A Roadmap for a pan-European eIDM Framework by 2010

- v1.0 –

In today's world, most interactions among citizens, businesses and administrations revolve around the concept of 'identity'. Governments and businesses face the challenge of identifying citizens, customers and users reliably and accurately on a daily basis. Identity plays a central role in processes as varied as paying for an online order, getting a mortgage, and claiming unemployment benefits.

The modernisation and streamlining of businesses processes in the public sector offers the potential of increasing efficiency and accuracy, reducing costs, and improving the end user experience. However, in order to reap the full benefits of such increasingly digitalised environments, an assured way of authenticating our identities is required that does not fail us in a pan-European cross-border context.

Introduction

Identity is the dynamic collection of all attributes related to a specific entity, be it a citizen, enterprise, or object. An identity is what allows an entity to be distinguished from any other. This is what makes identity a key component in numerous economic, social and administrative transactions. The ability to link a set of information to its owner and the effective and secure handling of entity-specific data are essential to numerous different interactions. To this end, organisational and technical infrastructures are developed to define, designate and administer the identity attributes related to specific groups of people, such as customers, patients or citizens. These infrastructures are identity management systems.

Why eIDM at pan-European level?

In all EU Member States several initiatives are underway to introduce electronic identities (eID) for public services. While often used interchangeably, these notions are usually not defined clearly enough. For the purposes of this paper, "identification" should be taken to indicate the process of using claimed or observed attributes of an entity to deduce who or what the entity is. "Authentication[1]" is the corroboration of the claimed identity of an entity and a set of its observed attributes. Thus, identification in general refers to a process of deduction based on a set of information allowing to determine who a given person is (with varying degrees of reliability); while authentication implies that a

[1] More accurately: entity authentication, as opposed to data authentication, which is the corroboration that the origin and integrity of data is as claimed.

decision is made based on the actual corroboration of information, implying a larger degree of dependability.

A range of varying approaches and solutions has been proposed to address shortcomings inherent to cross-border electronic identity management (eIDM) approaches (e.g. federated versus centralized, driven by public or by private sector, different degrees of information assurance, different choices to trade-off between privacy and convenience). While this diversity is an inevitable and often desirable outcome of the Member States' principal competence in this field, it also complicates matters for any entity (e.g. citizen, business or administration; collectively referred to as the "user" of any given eIDM system) that desires to communicate with administrations outside the scope of its own local eIDM system. In such circumstances, there is a need to be able to connect the eIDM system from a local jurisdiction to a public service provided outside the scope for which the system has been designed. In short, there is a need for an interoperability framework to address eIDM requirement at an EU level.

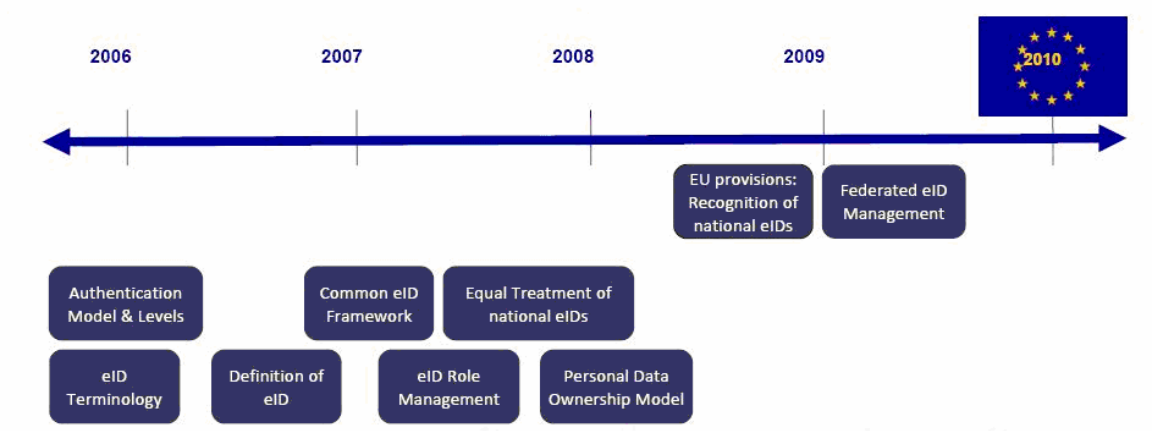
In the eGovernment action plan, adopted by the European Commission on 25 April 2006, the following commitment was made to this end[2]:

