ENISA Report

January 09

Report on the state of pan-European eIDM initiatives

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for enquiries on this study, please use the following details:

Technical Department

Email: eid@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Authors:

This study has been prepared by Hans Graux and Jos Dumortier

time.lex law offices

Internet: http://www.timelex.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Table of contents

Executive summary

The development and deployment of electronic identity management (eIDM) solutions in European electronic applications stands at a crossroads. Over the past decade, European Member States and EEA countries have gradually rolled out identity management solutions that were best suited to their national goals and ambitions. The goals of such initiatives were uniformly the same: improving administrative efficiency, improving accessibility and user-friendliness, and above all, the reduction of costs.

At the European level, these goals could be advanced by improving the interoperability of electronic identification/authentication solutions being offered at the national level. After all, by doing so, European citizens and businesses would be able to use applications in any European country, thus potentially benefiting citizens, businesses and administrations alike. Significant efforts have been made in recent years to chart the European interoperability difficulties related to electronic identities (eIDs) and to propose solutions to these problems.

More recently, efforts are moving beyond this largely theoretical level, and are geared towards creating functioning applications. This report charts the origins and scope of the ambitions for European eID interoperability, and looks specifically at how these are reflected in three specific initiatives:

- At the **policy** level, the so-called **eID Roadmap** is examined. This document outlines the European eID goals to be reached by 2010, and defines a number of specific objectives and milestones that should be covered along the way.
- At the **infrastructural** level, the recently initiated **STORK Project** is discussed. This project aims at developing a series of pilot projects which should be available to citizens of several European countries, using the identification/authentication means favoured by the governments of those countries. Thus, the STORK project should pilot a basic infrastructure for cross-border electronic identification/authentication.
- At the **application** level, the report also examines the efforts surrounding the **implementation of the Services Directive**. The Services Directive requires Member States to put electronic points of single contact in place by 28 December 2009, which service providers from any Member State should be able to use to complete the necessary procedures and formalities in order to be allowed to offer their services in the relevant country. In many cases, this implies that service providers will have to be able to identify themselves electronically in a way that is considered sufficiently reliable.

All of these initiatives have the potential to act as a catalyst in furthering the European vision for eID interoperability. However, in order to do so, it is important to assess their role and contributions in the general strategy for eID interoperability, to determine the relationship between these initiatives, and to identify any remaining gaps or inconsistencies.

The main role of the eID Roadmap consisted in defining the desired outcome of European eIDM ambitions, namely the creation of an interoperability infrastructure that would be:

1. Federated in a policy sense, ie, 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.

2. Multi-level, 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 services, and which level of authentication is required for each eGovernment service.

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.

4. Permitting a context or sector based approach where this is deemed desirable by the Member State of origin.

5. Enabling private sector uptake, where Member States choose to rely on private sector partners (eg, financial institutions) for the provision of eIDM services.

The STORK project is expected to advance these ambitions by creating specific cross-border pilot applications supporting eID tokens from multiple countries. Given the available timeframe and scope of the project, these applications and any supporting infrastructure established by the STORK consortium will not be an end point for interoperability developments. Nonetheless, it will play the crucial role of providing a functional infrastructural model for eID interoperability between a sufficiently large number of different technological solutions and countries. The STORK project is currently considering several approaches to reach its goal, including a model that relies on a proxy approach requiring the creation of identity providers (IDPs) at the national level (at least one per country), coupled with a network of proxy service providers to connect service providers to the appropriate identity providers in each country, and to validate the trust and security of the identity information sent by the identity providers. In this way, STORK should theoretically be able to handle any type of identification/authentication method – thus including non-PKI-based systems – supported at the national level.

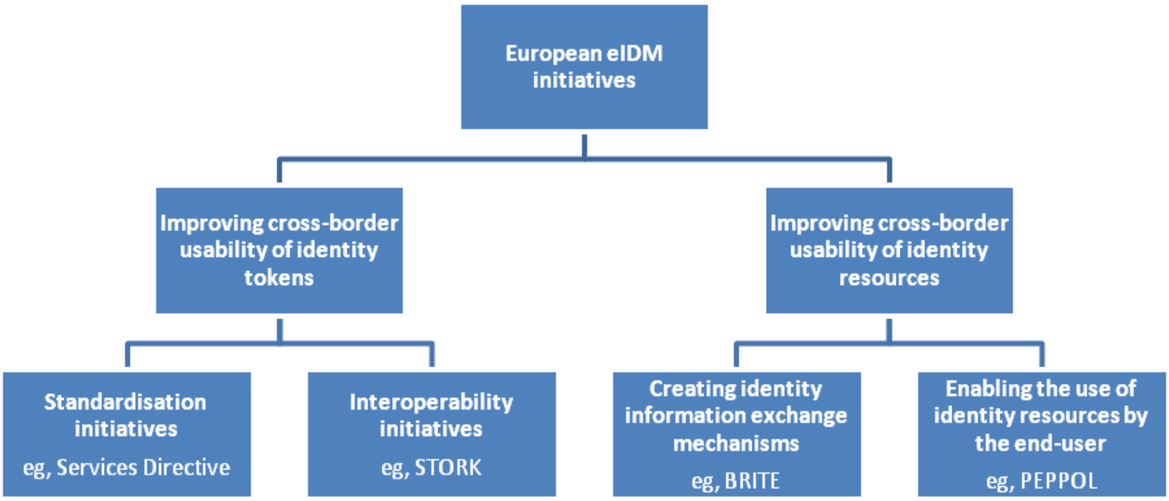
The efforts surrounding the implementation of the Services Directive on the other hand are bound by the restrictions resulting from the deadline of the directive, set at the end of December 2009. This leaves little time for Member States to conduct significant experiments. For this reason, a pragmatic approach is currently being taken that focuses on improving the interoperability of electronic signature practices between the Member States – thus targeting only PKI-based models – and leveraging the possibilities that this approach offers in relation to eIDM.

More specifically, support efforts in this field are currently focused on improving the interoperability of certain types of electronic signatures that are generally considered to be more secure, specifically so-called qualified signatures and advanced signatures based on qualified certificates. This should have a positive impact on eIDM issues as well, since part of the work is centred on charting how signatories are uniquely identified in the qualified electronic certificates used as a basis for these electronic signatures. As long as this information can be provided to the Member States, the use of these electronic signatures should provide the Member States with the possibility of identifying specific signatories.

With the support efforts related to the Services Directive serving as a catalyst to improving the use of PKI-based solutions for electronic identification in the shorter term, and the STORK project taking a more long-term technology neutral approach, these initiatives should collectively ensure that the European eIDM agenda can be advanced to a significant degree by 2010.

Of course, these three chosen key initiatives do not represent the entire spectrum of European eIDM related initiatives. Several other recent initiatives are equally likely to play a significant role in the future European eID arena, including such initiatives as the PEPPOL project, the BRITE project, ECRIS, and other initiatives discussed in greater detail below.

Globally, all of these initiatives cover two aspects, with some focusing more on one aspect than on the other: on the one hand, improving the interoperability or standardisation of specific electronic identification/authentication tokens issued to the public and, on the other hand, initiatives aiming to improve the utility and usability of authentic (or at least trusted) identity resources other than personal tokens. This can be represented through the schema below.


European eIDM initiatives
Improving cross-border usability of identity tokens
Improving cross-border usability of identity resources
Standardisation initiatives
eg, Services Directive
Interoperability initiatives
eg, STORK
Creating identity information exchange mechanisms
eg, BRITE
Enabling the use of identity resources by the end-user
eg, PEPPOL

- Approaches to improving eIDM practice in Europe -

Thus, the initiatives discussed in this report are complementary to a large degree. One of the key challenges for the future will be to integrate the outcomes of all of these different aspects into an updated global vision for European electronic identity interoperability. It is clear that no single initiative has defined the sole valid solution to European identity management issues. A coordinated approach combining the benefits of these proposals will need to emerge in future years.

Through such devices as the i2010 strategy, the eID Roadmap and the Services Directive, Europe has imposed extremely ambitious short-term eIDM goals on itself and on the Member States. This ambition has resulted in a significant number of relevant initiatives, all of which bring their own piece of the puzzle to the table.

It is clear that this approach will allow significant progress to be made by 2010, with the results of the implementation of the Services Directive, STORK and other initiatives such as PEPPOL taking a central role. However, not all eIDM objectives will be reached by then as noted above, and further initiatives will be needed to broaden and extend the outcomes of these initiatives. Furthermore, the integration of all outputs into a more unified eIDM vision will gradually become more important. Several considerations will need to be taken into account when doing so, including:

- the evolving responsibilities of the end-user in the process of identification/authentication: Traditionally, the role of the end-user in this process is rather passive and not particularly fine grained. Newer technologies allow the user to take a more active role, including by restricting the information transferred to the service provider to a minimum, and by more easily exercising his rights to access and correct his information (if applicable). Social networks can be considered an example of this, as they provide the users with an accessible way of controlling their personal data. A coherent approach will be needed towards this issue: what can and should be expected of the end-user, and how can data protection concerns be addressed?
- the issue of security and trustworthiness. Member States should be able to provide end-users with the means for identification/authentication that correspond best with their expectations of security and user–friendliness: This implies that there can be significant differences between the security and trustworthiness of eIDs used in different Member States. This is beneficial, if application owners are able to determine the reliability of the eID being presented by end-users from different countries and to decide on that basis whether the end-user is allowed to use the application. While efforts have already been undertaken to take the first step in this direction, it is unlikely that a full and systematic approach will be developed and taken up by 2010.
- the growing role of authentic databases of identity information as a potential way of strengthening the trust in identity resources and of further leveraging the identification process: Following successful identification of a citizen or enterprise, additional information is directly obtained from an authentic database. From a data protection perspective, a system that provides the end-user with greater direct control over which identity data can be transferred may seem preferable over one that allows automated data exchanges; however, automated exchanges can be more efficient and user-friendly. The integration of the relevant databases into the identification/authentication process can offer a real added value to all concerned parties. Reflection will thus be needed on how and under which conditions this integration can be accomplished.

- the questions of responsibilities and liabilities: Specific roles will need to be defined for end-users, identity providers and identity resources at the national level, proxy service providers who connect service providers to identity providers, the service providers making use of the identity resources themselves, and any variety of other entities involved in the process. When networks of identity resources are established (such as networks of business registers or criminal record registers), specific processes need to be put in place to ensure the reliability of the information and the availability of appropriate access management facilities and audit trails. For all of these matters, a sufficiently robust legal framework needs to be put in place, along with a clear framework of responsibilities and liabilities.
- the use-case of electronic means of identification: The eID Roadmap has already acknowledged that private sector uptake is an important factor in improving the popularity of electronic means of identification, since most citizens and businesses have only a limited number of interactions with public sector entities on a yearly basis. Sufficient private sector involvement and uptake is therefore important to ensure that any given eID tool is taken up in practice, and that its use becomes intuitive. While pilot projects are chosen with actual use-cases in mind, the use of electronic means of identification in private sector applications does not appear to be a European policy priority yet, which could turn out to be a weakness in offering an appealing use-case.
- finally, dependency on end-users: The uptake of any European eIDM initiatives is largely dependent on the creation of trust and usability with the end-users. The systems must not only be safe, they must also be perceived as such. This implies that significant efforts must be made to ensure the transparency and accessibility of the system, keeping in mind cultural differences in the approach to identity management and personal differences in familiarity with newer technologies.

Some of these matters have already been touched upon by the existing European eIDM initiatives in an embryonic form, and all of them will undoubtedly be explored further in the next year in the course of ongoing projects. However, it is important to keep in mind that none of the initiatives in the field of eIDM identified above aspire to be an end point for eIDM evolution, and this explains in part why some of the points raised above will likely need to be refined further and reprioritised beyond the 2010 horizon.

Based on the above considerations, the main policy priorities for European eIDM initiatives in the next few years can be expected to be the following:

- In the course of 2009, after the first outputs of current key projects such as STORK, PEPPOL and the implementation of the Services Directive become available, the policy objectives of the eID Roadmap will need to be updated. The current roadmap was drafted in 2006, and its building blocks were defined and planned with a 2010 deadline in mind. With this deadline drawing closer, it will be necessary to determine which parts of the roadmap still need to be realised, and if and how the building blocks need to be re-evaluated for the following years. This update of the roadmap will also need to examine how the benefits of all existing approaches can be combined in the future. In this stage, it will become increasingly important to link the output of the current efforts to external applications, such as social networking sites, or allowing the resulting infrastructure to be used for eCommerce purposes. This would likely improve the appeal and use-case to citizens.

- On the basis of the results of the STORK project, how the pilot infrastructure can be expanded into a full-scale system will need to be examined. This will entail the identification of any simplifying assumptions that needed to be made in the course of the project, and creating suitable and acceptable solutions to replace these assumptions with real-world constraints suitable for a full-scale deployment. Based on currently available information, further efforts will specifically be needed to ensure the trustworthiness and reliability of the infrastructure, by eliminating any remaining security weaknesses and by implementing a suitable legal framework within the Member States.
- Once an interoperability infrastructure is in place, Member States will be forced to reflect further on the reliability requirements they will impose when specific applications are used by foreign citizens or enterprises. Thus far, this question has not been dealt with systematically, since no interoperability infrastructure was available and the problem was therefore largely theoretical. With a viable electronic identification infrastructure in place, Member States will need to decide how they will define the security requirements of their applications, without unfairly discriminating against foreign citizens and enterprises.
- Finally, a citizen-centric approach requiring that individuals would be able to exert sufficient personal control over their data has always been considered a crucial component of European eIDM goals (and more generally of European data protection principles). It is not clear if this aspect will be taken sufficiently into account in the current eIDM initiatives. A greater emphasis on user-centricity will therefore be needed in the future.

The concepts of identity and identity management continue to evolve, as do peoples' use of and approach to personal data and the underlying technologies. It is important to consider these changes when reflecting on the future of European electronic identity management. When keeping in mind that 2010 is not an endpoint for eIDM evolutions, and that European eIDM policies will thus need to change with the times, it becomes all the more important to ensure the robustness of the building blocks that will be available in 2010.

From that perspective, the European eIDM policies have the particular merit of exploring most of the available options. If sufficient emphasis is then placed on the integration of these building blocks into a coherent and accessible whole after 2010, taking into account, in particular, the interests of the end-users whose information is being managed and the remaining issues outlined above, electronic identity management can become one of the strengthening pillars of the European information society.

I. Introductory overview of European eIDM initiatives and ambitions

I.1. Introduction to this study

The development and deployment of electronic identity management (eIDM) solutions in European electronic applications stands at a crossroads. Over the past decades, European Member States and EEA countries have gradually rolled out identity management solutions that were best suited to their national goals and ambitions[1]. More often than not, this has entailed a fundamental overhaul of existing infrastructures: electronic databases were created to replace legacy archives, new identification numbers were introduced or tweaked, privacy protection measures were put into place, and suitable means for electronic authentication were made available to the end-users, businesses and citizens alike.

While the exact choices on each of these points vary substantially from country to country, the goals of such initiatives were uniformly the same: improving administrative efficiency, improving accessibility and user-friendliness, and above all, the reduction of costs. These are the central ambitions espoused by any eGovernment system or, indeed, most applications being offered by public or private sector entities, and the underlying enabler – the eID infrastructure – is no exception to this rule.

As will be described in greater detail below, these goals were also embraced at the European level. It is clear that the competence for choosing and organising suitable means of identification and authentication is a strictly national competence, thus ruling out any imposed European identity cards and/or business or citizen registers. Nonetheless, it was also clear that the European Union could play a strong supporting role in attempting to improve the interoperability of the means chosen by the Member States. The aspired outcome would then hopefully be that European citizens and businesses would be free to use the means for identification and authentication supported by their national administrations in foreign applications as well.

However, the challenges to be overcome before this ambition can be realised are numerous and complicated. They include political issues (such as the permissibility of unique identifiers, the desirability of identity cards, the choice of appropriate security requirements, etc.), technical issues (resolving the semantics of identity, choosing and implementing appropriate standards to communicate identity information, identifying valid sources of identity information, etc.) and legal issues (putting into place appropriate privacy safeguards, assigning responsibility for the correctness of identification information, creating a legal framework for the exchange of personal data between authentic sources, ...). All of these issues are strongly interrelated, and revolve around the central question: how can trust in electronic identity information be created at a cross-border level?

[1] *For a recent overview of eID infrastructure and ambitions in the Member States, EEA Countries and Candidate Countries, see* http://ec.europa.eu/idabc/en/document/6484/5644

Many of these questions have been extensively studied at the European level in recent years, including through studies looking into the legal and market aspects of electronic signatures in Europe[2], studies on European[3] and local or regional[4] IDM solutions, the eEpoch eEurope Smart Card project[5], the GUIDE research project[6], the eMayor project[7], the FIDIS Network of Excellence[8], the PRIME project[9] and its successor PRIMELIFE[10], and recent studies on electronic signature interoperability[11] and eID interoperability in eGovernment applications[12]. All of these studies have helped shape the debate around the realisation of interoperable IDM solutions; however, their practical impact has remained limited so far. In practice, the cross-border interoperability of identity management solutions in Europe remains largely an ambition rather than a reality.

More recent efforts are moving beyond this largely theoretical level, and are geared towards creating functioning applications. Key drivers behind this development include the i2010 Policy Framework and its eIDM ambitions[13], the large-scale eIDM pilot project

[2] *Study on the Legal and Market Aspects of Electronic Signatures in Europe (ELSIGN), 2003; see http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf*

[3] *The MODINIS IDM Study; see https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome*

[4] *The MODINIS Study on Interoperability at Local and Regional Level; see http://www.epractice.eu/document/3652*

[5] *The eEPOCH - eEurope Smart Card Charter proof of concept and holistic solution; see the summary at http://ec.europa.eu/information_society/activities/egovernment/docs/project_synopsis/syn_epoch.pdf*

[6] *See http://istrg.som.surrey.ac.uk/projects/guide/*

[7] *The eMayor Project (Electronic and Secure Municipal Administration for European Citizens); see http://www.emayor.org*

[8] *The Future of IDentity in the Information Society (FIDIS) Network of Excellence; see http://www.fidis.net/*

[9] *Privacy and Identity Management for Europe (PRIME); see https://www.prime-project.eu/*

[10] *PrimeLife - Bringing sustainable privacy and identity management to future networks and services; see http://www.primelife.eu/*

[11] *Including the IDABC Study on eID Interoperability for PEGS; see http://ec.europa.eu/idabc/en/document/6484/5644; and the Study on the Standardisation Aspects of eSignatures; see http://www.esstandardisation.eu/index.php*

[12] *IDABC Preliminary study on mutual recognition of eSignatures for eGovernment applications; see http://ec.europa.eu/idabc/en/document/6485/5938*

[13] *See http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm*

STORK[14], and of course the mandatory implementation of the Services Directive[15] by the end of 2009. All of these initiatives have the potential to act as a catalyst in furthering the vision of European eID interoperability.

Thus, the European Union is currently at a vital and most delicate stage, where theoretical studies and models will for the first time be transformed into actual working systems. In the course of this work, crucial decisions need to be made with regard to the security requirements and guarantees to be offered by the identity management system(s) to be employed in the realisation of this goal.

