Workshop Report: eIDM towards 2015

11th May 2007

www.securegov.eu

Executive Summary

This document represents the results of a workshop held in April 2007 in Brussels, looking into the future of eIDM in 2015. This topic has been recognised as important at the highest levels and the Euroepan Commission has been tasked to prepare for the introduction of pan-European electronic Identity Management (eIDM), by 2010. Its objective was to establish: drivers and barriers to the development of a European eIDM system; a list of Pan-European citizen centric online services that could be expected to be available by 2015; possible wider socio-political and economic impacts of these service; suggestions as to what needs to be done today to ensure that a dependable and secure system for identity management is in place by 2015 to enable such services.

The workshop used an interactive 'breakout group' methodology, which posed five general questions to the participants in the context of three different scenarios, based on the applicability and relevance of outcomes of the Large Scale Pilot (LSP). Three scenarios were portrayed: "Just Do It" a world where the Large Scale Pilot demonstrates that anything and everything is possible; "Pick and Choose", where islands of interoperability and data exchange have resulted in a fractured approach to eIDM in Europe and finally "Only if you have to": a scenario where a simple common identifier is prevelant and used mainly as a back office check between different administrations. The questions posed to participants revolved around the types of services that could be envisaged; the things that need to be done to deliver these scenarios; the social, political, economic and environmental knock on effects, things that are driving or holding back uptake of such services and finally public policy actions. The participants were equally split amongst different types of stakeholder and the dicussions in the plenary session resulted in a number of high level concerns. These included the importance of dealing with legacy systems, how to overcome the inertia of relecutance to invest, deploying a pan-Euroepan system while still respecting core European values such as privacy (and what implicaitons this may have); the relevance of the use of investmnent stimulation to help reachign a critical mass of users and applications and finally the all important role of the private sector.

The rest of this document is structured in the following way. Chapter 1: Set up of the Workshop briefly covers the background, objectives and format of the event. Chapter 2. The Scenarios Workshop then elaborates on the scenarios themselves (preceded by short presentations from the Euorpean Commisison and the study team to set them in context) and brings in the key questions to be considered. Chapter 3. Workshop Results describes the discussions per question across the three breakout groups. Chapter 4: General Discussion concludes with some consideration of the common issues arising from each workshop. Chapter 5. Conclusions presents the conclusions of the day and, where appropriate, recommendations for policy makers. Four appendices contain further background information on the scenario framework; complete notes from the breakout sessions; a list of participants and finally an agenda for the day.

Table of Contents

Introduction

Across the world states and businesses are tackling the issue of identification in order to know who their clients are, and to ensure that clients get access to the right information and services, and only those that they are entitled to have access to. Getting identity management right is critical, as "electronic identity" is rapidly becoming the central organizing principle in the information society. European Ministers understand this and have asked the European Commission to prepare for the introduction of Pan-European electronic Identity Management (eIDM), by 2010.

To align actors in the field a powerful shared vision beyond 2010 is needed, driven by real user needs and public interest. The workshop, bringing together experts from industry and government from across Europe and from several disciplines, intends to contribute to shaping that vision by considering scenarios of pan-European eIDM in 2015.

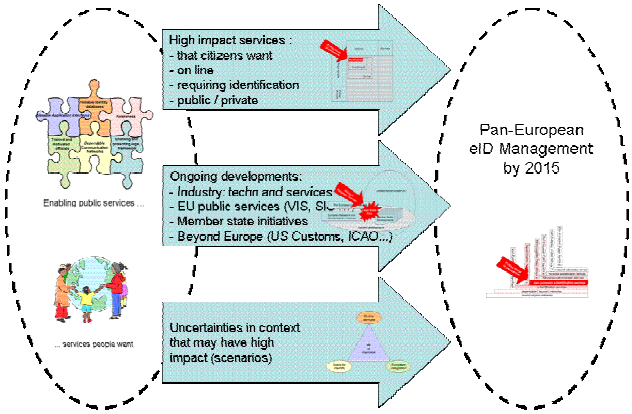
1. Set-up of the workshop

The workshop explored the use of Pan-European eIDM beyond 2010 (provisionally the horizon is set on 2015). It established:

1. Drivers and barriers to the development of a European eIDM system
2. A list of Pan-European citizen centric online services that could be expected to be available by 2015
3. Possible wider socio-political and economic impacts of these service
4. Suggestions as to what needs to be done today to ensure that a dependable and secure system for identity management is in place by 2015 to enable such services.

This workshop focused on the social economic, political and legal environment, not so much on technical approaches, which will be the focus of the large scale pilot that will be launched by 2008. A Roadmap towards the development of a pan-European eIDM system by 2010 has been published. This includes a number of specific milestones to be reached in order to ensure that the final objective of "secure means of electronic identification (eID) that maximise user convenience while respecting data protection regulations" is achieved. Given the existence of this Roadmap it is, however, important to understand what perspectives exist beyond 2010, as choices on how to implement such services and for what purpose will continue to be made for years to come.

Fig. 2 Workshop process: from input to results



2. The scenarios workshop

2.1 Setting the scene

Aniyan Varghese opened the meeting by exhorting the participants to open up and discuss as much as possible as freely as possible the issues concerning what the future of eIDM, after the large scale pilot might look like. He re-emphasised that the meeting was intended to provide background information, publicly available for those interested in the Large Scale Pilot and also in eIDM in general.

In order to provide a common framework for all and to get the discussions to be as concrete as possible, with a focus on real impact on users, Constantijn van Oranje presented possible use cases of Pan European eIDM based eGovernment Services (PEGS). A selection of possible future services was made on the basis of a set of criteria: proof of policy relevance and political support (rationale and likeliness of intervention at EU level); pan-European potential and eID dependency. These were then assessed on their potential impact; thus prioritising high impact services.

It is found that incentives for delivering PEGS for citizens is low, but that mobility and health care concerns could be drivers for such services at the pan-European level. Services will likely develop as clusters around these themes; however the level of complexity will determine the speed of their development. A first wave is likely to be driven by apparent policy concerns as related to "European competitiveness", "single market", "security", and lowering the administrative burden, and the relative ease of development because of the way the existing services are currently implemented. A second wave, would be for similar high policy priority issues, perhaps including services for which pan-European implementation would have a higher degree of complexity (like some aspects of the social service system). A third wave could be building on the success of the first two waves, bringing in new entrants using existing infrastructure for totally new services; also by combining various services on the same platform

Once critical mass of services has been achieved and the system has proven to be sufficiently robust, flexible and sophisticated, a tipping point may be reached that will lead to substantial increase in speed of uptake of new services. Much will depend on the success of preliminary applications and their triggering effect on new services by new stakeholders, particularly commercial parties. Other policy areas – where there is a clear political objective or benefit like security and law enforcement, or G2B and commercial services -are likely to drive developments. It is not clear if and how these developments will spill over into the eGovernment for citizen services domain.

Around healthcare we assume first the further development of EHIC, then a European eHealth card carrying health data and providing access to health records and later emergency services requiring linkages between law enforcement, health, insurance and other services through a single identifier. Around mobility the likely candidates are proof of work and work permits and subsequently residency registration and access to unemployment benefits and social security. On the back on this new business applications and cross-cutting joint up services are likely to emerge.

Following this, Neil Robinson presented a short overview of a review of different national private sector and organisational eIDM systems and models. The key differences which this presentation identified were those of closed and open models as well as the token in use and the degree of biometric identifiers in use. He also highlighted different types of application, from simple national eID to transport, banking, healthcare and a myriad of other applications on the same 'smart-card'. The development of relevant standards and specifications such as the International Civil Aviation Organisation (ICAO) ePassport and numerous ISO/IEC standards for contact and contact-less cards are also relevant when considering future development of pan-European eIDM..

