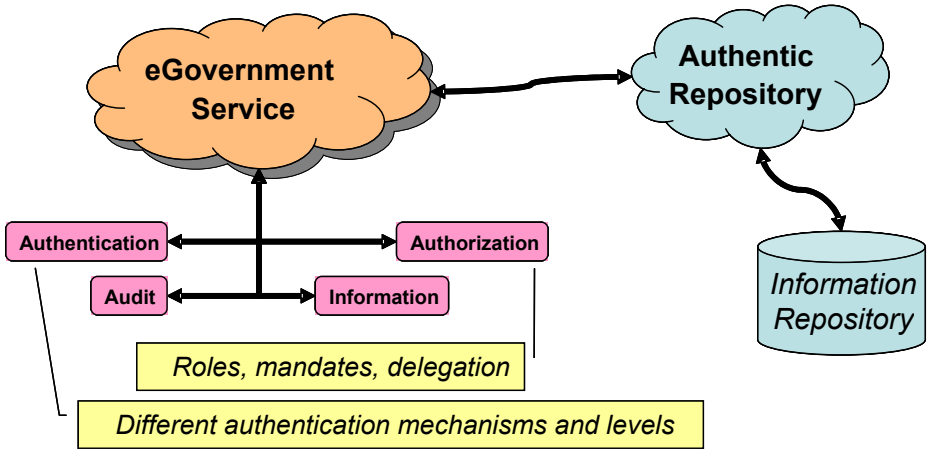

Figure 2: Authentic Repositories in eGovernment.

4.3 Identity management

The Modinis[IDM] terminology defines identity management as *"the managing of partial identities of entities[2], i.e., definition, designation and administration of identity attributes as well as choice of the partial identity[3] to be (re-) used in a specific context"*.

Identity management can be defined in many ways, but from the perspective of a government administration it basically comes down to the management of information associated with natural or legal persons, that can be identified, uniquely or non-uniquely. So this covers both citizens and enterprises, which both make use of eGovernment services.

It is not simply information management because it is linked to an entity that has an identity and that has to be, not necessarily uniquely, identifiable. In most contexts, e.g., taxation, it is required that an entity can be uniquely identified and therefore the use of identifiers is inevitable. On the other hand, there are also many applications when an entity just needs to prove having the right characteristics, e.g., age verification on chat boxes for kids, and as such does not need be uniquely identifiable. This is also part of the identity management problem.

The focus lies here on identity management for eGovernment in Europe. This brings along many new challenges: we need to be able to identify someone electronically, remotely, in a secure way and if needed in many different ways. Also member States have divergent approaches which should be covered by this framework. They use different means to establish electronic identities like digital certificates or electronic signatures coming in different forms like eID (smart) cards or hard and soft tokens. Their solutions are sometimes backed up by private sector solution or built on public-private cooperation. Similar to electronic signatures there will have to be legislative support to support the different forms to be recognised as identities.

In the following subsections we elaborate on some of the concepts mentioned so far.

4.3.1 Identity

According to the Modinis[IDM] terminology the identity of an entity is the dynamic collection of all its attributes. As it is practically impossible to manage all these attributes we have introduced the concept of partial identities. In order for an entity's existence to be acknowledged, it needs to have at least one unique (partial) identity. If it does not exist it cannot receive any benefits, it cannot execute its rights to act and it cannot be the subject of the actions of another entity.

An entity's existence is established by the creation of a unique identity in that context. This means that the entity is uniquely identifiable in that context and thus can be distinguished from all other entities in that context. This is concretised by the creation of an identifier for that entity. The act of assigning a partial identity in a context is referred to as the registration of the entity in that context. Registration of the entity results in the granting of one or more credential which can be used for authentication purposes afterwards.

4.3.2 Identifiers

An entity is *known* in a particular context if some of its attributes are managed, stored and maintained in that context. To be able to use these attributes in a transaction or to be able to act within this context, an entity must be uniquely identifiable.[4] An identifier is an attribute or a set of attributes and refers to one and only one particular entity in one particular context and is used to link all the information available in that context to that entity.