Given this crucial stage, ENISA has commissioned the present report. In it, the authors will describe the main tenets of European eID policy as leading up to the i2010 Policy Framework; the main infrastructural efforts being undertaken in the form of the aforementioned STORK project; and the shorter-term service-specific work being done in the context of the implementation of the Services Directive. Read collectively, this report will thus present a number of key European eID initiatives, including a description of how they relate to each other and which synergies and dependencies exist, along with an assessment of potential risks and gaps, specifically considering the need to align these initiatives into a global eIDM vision.

The document is not intended to go too deep into the details of the technical and legal complexities to be resolved at each level of these initiatives. Rather, the purpose is to provide persons involved or interested in European eID policies with an overview of some of the main initiatives in this field, including their goals, their approaches, current realisations and future expectations. It is the authors' hope that, in this way, the document can serve as a useful tool for informing policy makers, indicating how existing efforts might evolve, and perhaps helping identify future policy priorities.

With regard to structure, this document is made up of five major sections:

- The first section will provide a major outline of the European eIDM agenda, its history and goals, and a short description of the three key eID initiatives to be discussed in greater detail in sections two to four.
- Sections two to four will respectively describe the eID Roadmap as a European policy guideline, the STORK project as an infrastructural pilot effort, and the implementation of the Services Directive as a service-specific shorter-term initiative.
- Finally, section five will present a summary of the current status of eID, and will identify potential risks and elements of uncertainty in the European strategy for eID.

[14] *The ICT-PSP project Secure idenTity acrOss boRders linKed (STORK); see http://www.eid-stork.eu/*

[15] *Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT*

I.2. The European eIDM agenda – history and main goals

I.2.1. The Lisbon Strategy, the Signposts Paper and the Manchester Declaration

Before looking at specific elements of European eIDM policy, it is important to be aware of the goals that have been set at the European level, as most recently expressed through the i2010 Policy Framework for the information society and media[16] (hereafter the 'i2010 strategy').

The origin of the i2010 strategy can largely be traced back to a summit meeting held in Lisbon in 2000, which would culminate in the so-called Lisbon Strategy. At this summit, the European Council arrived at a consensus on a group of policies which collectively should lead to making the European Union into 'the most dynamic and competitive knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion, and respect for the environment by 2010.' Initially intended to be a broad plan for encouraging economic growth and improving social cohesion, the plan was re-focused in 2005.

At this time, the Commission issued a communication[17] restating its goals and targets for the Lisbon Strategy, including a number of issues that were directly related to the use of ICT in and by the Member States. While identity management as such was not yet directly mentioned in this high-level strategy document, the strategy was a significant driver behind the 2005 Ministerial eGovernment Conference in Manchester[18], where two crucial policy documents would be presented.

Firstly, the *Signposts towards eGovernment 2010* paper[19] (or in short the 'Signposts paper') was released. This document had been prepared by the eGovernment subgroup of eEurope, consisting of policy-makers and representatives of national eGovernment initiatives, as a precursor to an official policy statement. It defined four 'signposts' for

[16] *See the full description at http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm*

[17] *Communication from the Commission to the Council and the European Parliament - Common Actions for Growth and Employment : The Community Lisbon Programme, 20 July 2005; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0330:EN:NOT; see also the 2005 Communication to the spring European Council from President Barroso - Working together for growth and jobs - A new start for the Lisbon Strategy, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0024en01.pdf*

[18] *See http://ec.europa.eu/information_society/activities/egovernment/conferences/2005/index_en.htm*

[19] *See http://ec.europa.eu/information_society/activities/egovernment/docs/minconf2005/signposts2005.pdf*

improving eGovernment services by 2010 as required by the Lisbon strategy, one of which ('Key enablers for eGovernment') related directly to electronic identity management[20].

Its main ambition with regard to eIDs was stated as follows:

> *By 2010 all European citizens, businesses and administrations shall benefit from secure means of electronic identification (eID) that maximise user-convenience while respecting data protection regulations. Such means shall be made available under the responsibility of Member States but be recognised across the EU.*

The Signposts paper very emphatically declared electronic identity to be an enabler and facilitator to public services that could improve efficiency (and thus reduce costs), improve the accessibility and quality of services for businesses and citizens, while allowing them maximum control over their own data. Member States would however remain fully competent in choosing the appropriate means for electronic identification and authentication, and the paper stressed the distinction between electronic identity and electronic identity cards: while the former was considered to be an essential component of the information society, the choice of whether to opt for eID cards was left completely to the Member States to decide.

Regardless of the infrastructural choices made within the Member States, the Signposts paper emphasised that a suitable data protection framework would at any rate need to be put in place, and that a citizen-centric approach would be needed to ensure that individuals would be able to exert personal control over their data. The envisaged outcome would be to allow European citizens, businesses and administrations to benefit from an online presence that is secure, authentic, reliable and durable.

Nonetheless, the Paper also recognised the inherent interoperability risks in the Member States' freedom to introduce electronic identity solutions, and made several proposals to mitigate this problem by 2010. Central among these is the need to adopt a model that is both federated (under the responsibility of each Member State in order to respect the autonomy of different administrations) and multi-level (to allow different levels of authentication that might be needed to face differing security and authentication requirements).

This type of model would require the Member States to put in place a framework and policies which respect and interconnect national infrastructures, and which are based on the mutual recognition of electronic identities between countries. This mutual recognition depends on the definition of specific security levels, with each means of

[20] *The signpost identifying key enablers also described a similar strategy for ensuring the authentication of electronic documents; however, as this is not directly relevant to this report, it will not be discussed further.*

identification/authentication being accorded a specific security level based on its characteristics, and each application stating which security level would be needed. The Member States would then accept each means of identification/authentication as valid provided that it meets the security requirements of the application being accessed. Such policies could be implemented without any specific EU-level infrastructure being established.

With regard to the Signpost Paper's eIDM vision for 2010, the paper noted as follows:

> *By 2010, and in accordance with the principle of subsidiarity, a federated, multi-level e-Identity model will be agreed that is open and flexible enough to match national, regional, local and sectoral requirements based on a common policy framework (referred to in this document as eID). Appropriate governance principles will be developed in order to facilitate trust and security in line with Member States specific needs and as such provide the basis for the equal treatment of electronic identities throughout the EU, irrespective of the originating Member State.*
>
> *[...]*
>
> *Beyond the core of data used to uniquely determine identity, citizens often have to manage considerable volumes of personal data, as understood in a broad sense: whether userIDs, passwords, documents or site-specific data, they must keep these to hand for different types of service, and this represents a further burden on the citizen.*
>
> *The range of media, coupled with the range of data repositories that carry multiple (and often contradictory and erroneous) copies of such data and documents, represent an enormous waste of time, effort and money, both for citizens and agencies that have to correct those errors. This is even more the case when one adds the range of services available from the private sector.*
>
> *The eID framework could open the way to systems being introduced in the future that allow citizens greater control over the management and authentication of their personal data and documents. The need often for a specific card or authentication method per transaction type or per service would disappear as the eID framework would provide a basis for identifying and authenticating both the user and the data used in any transaction.*
>
> *By 2010, electronic authentication of entities (eg, citizens and businesses) as used for government processes will also be available for the private sector, to the extent that data protection legislation allows.*
>
> *One current restriction regarding online identity concerns the related issues of 'delegation', 'intermediary' and 'roles' management.*
>
> *In line with the principle of 'no citizen left behind' (see following section), any eID framework, including the eID, must allow citizens to nominate intermediaries to manage their electronic presence on their behalf (their authenticated presence, not their electronic identity), for as long as they determine, and in accordance with*

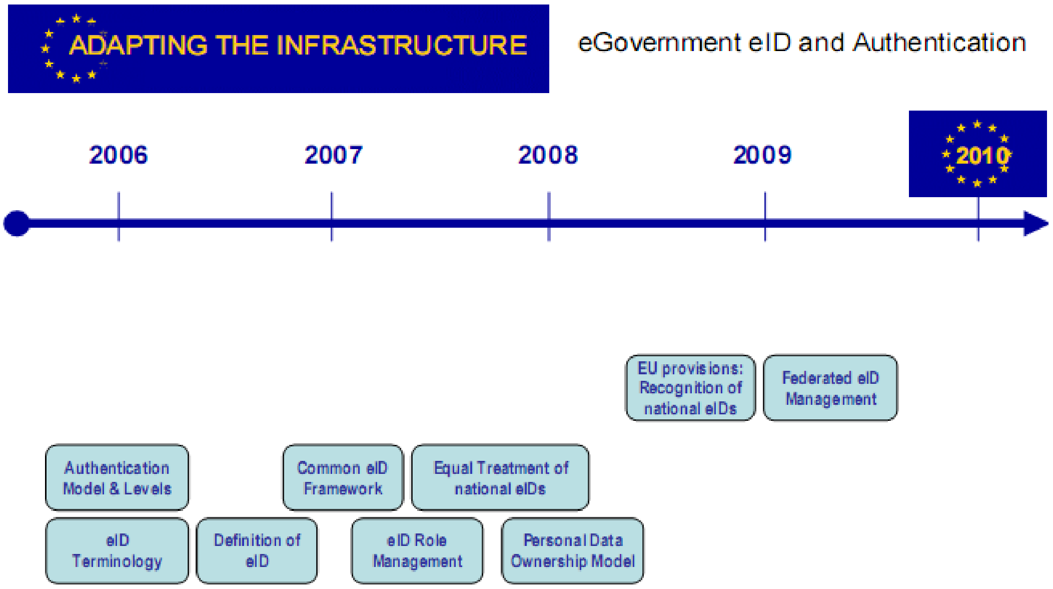
> *their instructions (as bank and post office tellers carry out client instructions against signature on a paper authorisation). In such situations, these intermediaries need to have explicit and authenticated roles that distinguish actions on behalf of another citizen from their own actions as citizens themselves.*
>
> *Further, many individuals may need other roles, determined by delegation. One person can, for example, be the treasurer and account holder of a local club and be the CEO of a company in additional to his or her basic role as a citizen. As such, different 'keys' are required according to different roles. Furthermore, the conceptual model for the eID must be able to take account of the role that an entity is playing in a given transaction.*
>
> *By 2010, eID compliant systems will support mechanisms to identify and authenticate natural persons together with their varying roles (principal, delegate, intermediary, authorised agent, etc), including roles on behalf of legal persons (administrations or businesses).*

The Signposts paper thus advanced a number of important policy principles that should be observed by future European eIDM initiatives, with a specific focus on public sector applications:

- Firstly, there is a requirement that the identity model to be created by 2010 should be *federated* and *multi-level*. The use of a federated model implies that control over electronic identity resources would remain entirely at the national level, and that identity information would be made available to relying parties based on a 'web of trust' model, ie, a model where identity information can be shared between parties which have established a relationship of trust based on a set of common agreements. Secondly, the multi-level requirement implies that Member States should remain free to choose between any number of technologies to identify and authenticate its users, and that the usability of that technology in foreign applications would be determined by its security level. In other words, every means of identification/authentication that would be usable in a cross-border context would be assigned a security rating based on its security characteristics, and should thereafter be usable in any application (including in other Member States) of an equal or lower security level.
- Secondly, the Signposts paper emphasised that future efforts should focus on optimising the benefits for the citizen as well. One way of doing this would be to ensure that the identity model to be adopted should ultimately reduce or eliminate redundancy: citizens would then no longer be required to handle duplicates of data or media, instead being able to rely on a single solution to handle all electronic transactions.
- To optimise the benefit to be gained, the identity model to be adopted by 2010 should also be usable in private sector applications, at least in so far as this is allowed under data protection regulations.
- Finally, the Signposts paper also indicated that an advanced identity management model should also address the question of mandates, delegation and roles. Both for general reasons of usability and to improve inclusion, the eID framework should allow

citizens to issue mandates to intermediaries to act on their behalf, in accordance with specific instructions.

In order to make this ambitious agenda somewhat more tangible, the Signposts paper also provided a timeline with specific building blocks to be put into place in order to realise the solution envisaged:


ADAPTING THE INFRASTRUCTURE
eGovernment eID and Authentication
2006
2007
2008
2009
2010
EU provisions: Recognition of national eIDs
Federated eID Management
Authentication Model & Levels
Common eID Framework
Equal Treatment of national eIDs
eID Terminology
Definition of eID
eID Role Management
Personal Data Ownership Model

- Interoperable eID implementation timeline, as presented on page 36 of the Signposts paper -

However, the Signposts paper itself was not a formal policy document. Therefore, in addition to the Signposts paper and, as a partial formalization of its goals, the Manchester Ministerial Declaration[21] was signed on 24 November 2005. This declaration formalised a broad commitment to the deployment and uptake of ICT resources in eGovernment applications, corresponding more or less to the ambitions of the Signposts paper, albeit in a less detailed form. Specifically in relation to identity management, the Declaration noted as follows:

> ***WIDELY AVAILABLE, TRUSTED ACCESS TO PUBLIC SERVICES ACROSS THE EU, THROUGH MUTUALLY RECOGNISED ELECTRONIC IDENTIFICATIONS***

[21] *Ministerial Declaration, approved unanimously on 24 November 2005, Manchester, United Kingdom; see http://archive.cabinetoffice.gov.uk/egov2005conference/documents/proceedings/pdf/051124declaration.pdf*

By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user-convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but be recognised across the EU.

By 2010 Member States will have agreed a framework for reference to and, where appropriate, the use of authenticated electronic documents across the EU as appropriate in terms of necessity and applicable laws.

As our eGovernment services become more transactional, the need for secure electronic means of identification for use by people accessing public services is essential for citizen and business trust and in ensuring the effectiveness and efficiency of our public administrations. Respect for, and recognition of, different forms of eID to achieve interoperability are therefore key principles for future eGovernment development.

Interoperable eIDs meeting recognised international standards and built on stable technologies would be a foundation for secure cross-border eGovernment services. As electronic identity technologies become proven in large-scale application, Member States should work together to pilot them with a view to adoption, by sharing expertise, good practices, and the tools and building blocks they have developed.

Other key enablers shall also be pursued in the future, such as recognition of electronic documents and electronic archiving.

Ultimately, there are also considerable macro-economic benefits to be gained from meeting these targets, as all economic actors would benefit. While fully respecting data protection legislation, effective use of eIDs may lead to fewer requests for the submission of data and therefore also to a reduction of the administrative burden on our businesses and citizens. eIDs, issued and managed at the national, regional or local level, that are portable, interoperable and meet an agreed common minimum standard of technical security, have the potential to support citizen mobility and create a more flexible labour market. There is also a competitive advantage for Europe in making available electronic identities that are used and accepted by both government and the private sector. These objectives and the associated benefits are therefore consistent with the Lisbon Agenda.

Related Actions

Member States will, during 2006, agree a process and roadmap for achieving the objectives of electronic identity and address the national and European legal barriers to the achievement of these objectives. Work in this area is essential if public administrations are to deliver personalised electronic services with no ambiguity as to the user's identity.

Member States will, over the period 2006-2010, work towards the mutual recognition of national electronic identities by testing, piloting and implementing suitable technologies and methods.

> *Member States will, by 2010, agree a framework for reference to and, where appropriate, the use and sustainable archiving of authenticated electronic documents.*

Thus, through the Manchester Ministerial Declaration of 2005, the Member States committed themselves to a number of specific eIDM related goals with a view of assisting in the realization of the i2010 Strategy. Most notably, the Member States agreed to strive for interoperability between the means of identification which were issued or relied on at the national level, with the goal of improving the efficiency and security of eGovernment services. This goal was to be achieved by relying on *recognised international standards and on stable technologies,* to be taken up and tested through pilots and the sharing of best practices*.* As also emphasized through the Declaration, eIDM efforts should not be focused strictly on optimizing public sector services, as private sector use-cases could prove useful in gaining the international competitive advantage sought through the Lisbon Strategy. However, some of the more detailed choices stated in the Signposts paper, such as the preference for a federated multi-level solution, were not taken up as formal goals in the Declaration.

More concretely, in reference to eIDM interoperability, the Member States committed to drafting a 'process and a roadmap' in the course of 2006 that would help them to achieve these objectives by removing national and European legal barriers to eID interoperability. In the four years after that, the process and roadmap were to be tested, piloted and implemented.

I.2.2. Follow-up through the i2010 eGovernment Action Plan and the creation of a roadmap

A first step towards drafting this process and roadmap was taken through the formal adoption in April 2006 of the i2010 eGovernment Action Plan[22], which was to be a key part of the i2010 Strategy, and which recognised interoperable eIDM as a key enabler for eGovernment, as the Signposts paper had done earlier. Apart from the reiteration of the 2010 deadline, the action plan set out a series of concrete activities to be undertaken at the European level to reach this goal:

> *The Commission, together with Member States, the private sector and civil society, will take the following action:*

[22] *The i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Communication from the Commission, 25 April 2006; see* *http://ec.europa.eu/transparency/archival_policy/docs/moreq/action_plan_i2010_en.pdf*

Year	*Ambition*
2006	*Agree with Member States on a* ***roadmap*** *setting measurable objectives and milestones on the way to a European eIDM framework by 2010 based on interoperability and mutual recognition of national eIDM.*
2007	*Agree* ***common specifications*** *for interoperable eIDM in the EU.*
2008	*Monitor* ***large-scale pilots*** *of interoperable eIDMs in cross-border services and* *implement commonly agreed specifications.*
2009	***eSignatures*** *in eGovernment: Undertake review of take-up in public services.*
2010	***Review the uptake*** *by the Member States of the European eIDM framework for interoperable eIDMs.*

Thus, the action plan was the first officially adopted policy document that indicated concrete milestones to be achieved in order to arrive at an interoperable pan-European eIDM framework by 2010.

The first step identified in this schedule was the drafting of a roadmap stating the 'measurable objectives and milestones on the way to a European eIDM framework'. As was noted above, a high-level eIDM timeline had already been defined in the Signposts document; however, this timeline was considered to be provisional and not necessarily complete. Thus, an updated and amended roadmap[23] was created within the framework of the Modinis IDM project[24] (the 'eID Roadmap'). This roadmap, which presented additional concrete building blocks, specific milestones and actions that needed to be undertaken in order to realise the ambitions of the action plan, will be further outlined in detail in section II below. It is this eID roadmap that still remains the basis for European eIDM policy within the i2010 Strategy[25].

[23] *"A Roadmap for a pan-European eIDM Framework by 2010", see http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf*

[24] *The MODINIS IDM Study; see https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome*

[25] *For a more detailed look at the roadmap and the surrounding background, see also http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/eid/index_en.htm*

The second and third ambitions of the eGovernment Action Plan in the table above relate to the creation of a set of common specifications for interoperable eIDM (in 2007), and the initiation of large-scale pilots to implement and test these specifications in actual eGovernment applications (2008). The first step was undertaken through the IDABC study on eID Interoperability for PEGS[26], consisting of a stock-taking exercise to identify the main eIDM systems in the Member States, EEA Countries and Candidate Countries[27], a comparative analysis of these systems[28], and the drafting of a set of common specifications[29] along with a proposal for a multi-level authentication policy[30]. The second step, the establishment of large-scale pilots, is currently ongoing in the form of the large-scale eIDM pilot project STORK[31], which will aim to take these common specifications to heart. Both of these initiatives will be further described in section III below, which will describe how the European eIDM ambitions are currently being translated into a pilot infrastructure.

