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

Modinis Study on Identity Management in eGovernment

Identity Management Issue Report

Deliverable: D.3.9
Identity Management Issue Interim Report II1

Paper copy formally delivered on
6 June 2006

eGovernment Unit
DG Information Society and Media
European Commission

K.U.Leuven, Belgium
Lawfort, Belgium
A-SIT, Austria

Table of contents

modinis^{IDM} **Identity Management Issue Report** **3**

1. Introduction **4**
1.1 Study Planning 4
1.2 Background of the paper: the 2nd and 3rd modinis^{IDM} Workshops 5

2. Identified difficulties **6**
2.1 Technical difficulties 7
2.1.1 Multitude of standards and a lack of a commonly accepted standard 7
2.1.2 Temporary character of most solutions 7
2.1.3 Lack of universal middleware between the many existing IDM systems 8
2.1.4 Management of authorisations 8
2.1.5 Mapping of partial identities in cross border transactions 9
2.1.6 Free choice of tokens 9
2.2 Legal difficulties 10
2.2.1 The availability of unique identifiers 10
2.2.2 Mismatch between technical possibilities and legal frameworks 10
2.2.3 Diversity of legal frameworks versus the need for technical interoperability 11
2.2.4 European competence with regards to IDM systems 11
2.2.5 Different emphasis on privacy related questions 12
2.2.6 Federation and legal framework 13
2.3 Organisational difficulties 14
2.3.1 Multitude of digital identities 14
2.3.2 Reliability and trust 14
2.3.3 The issue of delegation/representation 15
2.3.4 Lack of a common terminology 15
2.3.5 Tendency towards conservation of existing solutions 16
2.3.6 Conflict between technical choices and socio-cultural considerations 16
2.3.7 Public perception and acceptability of new solutions 16

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

modinis*IDM* Identity Management Issue Report

Out of MODINIS a project to identify good practice projects on eGovernment has been contracted by the European Commission. As one of three lots, the modinis*IDM* study will identify good practice projects on identity management and aim 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.

This document is the first coordinated and public document drafted by the modinis*IDM* study team describing the basic difficulties and barriers in creating a pan-European eGovernment IDM infrastructure that would allow existing national and/or regional IDM system to interoperate.

The document was last updated on 5 May 2006. A final iteration of the document is scheduled to be published in February 2007. The most up to date version of the document – as well as any other modinis*IDM* study output – will always be made available through the project website (https://www.cosic.esat.kuleuven.ac.be/modinis-idm). This information will be continuously updated as new information becomes available to the project team.

1. Introduction

1.1 Study Planning

One of the key aspects of the modinis^{IDM} study is the correct identification of the problems of creating a pan-European IDM infrastructure.

This information is of great importance in delineating the modinis^{IDM} study's research activities, which entail three distinct phases:

- *Phase I: Information collection*

The first phase consists of the identification of existing major European IDM systems, along with their scope, advantages, weaknesses, and lessons learned. This first phase resulted in D.3.5 – the European IDM Initiative Report, which set the parameters for the two following phases, since the current status of eGovernment IDM solutions is the basic input on top of which a solution framework is to be constructed. As indicated above, the contents of all reports are continuously updated through the modinis^{IDM} study website, and the final outcome will be summarised in a second iteration of this deliverable, to be published in February 2007.

- *Phase II: Analysis of problems and barriers to IDM interoperability*

A second phase, following the creation of the present overview of the status of IDM solutions in the Member States, is be the identification of the problems and barriers to making these solutions interoperable. If phase I results in the description of the situation at the time of the modinis^{IDM} study, then phase II results in a definition of the difficulties to be resolved by the modinis^{IDM} study's conceptual framework. The result of this second phase is the present paper (D.3.9 and, in a final iteration, D.3.10) describing and analysing the barriers to interoperability.

It should be noted that the lack of a suitable homogeneous, unambiguous and consistent terminology for discussing interoperability problems was the first problem identified by the modinis^{IDM} study. This specific realisation resulted in the creation of the modinis^{IDM} Terminology Paper, which has been presented through the modinis^{IDM} study website.

- *Phase III: Proposal of a conceptual framework for European IDM interoperability*

In the third and final phase, the modinis^{IDM} study envisages to present a conceptual framework, which would allow the existing solutions to exchange information, thus creating an interoperable pan-European IDM infrastructure. The proposal will keep into account the work already done by related initiatives both on a European and an international scale, in particular such initiatives as the Liberty Alliance and the Guide Project. The result of this final phase, which is also the final outcome of the modinis^{IDM} study, will be integrated into the Yearly Reports (D.3.19 and, in a final iteration, D.3.20).