When different contexts share identifiers there is a potential risk of privacy violation when an entity's attributes from different contexts are linked together by using that shared identifier (profiling). An eGovernment infrastructure should implement the necessary mechanisms and

---

[2] An entity is anyone or anything that exists because it has characteristics that can be measured.

[3] The terminology paper defines a partial identity as *"a certain subset of one or more attributes that does not necessarily uniquely identify the entity"*.

[4] This requirement may be relaxed when an entity acts on behalf of a group of entities and when it is of no importance that the entity is known. The group then becomes the entity that has to be uniquely identifiable.

regulation to prevent this. We will explain the concept of context-specific identifiers later on as one of the mechanisms to enhance privacy in eGovernment. The organisation and management of contexts, identifiers and sensitive data will always require the presence of an appropriate instance like the privacy commissions or officers that exist today.

4.3.3 Authentication

Once an entity exists in a context, i.e. its identity and identifiers have been created, it can start to act in this context. Before being allowed to do something an entity has to prove that he or she really is who he or she claims to be. This process is called entity authentication and is of crucial importance in identity management systems. As we shall see later on, different levels of authentication have to be defined depending on the IDM application.

Note that very often identity management systems are analysed from a client-server point of view. An entity, called the consumer or client (actually a citizen), wants to make use of a certain service provided by a server or service provider. Many current IDM solutions introduce a third party named the identity provider who is providing identity services to the service provider and the client. These services include, but are not limited to, the provisioning of an identity and authentication means, single-sign on mechanisms, verification of identities and assertions, etc.

We will not immediately focus on these concepts as it is just another approach of reasoning about identity management and it does not conflict with our high-level conceptual framework. In this paper it is assumed that certain mechanisms are in place to establish an entity's identity in a particular context. How this is done in practice or who is responsible is irrelevant here.

4.4 Swing between eGovernment and IDM

The Modinis[IDM] study looks at the identity management problem from an eGovernment perspective. For eGovernment services to work it is clear that there is a need to have unique identifiers for entities within a particular context. One person can act in many contexts as illustrated in Figure 3; he can be a civil servant, a lawyer and a father at the same time but will have a different role per context. We observe very divergent approaches of applying identifiers for natural and legal persons in the Member States: national insurance numbers in the U.K., sectoral identifiers in Austria, enterprise and national registry numbers in Belgium, etc.

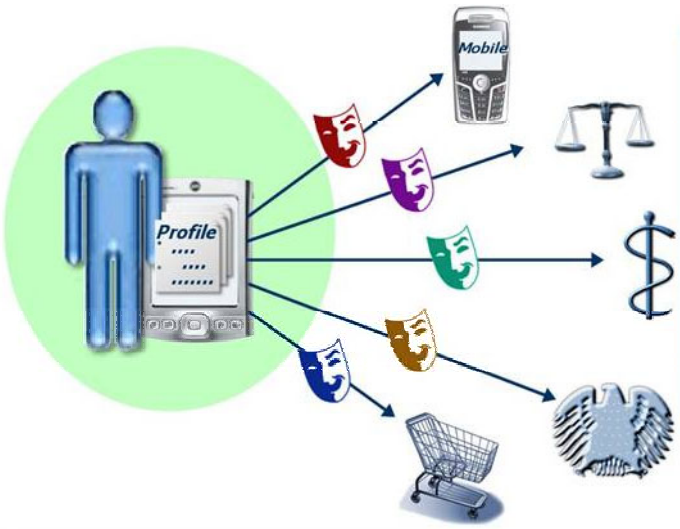

Figure 3: An entity acts in different contexts.
(copyright Martin Meints)

There appears to be a discrepancy between contexts and sectors. Typical examples of sectors are taxation, social security, education, providers of energy resources, telephony services, banking services ... A context is related to a certain activity or interaction and spans one or more sectors.

Due to exchange of information from one sector to another in a particular context the question that rises is where to use identifiers and how to map them to sectors and contexts. The approaches in national IDM infrastructures vary from one extreme to another: some countries tend to use one identifier per sector, the more privacy-enhanced approach; others tend to use for an entity one identifier per context or one for all contexts.

We alter the problem by stating that all sectors within one context should share the same identifier defined for an entity within that context. Consequently we say that countries, e.g., Austria, tend towards a "context equals sector" approach whilst others tend towards a "context equals one or more sectors" approach like in Belgium.