[26] *IDABC Study on eID Interoperability for PEGS; see http://ec.europa.eu/idabc/en/document/6484/5644*

[27] *All country profiles were published on http://ec.europa.eu/idabc/en/document/6484/5644*

[28] *The Final Report on Analysis and Assessment of similarities and differences - Impact on eID interoperability; see http://ec.europa.eu/idabc/servlets/Doc?id=29618*

[29] *Common specifications for eID interoperability in the eGovernment context; see http://ec.europa.eu/idabc/servlets/Doc?id=30989*

[30] *Final Report on 'Common specifications for eID interoperability in the eGovernment context'; see http://ec.europa.eu/idabc/servlets/Doc?id=30989*

[31] *The ICT-PSP project Secure idenTity acrOss boRders linKed (STORK); see http://www.eid-stork.eu/*

I.2.3. Summary: European eIDM policy objectives

Thus, the European eIDM ambitions have been refined through a number of iterations, starting from the high-level Lisbon Strategy, to the first tangible plans in the Signposts paper and the Manchester Declaration, to arrive at the i2010 eGovernment Action Plan which led to the drafting of the roadmap.

The ultimate European goal in relation to eIDM has gradually been made more concrete: in 2010, European businesses and citizens should be able to securely identify and authenticate themselves towards applications in other Member States. This goal is not to be achieved by enforcing a harmonisation of eID tools (such as eID cards) at the national level, nor by establishing an overarching European eIDM resource to replace national resources (such as a register of European citizens); but rather by ensuring that the solutions chosen and preferred by the national administrations would be able to operate across borders.

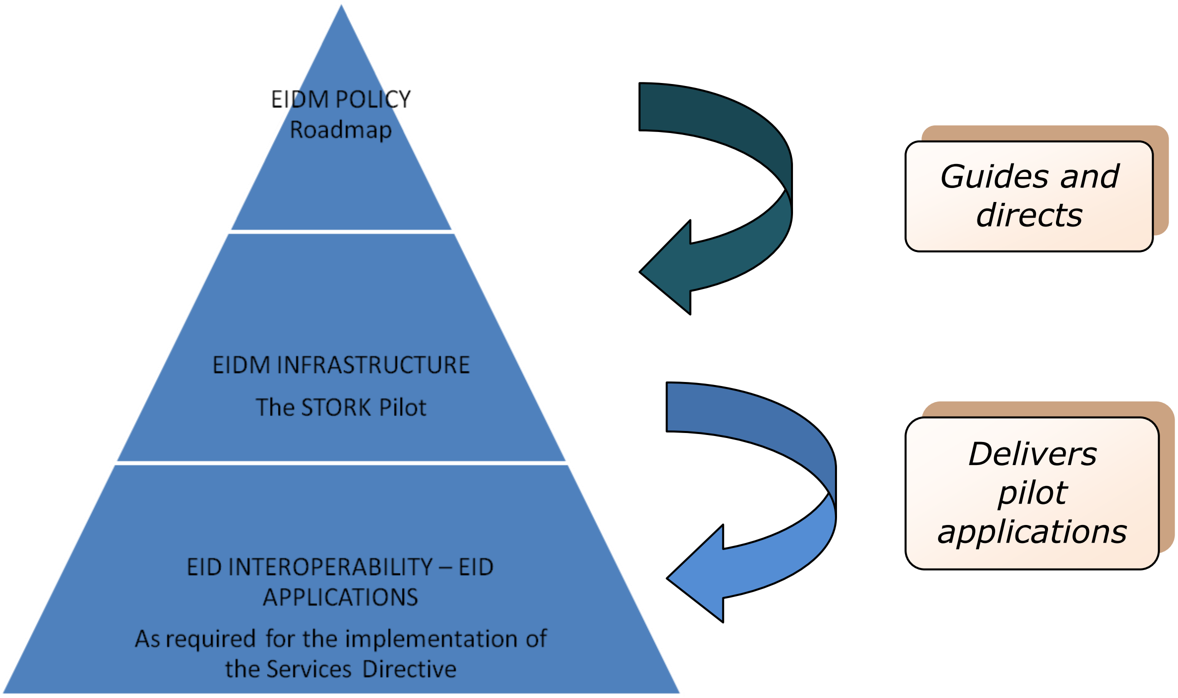
Thus, Member States will retain the freedom to organise their own identity infrastructures in accordance with their own preferences. European efforts will concentrate on establishing the necessary infrastructure to allow the national systems to interconnect and interexchange identity information. Ultimately, this should allow administrations to improve their efficiency and cut costs, open up new markets and opportunities for businesses, and improve accessibility and user experience for the citizen.

Specific details of these ambitions have been clarified through the eID Roadmap, which will be discussed in detail below. Obviously, the litmus test for any eIDM related initiative in Europe is whether or not any aspect of the roadmap is furthered. In the fifth and final section of this report, we will analyse whether Europe is on track to achieve its ambitions; and where the potential risks and uncertainties lie.

I.3. Summary overview of key initiatives for the future

This report will examine three of the aforementioned specific initiatives taken at the European level to improve eIDM interoperability and to realise the i2010 ambitions: the eID Roadmap (section 2), the STORK pilot project (section 3), and the efforts to support the implementation of the Services Directive (section 4). Each of these initiatives play out at a different level, and each of them provide an important piece of the eIDM puzzle.

From a simplified perspective, their roles and relationships can be represented as follows:


EIDM POLICY
Roadmap
EIDM INFRASTRUCTURE
The STORK Pilot
EID INTEROPERABILITY – EID APPLICATIONS
As required for the implementation of the Services Directive
Guides and directs
Delivers pilot applications

- Role of the key eIDM initiatives in this report -

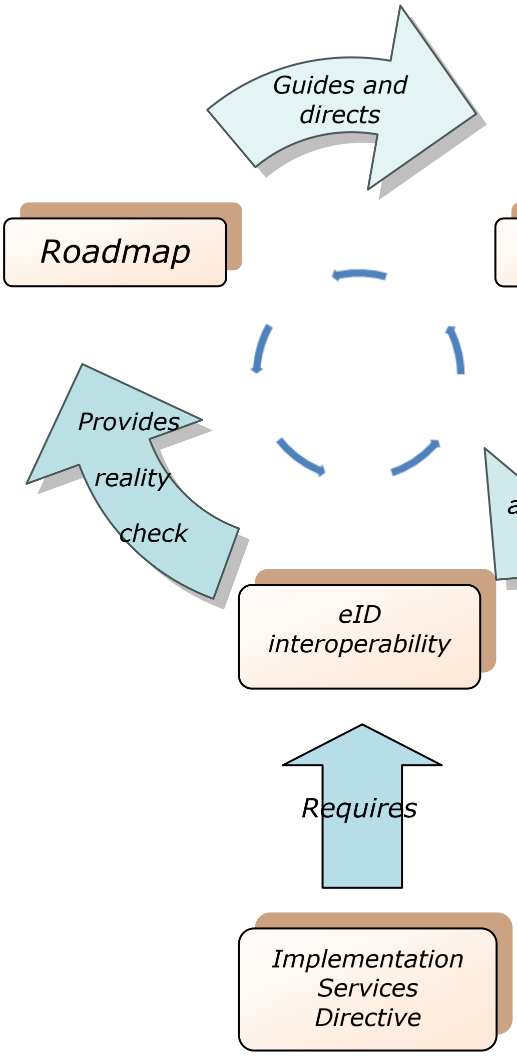
In this perception, the three initiatives are interpreted as constituting three tiers of European eIDM initiatives:

- At the first tier, the roadmap states the general eIDM policy. It determines the goals to be achieved and the principles to be respected by other European eIDM initiatives. Above and beyond that, it also defines the specific milestones for reaching these goals, and sets broad deadlines for progress in order to comply with the i2010 Strategy and the eGovernment Action Plan.
- The STORK project explores the infrastructure to be used to realise the objectives of the roadmap. The STORK project is in fact one of the milestones that was announced

and requested in the roadmap (the 'large-scale pilots' mentioned in the table above). In an ideal scenario, STORK would implement the infrastructure prescribed by the roadmap (as further detailed by other projects which have since explored the roadmap's ambitions), and this infrastructure would thereafter be the basis on which further applications could be built. More realistically, it should be kept in mind that the STORK project is a pilot initiative. While the applications to be built within STORK will be fully functional, it is thus likely that additional efforts would still be necessary to take them to a generalised public stage.

- Finally, the efforts surrounding the Services Directive play at the third tier, namely that of specific applications relying on an interoperable identity infrastructure. One of the main reasons why the Services Directive is of such immediate interest from an eIDM perspective is the fact that the directive effectively contains a deadline requiring the Member States to put in place an infrastructure that allows foreign service providers to identify themselves and communicate with competent bodies within that country. In effect, the Services Directive requires Member States to create an interoperable communications platform (a 'point of single contact' in the terminology of the directive) that incorporates an adequate mechanism to identify/authenticate users from other Member States by the end of 2009. Given the deadline involved, certain compromises will need to be made, as will be discussed in the relevant section below.

However, it is clear that this three-tiered model, which presents the relationship between the three initiatives as strictly hierarchical in nature, is overly simplified. In reality, they are all interconnected, with any progress made in any one initiative providing feedback to each of the others. This dynamic is illustrated below.



- Dynamics between the key eIDM initiatives in this report -

From this perspective, it is clear that the roadmap determines the direction in which STORK should work, but inversely it is also true that STORK will provide feedback on the feasibility of the roadmap and on potential alternative approaches. The implementation of the Services Directive on the other hand will have to explore the issue of eID interoperability in parallel with STORK, given the strict deadline which does not allow implementation to wait until STORK has concluded. Thus, the overview below will provide the key features and current status of all three initiatives, but it is clear that some aspects will continue to evolve as the initiatives mature further.

Obviously, the three initiatives described in this report do not compose the whole of European eIDM related actions. Other notable ongoing projects with eID relevance include the large-scale pilot on public procurements PEPPOL[32], information exchange initiatives such as BRITE[33] and ECRIS[34], and more fundamental research projects such as the aforementioned FIDIS and PRIMELife. However, this report will focus mainly on the roadmap, STORK and the Services Directive as a fair sample of current European eIDM initiatives and the general direction in which these initiatives are developing. This way, the reader will hopefully get a solid and pragmatic overview of the most recent developments.

[32] *Large-scale pilot on pan-European Public eProcurement Online; see http://www.peppol.eu/*

[33] *Integrated project aiming to achieve Business Register Interoperability Throughout Europe; see http://www.briteproject.net/*

[34] *European Criminal Records Information System (ECRIS), aimed at improving collaboration between European criminal investigators, as described in Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record; see also http://europa.eu/scadplus/leg/en/lvb/l14500.htm*

II. eIDM Policy: Roadmap for a pan-European eIDM Framework by 2010

II.1. Historical background and goals

As was already commented on above, the origins of the eID Roadmap[35] are firmly rooted in the Lisbon Strategy, the i2010 Strategy, and the i2010 eGovernment Action Plan[36] that was adopted in 2006. Especially in the latter document, the availability of interoperable eIDM solutions was recognised as a key driver in achieving the objectives of the Lisbon Strategy, and the action plan required certain initiatives to be taken to achieve this goal. The first of these, scheduled for 2006, was the creation of a roadmap *setting measurable objectives and milestones on the way to a European eIDM framework by 2010 based on interoperability and mutual recognition of national eIDM.*

The main purpose of this roadmap was thus to define the steps to be taken in order to achieve the European ambition of realising interoperability between the national eID solutions (whether smart card based, soft certificates, OTP, username/password, ...), particularly for the purposes of accessing eGovernment applications. An initial high-level eIDM timeline had already been defined in the aforementioned Signposts document, which identified a number of crucial building blocks, including the need to define an authentication model and security levels, the mutual recognition of national eIDs, and the implementation of a federated eIDM model.

However, the timeline presented in the Signposts paper was considered to be provisional, as the mentioned building blocks were not necessarily considered complete or understood. For this reason too, the eGovernment Action Plan required a more detailed roadmap to be elaborated.

At the time, under the umbrella of the MODINIS Programme[37], a number of eIDM related initiatives were already underway to examine interoperability issues between existing national eID solutions and to provide recommendations and strategies for improvement. One of these, under the heading of the MODINIS IDM study[38] was being conducted by a

[35] *A Roadmap for a pan-European eIDM Framework by 2010, see http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf*

[36] *The i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Communication from the Commission, 25 April 2006; see http://ec.europa.eu/transparency/archival_policy/docs/moreq/action_plan_i2010_en.pdf*

[37] *Multi-annual programme for the monitoring of the eEurope 2005 action plan, dissemination of good practices and the improvement of network and information security (MODINIS); established through Decision No 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 adopting MODINIS; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:02003D2256-20051227%20:EN:NOT; for a global overview of MODINIS Activities, see http://ec.europa.eu/information_society/eeurope/i2010/archive/modinis/index_en.htm.*

[38] *The MODINIS IDM Study; see https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome*

group headed by the K U Leuven - ESAT/COSIC (Belgium), supported by the A-SIT Secure Information Technology Center (Austria) and the law firm Lawfort (Belgium). This study was generally tasked with:

- assessing the impact of national eIDM initiatives on the policies supporting cross-border and cross-sector eGovernment services;
- providing a prospective analysis of possible initiatives and solutions at the European level;
- providing information on identity technologies, related market developments, and technical requirements; and
- identifying eIDM related good practice cases to be collected in the broader MODINIS Good Practices Framework.

While the specific needs of the eGovernment Action Plan were not explicitly included in the tasks of the MODINIS IDM study[39], the terms of reference were considered to be broad enough, and the study team was asked to prepare a draft roadmap. After a number of iterations, the MODINIS IDM project finalised the roadmap in collaboration with the SecurEgov study team[40] in December 2006. This document, which has not been modified since, presented additional concrete building blocks, specific milestones, and actions that needed to be undertaken in order to realise the ambitions of the action plan. The main tenets of the roadmap will be commented on further below.

[39] *This would not have been possible chronologically, as the terms of reference for the study were published in late 2004; whereas the eGovernment Action Plan was adopted in April 2006.*

[40] *SecurEgov: Security at the heart of eGovernment; see www.securegov.eu*

II.2. Current status and key characteristics

The eID Roadmap paper, as published on the DG INFSO website[41], consists of three major parts: an introduction commenting on European eIDM goals, an actual roadmap defining building blocks, support measures and milestones, and an annex commenting on each of the building blocks and explaining their importance. Each of these elements will be briefly examined below.

II.2.1. Introduction – Goals and design criteria

After recalling the policy background of the roadmap, the paper first defined the key principles to be observed by any proposal aiming to improve eIDM interoperability at the pan-European level, in order to define the restrictions to be respected by the roadmap. Central among these is the principle of subsidiarity, meaning that the Member States must retain the autonomy and responsibility to pursue their own eIDM goals using the means they see fit. Despite this principle, the adoption of the Manchester Ministerial Declaration also implies that certain minimal requirements will need to be put in place and followed by all parties involved. The final goal is to create an interoperability framework that is sufficiently attractive to end-users (and most notably to citizens) to ensure that they will want to embrace it, rather than being required to do so.

The roadmap defined the following design principles as being crucial to the development of such a framework:

> *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 each user with the means to identify and authenticate himself electronically, if it wishes to allow him to access and to benefit from eIDM services abroad. A user has the ability to act autonomously and to make use of the offered services.*

[41] *See http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/eid/index_en.htm*

4. With regard to authorisations of mandates or representations, each Member State should provide the means to manage the competences of 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. A high-level consensus must be established between Member States on an eIDM terminology in order to guarantee conceptual and semantic interoperability. Appropriate policy and legal measures can be used to corroborate this consensus.

Thus, the design principles put a strong emphasis on the consequences of consistently applying the subsidiarity principle: European initiatives should not prohibit Member States from deploying solutions that are well attuned to local needs, and Member States should remain in control of local eIDM infrastructure, including the choice and use of identifiers, attributes and mandates. The main task imposed on Members States is their duty to ensure that this infrastructure is functional: they must be able to uniquely identify and/or authenticate citizens and businesses established within their borders using electronic means, and to determine their authorisations or mandates in cases that require this. It is clear, then, that these principles point broadly speaking in the direction of a federated system.

This is also stated emphatically in the design criteria that the roadmap derived from these basic principles, and which are largely similar to the criteria noted in the Signposts paper. These criteria stated that any future pan-European eIDM system would need to be:

1. Federated in a policy sense, ie, 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. 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. Multi-level, 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 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 at a European level which must be met for each authentication level.

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

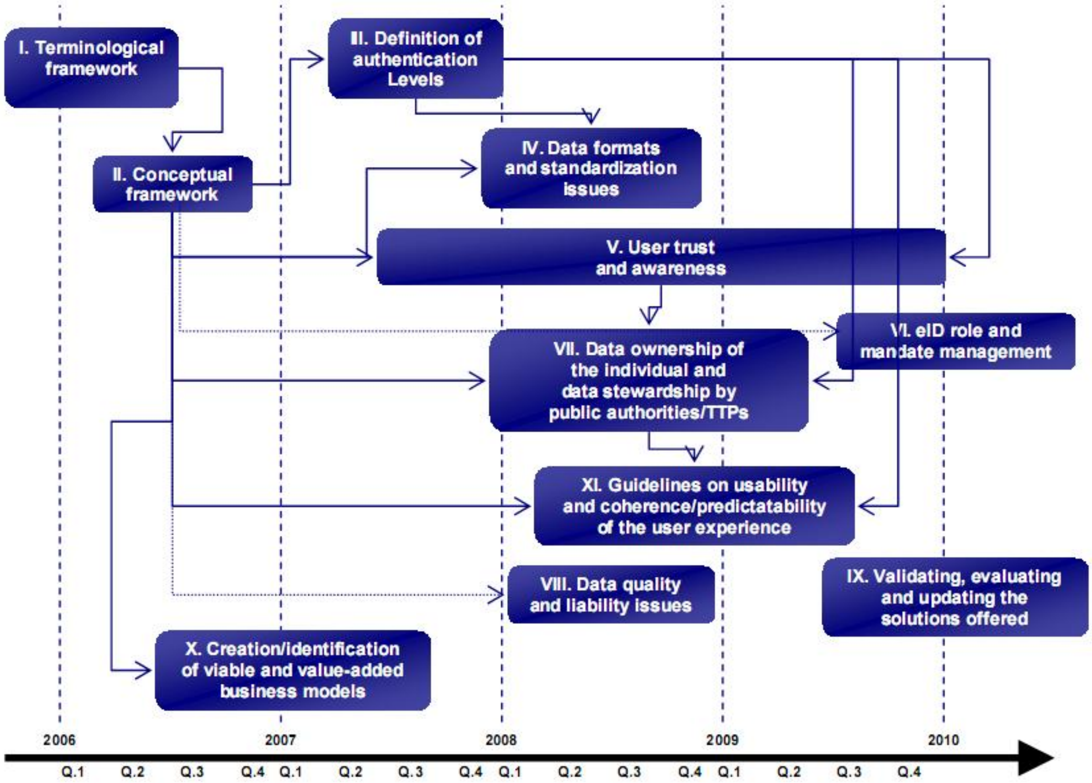
5. Enabling private sector uptake, where Member States choose to rely on private sector partners (eg, financial institutions) for the provision of eIDM services. Note that this only implies that private partners may be involved in identity management tasks, such as the definition, designation and administration 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 the public eIDM infrastructure may be necessary in order to ensure a sufficient return on investment.