2.2 Presenting the scenarios

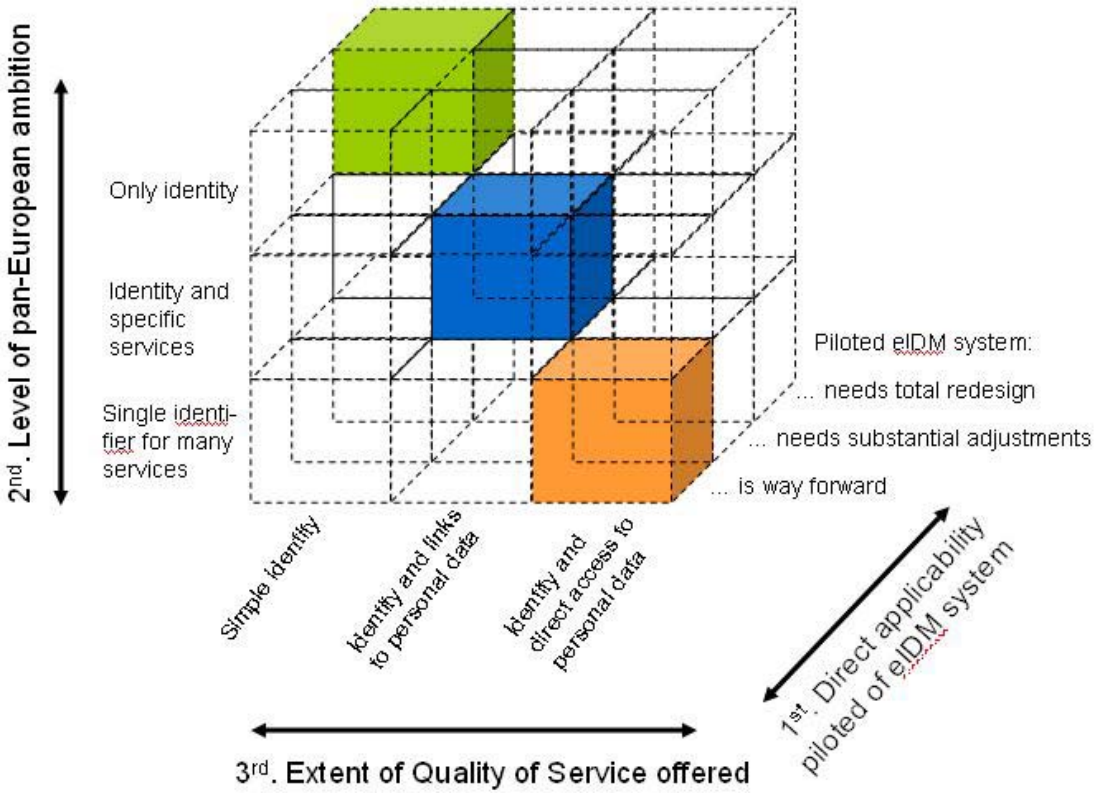
In order to explore future options from several perspective, three scenarios were presented by Maarten Botterman as starting point for the discussion in three subgroups of the participants to the meeting. In preparation of the scenarios we assumed that the current policy initiatives, as announced by the Commission already today and as planned in the eIDM Roadmap, will take place by 2010. The scenarios were build on a frame of three determinants:

1st determinant: direct applicability of piloted eIDM system: When the piloted eIDM system proves to be THE way forward, progress that can be made by 2015 is likely to be much higher than if the LSP experiences show that a substantially different approach is needed to get it right. The three gradations of "proven usefulness" of the piloted eIDM system are therefor important when considering 2015. It should be said that the impact of this by 2025, for instance, would be much less important than the next two determinants.

2nd determinant: the level of Pan-European ambition towards the use of a single eIdentity throughout Europe by 2015: Will policy makers of Commission and Member States agree on a system that is to support only simple identity; will Pan-European services be build/transformed in a way that they benefit directly from eID; or will there be a natural evolution towards one single European IDM, adequate for most national and Pan-European Government Services.

3rd determinant: level of ambition in terms of quality of service: Will the identity system offer simply name, nationality, date of birth, place of birth, and possibly up to date address details? Or will the system also provide links to other personal data, managed by different authorities. Or will the system by 2015 be able to provide direct access to personal data?

Figure 3: Scenario model



In theory we would be able to develop 27 scenarios. Even when taking into account that of those 27 many would be too unlikely to be considered, we choose to be more selective and limit ourselves to developing three scenarios:

1. The right bottom scenario is the one building on the assumption that the eIDM model used in the pilot is the way forward, and that eID is well established as single identifier for many services, giving access to abundant information to those authorised.

2. The middle scenario assumes that the eIDM model used during the LSP is useful but needs some adjustments, , with a system that supports specific pan-European services, built with using eID in mind, providing access to identity and links to other sources of personal data.

3. The upper left behind scenario would reflect that the piloted eIDM system is not directly applicable and that the pan-European ambition is to provide simple identity throughout Europe, with no access to personal data.

2.2.1 Scenario 1 "Just do it"

The most ambitious scenario (1) needs to build on successful security and implementation of PETs in order to ensure trustworthiness. In addition, the "intake" of identities which will need to take place on a distributed basis, is subject to the highest level of scrutiny. It assumes also that the advantages of scale are so dominant that European MS choose to share their resources on successful delivery, while still retaining their individual right to make exceptions on accepting Pan European Identity for access to specific services.

2.2.2 Scenario 2 "Pick and choose"

The "middle road" scenario (2) brings in an important 4th dimension: trust. One could say that even if we get the systems right in Europe, international forces pull on our ability to safeguard and protect personal data, like in the case of adherence to the provisions of the EU-US Safe Harbour agreement (regarding the assumption of the principle of adequacy of protection of personal data transferred outside the European Union). In the middle road scenario we consider a world in 2015 in which many forces may lead to a situation where citizens feel uneasy about releasing any personal data in the hands of government, certainly in an organised pan-European way. Because of the lack of trust citizens will "sit" on their personal data, laws will make it difficult to do sharing of data across institutions, and uptake of "opt-in" systems for instance for pan-European identity services will be very low.

2.2.3 Scenario 3 "Only if you have to"

The "least" scenario brings identity in Europe and will primarily focus on support of back-office communications. Incidentally, services will be built that benefit from this moderate level of secure identity. Obviously, distributed management of the system is challenged by the need to ensure a citizen is only registered in one European country, i.e. has a unique identity for obtaining access to government services. National autonomy is king.

2.3 Key questions for break out groups

The following questions were to be considered by participants for the different scenarios

- Question 1: What services (public and private) would be of most interest to citizens by 2015, should be on line available and require some component of identification management? Can the system serve both public and private services? How "open" should it be?
- Question 2: What can be done to enable this to happen effectively, while respecting core European values including privacy?
- Question 3: What could the socio-economic, political and environmental knock-on effects be of PEGS development? (in terms of support of EU policy objectives (4 freedoms,

inclusion, environment, growth and jobs, reduction of administrative burden) in the future?
- Question 4: What developments are driving or holding back the uptake of such services? The needs of the state or businesses for eIDM services should be considered as well.
- Question 5: What can public policy do to address these challenges? What are the most appropriate instruments for public policy to address these challenges (e.g. public-private partnerships, legislation, investment)? What actions should take place at European level? What type of research is required to support these policy activities? How can this research be pursued in an EU context?

The participants were split equally into three groups, with as broad a representation amongst the stakeholders as feasible, and were asked to discuss those questions in their respective subgroups.

