This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

2015: A connected and diversified Europe

eIDM Vision Paper

Constantijn van Oranje-Nassau, Neil Robinson,
Maarten Botterman

Prepared for the e-Government Unit of DG Information Society and Media, European Commission

RAND EUROPE

The research described in this report was prepared for the European Commission. The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

Published 2009 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

This paper is written to help look beyond the current policy developments and determine what demands and requirements there may be for a pan-European eIDM solution in 2015 and which services are likely to be developed based on this infrastructure.

The findings have been prepared through literature research and expressed in briefing papers on prevailing eID standards and models and possible use cases for pan-European eGovernment Services for Citizens (PEGS). These formed the basis of 3 scenarios, which were used in a gaming seminar with 33 experts from national governments, the European Commission, industry and academia.

The focus has been on identifying drivers and barriers and determining the value added of a European electronic Identity Management (eIDM) framework. The alternative futures presented in the scenarios, provided participants different angles to scope these issues and to identify which trends would be robust under different outlooks. Finally the experts were asked to identify policy measures that would need to be taken today to achieve the desirable outcomes of tomorrow.

For more information about this contact:

RAND Europe
Westbrook Centre,
Milton Road,
Cambridge
United Kingdom
CB4 1YG
+44(0)1223 353329

Contents

Summary

Europe in 2015 may be largely interconnected with pan-European eGovernment services (PEGS) being delivered to citizens based on a full scale common European electronic Identity Management (eIDM) system; providing seamless identification and authentication of individuals. However, it is just as likely that Europeans and their governments resists such coordination of efforts and interoperability of systems; thus opting for a very minimalist approach to eIDM; where a common identifier may support a very specific and limited set of basic applications. In between these two alternative futures we identify a scenario that is largely services driven and foreshadows a fragmented eIDM environment with different coalitions of countries and stakeholders, clustered around the utility that each service represents.

The landscape in 2015 will be largely determined by a number of factors:

- Outcomes of the large scale pilot
- Levels of identity
- Ambitions: Quality of service
- Prevalence of trust

With key drivers being: further European Integration, the implementation of the Services Directive, the stated ambitions on administrative burden reduction, and parallel private sector developments

There is no clear incentive for national public authorities for developing pan-European services for citizens, let alone a full scale European eIDM framework. However there are other developments and trends that will push or pull further cross border or even pan-European collaboration in these areas. As these do not all work in the same direction it is likely that a diversified supply of cross-border and pan-European services will emerge. Likely applications will be found in health care and in support of worker mobility. A possible third area could be education. In parallel, the exchange of ID information will increase in the field of law enforcement and specific niche applications for business sectors. The financial sector is also likely to go ahead and develop its own platform.

PEGS hold the potential to provide a new impetus to European integration and they may pre-empt the emergence of a pan-European Administrative space. The current inertia of public authorities to invest in cross border eIDM models, as well as to adjust legal legacy systems and coordinate organisational processes, still present a formidable barrier. Thus leadership is required and needs to be accompanied by effective governance of the process, with a firm hold on the principle of subsidiarity. The success of any European eIDM depends largely on trust. Trust

between Public Authorities (PAs) and trust of the citizens in administrations across the EU to defend their interests and rights and to deliver concrete benefits.

A European eIDM framework is also expected to yield economic benefits, the assumption being that businesses will use such an overarching identification system to develop new services. There is however substantial hesitation from the business community to proceed. The general attitude is characterised as 'wait and see', and for business to invest in any public eIDM system there clearly needs to be sufficient critical mass of users/consumers. To get the private sector on board earlier in the process the PAs involved would need to work with existing standards, draw in the business community to understand their needs, and to involve it in the development of the system. In particular, care should be taken not to re-invent the wheel and use or reference existing common standards.

Once effective solutions and good examples at local, national and regional level emerge political commitment to actual implementation is expected to grow. The current focus on the Large Scale Pilot is too limited to effectively develop a common eIDM system for Europe; given the various other platforms and avenues that could be explored and which are in fact being developed already. Any common solution would require strong leadership, in order to ensure a co-ordinated approach based on addressing the real needs of users, and facilitate a European application that is simple, secure, resilient, robust and effective. The most likely feasible and possibly desirable option is to aim for one common European Identifier; one number based on existing national ID numbers, without authentication at the EU level.