1.2 Background of the paper: the 2nd and 3rd modinis^{IDM} Workshops

The second workshop of the modinis^{IDM} study, organised on 15 November 2005 in Leuven, Belgium, had a very practical focus, examining the difficulties to be overcome in establishing and managing pan-European IDM systems. While public sector representatives were also invited to this workshop, other invitees also included representatives from industries as well as academics and project leaders, in order to ensure a balanced outlook on the topic.

The expected outcome of this workshop was an overview of potential interoperability solutions and of the different positions that the distinct stakeholders take. While the workshop's findings need not necessarily dictate the study's findings, this information is none the less essential to establish the viability of potential directions that pan-European IDM could evolve in.

A full report of the Workshop was drafted as deliverable D.3.12, and has been made available through the modinis^{IDM} study website (https://www.cosic.esat.kuleuven.be/modinis-idm/).

The first version of the present document was drafted as a brief four-page partial summary of the findings of this workshop report, attempting to catalogue a number of common problems in implementing cross-border IDM solutions in the eGovernment sector. It was first presented to the public as a short PowerPoint presentation during the third modinis^{IDM} study Workshop of 9 February 2006 in Vienna, Austria. This presentation is available through the modinis^{IDM} study website.

The presentation was generally well received, and many attendants inquired on the possibility of drafting a full-text report, integrating the comments made during the presentation into the four-page summary, in order to create a general and more thorough overview. The result is the current paper.

In it, we will identify the most prominent problems encountered in the course of the modinis^{IDM} study, along with a number of practical examples from the examined Member States. This will be the basis of further analysis work, in particular when examining the efficacy of potential solutions.
When referring to practical examples, the paper will use the following format to refer to sections of D.3.5 – the European IDM Initiative Report: (*Ref: [Name] country report, [section number], [page number]).*

The authors of course welcome any comments or input for this paper. They can be sent directly to the modinis^{IDM} study team at modinis-idm@esat.kuleuven.be.

2. Identified difficulties

In the course of the modinis^{IDM} study, a number of common difficulties were often mentioned in any eGovernment project confronted with cross border aspects of IDM. As a matter of focus, the modinis^{IDM} study team decided to try and bundle these concerns into the standard types below, in order to be able to more easily assess the suitability of any proposed future cross border IDM solution. After all, any solution would at a minimum need to be able to cope with the issues outlined below.

The result could also be considered a form of good practice identification and dissemination. After all, the difficulties presented below are not exclusive to the design of pan-European IDM systems, but often apply to any large scale IDM system that is required to function across multiple sectors. As such, anyone involved in the design of such systems may also find some use for the paper, by using it as a repository of potential difficulties to be taken into account during the design phase.

The difficulties outlined below have been structured into three categories: technical, legal and organisational difficulties. Within these sections, the problems have not been organised into a specific order (i.e. problems mentioned first are not necessarily the most serious or difficult to overcome, as such an order depends on the exact scope and function of the system, and can not be formulated abstractly).

It should be noted that these three categories are obviously not mutually exclusive, as most if not all of the difficulties identified will usually span several categories. As a provisional example, consider the issue of managing authorities:

- From an organisational perspective, the system designer needs to decide which authorisations are required in the system, who may give and hold them, and what they mean;
- From a technical perspective, the system designer needs to decide how to model this into his system, e.g. by creating a central authorisations database, or through referrals to related trusted systems; as well as who may manage the authorisations (e.g. the technical aspects of issuing/revoking authorisations) or how their validity should be checked before an authorisation could be exercised.
- From a legal perspective, the system designer needs to be aware of the legal requirements for authorisation (does it require a written contract, signatures, acceptance of the receiver, …) as well as cross-border aspects (i.e. is the authorisation valid in the country where it is given, where it is received, where it is exercised,…)

Despite this inherent ambiguity and strictly for reasons of clarity, each problem has been placed only into the category that was generally believed to be predominant, based on the feedback received by the modinis^{IDM} study team and its own analysis activities.

2.1 Technical difficulties

2.1.1 Multitude of standards and a lack of a commonly accepted standard

A commonly heard remark is that for any given technical difficulty in the IDM sector the problem is not the unavailability of technical solutions, but rather an overabundance of possible solutions. Overlooking legal, cultural and socio-political perspectives, from a strictly technical point of view most hurdles to interoperable IDM systems would be fairly easy to overcome.