> *The Commission, in cooperation with the Member States, will pursue policies to grant safe access to services EU wide. When citizens travel or when they move they want easy access to services. EU governments have agreed to facilitate this process by establishing secure systems for mutual recognition of national electronic identities for public administration web-sites and services. The Action Plan foresees a full implementation by 2010. The Commission will help make this happen by supporting wide-scale cross-border demonstrators, identifying common specifications for electronic ID management during 2007 and by reviewing the rules of electronic signatures in 2009.*

Background: A roadmap towards eID Management in Europe by 2010

In order to align activities and developments with regard to the provision of identity services across borders and sectors, the Member States signed up to an ambitious "eID Timeline" in the so-called Signpost Paper[3]. While provisional, the purpose of this timeline was to identify a number of key building blocks to the development of a pan-European eIDM system, and to set a number of specific milestones to be reached in order to ensure that the final objective of "secure means of electronic identification (eID) that maximise user convenience while respecting data protection regulations" by 2010.

[2] See http://europa.eu.int/information_society/eeurope/i2010/index_en.htm
[3] See http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf



The Roadmap presented in this document further specifies and capitalises on this time line by presenting concrete building blocks, specific milestones, and actions that need to be undertaken in order to realise the ambition as expressed in the eGovernment Action Plan for 2010.

In order to make the ambitious time plan, decisions about principles need to be taken on a very short notice.

Key principles for a pan-European eIDM system

As for any action on pan-European level, the principle of subsidiarity needs to be taken into account. The autonomy and responsibility of Member States to pursue their own eIDM goals and make appropriate arrangements thereto remain unchallenged. It is thus clear that this Roadmap does not seek to impose any technical, organisational, legal or infrastructural choices that would limit the Member States in exercising their competences and prerogatives to the fullest.

However, in order to realise the vision on a pan-European eIDM system as expressed in the Ministerial Declaration and the Signpost Paper, minimal requirements to put in practice an eIDM infrastructure need to be agreed and followed by all parties involved.

In the Ministerial Declaration, the citizen is put at the centre of developments. Therefore these minimal requirements will be set up with a focus on serving the user as a key player in the overall structure. The goal is to create a framework that offers added value to the end users, thus ensuring that users *want* to embrace it, rather than being *required* to do so. For this reason, the following principles should as a minimum be adhered to by the Member States, in order to come to an efficient and interoperable pan-European eIDM infrastructure:

1. Usability considerations should be the most pervasive design constraint when creating a pan-European eIDM framework. This means that the system must be secure, implement the necessary safeguards to protect the user's privacy, and allow its usage to be aligned with local interest and sensitivities.

2. Each Member State should be able to identify users within its borders, if it wishes to allow them access to eIDM services abroad. To this end, the consistent use of suitable identifiers is a necessity to allow the accurate identification and authentication of the entity involved, and to allow the exchange of information between administrations insofar as required for these purposes. The fundamental requirements for a system that addresses the needs of natural persons should be extensible to legal persons as well.

3. Each Member State should issue the means to each user to identify and authenticate himself electronically, if it wishes to allow him access to benefit from eIDM services abroad. A user has the ability to act autonomously and to make use of the offered services.

4. With regard to mandate/representation authorisations, each Member State should provide the means to manage the competences of the identified users within its borders, insofar as these authorisations are not subject to approval by or on the authority of another Member State.

5. Each Member State should support online validation mechanisms of identities, competences and mandates, if it wishes to provide eIDM services.

6. High-level consensus must be established between Member States on an eIDM terminology in order to guarantee conceptual/semantic interoperability. Appropriate policy and legal measures can be used to corroborate this consensus.