3. Workshop results

In the discussions per subgroup, the following observations were made by participants in the specific scenario:

Scenario 1: "Just do it" commented that their scenario assumed a high level of active political support at both EU and Member State level as a precondition to moving forward. Without active political support from Member State governments significant progress will be very difficult.

Scenario 2: "Pick and choose" envisaged identification based on biometrics rather than necessarily reliance on cards or tokens. Service oriented infrastructures were likely to develop for example drivers licence, passports, health cards, and in professional niches like tachographs for truck drivers. They also discussed an opt-in system for social welfare for mobile workers, although this might risk being too popular.

Scenario 3: "Only if you have to" stressed that the minimal eIDM scenario should not be regarded as a "failure" of the large scale pilot. Rather it felt that, technically at least, any service could nonetheless be pursued within the "limitations" of the scenario.

Workshop participants then reported on their answers to the 5 specific questions.

3.1 Question 1: What services (public and private) would be of most interest to citizens by 2015? Which should be available on-line and require some component of identity management? Can the system serve both public and private services? How 'open' should it be?

The first scenario identified a wide range of citizenship services and other services.

Principal range of citizenship services would include:

- Access to education
- Recognition of qualifications
- Access to and administration of pensions
- Access to and administration of health
- Cultural services
- Facilitating democratic participation for example by facilitating voting

Other categories would include

- Mobility: travel facilitation and control elements related to law enforcement;
- Commercial services (financial services identified);
- Banking and access to credit registration services for licensing and tax – e.g. when purchasing a car.

Scenario 2 (Pick and Choose) considered that the likely services present in their scenario would need to be inherently Pan-European in nature, for example passports, to drive forward truly pan-European eIDM. Level of sophistication of data exchange would determine the true PE perspective (for example with driver license). Direct access to a central data base or to data in national data base from abroad being the highest form of integration. Whereas, just getting a binary response to a query, with an opportunity to 'manually' contact that relevant authority for more information would be at the low end of sophistication.

Other types of service could include:

- Drivers license
- Healthcare for non-national residents
- Tachograph;
- One ID for e.g. opening bank accounts, registering a car

Not much is needed to provide an important benefit to citizens. Just having 1 single identifier to enable access to services –opening bank account, registering car - across Europe (does not need to be automatic).

Openness would depend on security level of the system. Therefore, eventually PE services will probably be PKI based, as this is the only condition under which MS will open up their systems to non-nationals. This raises questions as to how to integrate systems that apply different levels of security – like in the Netherlands. While some services will require a high degree of security, the vast majority will require light security. Can a more graded system be envisaged in the transition towards PKI? Will PKI prove to be robust enough in future?

The last scenario group (Only If You Have To) felt that minimum eID requirements should not necessarily limit the services that follow from it. The main considerations around services were how legal aspects would affect interoperability. With every country having different security and legal requirements, the country with the lowest level of security would offer a 'backdoor' to the whole system (as the highest possible level of security in any system is equal to the security of the weakest part of the system).

It was felt that responsibility for developing services would pass to industry and that industry would necessarily want to develop its own solutions that best met its commercial needs.

General observations

In the discussion, participants voiced concern there had to be a clear reason for using eID and focusing on what services would benefit from eID was a way of focusing on what benefits it would bring. There was a feeling that business would step in if there were clear commercial reasons to do so.

To illustrate this, the example of the Personal Identity Verification II initiative was cited in the US. Although this is a federal government wide scheme, one application that is being rolled out rapidly is eIDM for first responders at a large scale. This enables authorities from different organisations to properly identify individuals at the scene of an emergency or disaster.

3.2 Question 2: What can be done to enable this to happen effectively, while respecting core European values including privacy?

The first scenario group envisaged two key enablers. Firstly an enabler that would provide for secure access to services (a minimum standard for cross border operability); this should use technology that is as secure as possible.

Secondly secure access to individual data with several layers of related permissions – from a binary Yes / No to other more detailed sets of attributes with control over how much information is provided being vested with the individual (who; for whom; how).

Underlying enablers included legal adjustments, underpinned by insurance to provide monetary compensation for failures in the security in relation to access to the service.

Scenario group 2 thought that consent and access rights must be built into the system. A prime example of this requirement is for health services.

It was felt that there would in fact be a limited number of citizens for whom Pan-European eIDM services would be required. Most Pan-European services are incremental to national services which currently cope in a pragmatic way.

A key enabler would be the ability of business to add certificates or signatures to public eID cards.

Privacy is important in the third scenario. Identification would therefore need to be split from private data. There would be a different interpretation of what the public sector would want and what the private sector would want.

General observations

The role of the commercial sector featured throughout discussions. The relationship between the private and public sectors was important and the extent to which data can be shared and to which the public sector can rely on the private sector's identification process. The example was cited of Finland where separation of data and identification has been implemented such that citizens usage of private sector identification processes was the preferred method of interacting with the national eIDM system.

It was also emphasised that it would be important to include data protection issues from the design phase onwards, as to ensure compliance with privacy legislation and to ensure there is no doubt about privacy issues with the general public.

3.3 Question 3: What could the socio-economic, political and environmental knock-on effects be of PEGS development? (in terms of support of EU policy objectives (4 freedoms, inclusion, environment, growth and jobs, reduction of administrative burden) in the future?

The first scenario group identified that there would be environmental impacts to consider such as a reduction in paper consumption as well as possible effects on energy consumption through using eID solutions.

eIDM could help to further establish a single European market, just as the EURO has done. Furthermore it would bring down overall costs of both administrative and commercial transactions. There was a question as to whether these benefits would be passed on to consumers.

There would also be effects on choice, trust, mobility and development of new private services.

There was a question as to how the costs of the underlying infrastructure would be allocated amongst public and private parties, as commercial applications that might benefit from the infrastructure could additionally contribute to its build-up.

The second scenario group concluded that Pan-European eIDM would only have an impact on the Lisbon goals if it led to a reduction in the costs of running a business in Europe. Then business would participate and develop services over a public platform. Otherwise the direct economic relevance to business will be low and very little contribution can be expected to the Lisbon goals. In this scenario the identity space will be fragmented and service dependent. The utility of the service determines which MS/regions will participate (e.g. a service for cross border road haulage will not be very interesting for island Member States); as well as the cultural proximity of participating MS (and their administrations), as trust between them will be an important enabler for developing joint services.

The third scenario group considered that the process would be delayed until a certain level of trust had been reached. A possible risk is that strong authentication might jeopardise privacy. The legal status of participants would need to be considered as different norms would apply to different groups.

General observations

Could the next round of European integration be through the provision of Pan-European eServices? Fully interoperable PEGS would remove impediments for cross border activity and provide an impetus to mobility across the EU. These would allow interaction with central and

local government all across the EU, thus also providing content to a new notion of a 'pan-European administrative space'.

An open book approach to ensure transparency towards citizens would be required, in particular under the first and second scenario.

Inertia towards development of pan-European eIDM systems was feared, as it became clear that governments today are still not ready to prioritise their investments, and industry is hesitant to start investing in these services as long as government has not committed on a way forward, yet. It was said that typically for business to invest a three year time horizons for pay back on investment would be needed, and in the current context horizon is not there, yet.

3.4 Question 4: What developments are driving or holding back the uptake of such services? The needs of the state or businesses for eIDM services should be considered as well.