However, when existing IDM systems need to be interconnected in order to be able to exchange information, system engineers are often confronted with the difficulty that different organisations have chosen different solutions to the same problems. Even basic technical and infrastructural choices (e.g. data formats, communication protocols, security measures, acceptable tokens,…) can vary quite widely, all relying on different standardised solutions (e.g. compare the Irish approach to the Austrian approach; *Ref: Austrian country report, 1.2.2.1., p.8; and the Irish country report, 1.2.2.12., p.40)*. While each individual system may work perfectly, it can be extremely challenging to connect systems relying on different and possibly incompatible standards.

The main technical challenge in implementing an interoperable pan-European solution is in devising a framework that respects the existence of different choices, and allows them to co-exist without impairing the requirement of being able to exchange information. The eventual ambition of interoperability is not to eliminate difference, but to allow them to co-exist. This is a first indication that a federated solution may be necessary on European level.

2.1.2 Temporary character of most solutions

An inherent technical limitation in IDM solutions is than any choice made by any administration is by necessity medium-term, implying that no major changes can be made in the short run, and that no system can ever be considered completely stable.

The fact that (working) solutions cannot be expected to undergo significant changes in the short run stems from the fact that any relatively large scale IDM infrastructure typically requires a significant investment, both financial and in effort, of its organiser. As a consequence, there is a certain reticence to make any changes that would effectively nullify part of this investment, even if the final result could be an improvement over the original. For this reason, smaller updates (that have no significant impact on the general workings of the system) are possible in the short run, whereas larger shifts in technology or strategy are not.

In the eGovernment sector, this characteristic is even more pressing, for a multitude of reasons. First of all, political responsibility for lost investments is often a significant concern which can impede major infrastructural changes. Secondly, public administrations are required to provide complete continuity of service. As a consequence, public services can ill afford interruptions due to technical alterations. Finally, the scale of many eGovernment IDM systems is often significantly larger than that of private sector equivalents, making migrations to other solutions a more complicated affair.

Inversely, technical choices should also never be considered entirely permanent and unchangeable. Changes in standards, communication protocols and security measures ensure that any system will eventually need to be updated to meet current requirements, and public sector services are no exception to this rule. Additionally, political shifts in governments can also result in policy shifts in IDM systems, so that technical preferences are also susceptible to such external influences, at least on a long enough timeline.

As a result, technical choices in eGovernment IDM systems should be considered medium-term: while essential decisions are likely to remain in place for a longer period of time, standards will continue to evolve. This is a complicating factor to the technical realisation of a framework of interoperability, since this frameworks needs to be able to cope with changes in individual (sometimes fairly local and/or sector-specific) systems. As an example of an IDM system that is presently undergoing strong evolution, without abandoning existing solutions, see e.g. the Dutch approach; *Ref: Dutch country report, 1.2.2.18., p.54).*

2.1.3 Lack of universal middleware between the many existing IDM systems

"Middleware" in the current context can be taken to mean any software layer (i.e. possibly comprising multiple individual and interacting software components) which act as an intermediary between any IDM token and an IDM system that is intended to verify the attributes contained in the token.

Many Member States have working IDM solutions deployed and available to the general public. Often these rely on a specific token (in this case often a smart card), but many other solutions are available (see e.g. the Maltese approach, which includes mobile technology; *Ref: Maltese country report, 1.2.2.17., p.51).* In almost any of these cases, the technology (including the middleware) has been optimised for internal use, i.e. optimised to ensure that the system works adequately when the expected token is presented to the expected middleware in order to access a service that expects the information it requires in the information presented through the middleware.

However, the multitude of such systems and the underlying middleware impedes cross-border interoperability, due to the lack of a universal middleware which would allow these systems to accept each other's tokens/credentials.

2.1.4 Management of authorisations

Virtually all eGovernment services depend on IDM systems to store authorisation information. In some cases these systems only contain authorisations regarding public officials (e.g. the authorisation to access specific confidential information, to confer social security benefits, to withdraw driver's licences etc.) while in other cases private persons are included in such systems (e.g. authorisations to tax consultants to file another person's income taxes, authorisations to represent a minor or a mentally disabled person, etc.). The creation and maintenance of databases which can adequately represent such authorisations can become a very daunting charge.

In public administrations this difficulty is significantly greater due to the scale in which authorisations can be given. Public administrations can span thousands of persons, whose authorisations can be increased or revoked at any time. When authorisation services are made available to private persons, the database is sometimes required to span millions of subjects. This is e.g. the case for the Belgian income tax report system TaxOnWeb, where citizens may authorise their tax consultant of preference to submit their income report. Thus, the scope of this system ranges in the millions of citizens and enterprises (see also the UK Gateway approach to mandates; *Ref: UK country report, 1.2.2.25., p.73).*

Furthermore, in an eGovernment context it is particularly important to accurately define who may give and accept mandates, which authorisations these mandates entail, and how they can be managed and revoked. Errors in public sector systems are often even less acceptable than in the private sector, as information held by the government is often considered official and therefore correct by default, so that rectifications in case of misuse can be difficult, costly and time consuming.