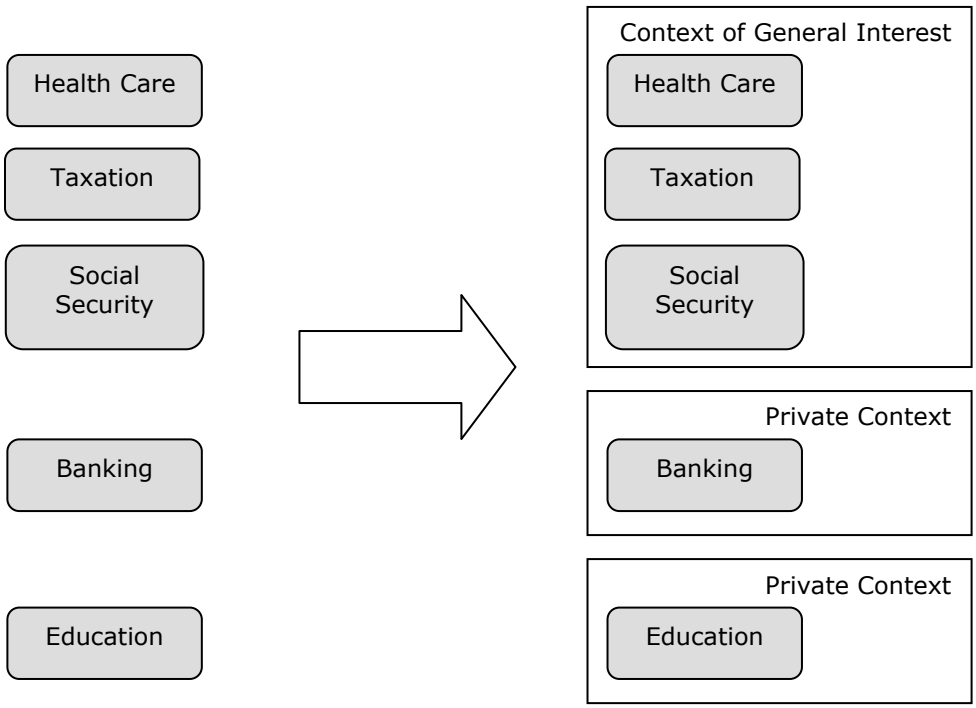

Figure 4: Contexts versus sectors.

The intention of this document is to present a framework that is compatible with the vision of all Member States. With the concepts presented here it is now possible to reason about the interaction between eGovernment administrations at an international level. One member state considers another member state as a sector in a particular context.

Each member state is responsible for the regulation of the existence and use of context-specific identifiers for its citizens on its territory. Accordingly one member state cannot prevent another Member State to issue context-specific identifiers for its citizens within a particular context where this may be forbidden in the first.

5. Swinging between different administrations

In the previous section we have discussed some of the basic concepts in identity management and made the link between eGovernment and identity management. We will now have a closer look at the complex structure of Identity Management in the European eGovernment landscape and discuss some key enablers.

5.1 Plane-view on administrations

In an attempt to expand our notions about eGovernment identity management to multiple nations interacting and communicating with each other we will now look at the different levels in eGovernment and the possible interactions between administrations.