Thus, to a large extent the roadmap was based on the same principles already stated in the Signposts paper, including the use of identity federation and the need to define multiple security levels for eIDM services to ensure the cross-border viability of a variety of identification solutions. A newer element was the requirement to rely on authentic sources for identity data, ie, an obligation to reduce data duplication and to ensure that each piece of identity information has only one official and correct source.

II.2.2. The Roadmap – Building blocks, support measures and milestones

Based on these principles, the roadmap defined a series of eleven building blocks to be put in place in order to reach the goal of interoperability between national eIDM solutions by 2010.

Graphically, their interdependency and timing (in quarters per year) was represented as follows:


I. Terminological framework
III. Definition of authentication Levels
II. Conceptual framework
IV. Data formats and standardization issues
V. User trust and awareness
VI. eID role and mandate management
VII. Data ownership of the individual and data stewardship by public authorities/TTPs
XI. Guidelines on usability and coherence/predictatability of the user experience
VIII. Data quality and liability issues
IX. Validating, evaluating and updating the solutions offered
X. Creation/identification of viable and value-added business models
2006
2007
2008
2009
2010
Q.1
Q.2
Q.3
Q.4
Q.1
Q.2
Q.3
Q.4
Q.1
Q.2
Q.3
Q.4
Q.1
Q.2
Q.3
Q.4

- Graphical representation of building blocks (timing and interdependency) in the Roadmap, page 6 -

These building blocks were divided into three major categories:

- Fundamental requirements, ie, requirements related to the basic principles stated above: 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); and

- Usability requirements: validation of solution models and business models, cooperation between public and private sectors and ensuring a harmonious user experience.

These building blocks were described in greater detail in the annex to the roadmap, along with certain success criteria to determine how the building blocks should be taken up. A few of these building blocks will be commented on further below.

In addition to these building blocks, the roadmap also specified a number of actions to be undertaken and milestones to be achieved. These will be addressed in section II.3 below.

II.2.3. Building blocks – Definition and follow-up

The roadmap defined eleven building blocks to be put in place in order to achieve its objectives by 2010. Some of these building blocks have been realised already, whereas others are to be explored further through forthcoming initiatives, most notably the STORK project. The table below summarises the main scope of each of the building blocks, and indicates whether and, if so, how they have been put in place.

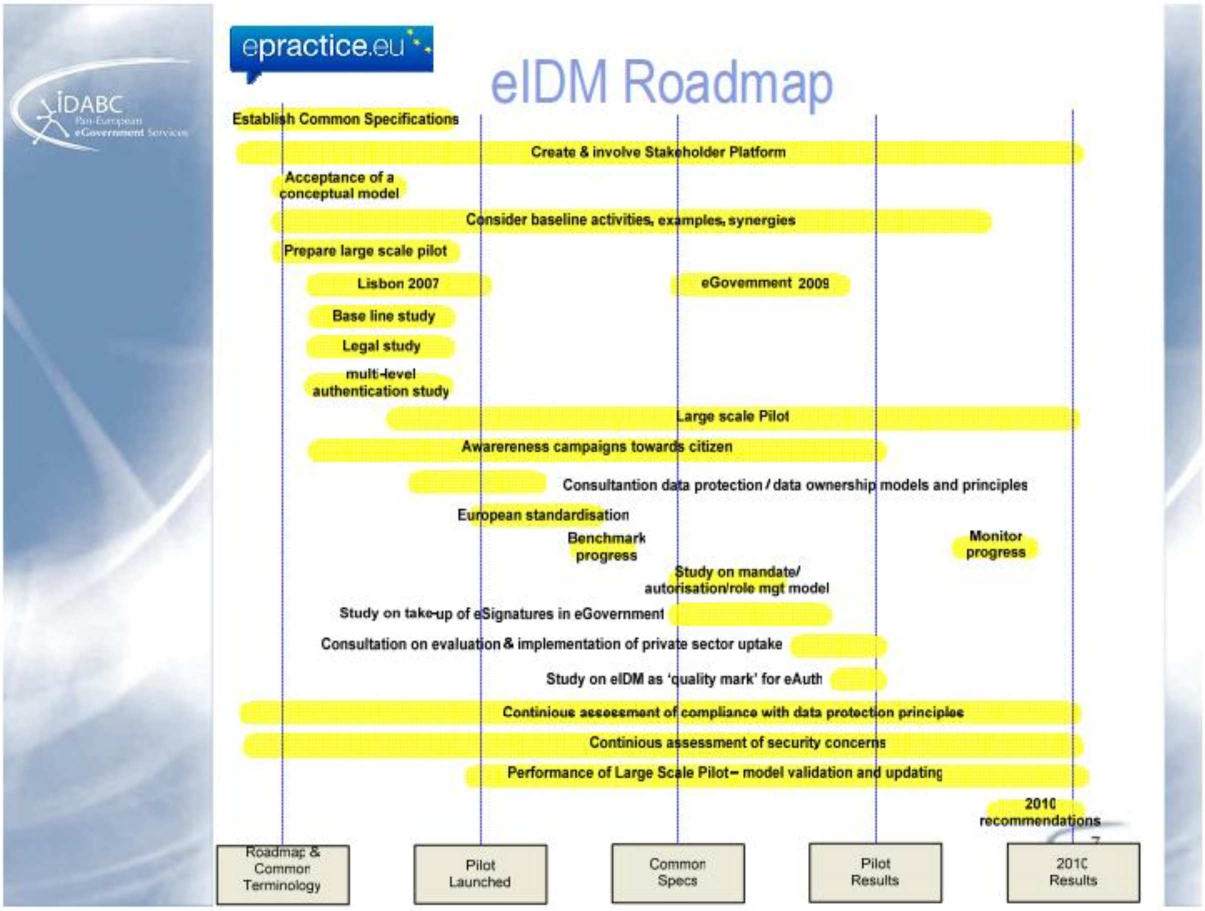
Building block	Deadline	Scope and follow-up
Terminological framework	Q2 2006	*Scope:* a standardised terminology document should be created to unambiguously define certain key notions. *Followed up through:* the terminology paper produced in the course of the MODINIS IDM study; see below.
Conceptual framework	Q2 2006	*Scope:* an infrastructural model for the implementation of an interoperability solution should be created to guide further efforts. *Followed up through:* the common specifications drafted in the course of the IDABC study on eID Interoperability for PEGS; see below.
Authentication levels	Q3 2007	*Scope:* a multi-level authentication policy should be drafted that defines requirements for security levels that can be applied to any identification/authentication solution. *Followed up through:* the proposal for a multi-level authentication policy drafted in the course of the IDABC study on eID Interoperability for PEGS; see below.
Data formats / standardisation	Q4 2007	*Scope:* implementation of an interoperability solution requires an adequate consensus on data formats and standards to be applied. *Followed up through:* to a small extent the common specifications; and to be explored further and implemented in a pilot stage through the STORK project.
User trust and awareness	Q3 2008	*Scope:* users must be adequately informed of the functionality and safeguards built into the system. *Followed up through:* to a small extent to be explored further and implemented in a pilot stage through the

		STORK project; but largely dependent on national efforts following the conclusion of the STORK project.
eID role / mandate management and delegation	Q2 2010	*Scope:* citizens should be able to designate persons to represent them in transactions, and the eIDM solution they use should support this. *Followed up through:* no follow-up as of yet.
Data ownership / stewardship	Q2 2009	*Scope:* the data protection model to be embraced should ensure that data subjects (citizens) retain optimal control over their personal data through a stewardship approach. *Followed up through:* to be explored further and implemented in a pilot stage through the STORK project.
Data quality and liability	Q4 2008	*Scope:* given the reliance on foreign data sources, the responsibilities and liabilities assumed by the data sources should be clarified. *Followed up through:* to be explored further and implemented in a pilot stage through the STORK project.
Validation of solution model(s)	Q2 2010	*Scope:* once an eIDM infrastructure has been set up, its operations must be continuously evaluated to look for possible weaknesses and desirable improvements. *Followed up through:* no follow-up as of yet (as not applicable yet, given that no implementation exists yet, even in the pilot stage).
Creation and identification of business models	Q3 2007	*Scope:* to ensure that the interoperability framework is actually used in practice, the emphasis should be on providing services with an added value to the user. *Followed up through:* implicitly through the choice of pilot applications for the STORK project; but to a large extent this is dependent on the local context.
Usability	Q3 2010	*Scope:* to improve the user experience, certain agreements will need to be put in place regarding the presentation of a homogeneous interface to the user. *Followed up through:* to be explored further and implemented in a pilot stage through the STORK project.

Thus, most of the building blocks have been implemented or are planned to be implemented in some form. In the section below, we will examine more concretely how this has been done.

II.3. Impact on European eIDM developments

As has already been made clear to some extent in the building blocks table above, the roadmap has had a significant impact on a number of European eIDM related initiatives, by steering their efforts in a certain direction or by defining the issues they need to focus on. A central tool to ensure that this would occur was the actions list included in the roadmap, which split the building blocks up into more manageable action items. The following graphical representation is occasionally used to represent this list:



eIDM Roadmap

Establish Common Specifications

Create & involve Stakeholder Platform

Acceptance of a conceptual model

Consider baseline activities, examples, synergies

Prepare large scale pilot

Lisbon 2007

eGovernment 2009

Base line study

Legal study

multi-level authentication study

Large scale Pilot

Awarereness campaigns towards citizen

Consultantion data protection / data ownership models and principles

European standardisation

Benchmark progress

Monitor progress

Study on mandate/ autorisation/role mgt model

Study on take-up of eSignatures in eGovernment

Consultation on evaluation & implementation of private sector uptake

Study on eIDM as 'quality mark' for eAuth

Continious assessment of compliance with data protection principles

Continious assessment of security concerns

Performance of Large Scale Pilot – model validation and updating

2010 recommendations

Roadmap & Common Terminology

Pilot Launched

Common Specs

Pilot Results

2010 Results

7

- Action item list, as presented on behalf of IDABC[42] -

[42] *Source: PowerPoint presentation on European eIDM schemes and eIDM interoperability, on behalf of IDABC by M Gzim Ocakoglu, presented at the eIdentity Workshop in Brussels, 14 February 2008; see http://www.epractice.eu/files/upload/workshop/65-1203068963.pdf*

Rather than focusing on the exact deadlines for each of the actions – not mentioned in the graphic above – this overview focuses more on the broader strategies to be followed. As indicated at the lower end of the graphic, this representation focuses on five categories of tasks:

- The preparatory work, including adopting the roadmap and a common terminology, but also (as indicated in yellow blocks) by conducting a number of preparatory studies and by preparing a large-scale pilot (ie, the STORK project);
- The actual launch of the pilot, which took place in May 2008, which will be commented on below;
- The elaboration of more detailed common specifications in the course of the pilot, including further efforts at standardisation and at conducting a study on the management of mandates, authorisations, roles and delegation;
- Finalisation of the pilot's results and preparing a full scale rollout; and
- Achieving the objectives of i2010 by deploying the outcome of the pilot.

As scheduled, a number of these actions have already been undertaken and completed in preparation for the STORK large-scale pilot.

One of the preparatory actions scheduled by the roadmap was the creation of a terminology paper. The aforementioned MODINIS IDM study examined this issue, noting that *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*[43]. Thus, the drafting of a common vocabulary was seen as an important step to facilitate discussions of interoperability. Consequently, a terminology paper was prepared within the framework of the Modinis IDM study[44]. However, the terminology paper was not officially endorsed, and it does not appear to have seen significant uptake.

In addition, the roadmap called for a number of preliminary studies to be conducted into national eIDM policies (identified in the graphic above as the 'baseline study', 'legal study' and 'multi-level authentication study'), in order to better define the interoperability problems to be resolved. Most of these elements were combined into a single study, the IDABC study on eID Interoperability for PEGS[45], which included, most notably, the following components:

- The identification of the main national eID approaches in the European Member States, EEA Countries and Candidate Countries, through the drafting of 32 national profiles[46];

[43] *As noted in the annex to the eID Roadmap, page 12.*

[44] *See https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc*

[45] *See http://ec.europa.eu/idabc/en/document/6484/5644*

[46] *See the 32 individual reports published on http://ec.europa.eu/idabc/en/document/6484/5644*

- The comparative analysis and assessment of the differences and similarities between these countries, resulting in the identification of the main interoperability issues[47];
- The identification of several key approaches to eID interoperability[48], along with a comparative assessment of these approaches[49] in order to determine possible models for a solution.

These reports eventually resulted in the drafting of a set of common specifications and of a multi-level authentication policy, to be tested and extended or updated during the course of the STORK project.

Thus, it is clear that the roadmap has played a significant role in steering European eIDM initiatives towards the next phase, the STORK project, and towards the eventual goal of achieving the objectives of the eGovernment Action Plan.

[47] *See http://ec.europa.eu/idabc/servlets/Doc?id=29618*

[48] *See http://ec.europa.eu/idabc/servlets/Doc?id=29619*

[49] *See http://ec.europa.eu/idabc/servlets/Doc?id=29620*

II.4. Considerations for the future

As was already outlined above, the roadmap's goal is to outline the steps that need to be taken in order to reach the objectives of the i2010 strategy and, specifically, the eIDM ambitions as stated in the eGovernment Action Plan. Thus, it has played an important role in shaping European eIDM initiatives and it is likely to continue to do so.

Its main future impact will lie in the further influence it will likely have on the STORK project, as the roadmap outlines the functionality to be provided by the project at a high level. Examining the building block table in section II.2 above and looking at the issues which have not yet been adequately covered, substantial contributions are still to be expected with regard to:

- Data formats and standardisation; Here the common specifications have remained at a high level of abstraction. The only standard that was directly referenced in the common specifications was SAML, which thus still leaves a large number of options and choices open to the STORK consortium. While this freedom is partially beneficial, as will be further discussed in the next section, substantial technical choices still to be made within STORK.
- Data ownership and data protection models[50]: Broad principles have been outlined in the roadmap, which emphasise that the citizen or enterprise using the infrastructure should be able to manage his identity attributes to a significant degree and that minimal personal data should be disclosed to applications. However, no pragmatic solution appears to have been presented yet in any of the current preparatory documents, which focus more on the technical and infrastructural issues surrounding interoperability, but not on the data protection aspect[51]. The issue of inspiring trust with end-users is, of course, strongly correlated with this.
- Data quality and liability, specifically in determining the responsibilities and liabilities which are assumed by each entity involved in cross-border identification/authorisation: The main question in this regard relates to the guarantees that need to be given by legal entities such as identity providers which manage identity attributes at the national level, or proxy service providers which are responsible for facilitating cross-border authentication, as will be further commented on below. The responsibilities of such entities cannot be defined until a specific interoperability model is established, and this question will be examined by STORK. Only once this question has been clarified can a suitable legal framework be created.
- eID role management and delegation: This has been identified as a strong enabler both to increased functionality (ie, by automatically determining the legal

[50] *See http://enisa.europa.eu/doc/pdf/publications/privacy_features_of_eid_cards.pdf*

[51] *Despite very laudable and promising efforts in a number of key projects such as the aforementioned PRIME project, which have created state-of-the-art models for personal data protection in online identification systems.*

> competence to represent an entity in a transaction) and improved data protection (ie, through role-based authentication). However, even at a national level very little progress has been made in modelling roles and delegations; thus, it is very unlikely that substantial cross-border progress will be made in this area by 2010. This building block of the roadmap is therefore unlikely to be put in place by 2010, and will likely have to be re-examined at a later stage, once national approaches to this issue have emerged.

As these are all issues identified in the roadmap, it can be expected that some progress in addressing them will still be made by 2010. However, the timeline of 2010 is very ambitious, especially when considering the time that will undoubtedly expire between the finalisation of the STORK pilot and the actual implementation of a similar solution that is open to the public. Similarly, there is no guarantee that the STORK pilot will attain all the goals it has set out to achieve, nor any guarantee that the approach adopted through the pilot will see active support and take-up in all Member States. Thus, the available time may prove to be inadequate to meet all the objectives of the eGovernment Action Plan. This is also implicitly acknowledged in the roadmap itself, which states:

> *Given time restrictions, [...] the priority should primarily be to realise the basic identification/authentication functionality as expressed by the milestones; and*
>
> *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.*

In order to determine the extent to which the roadmap – now almost three years old – is still accurate and realistic, the Commission has announced that a new action plan will be presented in 2008 *to further promote the implementation of mutually recognised and interoperable electronic signatures and e-authentication (electronic identity) among the Member States, thereby facilitating the provision of cross-border public services*[52]. It is not yet clear if and how this will impact the current roadmap. However, a future revision of the roadmap taking into account a broader time frame (eg, 2015) would be beneficial, once the impact and influence of the STORK project becomes clearer.

[52] *See the Commission Staff Working Document of 17 April 2008, Preparing Europe's digital future - i2010 Mid-Term Review - Volume 2: i2010 - List of actions; see* *http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2008/sec_2008_470_Vol_2.pdf*

III. eIDM Infrastructure: the STORK initiative

III.1. Historical background and goals

As was already noted in the introduction above, the concept of a large-scale pilot to explore an implementation of a pan-European eID interoperability system is a long-standing notion. It was first referenced in the 2005 Manchester Declaration, where it was considered as a method of consolidating good practices and common experiences:

> *Interoperable eIDs meeting recognised international standards and built on stable technologies would be a foundation for secure cross-border eGovernment services. As electronic identity technologies become proven in large-scale applications, Member States should work together to pilot them with a view to adoption, by sharing expertise, good practices and the tools and building blocks they have developed.*

The 2006 eGovernment Action plan and the eID Roadmap affirmed this role, calling for the Commission to *monitor large-scale pilots of interoperable eIDMs in cross-border services and implement commonly agreed specifications*. Thus, the pilot was conceived as an initiative to be supervised by the Commission, but in which the emphasis was otherwise to be left at the national level, in conformity with what one might expect, given the importance of the subsidiarity principle in determining European eIDM policy.

The eGovernment Action Plan called for the large-scale pilot to be launched in the course of 2008, and subsequently a call for proposals was announced within the framework of the Competitiveness and Innovation Programme (2007-2013) - ICT Policy Support Programme (commonly abbreviated as the CIP – ICT PSP Programme[53]). One of the themes of the call for proposals[54] was the provision of efficient and interoperable eGovernment services, to be addressed via four key objectives:

- the EU-wide implementation and access to electronic public procurement (eProcurement);
- the availability of an EU-wide interoperable system for the recognition of electronic identification (eID) and authentication;
- the provision of innovative ICT-based solutions that support administrations' efforts to process and deliver better public services to all and cope with secure document management and archiving; and
- the stimulation of experience sharing, re-use and cooperation in the uptake of innovative eGovernment services.