When cross-border functionality becomes a key consideration, it is all the more difficult to define which authorisations are internationally acceptable. The aforementioned example of revocation of driver's licences illustrates this fittingly: while it is usually sufficiently clear who is authorised to revoke driver's licences within any given country's national borders, this is significantly more difficult when a public official abroad claims to have the same authority. Modelling such requirements in any public sector environment is one of the more difficult challenges to the development of a pan-European interoperability framework.

2.1.5 *Mapping of partial identities in cross border transactions*

A fundamental technical question when implementing cross-border interoperability is how to map/convert an existing foreign partial identity to/into a corresponding partial identity in another Member State. After all, many eGovernment services require the service provider to have a given set of basic information about the service requester available (name, address, age, employment information, health information,…). However, Member States are free to collect and organise such information in any way they see fit, and there are no commonly accepted standards to how such personal data should be organised. As a consequence, a foreign public service provider may experience difficulties in obtaining certain information that is required under the laws of its own nation, but which may or may not be available in the requester’s home state, or which may be stored in a location/format which is unrecognisable to the systems of the service provider.

When the technical choices made by each Member State differ so fundamentally, the question is raised how information regarding a person/entity could be exchanged? It may be required to elaborate a “meta-data model for e-IDs”, so that individual service providers have a template of information that should at a minimum be available to them, under the same conditions that such information is available regarding their own citizens.

2.1.6 *Free choice of tokens*

Member States are free to implement their eID solution using any token of preference. A large majority of Member States has chosen to offer a smart card solution, or is considering to introduce this (e.g. Austria, Belgium, Finland, France, Spain, UK, Estonia, Italy,…). This is not surprising, considering that many European States (though not all countries in the list above) have traditionally issued paper identity cards to their citizens as a basic tool for entity authentication. Therefore, the choice of a smart card is intuitive to a large number of European citizens.

However, more and more Member States are realising that electronic identities should not be considered synonymous with smart cards. In an electronic context, many other token options (USB stick, certificates on standard PCs, cell phone,…) exist, all of which can potentially increase the accessibility, value and usefulness of the services to the public. As a result, some Member States have chosen to offer multiple options.

A common example of this includes Austria (*Ref: Austrian country report, 1.2.2.1., p.8)*, which has taken a technology neutral approach to eIDs by proposing a specific concept (the Bürgerkarte) rather than a specific concept as the norm for electronic identification. Other nations (e.g. Finland and Malta) are experimenting with using cellphone SIM-cards as eGovernment identification tokens, which offers a certain potential due to the relative ubiquity and general availability of such solutions.

In conclusion, each Member State is essentially free to define the criteria that any solution has to meet, including with respect to security. From an interoperability perspective, and ignoring the middleware issues identified above, the question then becomes if there could/should be a certain baseline that these solutions should meet in order to be acceptable on a pan-European scale, or whether this can be left entirely in the hands of individual Member States.

2.2 Legal difficulties

2.2.1 The availability of unique identifiers

From a purely technical perspective, and ignoring legal limitations and socio-cultural sensitivities, the use of unique identifiers greatly facilitates the design of any IDM system, and (especially) the exchange of data across multiple systems. It facilitates the exchange of data, thus increasing a system's efficiency and decreasing the risk of errors.

However, the concern exists in many countries that such exchanges of information are harmful to an individual's interests, by allowing governments to easily gather data that they should not have access to, or by tying together data that is ostensibly unrelated, thus assembling a complete profile of a user, without any need and without his consensus or even his awareness.

For this reason, the European Member States take greatly different approaches to the use of unique identifiers. Several legal frameworks in the European Union (e.g. Germany) forbid the obligatory assignment of unique identifiers to their citizens. Others (e.g. Belgium) do issue a mandatory identifier to their citizens. Some countries (e.g. Ireland) issue multiple identifiers which differ from service to service without a clear interconnection. Alternatively, there may be a central unique identifier, which is used as a basis to derive other identifiers which are each only used within a specific sector (e.g. Austria). Yet another approach (e.g. taken in the Netherlands) is to provide the citizens with a single identification number which remains constant, although it is referred to by a different name, depending on the sector in which it is used.