Design criteria towards pan-European eID management – the way forward

From these basic principles, a number of design criteria for a pan-European eIDM system can be derived, which were also included in the Signpost Paper. Most notably, in order to achieve eIDM interoperability, the pan-European eIDM system would need to be:

1. Federated in a policy sense, i.e. allowing administrations to mutually trust each other's identification and authentication methods, accepting these methods on the basis that they were considered acceptable by the administration of origin. It should be noted that this does not imply any choice towards any specific technical or infrastructural framework[4]. However, technical and organisational choices can be limited at a later stage by relying on policy measures that seek to encourage choices made by a majority of Member States.

2. Multilevel, in the sense that Member States should be permitted to provide multiple security levels for eIDM services, so that the authentication requirements for each eGovernment service can be tailored to the security needs of that service. Member States determine at which level they choose to offer authentication

[4] Specifically, the use of the word “federated” should not be taken to be a reference any specific solution model, such as e.g. the Liberty Alliance.

services, and which level of authentication is required for each eGovernment service (although they must accept as valid any authentication methods of the required level from other Member States). This implies that a set of criteria must be defined on a European level which must be met for each authentication level.

3. Relying on authentic sources: to ensure data quality and eGovernment efficiency, a single authentic source should be available for each piece of data regarding each registered entity in the Member State of origin. This does not necessarily imply the use of databases, as the authentic source might be a unique token. Additionally, commonalities in the eIDM approach among Member States can be encouraged to provide assurance on the quality of source eIDM data.

4. Permitting a context/sector based approach where this is deemed desirable by the Member State of origin (i.e. this is a logical extension of the federated model). Such context can be determined by the application framework or the conceptual framework within which eIDM is used.

5. Enabling private sector uptake, where Member States choose to rely on private sector partners (e.g. financial institutions) for the provision of eIDM services. Note that this only implies that private partners may be involved in identity management tasks, such as the definition, designation and administration of identity attributes; it does not imply that private partners necessarily need to be able to use the eIDM infrastructure to provide private sector services. However, the encouragement of the development of private sector applications that leverage public eIDM infrastructure may be necessary in order to ensure sufficient return on investment.

The federated level intends to deliver services in ways that are useful in support of the single market, and in support of the Lisbon objectives, yet respect the full autonomy of Member States with respect to the 2nd and 3rd Pillar as well as their own domestic policy priorities. The choice of a federated model is therefore a policy choice, not a technical or infrastructural one.

The Roadmap

Based on the key principles and subsequent design criteria, the Roadmap presents a series of building blocks that need to be brought in place in order to put pan-European eID into practice by 2010. In order to guide the process, several supporting activities will need to be undertaken, such as the ones presented below.