Scenario group 1 observed a likely bottom-up effect in that Pan-European government services would likely be based on successful national implementations with additional mobility. The perceived usefulness of the applications and services is a very important driver; availability of Pan-European identity services would likely be a driver for new services to develop. The fact of availability would lead to the private sector developing new applications. Inertia based on absence of political support, national security systems and legacy systems would hold developments back. There was a view that, depending on the implementation and proper communication to consumers, privacy could be an enabler rather than a barrier.

The second scenario group thought that the utility of such an eIDM solution is likely to be perceived differently in different Member States. It is possible to imagine that some applications will be seen in particular Member States as more useful and possible to see different clusters of countries going forward. Proportionality as regards the benefits of data exchange must also be borne in mind. Disproportionate effort and data exchange requirements for very little actual benefit must be avoided - also under privacy protection rules. The ID issuing authority is the weakest link as fraud or corruption may provide access to official eID, which is then very difficult to identify or combat. Trust is a key driver for nations and can result in regional co-operation. Cooperation requires trust in the processes and guarantees of the other country. Reaching a critical mass would influence when business would join in. Once a critical mass has been achieved, this would of course act as a driver. Convenience and costs to both government and citizens must be to be weighed up. Diverging national solutions would be a barrier; as would different national views. Whereas the damage of identity theft (or abuse of access to identity) would be less under this scenario than under the first (since any access key would only give access to a limited part of personal information) the efficiency gain of a pan-European eID in terms of sharing of data and ensuring single identification in communication with authorities is also more limited that with the other scenarios The technology is easy to solve. Key to success is the strong organisational framework in which standards and agreements are commonly accepted (e.g. with passport). There are also legal barriers to be addressed. Branding of the card might be an important value for business, which it will not want to give up. There are also many issues around privacy, for example financial data not being on the same token as personal data.

The final group concluded that if there is no overall European consensus, the different speed of implementation in different Member States may prove a barrier. Different privacy rules in the Member States may also be a barrier.

General observations

It is clear from the discussions that political commitment will be the main driver determining impact of pan-European eIDM. In order to move ahead with an ambitious pace fierce commitment is needed, of all of Europe, or at least for a subset of countries that would

implement such a system, like within a type of "Schengen" agreement of "Euro-zone" agreement in which a subset of EU member states is included as participant. Privacy issues and legal issues are seen as generally more difficult to tackle than technical issues.

3.5 Question 5: What can public policy do to address these challenges? What are the most appropriate instruments for public policy to address these challenges (e.g. public-private partnerships, legislation and investment)? What actions should take place at European level? What type of research is required to support these policy activities? How can this research be pursued in an EU context?

The break out group considering the first scenario identified that EC regulation was needed in order to implement and give authority to the single identifier. standards of registries and standard for delivery of process for the identifier would need to be defined. There should be an agreed chain of responsibility between the provider and the eID and underlying services. In the absence of agreement, legislation would be needed to account for liability.

There should be standardisation of the token, establishment of licensing and certification services and an anti-abuse process with authorities responsible for this. Legislation dealing with competition issues to prevent competitive abuse of eID or underlying services should be considered.

The second scenario concluded that there currently is a lack of co-ordination and leadership. Managing a PE eIDM system will require a 24/7 management effort. A centre of excellence might be able to assume this role; like a virtual ICAO. ENISA could perhaps fulfil this function. There was a question as to whether the use of such an agency to run a possible eIDM hub might be an appropriate way forward. Decisions would need to be taken as to what services were needed at EU level. The Commission does not have this competence and an IDABC bridge gateway is a likely model for comparing policies. Consideration should be given to grants to kick start development in order to avoid problems associated with reaching a critical mass.

The third scenario concluded that common standards should be agreed in terms of ethical, legal and processing standards. Bilateral discussions might be more useful in the first instance prior to EU level discussions.

General observations

There was agreement on public policy support for agreeing on standards, and legislative reviews in order to address all legal issues that are expected to arise in a pan-European, cross border application.

4. General discussion

The key to establishing pan-European eIDM is partnership between government and industry. However, Industry will not invest in solutions put forward by governments or the EU until there is a business case for developing those conditions. To produce and maintain the infrastructure will clearly involve the private sector. Seed funding by Member States may be necessary to build systems to achieve a critical mass.

Issues around privacy need to be addressed. The involvement of privacy experts in communicating the privacy benefits of eID would be useful as privacy concerns are often seen rather as a barrier. This is currently seen in the UK with the debate on identity cards. At the same time it would likely be difficult to get consensus between Member States as to what data should be protected at what levels. For example in Finland personal incomes and taxes are a matter of public record while in other countries they are jealously guarded.

With regard to a body to co-ordinate Pan-European eID, a 'virtual' body on the International Civil Aviation Organisation (ICAO) model might be useful. Such a body could be tasked with co-ordinating standardisation activities. It could perhaps act as a kind of piece of virtual middleware that would identify pointers to which other middleware were useful for accomplishing translations between different eIDM systems in use in the public and private sectors amongst the MS. The European Network Information Security Agency (ENISA) was suggested as a possible body to provide Member States with information to enable them to take decisions based on trust related information. It was noted that any such organisation providing information exchange middleware would be in a very powerful economic position.

The following points were noted in summing up the observations of the workshop:

- There are no killer applications for eIDM yet its potential is clear to see
- Government application for security reasons may be driving take up
- What is the appropriate use of regulation or legislation in this sphere?
- There is a clear parallel between the deployment of pan-European eIDM with that of the Euro.
- What about the questions of competency, leadership, case for an Agency?
- Who will foot the bill for the infrastructures; the equivalent of the theory that build motorways and the rest will come?
- How can cost savings be made how can they be passed on? How can they be made visible so that the benefits can be made obvious for citizens and the authorities? How exactly can citizens benefit?
- Is there a place for local grants to support critical mass to help get over the initial 'hump' of take-up, to act as a catalyst for widespread use across Europe.
- Pan European Administrative space (which would help with the reduction of administrative burden)

Some final observations were made by the European Commission:

- It was noted that identity theft had not been raised as a consideration during the course of the workshop.
- Common standards and specifications had to be addressed which was already underway and the Interchange of Data between Administrations Businesses and Citizen (IDABC) programme were taking forward the Common Specifications work previously developed as part of the SecurEgov project.
- There was also a question as to the extent to which the administrative burden would actually be reduced via eIDM. There is a lot of speculation about this but little metrics so far.

5. Conclusions

One of the first conclusions which came out in the discussions was that the issue of legacy systems must be addressed for the roll out of a Pan European solution, post the Large Scale Pilot (LSP). As was described in the State of the Art paper, many countries already have ongoing eIDM systems in mature stages of development. Added to this is the number of national public sector / e-Government IT-enabled business change programmes developed across a significant number of MS as part of a now ubiquitous drive towards efficiency gains as part of New Public Management. Finally, there are existing large scale pan-European systems which must be considered – e.g. those in the area of justice and home affairs, run by European institutions. To adapt those towards a new architecture proposed by a pan-European eIDM system can come with significant cost and needs to be carefully considered.

In all scenario discussion there was no doubt that some form of pan-European eID will be necessary. The experiences from the LSP, as well as the further applicability of the eIDM model used during the pilot are important for the rate of progress by 2015. At the same time it is clear that the world around us will evolve as well during the period of the LSP.