There is thus a great variety in national approaches, all of which may be considered valid by its users. In the words of one of our correspondents: "For some people, [a unique identifier] is the comparable to hara-kiri, for other people it is the enabler of a synchronized and cost-efficient e-government". It is worth noting however that the complete and consistent elimination of unique identifiers is a logical impossibility for most eGovernment services (with the exception of services provided anonymously), as most services require its users to identify themselves so that the government can determine their rights and introduce the required changes into their systems.

Therefore, Member States which ban unique identifiers as a matter of principle typically work around this problem by combining a set of non-unique identifiers into a unique identifier (e.g. the unique identifier would become "JohnDoe_DruryLane1_1000CityName_born01011970). This approach seems to have an adverse effect on privacy considerations, as the final result is that the user often reveals a good deal more personal information than might be the case if a content-neutral unique identifier would have been used. Purely from a privacy perspective, the use of sector-limited unique identifiers seems to be the solution of preference.

Regardless of the solutions chosen on a national scale, the use of unique identifiers is typically tightly regulated (e.g. such identifiers can only be used by the issuing public administrations, or only after permission is obtained from the National Data Protection Commissioner). As a consequence, cross-border use of unique identifiers from another country will need to comply with the applicable legal framework.

2.2.2 Mismatch between technical possibilities and legal frameworks

One of the larger (and less often examined) legal difficulties in setting up eGovernment IDM services is the conceptual mismatch between a given technical act and its legal equivalent.

An obvious example is the delegation of an authorisation from one person to another. This can be a fairly simple matter from a technical perspective, but it tends to be noticeably more complicated form a legal perspective. From a technical perspective, it may simply entail inserting certain information into an authorisations database, after which point the mandate holder is technically capable of performing the same actions as the mandate giver.

However, from a legal perspective, the situation can be much muddier. A national law might not only require that a mandate is offered, but also that it is implicitly or explicitly accepted by the receiver before it may be exercised. Additionally, a written document may be required, with or without signatures from the giver and the receiver.

As a consequence, one could imagine a system in which a natural person can authorise another person to represent himself, purely through a series of technical steps, while national law may require a signed contract. If the mandate receiver chooses to act on behalf of the mandate giver, the legal consequences are uncertain. Additionally, the system should be entirely clear on the scope of the mandate. As an example, one might consider the situation where a private person authorises his tax consultant to file his income taxes, only to find a few months later that the latter has not done so. In this case, the mandate must be clear on whether the mandate receiver was mere *authorised* to act on behalf of the giver, or whether he was also *obliged* to do so.

In fact, a similar ambiguity extends to any form of representation. From a legal perspective, many European legal systems allow parents to act as guardians for their underage children by default. However, implementing such a system automatically (especially in a cross-border context and across multiple IDM systems) may not be trivial.

Additionally, many eGovernment services are specifically targeted at legal persons, who obviously and by necessity also need to be represented by a natural person. The question of determining who is legally allowed to represent legal persons is complicated even within a national context, often requiring either one signature or multiple signatures, depending on the type of legal person and the legal act involved. In a cross-border scenario, this question becomes exponentially more complicated.

2.2.3 Diversity of legal frameworks versus the need for technical interoperability

This issue is in fact a logical extension of the problem discussed directly above. Respect for each Member State's legal autonomy, to the extent defined by European law, is a prerequisite for the viability of any IDM solution. This can present difficulties when legal requirements for one activity differ from Member State to Member State, while technical solutions need to be interoperable.

To resume the aforementioned example of delegation: what would occur when the mandate giver's Member State does not require a written contract, whereas the mandate receiver's does? Or to further complicate matters: what if the mandate receiver chooses to exercise the mandate in a third country, where a written document is needed that is signed by both parties and registered with the local administration? The question then becomes which legislation applies.

A great deal of the surrounding discussions can of course be avoided by requiring users to accept usage policies, End User Licence Agreements (EULAs), internal regulations and other means of regulating through convention; but in cross-border transactions the issue then becomes what happens when multiple contradicting EULAs apply, and to which extent such regulations have the power to overrule local law.

In an analogue manner to the technical difficulties, the only feasible solution might be to apply a system of "legal federation", where the system in which the mandate is exercised is simply required to rely on the effectiveness and validity of the mandate in the system in which it was originally registered, regardless of its own legal requirements.