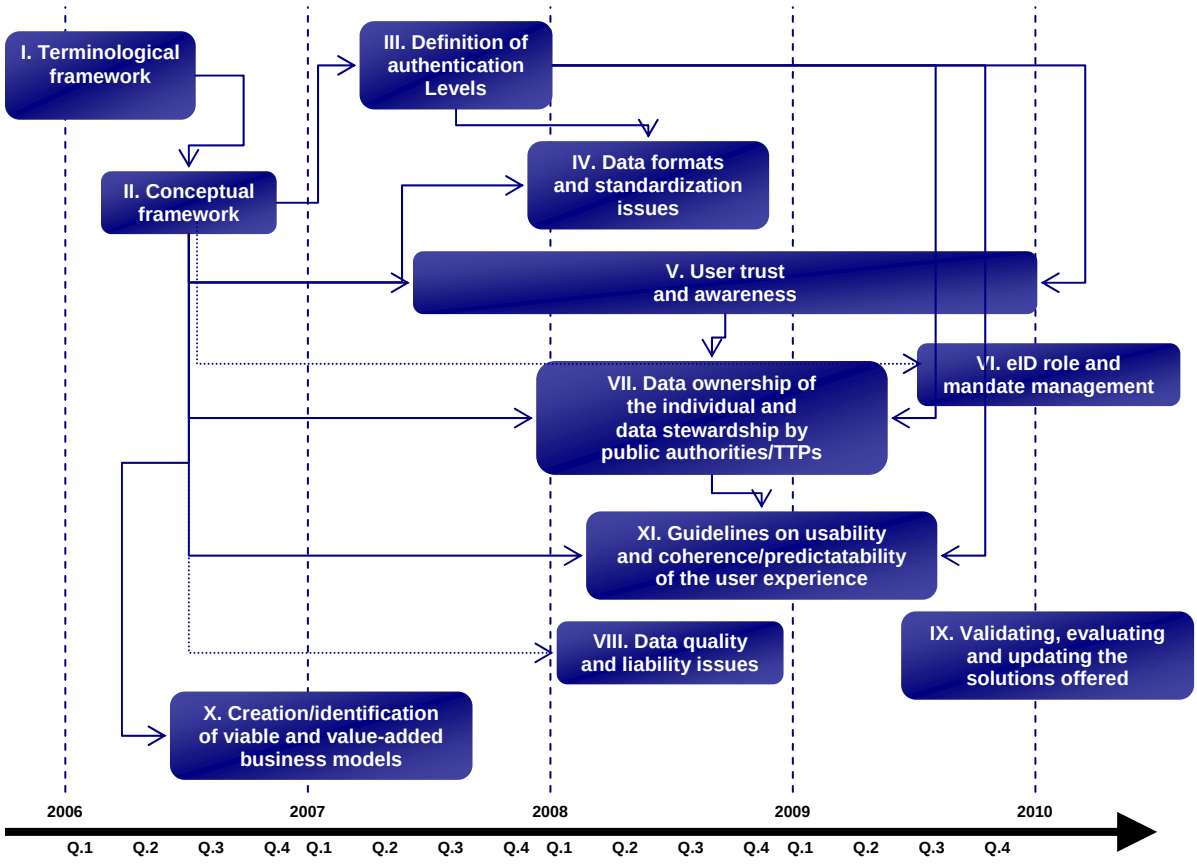
Building blocks

The Roadmap requires a number of building blocks to be taken into account, covering principles of European eIDM, infrastructural choices and usability considerations. All of these elements need to be considered when making choices regarding the realisation of the milestones described below.

It should be noted that these elements should not be considered as "building blocks" in the most literal sense of the metaphor, implying that one block can be completed and that others can thereafter be stacked on top. Rather, they should be considered as a collection of essential elements, each supporting the other, and in continuous interaction. No building block can be considered complete or finalised until or others have been put in place; a consideration which is most obvious for fundamental building blocks such as trust and awareness (including security concerns), and data protection issues which underpin all other blocks. Thus, the realisation of the building blocks is an iterative process requiring continuous (re-)evaluation.

These building locks include:

- Fundamental requirements: a consistent eIDM terminology, creation and maintenance of user trust and awareness, and the realisation of a personal data ownership/stewardship model that also takes into account privacy requirements mapped on a Member State level.
- Infrastructural requirements: a clear conceptual framework (including common specifications), the definition of authentication levels, choice of data formats and standardisation issues, implementation of role and mandate management, information security and legal issues (including data quality and liability).
- Usability requirements: validation of solution models and business models, cooperation between public and private sectors and ensuring a harmonious user experience.



Support measures

Several support measures are necessary in order to bring to about the goals of this Roadmap and address political ambitions, key principles and design criteria. The following support measures are currently envisaged as priorities:

Support measure	Timing
Base line study: what systems are currently in place in Member States in support of identity and authentication services regarding public and possibly private services, as appropriate; and what possible solution models have been examined thus far to realise cross border interoperability.	2nd quarter 2007
Legal study: what legal provisions – if any – exist with regards to identity and authentication services in the Member States and on a pan-European level[5], and what restrictions do legal constraints place on pan-European identity and authentication services?	2nd quarter 2007
Stakeholder platform: in order to ensure that stakeholders are involved in the development of pan-European eIDM services a stakeholder platform needs to be formalised that supports: a. Awareness about plans and progress marked by milestones among stakeholders emphasising data protection, privacy and information security aspects. b. Easy way in for stakeholders to present their interests, practice experiences and solutions. c. Collection of information from a wide range of stakeholders, in order to provide input to the system design. d. Action with all involved stakeholders to support the development of pan-European eGovernment services, training activities, supportive products and services etc. e. Encouraging discussion regarding organisational and technical aspects to encourage commonalities and avoid fragmentation.	2nd quarter 2007