The implications for privacy are a key concern in all scenarios. Within Europe there is a complex landscape of privacy measures, ranging from regulation such as the European Privacy Directive, to national laws, to co- and self-regulatory measures such as codes of conduct and privacy labelling schemes and finally technical and organisational measures that public and private sector organisations put in place to meet the privacy requirements of regulatory authorities and customers. Implementing any Pan European eIDM solution would have to take into consideration the different impacts on privacy for each of the possible scenarios. In order to take these issues into account, some form of **privacy impact assessment** might be associated with the more usual regulatory impact assessments which might be conducted prior to the formulation of any EU level enabling legislative instruments for a pan-European eIDM system. One example of such a conclusion was that given the development of a Pan European system along the lines of the first 'Just do it' scenario, significant modification of the European Privacy Directive may be required. This would be necessary for the clause concerning use of data for the purposes for which it was not initially collected (e.g. personal information collected in one MS for one application, being then used in another MS for an entirely separate application). European level instruments that provide strong (at least in the letter of the law) protections for privacy may thus be weakened by the implementation of a Pan European eIDM system if changes to the regulatory regime mean the greater use of more generalised terms. In general, early involvement of Data Protection experts (like the European Data Protection Supervisor or National Data Protection Supervisors) will be critical to development of a system like this.

Culturally, the perception and reaction to any eIDM system is important and those deciding the strategy and selecting industrial partners to deliver a pan-European system must be aware of these differences. Although it has become a cliché when rolling out new IT systems to mention 'education and training' simple yet effective demonstration of the clear benefits of any system must be seen as a top priority by policy makers. The experience of the UK in the early stages of the National Identity Cards programme (i.e. the intermittent alteration of the justification of the cards from 'entitlement cards' to being necessary for national security reasons) illustrates the pitfalls of not giving enough consideration to these issues. Indeed, if the results of some investigation and research are to be believed, it is clear that having an ID card does not make personal data any less private. There is already a significant abuse of identity information in the public and private sector and a great deal of identity information flowing around at present – much more than people perceive. Nevertheless the perception remains in some countries that handing over such information to the public sector particularly will result in a reduction in privacy. If the benefits of such a system are properly elaborated to a receptive audience, perhaps by reference to attitudes of a smaller pan-European target group that have successfully been using a system for some time, then this will certainly help

to smooth the way for the broader delivery of any such system (particularly one falling out from the first scenario). In order to establish the baseline of attitudes towards a pan European eIDM solution, it is recommended that a **large scale, statistically valid, survey of attitudes of European citizens and consumers to pan European eID** be undertaken (either as part of or concurrently to the Large Scale Pilot) to determine views and attitudes and identify where the focus of elaboration of the benefits should rest.

Throughout all three scenarios, the important role of the private sector was acknowledged. As can be seen from the State of the Art Paper presented there are a wide variety of models and architectures in use in the private sector. The private sector is leading the way with the use of standards, innovative models and common languages for exchanging identity related data between organisations and for allowing interaction between different identity management systems. Not taking advantage of this eco-system could lead to serious inconsistencies and challenges to the deployment of pan-European eIDM. The terms of reference for the LSP must therefore carefully consider ongoing developments in the private sector and ensure that the **LSP takes into account as many different models, specifications, meta-languages and frameworks as possible**, to stimulate market responses to the requirement. Businesses will be more attracted to using pan-European eIDM if it means they can rationalise and adopt simpler processes to deal with a single, common mechanism regarding the processing of identity related information and use a common platform present across Europe. In order to demonstrate this, **the LSP should focus applications on one homogenous group or community** to illustrate to businesses how using a pan-European platform would benefit them in terms of the roll out of commercial applications.

Following on from this, the LSP will have its part to play in the formal agreement of standards for use in such any Pan European system. Whilst the work on the identification of Common Specifications was subsequently taken forward by the Interchange of Data between Administrations Businesses and Citizen (IDABC) programme at the European Commission, no doubt the Large Scale Pilot will point at (the need for) further relevant common standards will have been identified which will need to be assessed and accepted at all levels.

One important concern is the myriad of different legal systems and frameworks in use that relate to identity information across the Member States. Currently no useful work has been done on how different legal frameworks in the Member States compare when it comes to managing identity information. Although a canon of privacy legislation and regulation is present at European level, this may be implemented slightly differently in the Member States and does not represent the full spectrum of applicable legislation (e.g. laws covering libel, pseudo identities such as Company Secretaries, criminal law etc). As can be seen from the problems concerning trans-national and cyber-crime (where cyber-criminals deliberately operate from countries that have poor legal and regulatory frameworks making pursuit difficult or impossible) there may well be a 'drive to the bottom', where, in spite of commonly held understood and accepted standards for eIDM across Europe, many countries will seek to push towards the most insecure, cheapest or unreliable standard in order to ensure that they can participate with the minimal level of investment.

Some concerns were raised with in this respect, as this undermines the requirements for strong authentication that were seen to be needed in all of the scenarios. One parallel that can be seen is that of the implementation of the Euro where a sufficient fiscal benchmark had to be set for those countries participating taking into account highly divergent macro-economic standards. **A scoping exercise should be undertaken as soon as possible to identify how other common systems such as the Euro have dealt with divergent participating standards.** Such an exercise might be part of the LSP. The opportunity for certain Member States to end up as the 'Sick Man' of any pan-European eIDM scheme must be minimised. Another way of addressing this problem might be via the extension of 'opt-in' schemes (the parallel was made with the European ePrivacy directive on unsolicited commercial email) on an application basis. Making participation on the basis of opt-in or opt-out model might allow for a two or even three speed deployment of pan-European eIDM, but could also backfire in making it challenging to raise the all important critical mass for wholesale deployment, as

some Member States might use it as an easy alternative to taking difficult national decisions necessary to make such an ambitious yet potentially worthwhile initiative succeed.

Legal differences exist between countries, and also between different types of audience that the eIDM card might be useful for. For example, identity information relating to children can be extremely closely protected by law and regulation, as with government workers, those in the law enforcement community and military personnel. The different legal and organisational frameworks surrounding such types of user would also need to be taken into consideration. **A mapping exercise of the different frameworks of user identity information** (to see how different legal, organisational, administrative, socio-economic norms apply to different groups for law enforcement, children etc) into one easily accessible overview would be a useful exercise to raise understanding within the large scale pilot.

"Inertia" came up as possibly the strongest enemy of effective development of a pan-European eID. National governments and policy makers continue to circle round these thorny issues as well as around each other and other European institutions in deciding who will take the lead in suggesting or establishing priorities for investment. Meanwhile, the private sector, which will be required to not only deliver the systems as a service provider but also use pan-European eIDM as a common platform for the deployment of other forms of market led strong authentication continues to observe, develop and deploy eIDM solutions according to the drumbeat of market priorities. Given the time frames for business cases in the private sector normally stretch to a return on investment within three years (a timescale that is currently not envisaged in the proposed eIDM Roadmap) there may be **a need to allocate, after the completion of the LSP, some investment or grants to stimulate take up by the commercial sector**. The potential is seen to be there – the example was made of Finland where the default usage of authentication in the national eID system is an offering from the private sector. Investment and grants would help generate the critical mass necessary for the widespread take up of eIDM outside of the focused constituency that may be necessary in the initial stages of the LSP.

A final conclusion was that the creation of some kind of eIDM knowledge centre would be a useful way of collating and managing information relating to different ongoing eIDM initiatives and efforts with national, regional, commercial group and organisational efforts. Clearly, as the State of the Art paper has demonstrated, there is a lot of work going on and it is important to have adequate understanding of some of these developments in order to maximise progress and not re-invent the wheel. Such a centre would not only have a portal like aim (in the collection, sifting and dissemination of information), but might undertake directly operationally useful activities. One possible such activity might be that of 'virtual middleware', that would not necessarily directly undertake the translation between different eIDM systems in existence or development, but might usefully point toward where the appropriate middleware might be found. With the advent of Service Orientated Architectures (SOA) and the 'web-services' model in IT-enabled eGovernment programs, this may be an extremely effective way to deal with the challenge of multi-speed membership of a pan-European eIDM system.