The first three objectives were to be implemented via large-scale pilots, with the second, of course, eventually resulting in what would later become known as the STORK project.

[53] *For more information on the Policy Support Programme, see http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm*

[54] *See http://ec.europa.eu/information_society/activities/ict_psp/documents/ICT_PSP_WP2008.pdf*

Strategically, the second objective (the availability of an EU-wide interoperable system for the recognition of electronic identification and authentication) was envisioned to be achieved by supporting only one pilot, characterised as a so-called Pilot Type A. Type A pilots emphasise the need to build on initiatives in Member States or associated countries, and require that these countries organise a framework for collaboration to improve the interoperability/interaction between applications that already exist at the national level. Applied to the eID context, the pilot should aim to create cross-border interoperability between existing applications by relying on existing means of electronic identification/authentication.

Thus, the emphasis was to be on creating functioning applications which would effectively be accessible to the end-users, and which would have a significant and meaningful impact in practice. Out of the 36 month duration of the pilots, at least 12 months should include an operational phase during which the pilot applications can actually be used. Furthermore, the pilots should aim to ensure that the outcome is durable, in the sense that successful pilot applications should be able to keep running after the conclusion of the project with limited additional modifications.

As prescribed in the ICT PSP Programme, the pilot should:

- contribute to accelerating the deployment of eID for public services, while ensuring co-ordination between national and EC initiatives in the field and support federated eID management schemes across Europe based on open standard definitions where appropriate; and
- test, in real life environments, secure and easy-to-use eID solutions for citizens and businesses, in particular SMEs and government employees at relevant levels (local, regional, national and cross-border levels).

Thus, the resulting integrated pilot solution should support the cross-border recognition of eID and authentication solutions across Europe, and should be tested for a set of relevant services to be proposed by the consortium. As required by the eGovernment Action Plan, the pilots should be based on an interoperability layer and federated eID management schemes characterised through common specifications including a reference architecture. Prior inputs (such as the common specifications drafted in the course of the aforementioned IDABC study on eID interoperability for PEGS) should be taken into account, although the call for tender did not consider these to be binding on the efforts of the consortium[55]. Given the current state of these common specifications, they will be taken up as a general guideline to STORK's efforts.

As was already noted above, these common specifications[56] were drafted in order to describe a high-level federated model for interoperability that would be technology neutral

[55] *Which would indeed not have been prudent, as the common specifications document had not yet been finalised at the time of publication of the call for proposals.*

[56] *Common specifications for eID interoperability in the eGovernment context; see http://ec.europa.eu/idabc/servlets/Doc?id=30989*

(ie, allow the integration of any identification/authentication solutions) and support multiple security levels of authentication. Within the aforementioned IDABC study, a model was presented that relied on a proxy approach requiring the creation of identity providers (IDPs) at the national level (at least one per country). This system of national IDPS is coupled with a network of proxy service providers referred to as Pan European Proxy Services (PEPS). These will typically be created at the national level, although the model also allows for a centralised European PEPS to be put in place, or even for a 'mixed model' in which certain countries rely on a national PEPS, whereas others rely on a centralised European PEPS.

These proxy service providers essentially serve to overcome the technical middleware barrier that presents itself when vastly different electronic identification/authentication solutions are used, as is the case in the European eID scene. For example, in some cases, a citizen may want to use a username/password combination to identify himself towards a foreign application, whereas another citizen will want to use his eID card. Provided that the application owner considers both of these methods to be acceptably safe, the technical infrastructure should be able to support both solutions. This is where the PEPS is involved.

Briefly summarised, the main function of the PEPS is to connect service providers to the appropriate identity providers in each country and to validate the trust and security of the identity information sent by the identity providers. Thus, the multitude of PEPS would form a 'circle of trust', in much the same way as other solutions such as, for example, the Liberty Alliance. In order to transport identity attributes from the IDP to the service providers through the PEPS, the use of SAML assertions is suggested. It remains to be seen to what extent the STORK consortium will be able to take up this aspect, given that there are still security concerns related to the use of SAML that must be resolved, specifically the risk of possible man-in-the-middle attacks.

This general approach of relying on proxy service providers is sometimes contrasted with other viable interoperability solutions, such as a so-called middleware approach where the emphasis is on harmonising the middleware used by different authentication solutions or a model in which x.509-compliant soft PKI certificates are generated 'on the fly' for non-x.509-based solutions, making these certificates and OCSP lookups the uniform identification mechanism instead of SAML assertions. However, the common specifications as drafted in the IDABC study favoured a proxy-based approach using SAML, as it was felt that SAML constituted a key standard with a certain degree of maturity (eg, the existence of SAML contexts) and acceptance in the field and also because SAML would allow for better modularity, ie, it would be easier to adjust the amount of information in a specific SAML assertion, which would be favourable for privacy protection.

STORK also plans to explore the middleware approach and, specifically, the question of how it could interact with the PEPS model broadly described in the common specifications. This will largely depend on the viability of connecting both models, ie, on whether it will be possible within the means of the STORK project to interconnect systems based on a PEPS approach and systems based on a middleware approach. This issue is currently being evaluated.

Apart from this general architecture, the common specifications also outline a number of more technical elements, including the use of SAML contexts, IDP service requirements and service provider requirements. However, it remains to be seen if, and to what extent, these requirements will be followed within the STORK project.

The call for proposals containing these requirements (CIP-ICT PSP-2007-1) was published on 23 May 2007. With regard to the composition of the consortium, the call noted that the participating administrations should have the required competence and expertise on the subject, and that the consortium should also comprise all necessary stakeholders in the value-chain (eg, service and content providers, industries including SMEs, end-user representatives, etc). Thus, while public administrations were required to take a leading role in the consortium, the involvement of private partners was encouraged and even required. To ensure that the consortium would qualify as a representative 'large-scale' pilot, a minimum of six relevant national administrations was required, with six to ten Member States or associated countries being recommended.

In response to this call for proposals, the STORK (Secure idenTity acrOss boRders linKed) consortium was formed. Coordinated by ATOS Origin Sociedad Anonima Española, it comprised 13 Member States (Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden and the United Kingdom), one associated country (the EEA country Iceland), and 14 other participants from the public and private sector, including NGOs[57]. It is this consortium which is presently conducting the STORK project, which will be described in greater detail below. The total budget of the project is set at 20 million EUR, 50% of which is funded by the European Commission.

[57] *For a full list of partners, see http://www.eid-stork.eu/index.php?option=com_content&task=view&id=53&Itemid=74. It should be noted that in some cases private parties have been mandated to represent Member States during the course of the project.*

III.2. Current status and key characteristics

The STORK project[58] was launched on 30 May 2008, and had its kick-off meeting on 19 June 2008. Given this recent start and the three year running period, thus far no deliverables or output have been made public yet. However, certain information on the structure of the pilot, key ambitions and characteristics can already be provided.

Structurally, STORK is subdivided into the following work packages:

- WP1: Project management, lead by ATOS Origin Sociedad Anonima Española.
- WP2: eID Inventory, Trust and Application Groups, ie, the identification of eID mechanisms and relevant eID interoperability solutions in all participating countries, using the IDABC study as a baseline for further work. This will also include the identification of authentication levels and corresponding trustworthiness in each of the countries, with a view to determining the levels which it would be appropriate to examine further in the context of the pilots. This work package is headed by the Netherlands as WP2 leaders.
- WP3: eID and Upcoming Technologies, ie, ensuring that future developments (such as the use of mobile phones for electronic identification, harmonisation of middleware, RFIC, etc) could be integrated into the final outcome; this work package is headed by Austria.
- WP4: eID Process Flows, ie, identifying and defining the exact processes behind the cross-border identification/authentication process; lead by the UK.
- WP5: eID and Common Specifications, ie, the development of the existing common specifications into a workable implementation. This work package is headed jointly by Belgium and Spain.
- WP 6: the creation of working pilots, which will be further discussed below.
- WP 7: Communication and Dissemination, including through the project's website, www.eid-stork.eu, lead by the Greek tech NGO Gov2u.

The issue of e-signature interoperability is considered outside the scope of the STORK project, as it is already being examined by other European initiatives, including the PEPPOL project and the efforts surrounding the implementation of the Services Directive, as will be explained further below. Thus, with regard to this issue, responsibilities have been well divided between the initiatives.

With regard to the pilots to be created, the ICT PSP Programme already noted that the emphasis should be on creating functioning applications which would be accessible to the end-users (including citizens, businesses and government employees), and which would have a significant and meaningful impact in practice. According to the most recent

[58] *See http://www.eid-stork.eu/ for the most current information.*

information[59], the applications currently planned to be covered by the STORK project include:

- The cross-border authentication platform for electronic services which will consist of building a demonstrator showing that cross-border electronic services can operate in a number of Member States. National eID applications to be tested include the UK Government Gateway, the Belgium LIMOSA, the German 'service-bw' portal, the Austrian 'help.gv' portal, and the Estonian integrated citizen portal. The countries involved include Austria, France, Germany, the Netherlands, Spain, Portugal and the UK, with the latter taking the lead.
- Safer Chat, consisting of a platform aimed specifically at minors and which would allow them to use their eIDs to communicate on-line. This should encourage and facilitate safe use of the Internet by children and young people. The countries involved include Austria, Belgium and Iceland, with the latter taking the lead.
- A Student Mobility pilot, to help people who want to study in different Member States by making on-line administrative applications accessible using their own means of identification. The countries involved include Austria, Estonia, Italy, Spain and Portugal, with Spain taking the lead.
- The eID Electronic Delivery pilot, to develop cross-border mechanisms for secure the online delivery of documents based on existing national infrastructures. Participating countries include Austria, Luxembourg and Slovenia, with Austria taking the lead.
- A Change of Address pilot, to assist people moving across EU borders by offering them an eID based application to register any notifications. The pilot will be implemented by Iceland, Slovenia, Spain, Sweden and Portugal, with Portugal taking the lead.

The pilots are currently scheduled to begin operating in 2009. With regard to the means of identification/authentication to be supported by these pilots, the solutions will vary from pilot to pilot, depending on the scope of the application and the countries participating in the pilots. However, the STORK project as a whole will consider all electronic identification/authentication models in use, including eID smart card models (such as the Belgian and Estonian eID cards) and virtual identification models (such as the Austrian citizen card [*Bürgerkarte*] concept).

Given that the STORK project was a part of the eGovernment Action Plan, it is unsurprising that most of the currently planned pilot applications relate to public services. However, this is not exclusively the case, as witnessed by the Safer Chat application aimed at minors. Thus, the use of electronic means of identification outside a public sector context is also being considered. Nonetheless, there are currently no plans to link the output of the planned pilots to external applications, such as the integration with social networking sites, or allowing the resulting infrastructure to be used for eCommerce purposes. However, it is

[59] *As published on http://www.eid-stork.eu/index.php?option=com_content&task=view&id=55&Itemid=76*

not inconceivable that such value added integrations will be examined by initiatives after the conclusion of STORK.

As regards the technological framework chosen to interconnect these solutions or the conceptual model behind this framework, no decisions have been made public yet. However, the central ambition is to ensure that STORK *will be as technology-transparent as possible and ensure interoperability solutions can operate with existing national eID systems. STORK will rely as much as possibly on open standards*[60]*.* These are also the ambitions that were indicated in the ICT PSP Programme.

Stakeholder participation in the STORK project is actively encouraged through the creation and consultation of stakeholder groups, most notably the STORK Member States Reference Group[61], which incorporates representatives from countries which are not formally members of the STORK consortium but which would nonetheless like to contribute their feedback, and the STORK Industry Group[62] which serves a similar purpose towards industry representatives. Input can be voluntarily provided on a continuing basis and will also be actively sought by the STORK project through a series of workshops. Any other interested parties can become members of the STORK community of interest via the STORK website, to remain informed of the project's progression. In this way, the project aims to ensure that its proposed solutions acquire the broadest possible support.

[60] *As indicated in the STORK FAQ; see http://www.eid-stork.eu/index.php?option=com_content&task=view&id=55&Itemid=76*

[61] *See http://www.eid-stork.eu/index.php?option=com_content&task=view&id=56&Itemid=78*

[62] *See http://www.eid-stork.eu/index.php?option=com_content&task=view&id=62&Itemid=78*

III.3. Impact on European eIDM developments

Given the recent starting date, STORK has not yet had any real impact on European eIDM developments at this time. However, considering the role that the large-scale pilots have been given in the eGovernment Action Plan, it is clear that STORK can have a defining impact in the future.

Examining its role and ambitions, STORK's goal for the future is to take the first steps in creating a functioning interoperability framework for electronic identity management, in the form of a federated multi-level identity management system. This implies that all of the interoperability issues discussed in the introduction above (including technical, semantic, organisational and legal questions) must be handled at least in a sufficiently advanced way to allow the pilots to operate in practice and to permit successful pilots to be extended to a larger (general) user base in the future. As was recently stated in a workshop announcement[63]:

> *The project will result in the smooth cross-border operation of several key public services. The solution will be scalable to all EU Member States with measurable benefits and save time and money with safer transactions, less fraud, better control over personal data and simplified procedures. The solutions developed and the experience gained by the project team will be shared with all states whether or not they are participating in the pilot.*
>
> *Without replacing national schemes, the new system will allow citizens to identify themselves electronically in a secure way and deal with public administrations either from public offices, from their PC or, ideally, from any other mobile device. It means, for example, that a student will be able to register in a foreign university using his or her home country's electronic identity. Some cross-border services already exist, including a Belgian web portal which allows foreign companies to register to employ citizens from Sweden, for example. After completion of the project this should be possible using their national electronic identity cards.*

Thus, the impact of the STORK project on European eIDM developments can be expected to be very significant. At the cross-border level, the creation of operational pilots implies that an interoperability infrastructure is created which will at least serve as a proof of concept to be considered as a model for any future initiatives in the field. The impact at the national level can be expected to be equally influential, as any participating countries in the STORK project will need to evaluate and potentially update their national infrastructures to ensure that they will be able to be integrated in the STORK solution model(s). Furthermore, even for non-participating countries, the STORK project can act as a very significant source of good practices that will allow them to identify and remedy any weaknesses in their own national eIDM practices. The requirements to produce reference material, including guidelines, manuals, and educational materials, and to put certain

[63] *Announcement of the STORK Workshop on Electronic Identity: easy access to public services across the EU, 8 October 2008, Madrid, Spain; see* http://www.isse.eu.com/images/STORK_workshop_8thOctober.pdf

outputs in the open domain and to license basic building blocks under an EUPL license[64] or similarly permissive model will certainly facilitate reaching this goal.

In summary, if STORK can achieve all of its objectives, it seems likely that the mechanisms it will adopt will serve as a baseline for any future European eIDM initiatives.

[64] *As stated in the 2007 ICT PSP Programme: 'The common specifications, the periodic progress statements and a final assessment of the pilot operation should all be in the public domain. Common building blocks must be shared under the EUPL license (or equivalent).'; see* *http://ecentres.net/node/361*

III.4. Considerations for the future

Given that the STORK project was initiated only recently, it is not yet clear how and to what extent its ambitious agenda will be realised. However, its role in advancing the eGovernment Action Plan can be expected to be significant, as it is expected to touch upon a large number of fundamental building blocks, including the further development of common specifications, the uptake and support of multiple authentication levels, the creation of guidelines on data formats or standardisation issues, and the interaction with the end-user (citizen, business, or civil servant).

Nonetheless, it goes without saying that the STORK project is only intended to provide pilot applications in certain domains[65] and that the successful completion of these pilots will not be sufficient in itself to fully realise the i2010 objectives. Specifically, after the conclusion of STORK, the following will need to be evaluated:

- If and how the pilot applications can be taken from a pilot status to a permanent status: The legal framework will also need to be assessed to iron out the responsibilities and liabilities for each of the pilots’ components, and it will need to be determined which conditions would be imposed on the certification authorities who will be involved at the national level in a large-scale roll-out.
- Opening the applications to other countries or contexts: This will require significant investment in some countries, given that participation in the STORK project is still limited to a relatively small number of countries, many of which can be considered frontrunners in the area of eIDM. This should not be considered to be a negative point, as it will allow STORK the possibility of making progress more rapidly. However, it should be acknowledged that the fact that the STORK consortium consists of countries that expressed a desire to participate inevitably implies a positive self-selection bias. In other words, countries that participate in STORK are likely to have a more advanced identity infrastructure already available than other (non-participating) countries, whose eID infrastructure may not be so readily integrable in the proposed solution(s).
- Whether the evaluation of all presented solutions and pilots is positive with regard to certain issues such as technical flexibility (ie, the ability to integrate different identification and authentication solutions), technical security, legal certainty, usability, added value compared to traditional (paper) processes, and data protection.
- The building blocks presented in the eGovernment Action Plan which still need further significant effort after the conclusion of STORK, which may include issues of end-user trust, management of roles or mandates or delegation, or the application of a data stewardship model to protect personal data.

[65] *As noted above, STORK will not examine e-signature interoperability issues and the pilot applications have a strong focus on public sector services, thus excluding integration with private sector initiatives as its focus.*

- How the proposed mechanisms can be extended to cover types of applications other than those examined in STORK: Extension to other public sector services (public procurement, tax declarations, checking the accuracy of information stored in official registers and facilitating its correction) are one aspect of this extension of functionality. However, as noted above, in the longer term it would be beneficial to see an integration of STORK's output with private sector applications as well, such as an interaction with social networking sites or allowing the resulting infrastructure to be used for eCommerce purposes. While this may seem contrary to the current public sector focus (as the STORK project is a component of the eGovernment Action Plan), this is not necessarily the case, as public sector identity resources such as identity cards are also commonly used for identification purposes towards private sector parties (eg, for hotel registrations) in countries that have them. Thus, using public sector identity resources for identification/authentication purposes in a private context can be very beneficial. This is an element which should be considered: ideally, the resulting infrastructure should be re-usable in contexts other than public sector services, provided that the citizen or enterprise can retain optimal control over its identity data.
- How the proposed mechanisms relate to other initiatives currently undertaken at the European level including, in relation to electronic signature interoperability, the implementation of the Services Directive, and eProcurement: The relevant projects in each of these fields will certainly be monitoring STORK's progress and interacting with it to ensure that valuable good practices can be exchanged, which will result in some degree of spontaneous convergence of their approaches. However, it is quite likely that significant changes will persist, and whether such differences need to be reduced through further harmonisation and convergence efforts will need to be evaluated or whether, instead, the slight differences are seen as a favourable and worthwhile aspect of each application's different scope and goals.

Thus, it should be kept in mind that STORK's role is to provide workable pilot applications that can be extended to cover additional countries and other fields of application. However, the STORK project will not be the conclusion of European eIDM efforts, and further initiatives will still be needed to reach the i2010 objectives. The necessity and scope of such initiatives will have to be evaluated during the course of the STORK project itself; however, it is expected that STORK will be followed up by another project aiming to extend STORK's results to a non-pilot stage and to countries that were not participating in STORK itself.