2.2.4 European competence with regards to IDM systems

At a very basic level, the question can be asked whether or not the European Union has any legal authority to undertake any harmonisation activity in the field of IDM? Article 18 of the EC Treaty states that:

> *"1. Every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in this Treaty and by the measures adopted to give it effect.*

> *2. If action by the Community should prove necessary to attain this objective and this Treaty has not provided the necessary powers, the Council may adopt provisions with a view to facilitating the exercise of the rights referred to in paragraph 1. The Council shall act in accordance with the procedure referred to in Article 251.*
> *3. Paragraph 2 shall not apply to provisions on passports, identity cards, residence permits or any other such document or to provisions on social security or social protection."*

As a consequence, the Council is restricted in its possibility to invoke reasons of free circulation of persons to undertake harmonisation initiatives with regard to identity cards or other such documents.

While this should not be read to imply that no IDM harmonisation initiative is possible, it is certainly a significant factor at a time when smart cards are rapidly becoming a de facto standard strategy for electronic authentication. This is another element suggesting that a federated approach is currently a more favourable solution.

None the less, article 18 does not prohibit the development of any standardisation/harmonisation initiatives that Member States could voluntarily subscribe to, nor does it disallow the development of a pan-European IDM infrastructure. After all, neither of these could be considered as a Council intervention concerning "identity cards or other such documents".

2.2.5 Different emphasis on privacy related questions

While the privacy directives have resulted in a large degree of European harmonisation with regards to data protection, Member States still emphasise the importance of privacy in a widely varying manner.

The mere presence and use of ID cards is a suitable illustration of this fact: some Member States consider any obligation to carry an ID card as unacceptable, others have an optional ID card system, while other have made carrying these cards mandatory a long time ago. Similarly, some Member States are considering the inclusion of biometric technologies into their eID cards, whereas others consider this a disproportional invasion of privacy.

The aforementioned use of unique identifiers is another example: some Member States formally forbid such identifiers as a matter of principle (e.g. Germany); other have introduced such identifiers but in principle only allow them to be used for public administration purposes (e.g. Belgium), whereas others (most notably the Scandinavian countries, see e.g. the Swedish approach; *Ref: Swedish country report, 1.2.2.24., p.69)*) have a long standing tradition of allowing their eID systems to be used for private sector initiatives (most notably eBanking applications). In Estonia, the national eID card can be used for a wide variety of services, including traditional eGovernment services, eBanking, public transportation and even eVoting, despite the fact that the infrastructure is largely privately held (*Ref: Estonian country report, 1.2.2.6., p.23)*.

Despite this variety in approaches to privacy, none of these systems intrinsically violates the requirements of European privacy regulations. However, it is clear that national policies are a reflection of differing socio-cultural perceptions of the citizen's right to privacy, and of the nation's governmental structural and attitude towards public/private partnerships where sensitive data is involved. National Data Protection Commissioners play a central role in this regard, as they are typically required to advise national governments concerning the compatibility of any planned or considered IDM framework with European privacy regulations.

These different national sensitivities should be taken into account when proposing solutions for interoperability, as the final result is that a solution which functions perfectly in one specific country is not necessarily suitable or even feasible in another. Thus, even best practices are not necessarily transposable between countries.

2.2.6 *Federation and legal framework*

A federated solution is an often suggested possibility for solving many of the technical and organisational difficulties inherent to the development of a cross border IDM solution. From a technical and organisational perspective, this certainly would appear to be a suitable solution.

However, this also requires a solid legal substructure to defuse possible risks. After all, the element of trust is a core aspect of a federated approach: IDM systems which are grouped together in a so-called circle of trust are required to rely on the correctness and accuracy of the information provided to them by other members of the circle.

From a legal perspective, the concept of “trust” requires exact and binding legal agreements, in particular with regard to reliability and privacy. After all, any member of the circle must be sure that the other members have implemented suitable procedures for the issuing and management of electronic identities. This is even more true where public services are concerned, given the more serious potential consequences of errors in such data.

These requirements must meet with European standards (in particular the privacy directives), and yet must allow Member States sufficient autonomy to determine their national policies. Within the framework of the Liberty Alliance, a great deal of research has already been done with regard to the legal requirements for the compliance of a circle of trust infrastructure (see e.g. http://www.projectliberty.org/resources/guidelines.php), although it remains to be examined if these guidelines strike the appropriate balance between uniformity and national autonomy, and whether the provided solutions are suitable in a public sector undertaking, especially considering the large scale on which a pan-European solution would be required to operate.

2.3 Organisational difficulties

2.3.1 Multitude of digital identities

In the modern information society, virtually all European citizens are obliged to manage multiple digital identities covering every aspect of their life. This is equally true in the public sector, where even on a national level any given citizen may have many eIDs, for very valid reasons. For example both the Spanish and French governments fairly strongly emphasise the availability of decentralised IDM services, respectively through the Digital Cities and the Carte de la Vie Quotidienne programmes (see *Ref: Spanish country report, 1.2.2.23., p.67; and the French country report, 1.2.2.8, 29)*, allowing local governments to offer services at the level which is best suited for the target user group. This can certainly result in an increase of user convenience, and improve the general usage experience.