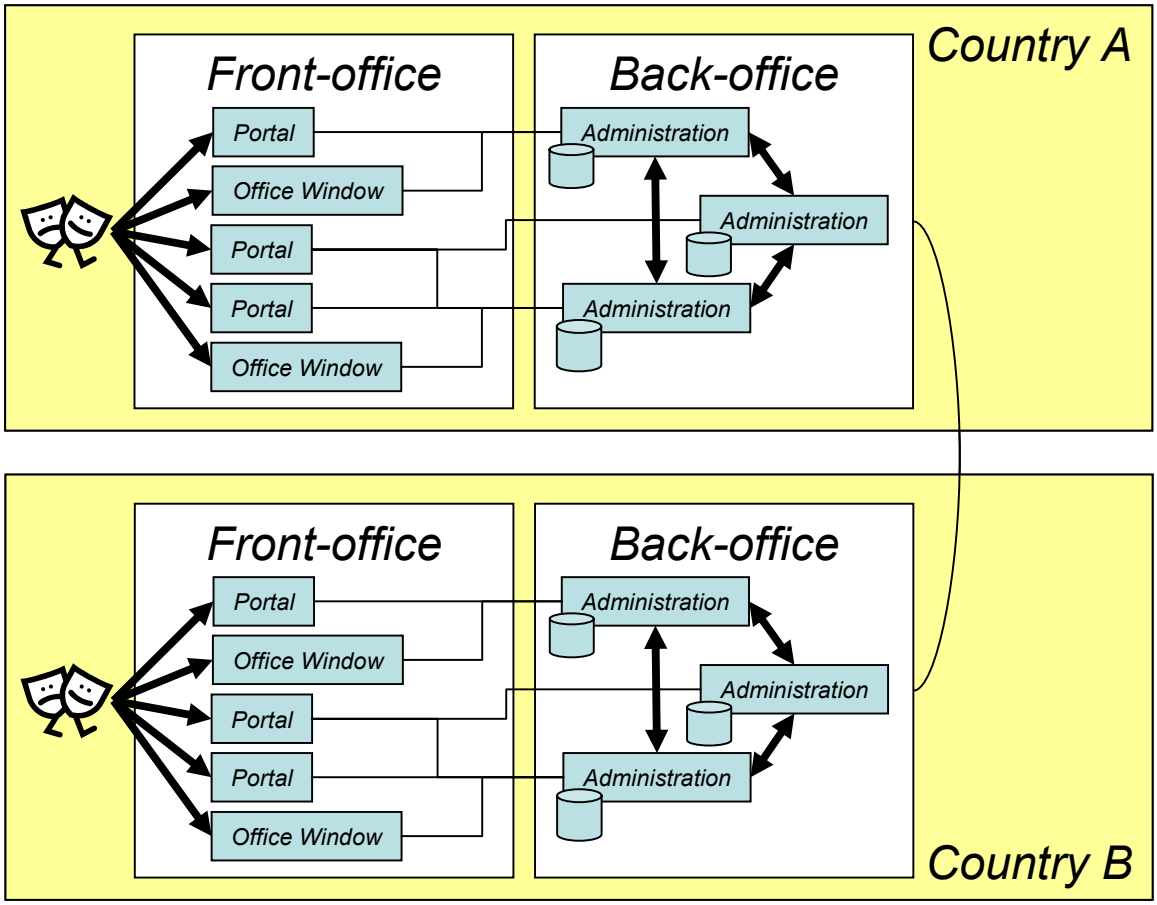

Figure 5: eGovernment information exchange.

When Member States communicate, their administrations may talk to each other directly or information may be exchanged via some kind of mediating service at European level. How this happens is irrelevant, we should rather look at the different levels, sectors and contexts involved in this communication.

Of course the citizen should also be taken into account and more in particular its mobility should be supported by the different national infrastructures, possibly by some sort of pan-European generic citizen portal.

5.1.1 *Different levels of eGovernment*

Typically three levels in eGovernment are defined: local, regional and national. Often pan-European or international is added as an extra one. Figure 5 illustrates the possible interactions between government administrations at different levels.