IV. eIDM Application: implementation of the Services Directive

IV.1. Historical background and goals

In the sections above, we've taken a summary look at a number of European eIDM policy initiatives (notably the eID Roadmap) and at the major eID infrastructural initiative (notably the STORK project). As was already noted in the introduction, the dimension of specific applications relying on electronic means of identification also needs to be examined. The STORK initiative described above also covers this dimension, as it aims to create several working pilot applications. However, the implementation of the Services Directive offers another interesting perspective.

Typically, the choice of the specific means of electronic identification to be used at the application level is made at the national level by the authority planning to use the application, taking into account the available infrastructure, legal framework and need for security. As such, European initiatives can play only a limited role in this choice. Nonetheless, certain activities at the European level such as the efforts undertaken by the Commission to assist Member States in the implementation of article 8 of the Services Directive, namely to facilitate the interoperability of information systems and use of procedures by electronic means between Member States, are clear examples.

The Services Directive was adopted in 2006, with the broad goal of opening up the European market for specific types of services, specifically by removing legal and administrative barriers to the development of these services between Member States[66]. The directive imposes a number of obligations on the Member States to achieve this goal, one of which, under the heading of administrative simplification (Chapter II of the directive) is directly related to this study. A specific handbook[67] was drafted and published by DG Markt to assist the Member States in their implementation efforts.

In general terms, the directive's provisions on administrative simplification require Member States to ‘examine the procedures and formalities applicable to access to a service activity and to the exercise thereof. Where procedures and formalities examined under this paragraph are not sufficiently simple, Member States shall simplify them' (article 5.1 of the directive). This general obligation thus requires the Member States to assess if any conditions that have been imposed in relation to a service activity are necessary and whether they can be replaced by less restrictive means. The result of this simplification process should be that service providers should find it easier to provide and use cross-border services in the EU, thus increasing competition between service providers and ultimately benefiting consumers.

However, the simplification requirements of the directive go significantly further than the mere simplification of existing procedures and formalities. Member States are also

[66] *For a more in-depth look at the Directive, see* *http://ec.europa.eu/internal_market/services/services-dir/index_en.htm*

[67] *Handbook on implementation of the Services Directive, see* *http://ec.europa.eu/internal_market/services/docs/services-dir/guides/handbook_en.pdf*

required to create so-called 'points of single contact', through which any service provider covered by the directive should be able (irrespective of the Member State of establishment) to complete:

> *(a) all procedures and formalities needed for access to his service activities, in particular, all declarations, notifications or applications necessary for authorisation from the competent authorities, including applications for inclusion in a register, a roll or a database, or for registration with a professional body or association; and*
>
> *(b) any applications for authorisation needed to exercise his service activities.*
>
> (article 6.1 of the Services Directive)

Thus, after the implementation deadline set by the directive (end of December 2009), service providers must be in a position to access and complete the electronic procedures necessary to access or exercise a service activity through a point of single contact in each Member State. The service provider shall be able to communicate exclusively through a point of single contact, without needing to enter into direct contact with the competent authorities, if he so chooses. In the words of the handbook on the implementation of the Services Directive, the point of single contact should constitute a 'single institutional interlocutor'.

However, the concept of 'points of single contact' does not mean that Member States have to set up one single centralised body in their territory. Member States may decide to have several points of single contact within their territory. The point of single contact must however be 'single' from the individual provider's perspective (ie, the service provider should be able to complete all procedures by using only one such point of contact).[68] This means that the point of single contact must be able to handle any applications, requests for permits, registrations with public administrations or notifications to professional organisations and to inform the service provider directly of the outcome of this process.

Finally, in order to ensure that these points of single contact are easily accessible to the service provider, the Services Directive requires that it should be possible for all of the aforementioned procedures and formalities to be 'easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities' (article 8.1). As noted by the handbook:

> *Electronic procedures are an essential tool to make administrative procedures considerably less burdensome for service providers and for public authorities alike. The possibility to complete administrative procedures at a distance will be particularly important for service providers from other Member States. Moreover, electronic procedures will also contribute to the modernisation of public administrations by rendering them more efficient. Following an initial investment,*

[68] *Page 18 of the Handbook.*

> *the use of electronic procedures should prove to be money- and time-saving for administrations.*[69]

This means that the points of single contact to be created by the Member States will need to provide an on-line presence, such as a website, through which service providers can actually complete these procedures and formalities[70]. It is thus not sufficient to implement points of single contact as a mere portal site containing hyperlinks to other organisations or authorities[71].

While simple in concept, the ramifications of these requirements are very significant. To set up full-fledged points of single contact, Member States need to resolve a number of key issues that have already been examined at the EU level, but for which no conclusive solutions are readily available in the Member States. These issues include:

- The electronic exchange of original documents: Registration, notification and/or authorization procedures and formalities in certain cases may require the use of original or certified documentation (eg, tax attestations, register extracts, diplomas), which is currently often only available in a paper form. It is unclear how these will be transformed into an electronic format for the purposes of the completion of electronic procedures. The question of re-using original paper documentation in an electronic context has recently been examined for the public procurement domain in the 'Preliminary study on the electronic provision of certificates and attestations usually required in public procurement procedures'[72], which resulted in several conceptual models of solutions being defined and assessed. However, none of these models have yet been taken up on a significant scale in any of the Member States, so that the problem of the electronic exchange of original documents is still largely unresolved.
- The question of the use of electronic signatures which is related to the issue of authentic electronic documents: In a number of countries, the use of electronic signatures will be needed, at least in procedures or formalities where original electronic evidence is required. However, the Member States currently do not have clear information on which eSignature mechanisms are likely to be used by service providers established in other Member States, how they can be validated, or what legal value they should attach to those signatures.

[69] *Page 22 of the Handbook for the implementation of the Services Directive.*

[70] *Article 8.2 of the directive foresees certain exceptions for procedures and formalities which inherently require physical proximity and thus cannot reasonably be performed electronically and at a distance, namely 'the inspection of premises on which the service is provided or of equipment used by the provider or to physical examination of the capability or of the personal integrity of the provider or of his responsible staff.'*

[71] *Page 19 of the Handbook for the implementation of the Services Directive.*

[72] *For the final report of this study conducted for the European Commission – DG Markt, see http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/ecertificates-study_en.pdf*

The status of a qualified or non-qualified signature is particularly significant in this regard. The eSignatures Directive[73] has introduced the rule that advanced electronic signatures based on a qualified certificate and created through a secure signature creation device (also commonly referred to as a 'qualified signature', even though this is not a legal term) is legally equivalent to a handwritten signature (article 5.1 of the eSignatures Directive). Thus, in principle[74] such signatures should be legally valid in any application requiring electronic signatures, including points of single contact. However, the status of a qualified signature is difficult to determine, as it requires the relying party to establish that the certificate itself is qualified (which should be indicated in the certificate [annex I (a) of the directive], but sometimes isn't) and that a secure signature creation device was used (which again is not always indicated in the certificate itself). These elements can be even harder to establish when the signature relies on certification service providers established in other Member States, as the relying party may then not be aware of how it can determine the status of the certificate and the use of a secure signature creation device. Thus, in practice, signature solutions from other Member Countries are less acceptable, irrespective of their qualified or non-qualified status. On this issue too, several relevant studies have recently been conducted on how to improve interoperability between signature solutions across borders[75], but interoperability in practice so far remains limited.

- An identity issue to be resolved, which is most important for the purposes of this report: Since service providers must be able to complete electronically any of the procedures and formalities covered above through the points of single contact, in cases where identification is needed it must be possible for these points to identify the service providers. Since there is no universally valid identifier that would cover all possible service providers, nor any identification mechanism that is universally available, it falls to the Member States to find a solution to resolve this issue.

Now, with the deadline for implementation of the Services Directive drawing nearer, Member States are seeing themselves confronted for the first time with a tangible and binding obligation to implement working cross-border solutions by the end of 2009. In effect, the Services Directive has the potential to act as a catalyst in European eID

[73] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Publ.L. 013 of 19 January 2000, p. 0012 – 0020.*

[74] *Keeping in mind the exceptions allowed under the public sector clause (article 3.7), which allows Member States to 'make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens. '*

[75] *See in particular the aforementioned IDABC Preliminary study on mutual recognition of eSignatures for eGovernment applications; see http://ec.europa.eu/idabc/en/document/6485/5938; and the Study on the Standardisation Aspects of eSignatures; see http://www.esstandardisation.eu/index.php*

interoperability initiatives, for the simple reason that Member States have committed themselves to setting up electronic procedures available across borders under article 8.

This commitment to implement functioning points of single contact by the end of December 2009 is of course crucial to understanding the current activities surrounding the implementation of the Services Directive: the obligation to provide functional electronic points of single contact is incumbent on the Member States. It is thus an entirely national responsibility in which the European Commission has no direct competence *per se*. However, it is also clear that all of these aforementioned issues, including the identification aspects, have a fundamental cross-border component. Member States planning to implement a point of single contact relying on e-Signatures and e-Identification can benefit from a solid knowledge of solutions currently being considered or implemented by other countries, and from joint efforts to improve the interoperability between national solutions.

As stressed in the handbook:

> *The implementation of the obligation undertaken in article 8 by the end of 2009 will be a considerable challenge for Member States, which should increase their already ongoing efforts to work towards interoperable e-Government services for businesses. Member States are encouraged to build upon the existing initiatives. Indeed, the obligation in the Services Directive should be seen as a chance to boost current efforts and to help Member States to focus and deliver the objectives they have set themselves as part of their e-Government work.*
>
> *One of the core issues to be tackled in order to put in place functioning electronic procedures across the EU is interoperability. Given the fact that at a national level different requirements and legal, organisational, semantic and technical arrangements are in place with regard to existing or planned electronic procedures, several issues may arise, be they political, legal or technical (linked to identification, authentication, electronic document exchange or recognition, etc), which would require a certain level of coordination and cooperation between Member States.*
>
> *This, however, does not mean that Member States are expected to harmonise their e-Government solutions or to use one model only. Member States are free to choose their models, while bearing in mind that electronic procedures have to be available both to their own nationals or residents and to service providers from other Member States, who should in principle be able to use their national means to deal with public authorities in other Member States. This would be in line with the objective of cross-border interoperable e-Government services, the idea of administrative simplification and the facilitation of cross-border service provision.*
>
> *If access to e-Government services in another Member State requires service providers to use the (identification/authentication) means of that other Member State, new complications and burdens for services providers may arise. Indeed, if service providers need to obtain the national means of all Member States where they wish to provide their services, this may result in delays and costs which in principle should be avoided. (Moreover, in some Member States they may even be required to obtain several means, a separate one for each application, which*

> *further complicates the situation.) When considering how to tackle this issue Member States need to avoid creating additional burdens or adopting solutions that may slow down the introduction of interoperable e-Government services across borders in the long-run.*
>
> *In order to work towards interoperable solutions, the Commission will play an active role and assist Member States in the task of setting up electronic procedures. In particular, the Commission will encourage the exploitation of synergies between the existing e-Government initiatives under the i2010 strategy and the objective of achieving electronic procedures across the EU by the end of 2009.*

The Services Directive specifies that the Commission may adopt 'detailed rules for the implementation of [an electronically accessible point of single contact] with a view to facilitating the interoperability of information systems and use of procedures by electronic means between Member States, taking into account common standards developed at Community level' (article 8.3). The Commission can thus, for example, adopt specific standards under article 8.3 of the directive insofar as this would improve the cross-border interoperability of electronic systems and procedures. A specific procedure for the adoption of such decisions has also been provided (a so-called comitology procedure, specified in article 40.2 of the directive).

So far, no decisions have been taken to follow this procedure, as the emphasis of the work carried out so far has predominantly been on administrative simplification, ie, on efforts that require Member States to take stock of their existing procedures and formalities covered by the directive and to focus on the simplification of these. However, several preparatory actions have been undertaken which may lead to specific decisions under article 40 in the future. These will be commented on below, insofar as they may be relevant to the European eID debate.

IV.2. Current status and key characteristics

IV.2.1. Introduction

The implementation of the Services Directive is a national responsibility, and any choices to be made in this regard, including the facilities to be used for the electronic identification of service providers, should be in principle determined by the Member States, provided that they allow the cross-border completion of formalities and procedures. The national administrations are free to choose any solutions they wish, provided of course that the goals of the Services Directive are achieved and that other Community regulations are respected. Thus, their autonomy is quite extensive.

Nonetheless, the issues being examined here have been explored for many years in other areas, both at the national and European level, without fully and universally acceptable solutions being presented. Furthermore, the very nature of the points of single contact – whose essential functions revolve around simplifying and facilitating communication between service providers and any competent bodies – requires intense cooperation between public authorities. The Commission supports these efforts at implementation in multiple ways.

Firstly, the Commission has contracted a number of studies and carried out consultations, in order to ensure that the Member States' activities and choices in implementing the directive are identified and known at the European level. These studies and consultations have covered the identification of specific interoperability issues and the discussion of possible approaches to resolve them, keeping in mind the 2009 deadline. This technical work is carried out in close cooperation with the Member States and EEA Countries, specifically by frequently interacting with national experts. In this way, the Commission aims to play an active supporting role and assist the countries in the task of setting up electronic procedures.

Secondly, article 8 (3) of the Services Directive enables the Commission to adopt detailed rules for the implementation of electronic procedures through a comitology procedure according to the rules of article 40 (2) to adopt specific decisions that could serve to facilitate the interoperability of Member States' procedures, in order to make these accessible across borders. In the future, it would thus be possible to use this procedure to adopt specific technical standards, formats or semantic agreements.

In the sections below, we will briefly examine the main initiatives that have been taken so far in relation to both of these aspects, insofar as they apply to electronic identity management.

IV.2.2. Preliminary study – status in the Member States and initial recommendations

One of the earlier initiatives taken by the European Commission to support the Member States was the organisation of a specific study on electronic procedures as foreseen under Article 8 of the Services Directive[76]. Performed between November 2007 and April 2008, the study had a threefold goal:

- to identify typical procedures and formalities that service providers would need to be able to complete via a point of single contact;
- to determine the main interoperability challenges to be resolved by the Member States as a part of their implementation obligations; and
- to provide recommendations on the efforts that the Commission could undertake to support the Member States.

As a general conclusion, the study showed that, at that time, out of the 27 Member States surveyed, only 5 had advanced to the point of planning their implementation efforts for the point of single contact, whereas the remaining 22 were still debating the organisation of responsibilities and the technologies to be chosen. None of the surveyed countries had thus moved to the actual implementation stage. The reason for this was generally one or more of the following three specific problems:

- The country was still conducting consultations or screening exercises to determine the exact impact of the Services Directive and to devise an appropriate response strategy;
- The country was considering the roles of the stakeholders that had been traditionally involved in managing access to their markets (ie, mainly public sector administrations or private sector professional organisations) and determining if and how these should play a role in the point of single contact; or
- The country was still developing the underlying infrastructure that would be required before work on the Services Directive could realistically begin. This included the development and deployment of electronic communication solutions (often including a PKI infrastructure), the creation of an adequate legal framework for electronic communication with the relevant bodies, and the establishment of the electronic commercial registers or other databases which would be needed to be able to identify enterprises or entrepreneurs on a national level.

Out of the five countries that had moved to the planning stage, all were noted to be planning to rely on PKI-based solutions; and in all cases the main issue of concern was then the accessibility of the system to service providers established in other Member States, who would be likely to have difficulties in obtaining a PKI certificate from a

[76] *The study on electronic procedures as foreseen under Article 8 of the Services Directive was performed by Siemens IT Solutions and time.lex. However, the resulting reports (comprising national profiles, an analysis and impact assessment report, and the final report) have not yet been published at this time.*

supported CSP. The Commission's assistance in resolving the eSignature interoperability issue was thus considered to be of key importance.

Specifically with regard to electronic identification in the context of the points of single contact, the study noted that most countries had not yet moved discussions beyond the point of wanting to use certain PKI-based eSignature solutions. In this case, the signature certificates being used by the service provider would need to contain sufficient identification information to allow the owner of the point of single contact to uniquely identify the service provider with a satisfactory degree of certainty and reliability. In short, the point of single contact should be able to receive adequate identification information when and if necessary and to rely on its correctness.

The recommendations of the study built on these considerations. Central among these recommendations was the need to undertake further efforts to ensure that certain types of electronic signatures would be usable across borders for the purposes of the points of single contact. Consultations with the Member States and EEA countries have led to the conclusion that qualified signatures and advanced signatures based on qualified certificates should be considered a priority; the former based on their legal equivalence to handwritten signatures and the latter based on the consideration that an exclusive focus on qualified signatures would likely set the bar too high to have a real impact on the accessibility of the points of single contact, especially keeping in mind the directive's deadline of December 2009.

This recommendation on improving the interoperability of electronic signatures was also considered as a way to simplify the problems linked to cross-border identification of service providers. Specifically, qualified signature certificates already contain certain information which allows the CSP to identify the signatory with sufficient legal certainty; otherwise, the signature is useless and has no practical or legal value. In some cases, this identity information could already be sufficient for the point of single contact as well to uniquely identify the signatory.

However, this is not always the case, due to differences between the available identity information and its exact meaning in different signature certificates. In order for qualified signatures to function adequately for identification purposes, more extensive solutions would be needed, either in the form of improved interoperability between the existing solutions in the Member States, the implementation of validation platforms which can overcome the lack of interoperability, or even models that are not limited to PKI-based identification solutions[77]. When choosing between these alternatives, the limitations of the December 2009 implementation deadline of the Services Directive obviously play an important role.

For this reason, with regard to electronic identification, the main approach favoured by the study was to leverage the opportunities offered by qualified signatures and advanced

[77] *In this context, we can refer to the recent IDABC Study on eID Interoperability for PEGS, which dealt specifically with the question of allowing any type of electronic identification solution to interact. See http://ec.europa.eu/idabc/en/document/6484/5644*

signatures based on qualified certificates, for the simple reason that these solutions seemed likely to be used by the Member States in a significant number of cases at any rate and that they would offer a pragmatic way to make some progress within the available timeframe. Of course, alternative sources of identity information in addition to the signature certificate should also be considered. For example, the signature will typically be applied to a document which requires the service provider to fill out any needed contact or identification information, as has always been the case in paper processes. While this is not a very reliable process, this process has always been considered adequate in a paper context, and here too the main question is one of proper risk assessment.

More extensive and refined identity management solutions will be explored and implemented through other initiatives, including through the STORK project discussed above. However, it is also clear that such initiatives will still take several years to come to fruition. Thus, the study recommended focusing on the use of qualified signatures and advanced signatures based on qualified certificates both as a signature mechanism and as an identification mechanism. It was felt that these recommendations should allow the Member States to make significant progress towards the implementation deadline of December 2009.