[5] Including the potential applicability of the eSignatures Directive to this issue; see Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ L13*, 19 January 2000, p.12

Study on the potential impact and implementation of a multi-level authentication mechanism, including the definition of requirements for these levels.	2nd quarter 2007
Awareness raising campaigns towards the citizen. In order to get the citizen to make use of the pan-European eID services, she/he needs to know what services are available, for what purposes, and what it takes to access these services.	2nd quarter 2007
Consultation on data protection / data ownership models and principles, based on stewardship of personal data with public sector parties.	4th quarter 2007
European standardisation activities to be undertaken pursuant to shared policy goals among the Member States – assessment of available standards and their adequacy for the envisaged conceptual framework, and initiation of studies for any missing standards.	3rd quarter 2008
Study on the implementation of a suitable mandate / authorisation / role management model.	1st quarter 2009
Consultation on evaluation and possible implementation of extended private sector uptake (focusing on privacy and security aspects).	3rd quarter 2009
Study on the suitability of the use of the eIDM as a "quality mark" for electronic authentication after 2010. Principles for quality mark evaluation and allocation (labelling) need to be created.	4th quarter 2009

The large scale pilot on a pan-European eID system that is scheduled for a start in 2008 will be a useful vehicle for these activities, as it will lead to practical cross-border eIDM experiences from real people, and as it will be an excellent focal point for stakeholders to meet and jointly progress their vision as well as action.

Milestones

The Signposts towards eGovernment 2010 paper[6] stated a number of goals expected to be reached by 2010:

- European citizens, businesses and administrations should benefit from secure means of eIDM to make the most of user convenience while respecting data protection regulations.
- European citizens, businesses and administrations should benefit from an online presence that is secure, authentic, reliable and durable, a veritable web of trust.
- A federated, multilevel eID model should be agreed that is open and flexible enough to match national, regional, local and sectoral requirements based on a common policy framework.

It should be noted that a number of technical, organisational and legal choices must urgently be made, if this goal is to be met to any significant degree. To this end, a number of concrete and specific milestones can be defined at this stage that will be required regardless of the outcome of these choices.

In defining these milestones, the focus should be on the creation of basic identification and authentication functionality, rather than on such added value aspects that were also included in the Signpost paper, such as mandate management, labelling, and private sector uptake.

Apart from pilot projects, to be run in parallel and continuously with other activities, priority milestones include the following:

Milestone	Timing
Availability and acceptance of a standardised eIDM terminology to enable clear and unambiguous discussions.	1st quarter 2007
Identification and acceptance of key applications to be supported by the eIDM framework.	1st quarter 2007
Availability and acceptance of the basic principles of a conceptual model, detailing the interoperability model to be strived for. The principles must be sufficiently detailed to allow studies to be conducted which will define concrete technical, organisation and legal solutions in as far as required, and must allow the allocation of responsibilities.	1st quarter 2007

[6] Signposts towards eGovernment 2010, European Commission, 2005.

Availability and acceptance of a full conceptual framework, including: • Full allocation of responsibilities for each aspect of the technical, organisational and legal framework; • Initiation of any studies to be conducted to define concrete technical, organisation and legal solutions • A conceptual description of the functioning of the multi-level authentication system.	2nd quarter 2007
Availability and acceptance of requirements for electronic identification / authentication facilities imposed on all Member States wishing to offer eIDM services; and acceptance of principles/standards of semantic interoperability to enable information exchange to the extent required by the conceptual framework. Additional standardisation work to be planned as appropriate, especially with regard to technical and organisational aspects. Emphasis is placed on data protection, privacy schemes and information security.	4th quarter 2007
Finalising the technical interoperability model, including technical and semantic standards and information exchange mechanisms.	1st quarter 2008
Availability and acceptance of a legal trust model, including: • Definition of authentication levels and mapping of existing solutions to these levels; • Conclusion of binding legal instruments in which the Member States accept each others' authentication methods of any given level as equivalent to their own solutions of the same authentication level; • Conclusion of binding legal instruments regarding Member State liability for information contained in authentic sources and identification/authentication on the basis thereof.	2nd quarter 2008
Availability and acceptance of data protection / data ownership models and principles, based on stewardship of personal data with public sector parties	2nd quarter 2008