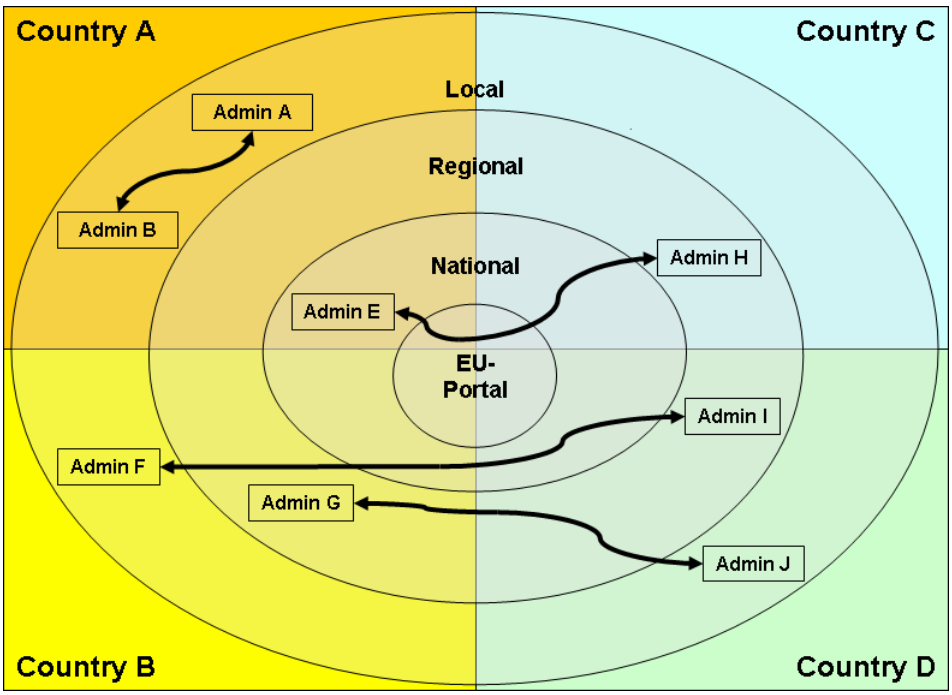

Figure 6: eGovernment cluster view.

5.1.2 *Travelling through the eGovernment planes*

Information exchange between two administrations throughout the different levels can occur in the following ways: they either communicate directly or they communicate via some kind of mediating service. When they do not communicate directly it depends on the country's policies and regulation to see how high, to what level, the communication goes. Note that the regional and national level are not always that strictly separated.

There are however many more possibilities to combine two administrations:

- Vertically: they are at the same level or not, e.g., two municipalities talking to each other are at the same (local) level;
- Horizontally: they are in the same geographical bounds or not, e.g., two administration in the same country;
- A combination of the above.

5.1.3 *Cross-context travelling*

Another complication that occurs is that administrations need to exchange information coming from different contexts. This situation is not typical for European eGovernment and was already discussed in the section on the swing between eGovernment and IDM. However, it complicates the situation, even more than on a national level, because of the differences between Member States concerning the use of identifiers and semantics. The consequences of this will be discussed in the next section.

5.2 Implications of a pan-European eIDM infrastructure

In this section we will look at the consequences of expanding the eGovernment IDM model to the pan-European level.