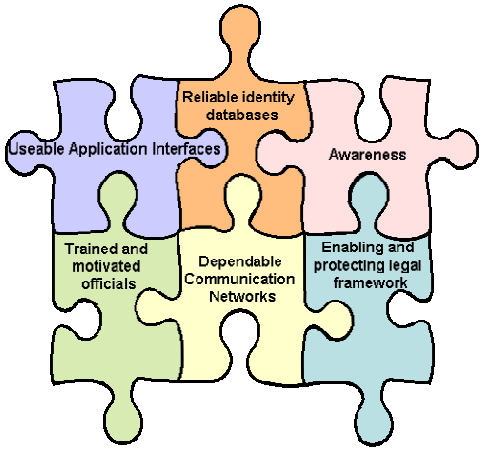
The use of the European Network Information Security Agency (ENISA) or a specific eID Agency as possible candidates for such a capability was raised, however significant barriers to achieving this exist, most notably the reconfiguration of the aims and remit of the Agency, a complex task fraught with extensive political negotiation at the European level. **A feasibility study might be undertaken to identify what would be the most appropriate vehicle to act as an eIDM clearing house or virtual middleware repository**. Candidate types of organisation might be an EU institution e.g. new or existing Agency or programme; long term study; public-private partnership or research or academic institution.

Appendix 1: Workshop structure

Background
Interactions among citizens, businesses and administrations increasingly revolve around the concept of 'identity'. Governments and businesses face the challenge of identifying citizens, customers and users reliably and accurately on a daily basis. Identity plays a central role in processes as varied as paying for an online order, getting a mortgage, and claiming unemployment benefits, but it is also important for the purposes of security and crime fighting.

The modernisation and streamlining of businesses processes in the public sector offers the potential of increasing efficiency and accuracy, reducing costs, and improving the 'end user experience'. However, in order to reap the full benefits of such increasingly digitised environments, an assured way of authenticating our identities is required. When this is to be implemented at a Pan-European level, this requires that identity is assured in a cross-border context.

Fig.1 Basic elements for achieving successful eIDM



European Ministers support this and have asked the European Commission to prepare for the introduction of Pan-European electronic Identity Management (eIDM). In the eGovernment action plan, adopted by the European Commission on 25 April 2006, the following commitment was made to this end[1]:

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

Across the world states and businesses are tackling the issue of identification in order to know who their clients are, and to ensure that clients get access to the right information and services, and only those that they are entitled to have access to. Getting IDM right is key, as

[1] See http://europa.eu.int/information_society/eeurope/i2010/index_en.htm

"electronic identity" is rapidly becoming the central organizing principle in the information society,.

Ensuring availability of an eIDM backbone across Europe will help to serve the citizens in their interaction with governments as they move across the EU. If high quality eIDM services on a Pan-European level are also made available to the private sector, new commercial electronic services that require IDM can be set up that serve the entire European market: Pan-European eIDM thus exists as enabler for innovation of public and commercial services benefiting citizens, but also businesses and in particular SMEs.

To align actors in the field a powerful shared vision is needed, driven by real user needs and public interest. This vision will inform further steps on the realisation of eIDM objectives by 2010 and beyond.

Workshop Scope

The workshop looked at:

1. Services by government and/or private sector;
2. For citizens,
3. that they want
4. On-line;
5. Requiring some form of identification;
6. At a Pan European level.

It explored the drivers and thresholds for development of services that potentially benefit from eIDM rather than just on the eIDM backbone.

Structure
The workshop examined the eIDM strategy by describing a set of scenarios based on key uncertainties related to European integration, methods of identification, and take up of online services. Experts and key stakeholders were brought together to support this process. Introductions on several key topics were made to develop a common ground for discussion, the scenarios were presented and explored, and a set of questions was used as a coat hanger for discussions in break-out sessions per scenario (three groups). The objective of using scenarios is to determine what measures or issues appear under all scenarios and which are scenario specific. Moreover the scenarios provide a good context for thinking beyond the ordinary. Following this the results were presented and discussed in a plenary setting. The day finished with a wrap-up of the lessons learned.

Participants: The workshop comprised of 39 participants (full list provided in Appendix 3: List of Participants), of which:

- 12 national experts
- 15 Industry representatives
- 8 Representatives from European Institutions
- 4 Members of the project team

Specific contributions
At the end of the workshop, specific contributions were delivered from three individuals representing different communities to illustrate varying aspects of what the barriers and enablers for the take up of eIDM by 2015 might be.

Ioannis Maghiros (IPTS)
eIDM is more triggered by the technological possibilities rather than issues of terrorism. Lessons learned from reviews of eID services, for example, FIDIS offer a wealth of knowledge of eIDM. The current issues in the EU are not about technology but rather about market

integration and what barriers there are. These are primarily issues around definition, with the legal profession at odds with the possibilities offered by the technologies.

Questions to address include what eGovernment services will be provided and how dependent will we be on these services. It was noted that the pressure for change is not at the moment so great because what we have works.

The scenarios discussed, taking a bottom up approach, can be contrasted with the work undertaken by IPTS which takes a more futuristic approach. Consideration might also be given to Web 2.0 and the fact that the younger generation has grown up using technology and is very used to the concept of multiple identities for different purposes. It would be useful to consider the disruption this might pose to the current pattern of extrapolation.

Hendrik Tamm (Project RISER)
Project RISER is a Pan European eService for address verification involving seven countries and now running as a business. eIDM in the EU presents us with a clash of cultures. Registries are also very different across the EU and the legal situation is very relevant. Countries for the project were pre-selected on the basis of their systems. It was essential to introduce privacy protection right at start of the project. With regard to citizens or business applications it is easier to roll out once there is a clear business case.

Lorenzo Gaston (Gemalto / CEN)
For the card holder privacy, eInclusion, interoperability are important. From a practical perspective legacy issues must be taken into account as well as existing standards. We must look at infrastructure (middle ware) and lower costs at every level, e.g. USB technology to reduce cost of reader. At the operating level existing standards must be considered as must ICAO. Pan-European eID is ambitious when thinking about integrating 25 members. There are also opportunities to think about exporting EU technology and setting standards.

Appendix 2: Complete notes from the breakout sessions

The following appendix represents the notes taken during each breakout session.

Breakout Group 1: "Just do it"

As well as the underlying assumptions of a successful long term pilot and a single identifier giving a common *starting* point for access to a range of services, we identified push/support fro the MS as a fundamental underlying assumption of this scenario.

Group 1 expected that a principal range of citizenship services would derive from the scenario:

1. Citizenship
    - Access to education
    - Recognition of qualifications
    - Pensions
    - Health
    - Cultural (eg library services)
    - Voting
2. Another classification of services involving mobility
    - This might involve travel
    - But also certain control elements related to law enforcement
    - Clearly also a factor facilitating
3. Commercial services
    - Banks
    - Access to credit
4. Registration services – for licence and tax purposes – car example

The following two principal categories of enablers were distinguished:

1. Secure access to services (+ minimum standards for cross border operability) using as secure as possible technology.
2. Secure access to individual data with several layers of permissions from simple yes/no to the different sets of attributes would be ..... by the individual not *centrally.*

In this it is important to distinguish the access criteria very well: Who – What – For whom – How - What attributes required?

However secure a system is, it needs to assume failures of the system will take place, and needs to include a fall back (insurance) in case of failure of access.