However, there is also an inherent risk to offering a multitude of digital identities. Governments must walk a thin line between offering too many identities, which may confuse the user and discourage use, or offering too little (or even a single identity), which could pose a security/privacy risk. As noted above, some Member States have opted for sector bound identification solutions, either in name (e.g. The Netherlands, which renames its unique identifier depending on the sector), or in reality (e.g. Austria, which actually has different identifiers for each citizen depending on the sector).

In the second Modinis^{IDM} workshop of 15 November 2005, Dr. Martin Meintz presented three theoretical constructs for eGovernment related eIDs in this respect:

- Type A: one Person - one eID
- Type B: one Person - several managed eIDs
- Type C: one Person - several independent eIDs

As a matter of basic modelling, it was suggested that the European level will likely have to deal with type C, whereas Member States might solely use Type A and B.

2.3.2 Reliability and trust

As has been mentioned above, any solution that requires IDM systems to interconnect and exchange data (including, if not particularly in a federated model), is strongly dependant on the reliability and trustworthiness of every single data provider. However, there currently does not appear to be any manner to objectively grade this reliability and trustworthiness.

This is an important issue, as a service provider needs to be able to assess the procedures used for the issuance and management of credentials, in order to determine whether the outcome of an entity authentication procedure is sufficiently reliable to allow a user access to its services. This is even more true when eIDs are issued by private institutions, such as banks; only to be used thereafter in public sector services.

As mentioned above, federation can provide a manageable solution to this issue, provided that a suitable and sufficient regulatory framework can be established in which each participating party vouches for the reliability of its services and data, and accepts liability in case of failure to meet its obligations.

Furthermore, it would appear that not all services require the same strength of user authentication, as not all services are equally prone to abuse. For this reason, it has been proposed to introduce a tiered system of authentication, in which several distinct authentication levels would be proposed. For each of these levels, a set of requirements would have to be met, so that a hierarchy of reliability exists between these levels. Each Member State would then have the option of implementing the appropriate national procedures for each specified authentication level, in order to satisfy the requirements imposed on that particular level.

This would facilitate a federated approach, as Member States who are providing a service to a non-national would no longer have to concern themselves with the particular procedures used abroad in the requesting party's country, but would be able to rely on the fact that the data provider ensures that the credentials presented during an authentication procedure were managed according to a certain required level, which the service provider can set at the desired level.

2.3.3 *The issue of delegation/representation*

As has been mentioned above, many eGovernment services allow a user to delegate certain authorisations to another user. Managing such systems can be a difficult task, as it needs to be made perfectly clear which activities are covered by the delegation. This specific problem has already been outlined above.

Furthermore, adequate mandate management/revocation policies need to be installed. Such procedures must be made sufficiently transparent to allow services providers to verify whether any issued eID is indeed still valid at the time of attempted use. In addition, service providers must also be able to notify an identity provider that an identity could be compromised, so that the identity provider may take the appropriate action. From a pan-European perspective, this would likely necessitate the creation of national contact points where compromised identities issued in that country could be reported.

2.3.4 *Lack of a common terminology*

During the first Modinis^{IDM} Workshop of 4 May 2005 in Leuven, Belgium, one of the first problems identified as a barrier to the development of interoperable IDM systems in eGovernment was the lack of a common conceptual framework. This was identified by the Modinis^{IDM} Study Team as a key issue that needs to be resolved; a position which was subsequently supported by the eEurope eGovernment subgroup – Ad hoc group on Identification and Authentication during its session in Brussels on 30 June 2005.

Part of the conceptual framework – which includes every aspect of the IDM infrastructure – is made up of the terminological framework: the definitions of all concepts of the infrastructure. The lack of a common understanding of even the most prevalent IDM notions constitutes a meta-problem which obstructs a constructive dialogue on the problem of interoperable identity management as a whole. There is no common agreement on the definition of essential concepts such as identity, entity, attribute, delegation, or even entity authentication and identity management.

The current definitions vary widely, since they reflect a complete different point of view on such issues as the use of unique identifiers, who should manage identities and the scope of the definitions. As a practical example, it is nearly impossible to discuss privacy protection questions when there is no consensus about the attributes that define an entity, or if an entity can be something other than a natural person (e.g., a legal person, or even an object such as a computer system, where privacy concerns would not apply).