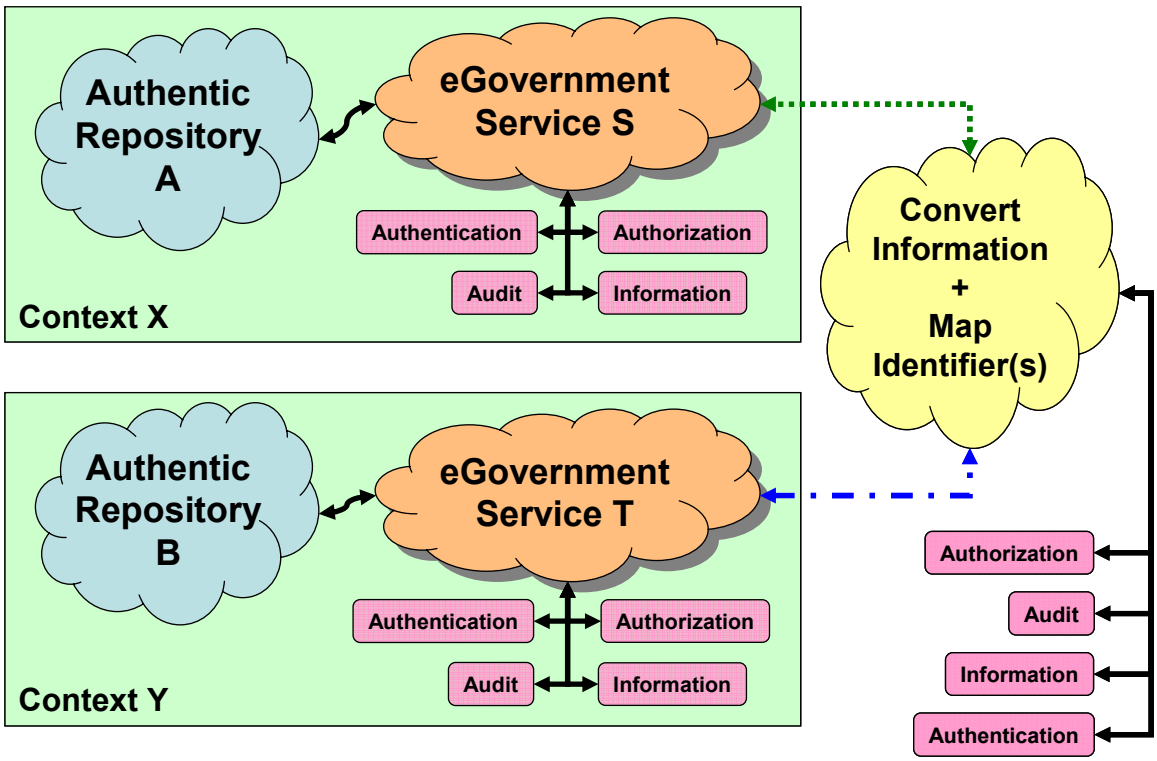

Figure 7: Cross-context information exchange.

5.2.1 *Semantic interoperability and identifier mapping*

Basically the European Identity Management problem is an interoperability problem. On a European level context-specific information is exchanged from on sector to another, most likely from one country to another. The personal information that gets exchanged, usually has a type and a value, e.g., when communicating someone's birth date, the type would be 'date' and the value would be the actual date. If administrations do not use the same conventions (time zone, meaning behind concepts…), they cannot communicate correctly. A simple example is the different numeric notation for dates in countries where the month is written before the day and vice versa, e.g., the 2nd of January 2006 could be written as 02/01/06 or 01/02/06. Therefore there is a very strong relation between identity management and semantic interoperability.

Besides the correct interpretation of information, it also needs to be uniquely identified. Whenever information is exchanged between different contexts a conversion of information and a mapping of identifiers are required. Recall that all sectors in one context share the same identifier and that the identifier should not be shared among context.

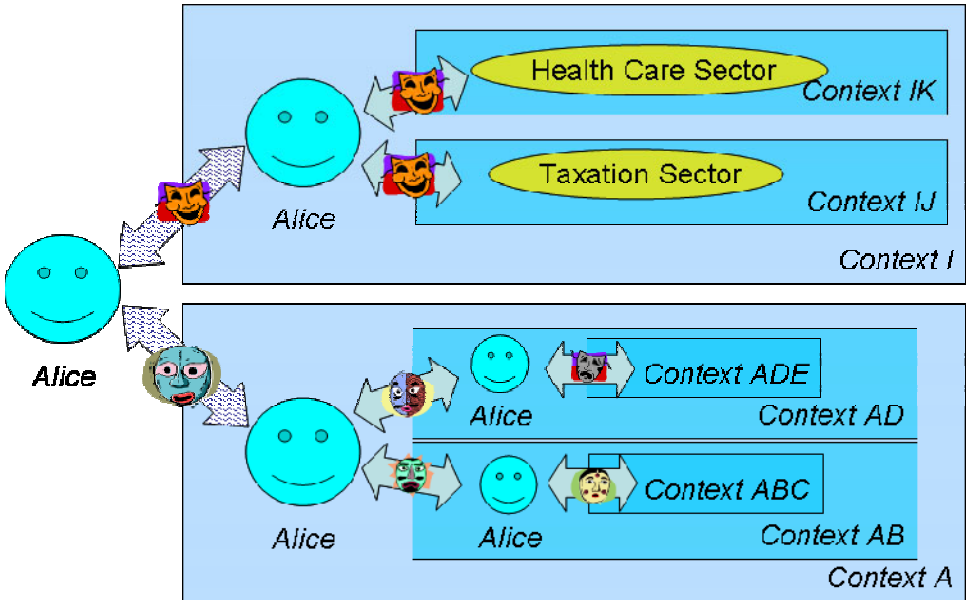

Figure 8: Using context-specific identifiers.