Start of trust and awareness creation through suitable mechanisms, including information campaigns towards the envisaged end users, emphasising usability, security and privacy.	4th quarter 2008
Availability and sufficient testing of any required pan-European technical infrastructure. This entails the verification of the infrastructure's compatibility with the goals defined in the Signpost Paper and of its capability to recreate all functionality explored through the large scale pilots and the identified key applications.	2nd quarter 2009
Reaching the i2010 objectives	1st quarter 2010

Risk analysis

The first and foremost risk is that discussions regarding the requirements of a future solution will continue, while no real steps in progressing toward the vision will be undertaken. In order to be able to achieve the vision by 2010, decisive steps need to be taken now, and in the years to come. In taking these decisions it is key that the interest of the end user, the citizen, is taken into account. A system that is too difficult to use or too expensive for users is to be avoided at all costs.

Secondly, it must be recognised that the effective usability of the system will not be sufficient if the system is not perceived as trustworthy and secure. Privacy protection and security are central design criteria, which must also be clearly communicated to the end users. Uncertainty in this regard will hamper take-up, and create the risk of the system being perceived as an unwanted intrusion into European citizens' private lives.

These are the main risks, and handling those risks is very much in the hands of the Member States and the Commission. On an operational level, additional risks underlie the main risks sketched above in terms of not recognising the technical, legal, or organisational challenges ahead in time. Whereas it is impossible to oversee all technical, legal, and organisational consequences at this time, before any specific design choices are made, in every decision and next step in concretisation of the pan-European system these challenges need to be explored. A solid and in depth understanding of the current situation in Member States on technical, legal and organisational level would be a useful starting point. Also the eIDM pilot should pay attention to these aspects, in iteration, throughout the different phases of its development.

Conclusion

Given time restrictions, while the latter objectives are also included in the Signposts towards eGovernment in 2010 Paper, the priority should primarily be to realise the basic identification/authentication functionality as expressed by the milestones.

By offering access to such basic identification/authentication functionality to European citizens, businesses and administrations, a significant first step is made to the realisation of the Manchester declaration and the eGovernment action plan.

Annex to the eIDM Roadmap

Building blocks: what needs to be done to get it right

A number of key building blocks of the eIDM Roadmap have been identified which are considered to be of paramount importance for the realization of the goals outlined above. These building blocks will be briefly commented below.

As indicated in the Roadmap document itself, it should be noted that these elements should not be considered as "building blocks" in the most literal sense of the metaphor, implying that one block can be completed and that others can thereafter be stacked on top. Rather, they should be considered as a collection of essential elements, each supporting the other, and in continuous interaction. No building block can be considered complete or finalised until or others have been put in place; a consideration which is most obvious for fundamental building blocks such as trust and awareness (including security concerns), and data protection issues which underpin all other blocks. Thus, the realisation of the building blocks is an iterative process requiring continuous (re-) evaluation.

Block I: The terminological framework

Description

Currently the Member States have implemented / are implementing their own national IDM infrastructures without a common agreement on the definition of essential concepts such as identity, entity, attribute, delegation, or even entity authentication and identity management itself. As a result, serious problems can arise on a European level, where 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. Thus, a terminological framework is required as a basic

resource before European level solution can be contemplated. This framework should provide a technologically and philosophically neutral definition of the most common notions with regard to identity and identity management.