In order to realize this goal, the study recommended following the approach outlined in an earlier INFSO study on the standardization aspects of e-signatures[78] in relation to 'Quick-wins on Qualified CA recognition and QES validation' where standardization initiatives have been proposed focusing on a more harmonized approach to the supervision of certification-service-providers issuing qualified certificates to the public and to improve technical standardisation, in order to facilitate the validation of electronic signatures issued by these certification-service-providers.

[78] *See p. 114 of the INFSO Study on standardisation aspects of e-signatures;* *http://ec.europa.eu/information_society/eeurope/i2010/docs/esignatures/e_signatures_standardisation.pdf*

IV.2.3. Current activities: improving trust in electronic signature solutions and examining current trends

The emphasis of the ongoing work is currently on improving the interoperability of qualified electronic signatures or advanced electronic signatures supported by a qualified certificate. To assist the Commission in its general efforts to further promote the implementation of mutually recognized and interoperable electronic signatures and e-authentication, a new study was recently launched under the auspices of DG INFSO, entitled the *Study on the CROss Border Interoperability of Electronic Signatures* (abbreviated as CROBIES).

The CROBIES study kicked off in August 2008 and will run through the third quarter of 2009, with the last few months being dedicated to supporting implementation actions. Thus, the study is still in its initial stages, and a definitive outline of the work cannot yet be given. Nonetheless, we will attempt to provide a description of the main efforts involved and the anticipated impact on eID issues.

Generally, the CROBIES study aims at improving eSignature interoperability in the shorter term, by supporting the uptake of specific standards in a number of key domains. To the maximum extent possible, the study takes into account existing standards and builds on these, to minimize the additional effort for the Member States. The study will work in five different domains:

- The creation of a trusted list at Member States' level of supervised or accredited qualified certification service providers (QCSPs), ie, certification service providers issuing qualified certificates to the public: In this first step, a list is compiled of all QCSPs established in the Member States. Under the terms of article 3.3 of the eSignatures Directive, such QCSPs must be supervised or accredited at the national level, which should ensure the reliability of these service providers to a certain degree.

  For each supervised or accredited QCSP, the trusted list will detail the relevant certification authorities, information on the qualified electronic certificate supporting the signature and whether it is supported by a Secure Signature Creation Device (SSCD). These elements should facilitate the validation of electronic signatures created using the services of these QCSPs.

  It should be noted that the trusted list is conceived as an information dissemination tool, ie, as a uniform way of structuring the presentation of information on supervised or accredited QCSPs in the Member States. Initially, the efforts will focus on creating a human readable list as a minimum, leaving the decision on when to migrate to a machine-processed list up to the Member States.

  The efforts of the CROBIES study in this domain will be based on existing standards, most notably the standard ETSI TS 102 231[79]: Electronic Signatures and Infrastructures (ESI) - Provision of harmonized trust-service status information.

[79] *ETSI Technical Specification 102 231 of May 2005 on Electronic Signatures and Infrastructures; see http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc*

- The development of a common supervision model for QCSPs: As noted above, the value of QCSPs lies to some degree in the fact that they are supervised or accredited by specific competent bodies in each of the Member States. However, the eSignatures Directive does not specify how this supervision is to be organized; it only states that the system of supervision must be 'appropriate' (article 3.3). It is likely that supervision practices diverge to some degree between the Member States, with some Member States setting the bar higher than others.

  In order to ensure that these divergences are minimal (ie, to ensure that supervision standards are high enough for QCSPs in any country to be trusted), CROBIES will also develop a common supervision model for QCSPs.

- The development of an interoperable qualified certificate profile: While the use of the aforementioned trusted lists can solve a number of problems (clarifying the qualified status of certificates, declaring whether a SSCD was used, linking to applicable policies), it would be more efficient if this information was included within the qualified certificates (QCs) themselves.

  Thus, in order to simplify the tasks of the trusted list, a set of common data should be present in each QC. The CROBIES study will propose a draft template for QECs, based on existing ETSI standards.

- The development of a profile for interoperable Secure Signature Creation Devices (SSCDs): While the eSignatures Directive has developed certain high level requirements that SSCDs must meet (annex III to the directive) and specific standards have been put in place to further detail these (specifically CWA 14169[80]), their interpretation and implementation at the national level still varies quite widely. To resolve this issue, CROBIES will examine how these guidelines can be further elaborated to ensure a more homogeneous interpretation at the European level.

- The development of an interoperable qualified or advanced electronic signature format: Again, the eSignatures Directive has defined a number of high-level requirements for advanced signatures based on qualified certificates (and thus indirectly on qualified signatures, which require the use of qualified certificates), which have subsequently been elaborated in a specific standard, but the remaining diversity at the European level is still too great. The CROBIES study will examine how some of these standards (specifically ETSI XAdES TS 101 903[81] and ETSI CAdES TS 101 733[82]) can be further detailed and taken up at the national level.

[80] *CEN Workshop Agreement 14169 of March 2004 on Secure signature-creation devices "EAL 4+"; see ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf*

[81] *ETSI TS 101 903: ETSI Technical Specification Electronic Signatures and Infrastructures (ESI): "XML Advanced Electronic Signatures (XAdES)".*

[82] *ETSI Technical Specification Electronic Signatures and Infrastructures (ESI): "CMS Advanced Electronic Signatures (CAdES)".*

This way, it should become significantly easier for Member States to validate foreign signatures.

Thus, substantial efforts are being made to improve the standardization of European electronic signature practices. Some work has already started within the context of the Services Directive which will be continued and complimented at a horizontal level under the action plan on e-signatures and e-authentication.

The activities described above also have an impact on electronic identification, specifically in cases where Member States choose to use electronic signatures as a practical and temporary solution to deal with identification issues, as was recommended by the Study on Electronic Procedures discussed above.

Principally, the approach taken by the CROBIES study should facilitate electronic identification initially through the trusted lists of the Member States, which could contain - in addition to the information on the qualified status of the certificate and the supervised or accredited status of the issuing QCSP - the information needed for identification from the relevant fields of the QC (eg, name and unique identifier of the signatory) or any additional information provided together with the qualified certificate. It is up to the Member States to agree what identity information would be necessary to satisfy their needs (eg, the schemes used for unique identifiers, so that the receiving side knows which type of unique identifier is used and how it will be provided). Nonetheless, the trusted list could play an enabling role by providing the needed information that would allow Member States to electronically identify service providers with the same legal certainty as other recipients of an electronic signature.

IV.3. Impact on European eIDM developments

The obligations of the Services Directive are very far reaching, and the available timeframe for the Member States to implement them is limited (December 2009). At the European level, the overview above has shown that the emphasis has been placed on improving the interoperability of qualified electronic signatures and advanced electronic signatures based on qualified certificates.

These efforts are still at an early stage, and discussions on the precise scope and desired outcome of the work are still ongoing at the expert level. Nonetheless, it is likely that the EU level discussions related to eID within the framework of the Services Directive will initially remain focused on the supporting role that electronic signatures can play.

Subject to the outcome of the ongoing discussions, these efforts could create synergies for other European eID related initiatives, given the important role that electronic signatures have been given in eGovernment initiatives in a number of countries, most notably countries that have rolled out eID cards (or are planning to do so) or which rely strongly on collaboration with private sector QCSPs. For these countries, it is conceivable that the outcome of the CROBIES study could provide an acceptable first answer to the European eID interoperability problem. Of course, the success of these efforts depends largely on the response of the Member States to these initiatives, as they imply that the Member States should adopt the resulting output. In some Member States this may not be obvious, due to a certain reluctance to rely on unknown supervision schemes or opposition towards any approach that can be seen as favouring qualified electronic signatures and advanced signatures based on qualified certificates over other approaches.

The resulting output will likely also be influential on European eIDM policy in general, given that it will at any rate create new and more harmonised resources, such as the proposed standards and the creation of a trusted list of QCSPs with detailed information. These can prove to be an important asset for any European scale PKI-based project, as it will provide the fundamental building blocks to create trust in foreign CSPs meeting its requirements and to more easily validate electronic signatures of other Member States. In this way its output will undoubtedly prove useful to projects that also aim to resolve some of these issues, such as the aforementioned STORK and PEPPOL projects.

IV.4. Considerations for the future

As noted above, the European efforts to support the implementation of the Services Directive have now entered a phase where detailed proposals are being discussed at expert level with the objective of improving the interoperability of certain types of electronic signatures.

In the shorter term, this approach - provided that it is taken up by the Member States - could provide a basis for a solution for the electronic identification of service providers when and if required by the points of single contact. From that point, it would be possible for Member States who desire to do so to expand the scope of the solutions provided to contexts other than the Services Directive. Of course, such extensions are beyond the scope of current efforts.

It is however also clear that improving the interoperability of electronic signatures will not be an all encompassing or definitive solution in relation to electronic identity management. A series of issues still have to be solved in a wider context, such as:

- The fact that the current discussions cover only PKI-based solutions: This excludes mechanisms with less complexity (eg, username/password systems) or different technical foundations (eg, one-time password calculators).
- The focus on qualified signatures and advanced signatures based on qualified certificates: This leaves the choice of relying on PKI solutions based on non-qualified certificates and their acceptance up to the Member States.
- The extent to which the semantics of electronic identification will be addressed, which is not yet clear: This will largely interrelate to the work being done on the electronic certificate profile in the context of the action plan on e-signatures and e-authentication.
- The issue of legal mandates/roles/delegations: This problem has not yet been addressed systematically at a national level in most countries and will therefore likely not be extensively addressed in the current European discussion either. However, particularly in cases where legal entities are being represented, it may be unavoidable that further information on the legal capacity of the signatory is required.
- Integration with other identification resources: Some Member States could argue that the approach overemphasises electronic certificates as an identity resource, while not leveraging the value of other data resources (such as electronic registers) in an adequate way. Of course, Member States are free to use or integrate such other identity resources if they wish. The efforts described above are only aimed at helping Member States who want to use electronic signatures to achieve interoperability more easily, notwithstanding their right to make other technological or infrastructural choices.

However, it is important to stress that the efforts undertaken are not conducted in a vacuum. A significant number of other European initiatives are underway which address all of the open issues in a more comprehensive manner (with the STORK project discussed above being the main example). In that respect, it is important to underline that the activities targeted on the facilitation of the implementation of article 8 of the Services

Directive can be considered as first step to provide support for electronic identification when and if required for the completion of electronic procedures.

The ongoing discussions in the framework of the Services Directive are concentrated on providing Member States with the minimum of means that would assist them in meeting the requirements of the Services Directive. The outcome of these efforts will still have to be enriched and refined in combination with the outputs of other efforts in order to obtain a sustainable long-term eID solution.

V. General conclusions on the state of the European eIDM agenda

V.1. Overview of key realisations and trends

V.1.1. Role of the Roadmap, STORK and the Services Directive

Based on the three initiatives commented on above (the eID Roadmap, the STORK project and the supporting efforts surrounding the implementation of the Services Directive), it is clear that the European eIDM agenda has been advanced in a number of crucial ways:

- The eID Roadmap has helped to formalise a number of high-level eIDM objectives to be reached at the pan-European level.
- The Services Directive has provided a clear incentive (or more accurately an obligation) for Member States to invest in achieving these goals, thus ensuring that the discussion and study stage can be passed in the near future.
- The STORK project will attempt to formulate a more systematic and encompassing approach to eID issues by implementing specific pilots in which the participating countries agree to mutually recognise each others' means of identification and authentication, which can serve as a model for other types of applications.

Initial efforts (including the eID Roadmap in its entirety) have focused mainly or even exclusively on examining policy issues, identifying interoperability issues and defining high-level solution requirements. This has resulted in a relatively coherent definition of the desired outcome of European eIDM ambitions, namely the creation of an interoperability infrastructure that would be:

1. Federated in a policy sense, ie, 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.

2. Multi-level, 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 services, and which level of authentication is required for each eGovernment service.

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.

4. Permitting a context or sector based approach where this is deemed desirable by the Member State of origin.

5. Enabling private sector uptake, where Member States choose to rely on private sector partners (eg, financial institutions) for the provision of eIDM services.[83]

However, these initial studies were largely theoretical, and had a limited impact in practice. In contrast, more recent efforts such as the STORK project and the implementation of the Services Directive have focused on turning these principles into practice.

In the case of the STORK project, this will be done by creating specific cross-border pilot applications supporting eID tokens from multiple countries. Given the available timeframe and scope of the project, these applications will be limited in a number of important ways:

- The applications will be developed as pilots. This implies a smaller and more manageable user-base, which is not necessarily representative of the broader European population.
- Given their pilot character, the applications will possibly apply a simpler technical or legal framework than would be required for a generalised roll-out.
- The timeframe, budget and participation do not realistically allow the STORK project to solve all eID related problems. It is likely that the implementation of certain applications will require that certain assumptions are made, eg, in relation to the reliability of the available eID infrastructure, security, user awareness and understanding of the technology, or simply knowledge of specific languages. These will be reasonable in the context of a pilot, but will still need to be resolved at a later stage.
- Integration of STORK’s output with private sector applications (such as an interaction with social networking sites or allowing the resulting infrastructure to be used for eCommerce purposes) would be beneficial to improve the appeal and use-case of the developed infrastructure.
- The involvement of a smaller number of countries, implies that the applications will only need to focus on a smaller number of identification/authentication solutions, and also that restrictions related to the infrastructure of non-participating countries will not need to be taken into account.

Thus, it is clear that the STORK project will not be an end point for developments in interoperability. Nonetheless, it will play the crucial role of providing a functional infrastructural model for eID interoperability between a sufficiently large number of different technological solutions and countries. As described above, it is envisaged that STORK will do so by developing a model that relies on a proxy approach requiring the creation of identity providers (IDPs) at the national level (at least one per country), coupled with a network of proxy service providers to connect service providers to the appropriate identity providers in each country and to validate the trust and security of the

[83] *Partial quote from the eID Roadmap; see* http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/eid/index_en.htm

identity information sent by the identity providers. In this way, STORK should theoretically be able to handle any type of identification/authentication method – thus including non-PKI-based systems – supported at the national level.

The efforts surrounding the implementation of the Services Directive on the other hand are bound by the restrictions resulting from the deadline of the directive, set at the end of December 2009. This leaves little time for Member States to conduct significant experiments. Similarly, the European Commission has only limited options to offer support to the Member States, as their efforts should not prejudice the outcome of the STORK project. For this reason, a pragmatic approach is currently being taken that focuses on improving the standardisation of electronic signature practices between the Member States – thus targeting only PKI-based models – and leveraging the possibilities that this approach offers in relation to eIDM.

More specifically, the European Commission’s support efforts in this field will focus on improving the interoperability of certain types of electronic signatures that are generally considered to be more secure, specifically qualified signatures and advanced signatures based on qualified certificates. As the issue of eSignature interoperability falls outside of the scope of the STORK project, there is no risk of overlap or conflicts between the initiatives in this respect. This focus within the Services Directive efforts on eSignature interoperability should have a positive impact on eIDM issues as well, since part of the work is centred on charting how signatories are uniquely identified in the qualified electronic certificates used as a basis for these electronic signatures. Provided that this information can be provided to the Member States, the use of these electronic signatures should provide the Member States with the possibility of identifying specific signatories, albeit in a rudimentary fashion.

Thus, the STORK project and the implementation efforts surrounding the Services Directive each tackle the eIDM issues with different goals and in different ways. Whereas the implementation of the Services Directive focuses strictly on certain electronic signatures as a way of offering a basic tool that Member States can use for the purposes of electronic identification, the STORK project will not examine the interoperability of electronic signatures but rather will strive to interconnect national electronic identity resources, which should offer greater benefits in the longer term. Of course, it is possible that the STORK project will be able to reap some benefit from the outcome of the efforts related to the Services Directive, as any standards or practices emerging from these efforts could prove to be indirectly beneficial to the STORK project as well.

With the Services Directive serving as a catalyst to improving the use of PKI-based solutions for electronic identification in the shorter term, and the STORK project taking a more long-term technology neutral approach that does not focus on eSignature interoperability, these initiatives should collectively ensure that the European eIDM agenda can be advanced to a significant degree by 2010.

V.1.2. Other relevant European eIDM developments: seeing the broader picture

While the overview above focuses on the three chosen key initiatives, it is clear that they do not represent the whole of European eIDM related initiatives. Encouraging interoperability between existing e-identification initiatives has been a long standing European policy goal. Earlier examples of this interest can be seen in, for example, IDABC's 2004 European Interoperability Framework for pan-European eGovernment Services[84] which provides recommendations and generic standards with regard to the organizational, semantic and technical aspects of interoperability that are still relevant and valid today. Similarly, the European standardisation body CEN[85] has been engaged in a number of efforts to create and encourage relevant standards, in particular in the field of PKI, including the work surrounding the so-called European Citizen Card (ECC), intended to provide guidelines to Member States interested in creating national electronic identity cards with optimal interoperability features[86].

Several recent initiatives already briefly mentioned above are equally likely to play a significant role in the future European eID arena, and deserve further attention here on the basis of their potential impact and due to the alternative approaches to identity management which they offer.

In addition to the STORK initiative mentioned above, a second large-scale pilot on electronic public procurement has been launched under the acronym PEPPOL[87]. In the same way as discussed above in relation to the Services Directive, cross-border electronic procurement also requires public administrations to be able to securely identify or authenticate foreign entities (natural or legal persons) using the identification means at their disposal. PEPPOL addresses the issue of identity management in a slightly different way than is foreseen for STORK, by using a *virtual company dossier* approach[88].

[84] *IDABC's European Interoperability Framework for pan-European eGovernment Services; see http://ec.europa.eu/idabc/servlets/Doc?id=19528*

[85] *Comité Européen de Normalisation (CEN, European Committee for Standardisation); see http://www.cen.eu*

[86] *See in particular the efforts of CEN/TC 224/WG 15 on the European citizen card; see http://www.cen.eu/CENORM/BusinessDomains/TechnicalCommitteesWorkshops/CENTechnicalCommittees/TCStruc.asp?param=6205&title=CEN%2FTC+224; and the key documents CEN/TS 15480-1:2007 (Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics); CEN/TS 15480-2:2007 (Identification card systems - European Citizen Card - Part 2: Logical data structures and card services); CWA 15535-1:2006 (Multi-application multi-issuer citizen card scheme standardisation - Part 1: Business model agreement); and CWA 15535-2:2006 (Multi-application multi-issuer citizen card scheme standardisation - Part 2: Scheme architecture and implementation solution).*

[87] *Large-scale pilot on Pan-European Public eProcurement On-Line; see http://www.peppol.eu/*

[88] *See http://www.peppol.eu/workpackages/wp2-virtual-company-dossier for an overview of this approach.*

Briefly summarised, this approach entails the creation of a protected information package (the 'virtual company dossier') in which candidates for public procurement can store certain crucial authentic information about themselves. This includes identification information from official registers (such as the official name, place of establishment, VAT number, ...), but also electronic attestations that are commonly requested in public procurements, such as attestations showing compliance with tax or social security obligations. In this way, the virtual company dossier allows tenderers to create an authentic identity resource that can be submitted to public administrations in the context of public procurements. Fundamentally, this approach relies on the bundling and controlled re-use of authentic information that is collected and stored at the national level. The only issue that needs to be resolved then is the creation and validation of a link between a submitted offer and the corresponding virtual company dossier of the submitting tenderer. Electronic signatures can be an enabling technology for this purpose[89].