The following knock on effects were foreseen:

- Towards the environment, ultimately less paper, hopefully much less different plastic cards with chips.
- Socio-economic: introduction could have an effect similar to the euro in helping to establish a single market
- Might bring overall transaction cost down as identity becomes less of an issue.
- Choice / trust / mobility/ development of new private services

eID Infrastructure costs allocation may well be shared between government and commercial sector, as and when a business case for benefit can be made.

Stimulus for development and uptake of such a system would include:

- Perceived usefulness
- New implementations
- Availability – drives new applications
- Privacy as an enabler

The following factors may hold developments back:

- Inertia
- Legacy systems
- absence of political support
- privacy (perceptions) based on historical/cultural differences

Policy action needed include the establishment of minimal legislative harmonisation, standardisation of the e-ID token, establishment and licensing of certification services, establishment of a process and authority for handling abuse.

Breakout Group 2: 'Pick and Choose'

Development is likely to be regional or in groups of countries that have something in common thereby enabling an environment of trust

The citizen would have different ways of accessing services. However, it is not only about citizens; much of the eIDM effort relates to G2G, but allows citizens to profit.
eIDM can replace driver's licences and other cards or identifiers. Once there is a robust eID system it can be used to serve all ID related services and requirements. It would allow safe access to all kinds of information and specific identifiers would not be necessary. It could even be foreseen that biometric information would be sufficient, thereby making any token or other physical proof of identity redundant.
This would be backed up by online systems and mobile terminals. However, due to privacy, there would likely still be a mixture of systems.

Trust

Legal issues are the most relevant. A European system would mean that governments and citizens would need to rely on the accuracy of databases of other countries. This raises the questions about the extent to which it is possible to rely on the information of other countries. This is likely to be dependent on the sector as wrong decisions will have different effects in different areas.

Is the discussion about eID or more about sharing personal (ID) data? Simply exchanging identification across the EU is not a big issue. The real issue is sharing data.

How would it work: Cooperation or trust?

There is more to eIDM development then just trust. Cooperation is necessary to allow interconnection and interoperability. Common security requirements must be enabled, without sharing data. Proximity will be an important factor. There are commonalities in regions and regional mobility will be a driver.

What about the Pan-European context? The issues are not so much technical. If there are already standards why not use them? However, we are still missing a lot in organisational terms for eIDM to develop. For example, paper passports work because it is organised and generally accepted. EU-level organisation and setting of requirements (e.g. for readers) must precede or go hand in hand with the technical and legal interoperability.

Suggestions: to allow access to other state data bases: metadata bases should be developed that can be queried to find data and to clarify what the status of the data is: what rights, where to find it, what remit. "ID of Government", was the document really issued by a particular authority, etc.

Driver's licence as an example

Where there are a lot of exchanges there is meed for common acceptance.
The issue is exchange of data and not the document or the eID.

First there were no driver's licences, then national licences were issued as proof of driving ability, without international acceptance of national drivers licences. Subsequently an international driver's licence was developed. Then national driver's licences were accepted as proof of driving ability across Europe. It was then standardised and will now be replaced by a uniform European driver's licence. As such it may now become an ID paper and it may also give the ability to query the holder's track record in fines and his/her deduction of 'points' in other countries. How access to such data is organised is the real issue: just a telephone number for information by issuing authority; a binary (yes/no) response on a specific query; or the ability of law enforcement officers across Europe to query the national database of the country of issuance; or ultimately a central data base or a system connecting all national EU databases, that can be queried. Depending on the particular service or policy area, different solutions are likely.

Rarely will direct queries be needed. Most transactions could be solved with simple eIdentification and authentication.

Lisbon

How does this relate to Lisbon? What is the value added?

This scenario looks like what happens now: i.e. there are sectoral approaches. We see now, for example, tachographs, driver's licenses, EHIC developing parallel solutions. True added value would be if there were to be one EU eIDM backbone.
Is interconnection desirable? This would seem impossible as it would require a lot of new laws across Member States. It is likely therefore from national perspectives that different solutions may evolve. How can these different solutions converge to allow Pan-European eID?

For a full European eIDM solution national governments need to agree to certain standards. Levels of security, identification, authentication: only very few services need high security. DigiD in Netherlands has three levels of security. Belgium, in contrast, applies only PKI (highest level). Appropriate levels of security would need to addressed on a service by service basis. The level of security also determines the degree of openness that the systems can present
It will evolve to PKI; but this is the end state. In the development phase (towards full EU PKI) user name and password may be sufficient for certain services for the time being.
By 2015 will PKI be unbreakable? For now, however, PKI solves the problem of credentials. DigiD, for example, is layered; what should be done with copies made of entry in central data bases?

Weakest link in Pan-European eID is the issuing authority. In Europe there are many 'weak links' (e.g. Romania, Bulgaria….). Here there are huge benefits of using biometrics: issuance of double biometric document.

What Services?

If we take the example of health insurance, what is the real need to have the EHIC card. ID should be enough. Is it the token, or the access to records? Patient consent is an essential requirement for any healthcare related service to develop. The example of Connecting for Health is a case in point. Access rights have not yet been taken into account.

With business leading in these services, where is the role of government in emergency care? It is primarily about insurance companies willingness to pay. Hospitals will never refuse emergency treatment based on administrative restraints. Insurance is already dealt with: one can get extra insurance for travel.
The real issue therefore is healthcare for residents and not accidents of travellers: someone has to pay for giving similar treatment to non-citizens.
In the case of migrant workers one way forward might be an opt-in system. This would require an EU infrastructure parallel to national systems. Governments may not be too happy

to have a parallel system that allows circumventing national social security systems; however, this might also be a way to get migrant workers to pay tax.

Form filling. Might be too successful; thus scaling is required.

Utility will drive clustered development (instead of full Pan-European deployment). Taking again the example of the driver's licence there would be cooperation between Luxembourg and France; but not between Ireland and Cyprus. It is hard to see that they would all want to be a part of it and pay towards it. There would seem to be little argument for full Pan-European deployment.

Data protection: applications must be proportionate. Why would you want this given additional risk?

Demand for Pan-European Government Services or cross-border services remains mostly incremental: people register locally and then get access to local and/or national systems and services. This is not the same as Pan-European Government Services, as there is no seamless provision for all EU-citizens. The ID must enable the user to enter directly into the system. In niche markets (tachometer) such a European solution is already possible.

For instance, for EU citizens to obtain a UK national Insurance Number an interview is required The benefit of eID would be to do this online, the benefit being convenience and efficiency, saving time and costs.

There must be a benefit for Citizens and Government: Cost recovery vs convenience for citizen.

Car registration: insurance issue still requires local registration and governments want it for tax purposes and to allow to regular verification of the condition of the vehicle. The registration itself could be done online if the data on the car is also shared between MS.

Socio economic effects
Pan-European eID will only be fully endorsed if it reduces cost to business.
To encourage business participation, they will need to be allowed, for example, to store signatures/certificates on SIM cards.
In the case of bank cards an important issue is branding. If banks were to use a public platform, they could lose this branding opportunity, which could be a reason not to endorse it. Thus business and operational constraints may prevent large scale business take up from happening.
Belgium example 2 certificates but business is not allowed to store certificates.
-successful eID systems of good quality will be a platform eventually.
-Loosing cards is a big risk, you may still want different cards.
-Alternative eID options must be available
-privacy: not financial data on same card
-Just have one identifier to be able to sign up to services (opening a bank account). This would already a big step; more may not be needed.

EU policy

Coordination is required.
Organisation of such an interoperable eIDM system is a 24/7 job.
Consideration might be given to setting up an 'Agency', which would run an eIDM centre/information hub. This would create a centre for understanding what eIDs are around, what they represent, what the certificate is, etc. Like ENISA, it would enable the sharing of information.