Figure 8 illustrates the use of context-specific identifiers. Note the possible nesting of contexts. In order to exchange information between contexts, a conversion and identifier mapping is performed by a trusted party which is available for each context. It is up to the Member States to decide who this trusted party is going to be. A trusted party at a European level is not excluded but it is questionable whether the Member States will fully trust this third party.

5.2.2 *Federated authentication*

Communicating administrations need to be able to talk about the same concepts (semantic interoperability) and about the same entity (identifier mapping). However there is more. So far we have only considered a passive entity about which information was exchanged. We also need to consider the other facilities of eGovernment services as well: authentication, authorization, information sharing, auditing, etc. An entity willing to act or use an eGovernment service needs to authenticate itself before it is authorized to provide or use eGovernment services. Furthermore all actions should be logged to be able to detect violations to the policy of use.

A pan-European eIDM infrastructure obviously operates in a federation model. There is no need to register a citizen or user in a foreign system, when, for example, that citizen goes abroad for work and wants to make use of the services offered in that country. Instead that country should make use of the identifying solutions of the home country of the citizen. This is federation of authentication: another member state asserts that the identity of the entity is as claimed (cf. the broader term identity federation).

To be usable it is required that solutions in all Member States are considered to be equally secure and correct. However, to achieve this some authentication levels need to be well defined as not every application demands the same level of security. Limited roaming of authentication will also help to avoid abuses, e.g., trying to apply for benefits in more than 1 country.

The model can be taken further than federation of authentication: competences and mandates can be federated. This is already in place at a national level and can as well be applied on EU-level. Unfortunately there are as many different solutions for authorisation as there are solutions for identifiers and user authentication. Further work is needed to define methods for expressing and managing authorizations.

To be complete we mention federation of information as a last example of federation that can be applied on a European level. It is important for an administration to know where the correct information can be found. A service registration or registration of European repositories of authentic data might further improve interoperability and transactions.

5.3 Key enablers

This section lists a few key enablers that should be put in place in all Member States. Once these are present interoperability and mobility of citizens can be achieved.

5.3.1 Authentication means

Once a person is registered she should receive the means to authenticate herself, i.e., to prove that she is who she claims to be, otherwise it would be impossible to get authorized and to execute her rights. The public sector traditionally provides these authentication means in the form of identity documents which are linked to its owner by a visual representation or picture and a signature. In eGovernment these have evolved to their electronic equivalent with the introduction of digital certificates and electronic signatures as a form electronic identity established in the form of smart cards or other tokens.

Depending on the application and the risks involved it might be desired to have a stronger level of authentication. Commonly public sector administrations define different authentication levels based on the security these levels offer.

We define three levels here:

- No authentication,
- Weak authentication,
- Strong authentication.

The first level is where you do not have to authenticate yourself or where you just submit an identifier without having to prove that the number belongs to you. This is used to consult information that is publicly available and the identifier could be, e.g., an e-mail address. The next level provides weak authentication and is often based on username/password combinations. Although it is widely used in a variety of applications, this form is considered to be insecure but very easy to manage. The final level provides strong authentication by using some challenge-response protocol or multifactor authentication and should be used for critical applications.

We believe that this is the minimal categorization of authentication levels that covers any form of authentication, including biometry-enhanced authentication, pseudonyms, etc. For two Member States to interoperate it is required that both support the three levels in one or more ways and that the different solutions are accepted by each other.

5.3.2 Authentic data repositories

As mentioned above authentic data repositories are a key component in eGovernment. Besides information related to authentication and authorisation, there is much more information about citizens that has to be dealt with. After all Identity Management is management of information and eGovernment cannot be efficient without proper information repositories guaranteeing the availability of correct information. Particularly authorisation-specific data should be correct at all times.

5.3.3 Online mechanisms

Online mechanisms mostly deal with technical issues and are a basic requirement for eGovernment, where the goal is to provide fast, mobile and ubiquitous services. These mechanisms are quite straightforward and are automatically being implemented with the conversion of administration from the paper world to an online system.

An overview of online mechanism is given in figure 9.