Success criteria

The output of this building block should be a consistent list of eIDM definitions, which can be applied universally to all national IDM solutions. While such initiatives already exist[7], a formal review and adoption by both the Member States and the Commission will be required in order to give the final result the required moral authority.

Block II: The conceptual framework

Description

As a key step towards any kind of implementation activities, it is important to have a clear view and a substantial consensus regarding the general organisation and basic principles governing the pan-European eIDM architecture. 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 each component of the infrastructure. The conceptual framework will constitute 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 and provide the requirements that need to be met by some of the implementation-oriented building blocks below.

Success criteria

This block requires:

1) adherence by the Member States to the principles outlined above (e.g. the availability of authentic sources and authentication mechanisms within each Member State);
2) the creation of a set of common specifications for the creation of the required infrastructure
3) formal acceptance by the Member States of these specifications and the conceptual framework as a whole, and the allocation of responsibilities in this regard;
4) the completion of large scale pilots testing different solution models.

[7] See e.g. the Terminology Paper created by the ModinisIDM Project, also quoted above; https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc. It should be noted that this document is being reviewed by the article 29 Working Party, so that it should not yet be considered final.

Block III: Definition of Authentication Levels

Description

This building block consists of the definition of a set of authentication levels using concrete standards that describe different levels of security which can be mapped to levels of security already implemented by the Member States, and that would allow eGovernment service providers to choose an appropriate security level. Both the registration and authentication procedures need to be examined to this effect.

Success criteria

This block requires:

1) a definition of the authentication levels on a European level, along with the requirements demanded at each level;
2) a mapping of existing authentication mechanisms in the Member States to a specific level, based on their conformity to the definitions above;
3) an autonomous decision by the Member States regarding the authentication level required for each eGovernment service (which cannot differ between nationals and non-nationals).

Block IV: Data formats and standardisation issues

Description

Given the wide variety of existing national eIDM solutions and the relative unlikelihood of a common European eIDM token[8] being implemented in the medium term, the pan-European eIDM infrastructure will need to ensure the readability and exchangeability of user data, both locally (i.e. directly from a token) and at a distance (i.e. by relying on national authentic sources if they are not stored on a token), within the scope of existing data protection regulations. Given these requirements, certain standards will need to be accepted both for data formats and data exchange processes.

Success criteria

This block requires:

1) the acceptance of a conceptual model;
2) adherence by the Member States to the principles outlined above (e.g. the availability of authentic sources and authentication mechanisms within each Member State);
3) the acceptance of a set of common standards for data formats and data exchange.

[8] To be understood as a token defined, issued and managed; and not as a token which adheres to common European standards.

Block V: User trust and Awareness

Description

Trust and awareness are two basic preconditions that need to be fulfilled at the user's side, but which are closely linked to the organisation and functioning of the eIDM infrastructure, and which should therefore be considered a building block. Without trust (in the framework's security) and awareness (of its basic operating principles and the resulting guarantees) the system is likely to remain unused, or be viewed as an intrusion rather than as an enabler.

Success criteria

The end users should be willing to confide in the eID framework. To this end, concrete standards of security and privacy protection should be defined on a European level (in so far as existing guidelines such as formulated by the Data Protection Directive[9] and in the recommendations and policy papers from the Article 29 Working Party[10] would be deemed insufficient), and systematically evaluated in the Member States.
These standards must be defined, observed by the system, evaluated continuously and communicated to the user base in an understandable manner to ensure user trust.

Block VI: eID Role and Mandate Management

Description

Representation of another person can be mandated by contract or by law. Common examples include parents representing their underage children, legal guardians representing a mentally disabled person, notaries public or fiscal consultants representing their clients, business administrators representing their legal entity, etc. The pan-European eIDM model should ensure that a viable (federated) infrastructure can been created and implemented that allows a service provider to verify whether a third party has been given the legal right to act on behalf of a system's end user, if this is allowed by the Member State of origin.