A discussion is needed on what services should be developed at EU level. The Commission does not have this competence in this area and is not likely to acquire it either. Nonetheless, there remains a need for leadership.

IDABC bridge gate way; may be a good approach; compare policies; etc.
However, others in the group were not sure that this would serve a purpose.

Breakout Group 3: 'Only if you have to'

Comments on the scenario model

Why is this scenario associated with failure? The outcome of the large-scale pilot does not necessarily coincide with this scenario. If we get to this scenario we will have been very lucky. Just because the large-scale pilot is a success doesn't mean to say that this scenario will not happen. It may be that the LSP demonstrates a great deal of useful functionality from the first scenario described, yet Europe still ends up in this situation.

This scenario seems to have as one of its facets a patchwork approach (e.g. nations and governments using eID in isolation).

It might be useful to start with some definitions: ePrivacy as a definition? The ability to maintain unauthorised disclosure of personal information.

Within ePrivacy we might look at Control and Content. This goes back to a central facet of the scenario revolving around responsibility. In this scenario, the citizen has responsibility and control over his data.

In the context of the scenario eID is a political problem and a legal problem. In a world with strong authentication and encompassing different cultural norms of the Member States, there may be those who want to drive down the standards so that they can comply. No-one is studying the international legal aspects as to what differences exist in the legal frameworks as a whole (not just acceptance of digital signatures for example) between the different Member States.

What sort of services?

It is difficult to say what services might exist in this world. There was no solid consensus. In any case, these services might not be particularly useful to the citizen, but rather for back office applications. The utility for the everyday use is perhaps not so great. Services that have full distribution would be attractive to business in order to justify the investment / business case (justified by economies of scale, the fact that the users would be maximised and thus be a captive market).

Company use (of services present in this scenario) is important but how might this work, given previously elaborated points about roll out – (e.g. roll out being timed with deployment of commercial applications using the eID).

Points about selection criteria for services

The results / answers to the following list of selection criteria will be determined by the scenario and will determine what services exist in a privacy heavy world. The selection criteria themselves are 'neutral' and can apply for each scenario – it is the result that gives the thing its flavour.

1. Rollout – 5-10 years. The rollout of any PEGS based on a yes / no authentication model will very much depend upon choosing services that will be able to be rolled gradually. Services requiring a smaller (e.g. 80%) distribution of cards may not be appropriate for this scenario – services will need to be rolled out that require 100% distribution of cards.
2. A small identifiable user group – the size and coherency of the intended user group will inform what services we see based on this simple authentication model (e.g. the user group must be fairly homogenous, based around a single issue or application)

3. Any services would have to have a single means of identification – there would have to be no alternative means of using the same services which are cheaper, have greater penetration etc, otherwise the commercial sector particularly will use that instead
4. The type (and therefore cost) of infrastructure, for example the readers, would have to be considered
5. Any service should use a minimum of ID information – gender and age perhaps
6. Legal requirements will have to be taken into account – particularly in certain groups for example, children or young people who are protected by specific legal frameworks.

Being identified is not one thing however: identification opens up a world of applications. The process of identification will, however, have to give enough information to achieve the different requirements of different applications.

Strong authentication is the basis of privacy – without strong authentication there is nothing. Strong authentication itself, however, is a neutral concept.

There needs to be an 'ethical' umbrella above all these legal and infrastructural aspects, for example an ethical committee. The Belgian case provides an example. This helps with trust and transparency and provides an 'audit trail' so that the citizen can see who has had access to and what use has been made of his data, where and when etc.

A higher authentication level will be needed for data retrieval than insertion and there should be thresholds for sending out of data

Access control will need to be extended beyond the act of authentication. There should be parameters or locks on the data, once it has passed through the process of being used in an authentication context. Models of this access control will differ depending on whether the public or private sector is using the data. Each type of organisation has different uses for it, and different thresholds for which they are willing to accept credentials (e.g. at a basic level, businesses do not care too much as long as your money is good). There should be certain access rights attached to certain data which is used beyond the authentication process (known as extended authentication model – the process of authentication is the first step). This can be manifested in the notion that the method of authentication should be independent of the use of the data.

Drivers

Drivers are privacy, security and the need to rationalise identity documentation (as in the German example which is following this scenario model)

Knock on effects

Relevance of European residence permit / directive (AV did not know whether eID was a part of these discussions)
eID could improve the case for European standardisation

Interoperability is a common characteristic for it to be useful for the citizen

Policy Action

Talks to identify minimum common standards are essential. Member States need to agree on what constitutes minimum common level. This should be firstly done bi-laterally.

A matrix could be conceived of identity related parameters across the top as columns, then the Member States as rows and a tick in each box which is acceptable. This would help in getting agreement on what identifiers they are prepared to use in such a system.

Agreement on the level (and importance of) strong authentication is also necessary, as is interoperability testing, which is an important helper in the process.

Appendix 3: List of participants

Steven Adler	Microsoft
Anneli Andresson-Bourgey	European Commission, Internal Market and Services DG
Cord Bartels	NXP Semiconductors
Michael Bauer	Giesecke & Devrient GmbH
Laurent Beslay	European Data Protection Supervisor
Anthony Bisch	European Commission, DG Information Society and Media
Maarten Botterman	GNKS Consult
Olivier Briand	NXP Semiconductors
Marc Caen	SPF intérieur
Bruno Deschemps	Ministère de l'Economie, des Finances et de l'Industrie, Direction Générale de la Modernisation de l'Etat,
Francesco Fusaro	European Commission
Lorenzo Gaston	Gemalto
Valerie Gayraud	European Commission, DG Information Society and Media
Kjell Hansteen	European Commission, DG Information Society and Media
Heidi Havranek	Austrian Federal Chancellery
Leonard Hawkes	Solicitor (Juriste conseil)
Seppo Kurkinen	Ministry of Finance, Finland
Jean-Jacques Leandri	Ministère de l'Economie, des Finances et de l'Industrie, Direction Générale de la Modernisation de l'Etat,
Mireille Levy	Identity and Passport Service
Frank Leyman	Fedict
Ioannis Maghiros	European Commission, DG JRC – Institute for Prospective Technological Studies
Tarvi Martens	SK
Thomas Myhr	Ministry of Trade & Industry, Norway
Roger Nicolay	Coördinator EIK - Rijksregister
Gilles Polin	Microsoft
Patrick Pype	NXP Semiconductors
Neil Robinson	RAND Europe
Bruno Rouchouze	Eurosmart
Christian Sagstrom	Verva
Jon Shamah	Core Street
Rebecca Shoob	RAND Europe
Hendrik Tamm	PSI Business Technologies
Roberto Tavano	Unisys
Jan Timmermans	Ministry of the Interior and Kingdom Relations
Paul van der Pal	Ministry of Economic Affairs, The Netherlands
Constantijn van Oranje	RAND Europe
Aniyan Varghese	European Commission
Frank Zimmerman	HP Consulting and Integration

Appendix 4: Agenda

Thursday 19th April, European Commission, Rue Joseph II 54, Brussels

Time	***Activity***
09:30	Registration
10:00	Opening
10:15	Setting the scene: what Pan-European services; state-of-the-art of eIDM in Europe; introducing the scenarios
11:00	Plenary discussion on the issues, in general
11:30	Breakout sessions, exploring the issues *per scenario* around implementation of eIDM support for Pan-European services in the public interest
13:00	Lunch break
14:00	Plenary evaluation of dependence of eIDM issues on specific scenarios
15:00	Plenary discussion on the issues, in the light of an uncertain future
15:30	Moderated Roundtable: Conclusions and recommendations for eIDM policy
16:30	Closure