As a first step to resolving this problem, the Modinis^{IDM} Study Team drafted a terminology paper, which deals with this issue by attempting to propose a series of neutral and internally consistent definitions of such IDM concepts, thus creating eGovernment IDM ontology. The definitions are based on the preparatory work done through other European projects and initiatives (such as FIDIS, PRIME and GUIDE), amended and completed by inputs from several eGovernment initiatives (such as the aforementioned subgroup, IDABC and of course the Modinis^{IDM} Study itself).

A first draft of this paper has been made available to the public in September 2005. The first version has since undergone several updates, and is currently available through the Modinis^{IDM}

project website. It is important to note that this is a consultation paper, intended to draw criticism and generate constructive feedback. As such, it should be considered provisional in its entirety.

2.3.5 *Tendency towards conservation of existing solutions*

As outlined above, national governments will naturally be inclined to defend local choices, as they represent (usually large) national investments which need to be recuperated. As a consequence, there is a certain reticence to make any changes that would effectively nullify part of this investment, even if the final result could be an improvement over the original. For this reason, major revisions of existing solutions (either technically, legally or policy wise) are typically not feasible in the short term.

The necessity of continuity of public service is also a factor in this tendency, as is the typically larger than average scale of many eGovernment IDM systems. Finally, the fact that the original planning of many IDM systems tends to be too optimistic can also be a factor, as administrations are not typically inclined to restart procedures which have proven to be more troublesome than expected in the past.

2.3.6 *Conflict between technical choices and socio-cultural considerations*

When designing a public sector IDM system, a number of difficult choices need to be made, where a specific technical solution (e.g. biometrics, contactless cards) may provide a specific benefit (e.g. increased security/efficiency/ease of use), but where the introduction of such solutions contrasts with the public's perceptions or expectations of how eGovernment should impact their lives.

Not unlike the privacy considerations outlined above, the result is that there is sometimes a strong backlash against ideas that have some technical and organisational merit, for reasons which are mostly socio-cultural.

An example of this can be witnessed in the public responses to the proposed introduction of biometric eID cards (most notably through the inclusion of fingerprints) in the UK, France and Spain. The public reaction has been strongest in the UK, where no tradition of mandatory identity cards exists, whereas debates have also been heated in France and Spain, but with a noticeably smaller public outcry. While technical factors certainly also play their part (the technical implementations in the three countries and the planned use of the biometric features are fairly different), the difference in response can also be traced back to the traditional attitude towards government mandated identification devices in each of these countries.

Any European solution must therefore take into account the divergent national sensitivities to such issues, which can impede the implementation that may be technically well-suited, but which is none the less entirely unacceptable on a European scale.

2.3.7 *Public perception and acceptability of new solutions*

Finally, one of the most critical factors in determining the public acceptance of an IDM system is that every eID solution must offer attractive applications to its users. However, in many Member States this has not been the case: eID solutions often present attractive possibilities to their users in principle, but the surrounding framework was often rolled out before any attractive applications were made available to the public. Often this results in the eID holders perceiving the eID as a new intrusion or burden, rather than as a solution enabler. In order to encourage social acceptance of any eID solution, the public must be presented with a clear and present benefit to the holder.

An example of good practice in this respect is the Irish approach, where each Irish citizen receives an electronic identifier at birth, which is then immediately used to facilitate the provision of social benefits to the parents. As a consequence, many Irish citizens are immediately confronted with a possible positive application of the Irish eID solution (*Ref: Irish country report, 1.2.2.12., p.40)*.

Similarly, the Estonian government has also been quick to roll out applications for its eID card, including eVoting and the automated payment of public transportation (*Ref: Estonian country report, 1.2.2.6., p.23)*.

In a cross-border context, this would appear to be a smaller consideration, as a European approach would be unlikely to require the deployment of new tokens, but rather depend on federation between Member States, thus extending the use of existing national tokens.

Prepared by:

The Modinis IDM Study Team
B-3000 Leuven, Belgium

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

Lead contractor:
K.U.Leuven Research & Development, Belgium
Project manager: prof. Bart Preneel

http://www.esat.kuleuven.be/cosic

Subproject manager: prof. Jos Dumortier

http://www.icri.be

Subcontractor:

Secure Information Technology Center, Austria (A-SIT)
Director: prof. Reinhard Posch

http://www.a-sit.at

Subcontractor:

Lawfort – ICT Law Department, Belgium
Head: prof. Jos Dumortier

http://www.lawfort.be

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 europa.eu.int/eGovernment_research

eGovernment