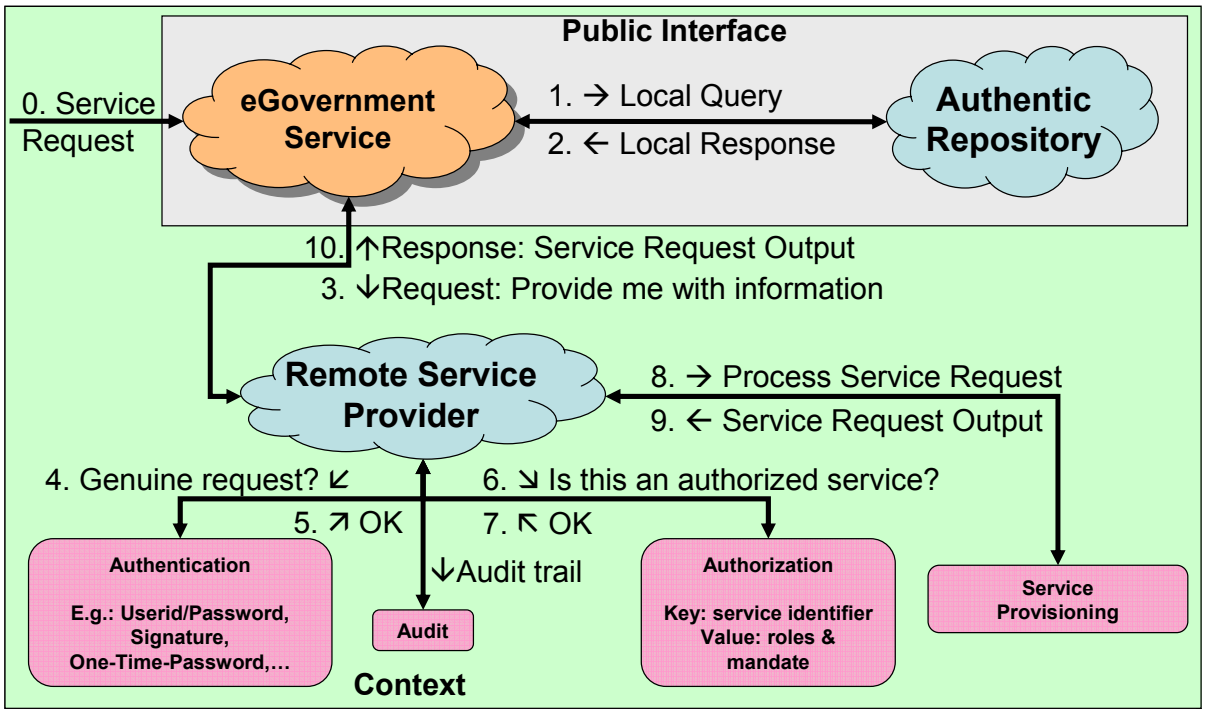

Figure 9: Online mechanisms for eGovernment IDM.

6. eID Roadmap Recommendations

To conclude and to summarize the principles explained in this document we define a set of recommendations that Member States should adhere in order to come to an efficient and interoperable pan-European eIDM infrastructure.

1. Each member state should be able to identify the persons, natural and legal, on its territory. It should therefore make consistent use of context-specific identifiers as explained in this document so that proper identifier mapping is possible when exchanging information across contexts.
2. Each member state should issue the means to each entity to authenticate itself electronically. An entity has the ability to act and to make use of the offered services.
3. Each member state should register the competences of the identified entities on its territory.
4. Each member state should register mandates of a natural person regarding other persons.
5. Each member state should support online validation mechanisms of identities, competences and mandates. This is required to enable the federation in the model.
6. High-level agreements between Member States on a dictionary with compatible concepts should guarantee conceptual interoperability.

Note that a Member states' individual legal or organizational preferences can always be respected by viewing an alien member state as a different sector within a particular context.

Prepared by:

The **Modinis**^{IDM} Study Team under the Service Contract number 29042, from

DG INFSO, EUROPEAN COMMISSION

For further information about the eGovernment Unit

European Commission
Information Society and Media Directorate-General
eGovernment Unit

Tel (32-2) 299 02 45
Fax (32-2) 299 41 14

E-mail EC-egovernment-research@cec.eu.int
Website http://europa.eu.int/egovernment_research

---

eGovernment