Success criteria

This building block requires a thorough study and categorisation of the types of mandates in eGovernment practice, and the most significant applications for which they are used. This should permit the assessment of how mandate relationships can be generically modelled, and how this can be plugged into the existing federated conceptual model.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[10] See inter alia http://ec.europa.eu/justice_home/fsj/privacy/policy_papers/policy_papers_en.htm

Block VII: Data ownership of the individual, and data stewardship by public authorities/TTPs

Description

End users are – or should be – entitled to maximum control over their own personal data in the pan-European eIDM scheme, following a mixed voluntary/involuntary data licensing scheme (a stewardship model), whereby the data subject "licenses" access to his personal data to a service provider, either voluntarily or forcibly on the basis of an overriding interest (e.g. emergency health care and national security issues). It is important that users have sufficient control and awareness of what personal data of theirs a service provider will obtain access to, keeping into account the proportionality principle of the Data Protection Directive and the Privacy Directive[11]. Data control also implies active involvement in issuing, extending, restricting and withdrawing of credentials; and in management of personal data (including accessing and updating personal data to a maximum extent), in order to ensure that data in official authentic sources remains as accurate as possible.

Success criteria

This building block requires the definition of data control principles that should be observed by anyone calling on the services offered of the pan-European eIDM system; and the verification of the observation of these principles (insofar as the provisions of the Privacy Directive would be shown to be insufficient for the purposes described above).

Block VIII: Data quality and liability issues

Description

The availability of authentic sources implies that each attribute should ideally be stored only once, and that end users should not be requested to provide this data again once it has been provide a first time. In order for this system to function adequately on a cross-border level, the Member States will be responsible for ensuring data quality with regard to data managed within their own systems. Furthermore, Member States need to accept objective liability for the accuracy of this data: they must guarantee that the data provided is accurate, and should be liable for any damages resulting from inaccurate data[12]. Such guarantees are the basis of a federated system: parties decide to trust each other's data, on the basis that they have received adequate assurance (including in the form of legal

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[12] Notwithstanding the obvious caveats that this requires the data request to have been presented properly, and that the providing Member State could have a standing to reclaim any damages from the entity that has failed to keep the information accurate and up to date.

guarantees) that the data will be accurate. It should be emphasised at this point that any data may only be processed in accordance with the Data Protection Directive (95/46/EC).

Success criteria

This block requires:

1) adherence by the Member States to the principles outlined above (e.g. the availability of authentic sources);
2) the creation of binding legal instruments (possibly in the form of multilateral agreements) in which guarantees are provided with regard to the accuracy provided through the eIDM system.

Block IX: Validating, evaluating and updating the solutions offered

Description

In order to realise the ambitions of the eGovernment Action Plan, it would be insufficient to merely establish the infrastructure described above without further follow-up. Its suitability needs to be evaluated periodically, to ensure that the solutions offered on a national level comply with European guidelines, and to ensure that they meet user expectations and security requirements. Only in this way can sufficient user trust be ensured.

Success criteria

A periodical evaluation mechanism needs to be created, at a European level but relying on the Member States' input, once the eIDM system has been put in place.

Block X: Creation / identification of viable and value-added business models

Description

Once a fully functioning framework has been designed, the main priority should be on the identification and implementation of key applications, combining quick wins and larger scale projects. Rather than initially attempting widespread pan-European applications (for example E101 applications) it might be more appropriate to demonstrate the effectiveness of the framework to all stakeholders by a smaller project, or in focused Pan-European applications.

Success criteria

This building block requires:

1) the identification of key applications;
2) their accelerated deployment in the Member States and subsequent implementation of cross-border functionality;
3) continuous evaluation of potential added-value models, including through further private sector uptake.

Block XI: Guidelines on usability and coherence/predictability of the user experience

Description

Confusion with end users can often result from a confrontation with considerably different interfaces to realise what is essentially the same function on two different systems. On a pan-European scale, this problem is exacerbated.

Success criteria

This building block requires the creation of a set of design principles to ensure a harmonious user experience, thus ensuring the usability of eIDM applications in practice.

For further information about the eGovernment Unit:

European Commission
Information Society and Media Directorate-General
eGovernment Unit

Fax (32-2) 29-6 41 14

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