In indirect relation to this approach, a number of other identity information exchange initiatives have recently been set up, including the aforementioned BRITE[90] and ECRIS[91]. Both of these initiatives are based on the philosophy that, in some cases, it is more efficient and justified to directly exchange identity information between the competent administrations in specific countries, rather than relying on the person whose identity is involved to act as an intermediary.

The BRITE project aims at interconnecting national business registers to ensure that certain authentic business information can be exchanged across borders in a standardised and interoperable manner. The BRITE consortium consists principally of national business registers and chambers of commerce from Denmark, Ireland, Italy, Germany, Macedonia, Norway, Spain, and Sweden, but also includes technical partners and research institutions. Given the project's goal of unlocking these authentic identity resources for re-use in a multitude of scenarios, it is not surprising that BRITE is one of the identity resources planned to be used in the aforementioned PEPPOL project[92].

The ECRIS system (European Criminal Records Information System) has similar goals, albeit in a much more restricted context. This initiative is aimed at improving collaboration between European criminal investigators, by facilitating the exchange of information regarding prior criminal convictions. For that purpose it lays down the basis for a

[89] *For PEPPOL's approach to electronic signatures, see http://www.peppol.eu/workpackages/wp-1-esignature*

[90] *Integrated project aiming to achieve Business Register Interoperability Throughout Europe; see http://www.briteproject.net/*

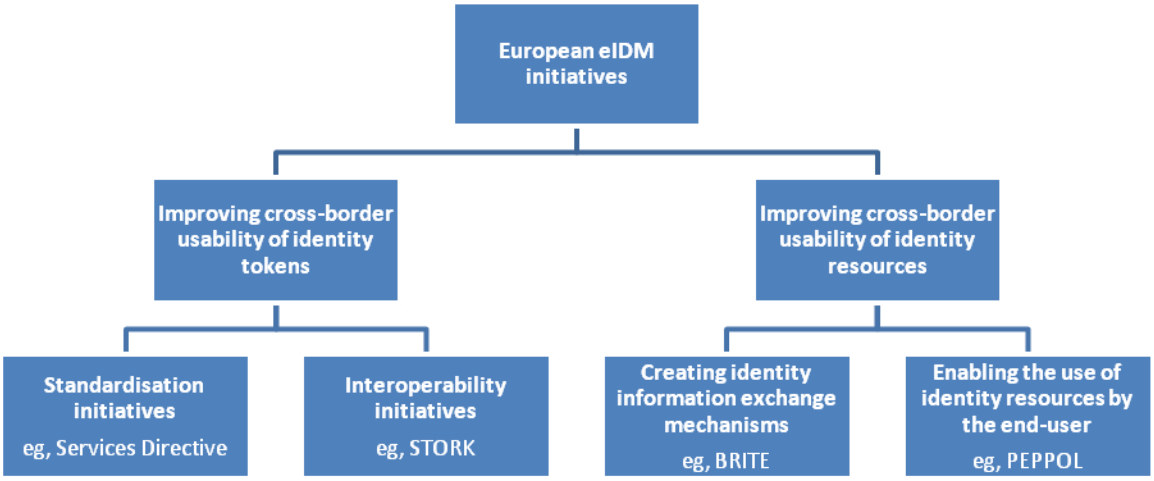
[91] *European Criminal Records Information System (ECRIS), aimed at improving collaboration between European criminal investigators, as described in Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record; see also http://europa.eu/scadplus/leg/en/lvb/l14500.htm*

[92] *For more information on eProcurement as a potential service case for the BRITE project, see http://www.briteproject.eu/project-overview/service-case-3*

computerised conviction-information exchange system[93]. The required infrastructure for this information exchange has already been established and is currently being used by six Member States to improve their judicial collaboration. While the use of ECRIS is currently limited to this context, there is no technical reason why such a system could not also be extended to be used as an identity information resource in other contexts. Obviously, before this could happen, sufficient privacy safeguards would need to be built in, given the extremely sensitive nature of the information made accessible through ECRIS. Nonetheless, both BRITE and ECRIS can be considered examples of projects in which authentic identity information is exchanged directly between the competent members of a federated network of trust in a specific context.

Thus, it is important to be aware that European electronic identity initiatives are not restricted to the three initiatives discussed in greater detail above. Globally, these initiatives cover two aspects, with some focusing more on one aspect than on the other: on the one hand, improving the interoperability or standardisation of specific electronic identification/authentication tokens issued to the public and, on the other hand, initiatives aiming to improve the utility and usability of authentic (or at least trusted) identity resources other than personal tokens. This can be represented through the schema below.

[93] *As described in Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record; see also http://europa.eu/scadplus/leg/en/lvb/l14500.htm, and related initiatives such as the establishment of Eurojust as a way of reinforcing the fight against serious crime at the European level (see http://europa.eu/scadplus/leg/en/lvb/l33188.htm).*


European eIDM initiatives
Improving cross-border usability of identity tokens
Improving cross-border usability of identity resources
Standardisation initiatives
eg, Services Directive
Interoperability initiatives
eg, STORK
Creating identity information exchange mechanisms
eg, BRITE
Enabling the use of identity resources by the end-user
eg, PEPPOL

- Approaches to improving eIDM practice in Europe -

Thus, the initiatives discussed above are complementary to a large degree. Efforts within the Services Directive related to eIDM are aimed at further standardising eSignature solutions so that they can be used across borders more easily, including for identification/authentication purposes if the Member States desire to do so. The STORK initiative on the other hand does not focus on standardisation as such but rather on putting in place the interoperability infrastructure required to use national eID tokens across borders. In contrast, BRITE's virtual company dossier approach does not focus on the identity token as such but on creating a network of trusted identity information providers in the sector of business registers. PEPPOL integrates this infrastructure and tries to leverage it to the benefit of the end-user (tenderers, in this particular context) by allowing them to manage specific information from authentic identity resources.

Thus, one of the remaining key challenges after the conclusion of the STORK project will be to integrate the outcomes of all of these different aspects into an updated global vision for European electronic identity interoperability. It is clear that no single initiative has defined the sole valid solution to European identity management issues. A coordinated approach combining the benefits of these proposals will need to emerge in future years.

V.2. Elements of uncertainty for the future

While it is clear that eIDM initiatives are ongoing in each of the fields identified above, there are still a number of elements of uncertainty, both in relation to the three key initiatives discussed in greater detail above, and in relation to European eID policy in general.

In relation to the roadmap, its horizon has always been defined in terms of the year 2010, in keeping with the i2010 objectives. However, it was known that this deadline would likely be too strict in relation to a number of important questions. While pilot efforts (including the STORK project) will contribute substantially to many of the building blocks defined in the roadmap, some elements will likely not yet be dealt with in adequate detail, including the issues of role, mandate and delegation management (which have not yet been resolved at the national level), and possibly the implementation of a data stewardship model. Furthermore, before implementations can be deployed at a level wider than the pilot stage, crucial questions in relation to data quality and liability will have to be settled as well. The first outcomes of STORK will have to be awaited before this issue can be settled, as responsibilities and liabilities can only be determined once a more detailed infrastructural model has been worked out.

The scope of the output of STORK will thus be crucial in outlining the work that will still need to be done after its conclusion, in a number of ways. The choice of an infrastructural model is important in this regard: will STORK follow a purely proxy-based model or a mixed proxy-middleware-based approach? This issue is not yet definitively solved at this stage. Furthermore, given the available timeframe and resources, STORK will need to make a number of assumptions, eg, in relation to reliability of the available eID infrastructure, security, user-awareness and understanding of the technology, or simply knowledge of specific languages. These will need to be ironed out at a later stage.

With regard to the Services Directive, it is clear that the eID aspects are considered to be a provisional solution, which should allow the Member States to use electronic signatures for basic electronic identification functionality as well, if they choose to do so. The strategy around the Services Directive at the European level is thus focused specifically on PKI, and specifically on the use of qualified signatures and advanced signatures based on qualified certificates. One element of uncertainty is the attitude that the Member States may take towards electronic signatures, as some Member States may not wish to use PKI technology in the context of the Services Directive, or as a means of service provider identification, while others may choose to use another approach rather than relying on qualified signatures and advanced signatures based on qualified certificates. Thus, it remains to be seen whether Member States will elect to use electronic signatures in significant numbers, and whether they will do so by the expiration of the Services Directive’s deadline at the end of 2009.

Apart from these issues which are specific to each of the initiatives, a number of higher level questions still remain open. Many of these are related to expected or possible technical developments at the national level, including the uptake and popularisation of newer eID technologies (biometrics, RFID, identification via mobile phone, ...). It will be important to ensure that the European identity infrastructure is technologically neutral enough to be able to handle these to the extent that this becomes necessary. Other developments at the national level can also play an important role, including the development of mandate management systems and data stewardship models to ensure that users feel comfortable with managing their personal data.

Socio-cultural developments will play a key role in this evolution. In recent years, the emergence of social networks and user-generated content sites has shown that it is possible to create trust in identity information without relying on formal validation processes, based on alternative trust creation practices. While this is not an accepted solution in public administrations at this time, it is important to be aware of the shift that this is causing in the general public's perception of personal data, privacy and data protection. Users are increasingly becoming aware of the need to create and manage online personas as digital complements to their real life identity. Irrespective of the potential that this may or may not offer for eGovernment applications, it is important to keep in mind that the task of managing one's own personal data, traditionally considered too complex for the average user, is increasingly becoming a familiar part of everyday life. Users expect greater influence in managing their electronic identities. If this trend continues, European eID initiatives will also need to be able to take this evolution into account.

Notwithstanding these observations, there also remains a clear digital divide between different user-groups. While more and more users become familiar with identity management – not as a concept but as an everyday reality in an electronic environment – the reality is that more sophisticated eID solutions still see only a limited take-up in everyday practice. In part this is due to the insufficient availability of attractive everyday applications; but another component is the unfamiliarity of the technology. In a cross-border context (which is after all the focus of this report), accessibility and usability become even greater concerns, as different cultural environments or simply different languages can become a greater barrier than the understanding of the technology. So far, it is not yet clear if there is a suitable European answer to the issue of eID accessibility in the aforementioned projects.

Another element of uncertainty is the role of private sector partners, both as eID infrastructure providers (eg, a private CSP issuing smart cards for the purposes of electronic identification) and as service providers (eg, a bank allowing the use of an eID card to ensure secure access to an e-banking application). The eID Roadmap already noted that the development of private sector applications that leverage public eIDM infrastructure could be necessary in order to ensure sufficient return on investment and to increase the usability and appeal of electronic means of identification to end-users. However, the initiatives discussed above do not deal with this issue in any detail. While use-cases are considered for the selection of pilot projects in the STORK project, the emphasis is still very much on public sector applications. The data protection and trust issues related to integrating private sector controlled eID tokens or applications are thus not fully appreciated at this time.

Finally, and perhaps most crucially, current European eIDM projects take different approaches to resolving the issues surrounding the trusted exchange of reliable identity information. These include approaches with a stronger emphasis on the user, on the infrastructure or on leveraging the available authentic resources. The main challenge for the future will be the integration of these different approaches into a single vision. Failure to achieve this objective may result in incoherencies in European eIDM policy.

V.3. Evaluation: are the policies working?

Through such devices as the i2010 strategy, the eID Roadmap and the Services Directive, Europe has imposed extremely ambitious short-term eIDM goals on itself and on the Member States. This ambition has resulted in a significant number of relevant initiatives, many of which have been discussed above, and all of which add their own piece of the puzzle on the table.

It is clear that this approach will allow significant progress to be made by 2010, with the results of the implementation of the Services Directive, STORK and other initiatives such as PEPPOL taking a central role. However, not all eIDM objectives will be reached by then as noted above, and further initiatives will be needed to broaden and extend the outcomes of these initiatives. Furthermore, the integration of all outputs into a more unified eIDM vision will gradually take a larger role. Several reflections will need to be made in this regard.

A first concern is the responsibilities that the end-user will assume in the process of identification/authentication. Traditionally, the role of the end-user in this process is rather passive: upon completing an identification/authentication process, a standardised set of identification information is made available to the service provider, who will then process the relevant elements as needed. While this is an adequate approach, it does not account for some of the more finely grained possibilities of newer technologies, such as restricting the information transferred to the strict minimum needed for the service provider's purposes, automatic privacy policy enforcement and facilitating the exercise of the end-user's rights to access and correct his information (if applicable).

Most of these possibilities are not yet typically made available to end-users, as they would likely be considered too complex for average users at this time. Nonetheless, as familiarity of end-users with identity management grows (including through their voluntary participation in social networks), offering these possibilities may gradually grow into a requirement, especially considering the inherent data protection weaknesses of the existing mainstream eIDM practices. A coherent approach to this issue will be needed: what can and should be expected of the end-user, and how can data protection concerns be addressed?

A second question is the issue of security and trustworthiness. It has never been the objective of European eIDM policies to culminate in a single electronic identification/authentication solution to be adopted universally and applied in all public sector applications. Instead, it has been made clear (and explicitly stated in the eID Roadmap) that Member States should be able to provide end-users with the identification/authentication means that correspond best with their expectations of security and user-friendliness. This implies that there can be significant differences between the security and trustworthiness of eIDs used in different Member States.

This is a positive element, provided that this diversity can be taken into account at the cross-border level. Application owners must be able to determine the reliability of the eID being presented by end-users from different countries, and they must be able to decide on that basis whether the end-user should be able to use the application. This implies that specific security levels are clearly defined, and that each eID intended to be used at the cross-border level must be catalogued in accordance with these security levels. While efforts have already been undertaken to take the first step in this direction, it is unlikely that a full and systematic approach will be developed and taken up by 2010. This is a clear gap which will still need to be resolved.

In relation to this, the direct exchange between trusted parties of identity data stored in databases is also increasingly being considered as a way of strengthening the trust in identity resources. The aforementioned BRITE project is an example of this trend. This is indeed a valid approach to increase the impact of electronic identification: following successful identification of a citizen or enterprise, additional information is directly obtained from an authentic database. From a data protection perspective, a system that provides the end-user with greater direct control over what identity data can be transferred may seem preferable over one that allows automated data exchanges; however, automated exchanges can be more efficient and user-friendly.

Furthermore, the fact that they require trusted networks of similarly competent bodies to be set up which manage comparable identity resources will improve administrative cooperation. This can be particularly relevant when identification/authentication requires the presentation of information which is highly specific to one sector and which is generally comparable across borders, such as citizen or business registers, tax registers, social security registers, etc. In such cases, the integration of the relevant databases into the identification/authentication process offers a real added value. Reflection will thus be needed on how and under which conditions this integration can be accomplished.

Tied to all of these issues are the questions of responsibilities and liabilities. Depending on the national and European eIDM infrastructure to be created in the next few years, specific roles need to be defined for end-users, identity providers and identity resources at the national level, proxy service providers to connect service providers to identity providers, the service providers making use of the identity resources themselves, and any variety of other entities involved in the process. When networks of identity resources are established (such as networks of business registers or criminal record registers), specific processes need to be put in place to ensure the security and integrity of the information and the availability of appropriate access management facilities and audit trails to ensure that the privacy of the individual is adequately protected. Furthermore, for a number of questions (including, for example, the very common question of representation of legal entities) the issue of roles, mandates and representation needs to be handled in a sufficiently systematic way. For all of these matters, a sufficiently robust legal framework needs to be put in place, along with a clear framework of responsibilities and liabilities.

Similarly, the use-case of the electronic means of identification needs to become more clearly established. The eID Roadmap already acknowledged that private sector uptake is an important factor in improving the popularity of electronic means of identification, since most citizens and businesses have only a limited number of interactions with public sector entities on a yearly basis. Sufficient private sector involvement and uptake is therefore important to ensure that any given eID tool is taken up in practice, and that its use becomes intuitive. While pilot projects are chosen with actual use-cases in mind, the use of electronic means of identification in private sector applications does not appear to be a priority of European policy yet. This current focus on public sector services could be considered a weakness and integration with other applications – including private sector initiatives – should receive further attention in the future.

And finally of course, the uptake of any European eIDM initiatives is largely dependent on the creation of trust and usability with the end-users. The systems must not only be safe, they must also be perceived as such. This implies that significant efforts are made to ensure the transparency and accessibility of the system, keeping in mind cultural differences in the approach to identity management and personal differences in familiarity with newer technologies.

Some of these matters have already been touched upon by the existing European eIDM initiatives in an embryonic form, and all of them will undoubtedly be explored further in the next year in the course of ongoing projects. However, it is important to keep in mind that none of the initiatives in the field of eIDM discussed above aspire to be an end point for the evolution of eIDM, and this explains in part why some of the points raised above will likely need to be refined further and reprioritised beyond the 2010 horizon.

Based on the considerations above, the main policy priorities for European eIDM initiatives in the next few years can be expected to be the following:

- In the course of 2009, after the first outputs of current key projects such as STORK, PEPPOL and the implementation of the Services Directive become available, the eID Roadmap will need to be updated. The current roadmap was drafted in 2006, and its building blocks were defined and planned with a 2010 deadline in mind. With this deadline drawing closer, it will be necessary to determine which parts of the roadmap still need to be realised, and if and how the building blocks need to be re-evaluated for the following years. This update of the roadmap will also need to examine how the benefits of all existing approaches can be combined in the future. At this stage, it will become increasingly important to link the output of the current efforts to external applications, such as integration with social networking sites or allowing the resulting infrastructure to be used for eCommerce purposes. This would likely improve the appeal and use-case to citizens.
- On the basis of the results of the STORK project, how the pilot infrastructure can be expanded into a full-scale system will need to be examined. This will entail the identification of any assumptions that had to be made in the course of the project and the creation of suitable and acceptable solutions to replace these assumptions. Based on currently available information, further efforts will specifically be needed to ensure the trustworthiness and reliability of the infrastructure, by eliminating any remaining security weaknesses and by implementing a suitable legal framework within the Member States.
- Once an interoperability infrastructure is in place, Member States will be forced to reflect further on the reliability requirements they will impose when specific applications are used by foreign citizens or enterprises. Thus far, this question has not been dealt with systematically, since no interoperability infrastructure was available and the problem was therefore largely theoretical. With a viable electronic identification infrastructure in place, Member States will need to decide how they

will define the security requirements of their applications, without unfairly discriminating foreign citizens and enterprises.

The concepts of identity and identity management continue to evolve, as do peoples' use of and approach to personal data, and the underlying technologies. It is important to consider these changes when reflecting on the future of European electronic identity management. When keeping in mind that 2010 is not an endpoint for eIDM evolutions, and that European eIDM policies will thus need to change with the times, it becomes all the more important to ensure the robustness of the building blocks that will be available in 2010.

From that perspective, the European eIDM policies have the particular merit of exploring most of the available options. If sufficient emphasis is then placed on the integration of these building blocks into a coherent and accessible whole after 2010, in particular taking into account the interests of the end-users whose information is being managed and the remaining issues outlined above, electronic identity management can become one of the strengthening pillars of the European information society.