This raises the issue of what security level would be required for accepting non-nationals to the system. Either a common EU system is developed with accepted standards for a given set of applications or any Pan European (PE) application would most likely require the highest security level, which may still be Public Key Infrastructure (PKI) in 2015. Much also depends on trust between public authorities. Even the safest systems are worth little if the process of eID enrolment is fraught with inaccuracy and fraud. It will be difficult to achieve this high level of trust among citizens of the EU 27 (or maybe 30 by 2015). Thus accompanying measures and guarantees are required that provide assurance of fraud free enrolment. In addition serious sanctions for inaccuracies and incompetence need to be in place, as well as guarantees for liability and damages.

Citizens need to trust that their information is safe and that neither government nor unauthorised third parties have access to this data. If this cannot be guaranteed or if the perception of abuse prevails – through actual breaches or false perceptions – the system will fail because of a lack of users. It should also be envisaged that the system decouples the electronic Identity (eID) from the personal data, which would allow usage of the (non-personalised) data for socio-economic and health research purposes.

The expected lacklustre demand could be partially overcome if other actors would have access to the PE eIDM backbone to support the development of their services, thus creating a multiplier and a network effect which would increase the overall value of the system. Public spending could be applied to stimulate take up by the private sector. Also public policy can help creating more transparency. The plethora of standards, models, specifications, meta-languages and frameworks risks drowning practitioners in the total number of alternative and possibly incompatible approaches, leading to a loss of opportunity and effectively doubling the amount of work. It would be desirable to set up a PE "knowledge centre" on identity management, and "virtual

middleware" that would support the various different systems across Europe to interconnect by indicating or referencing which technical middleware would be appropriate to allow different eIDM systems to interconnect.

Acknowledgments

The authors would like to thank Stijn Hoorens and Lorenzo Valeri for their thoughtful and insightful comments on this paper.

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 people only get access to the right information and services that they are entitled to. As "identity" is rapidly becoming the central organizing principle in the information society, getting Identity Management (IDM) right is key.[1]

Ensuring the availability of an electronic Identity Management (eIDM) backbone across Europe will help to serve the citizens in their interaction with governments. 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, in particular Small to Medium Enterprises (SMEs).

To align actors in the field a powerful shared vision is needed, driven by real user needs and public interest. This vision is to inform further progress on the realisation of eIDM objectives by 2010 and beyond. It is based on discussions between September 2006 and March 2007 with industry, civil society, the European Commission and Member States of the EU. The vision presented here does not necessarily reflect the opinion of any specific stakeholder, and is fully the responsibility of the authors. A more detailed description of the methodology is provided in Appendix A.

[1] Information Assurance Advisory Council Position Paper on Identity Assurance (IdA) - Towards a Policy Framework for Electronic Identity; IAAC; Cambridge 2006; p1 available from http://www.iaac.org.uk/Default.aspx?tabid=105 (visited 18th July 2007)

CHAPTER 1

Looking ahead: possible future scenarios for pan-European eIDM development

"Only if you have to" represents a minimalist scenario for 2015. Even under this scenario more national eIDM systems and services will be emerging across Europe than are present today and also there will be some limited cross-borders applications available. Nevertheless the use of identity at the EU level will be primarily as back office vehicle for (binary) identity confirmation or denial. The inertia of public authorities is compounded by the lack of trust that prevails between public authorities and of the citizens in the EU. Physical and legal separations are carefully guarded to ensure a sense of national sovereignty. Thus further interconnection and interoperability of systems becomes highly unlikely. In areas where specific user groups do find sufficient value added in cross border or even pan-European services they may be developed by commercial suppliers outside the public sector, whereby likely candidates are healthcare and education services.

"Pick and choose" is a services and utility driven scenario. Given the current fragmented approaches, it is not unlikely that the European eIDM landscape will be a patchwork of sector driven (or thematic) initiatives, competing with each other or existing in parallel. Different groups of countries will be co-operating in different areas and at different levels of integration and interoperability. Such cooperation builds on common interests, whereby the utility of the service determines which countries participate (e.g. a service like EUCARIS[2] for tracking and retrieving stolen cars may be less interesting for Malta then for Germany and Poland). More generally, co-operation will happen where mutual trust between public authorities exists, further supported by similarities in organisational and legal structures and cultures. There may eventually be common European identifier and in certain specific areas there could also be authentication at the European level. The overall picture however, will be one of different speeds and intensity of progress, interconnection and overall fragmentation between sectors and geographies.

"Just do it" is an optimistic scenario. Though a sectoral, geographic and multi-layered patchwork is likely, a scenario with a more unified system is not impossible either. There are significant benefits for citizens, governments and commercial operators to have a more standardised system that would support a large range of eGovernment services and functions. One system would eliminate the need for multiple cards, would increase the possibility for interconnecting systems, would allow the provision of services across 'policy silos' and would have the scale and critical

[2] About EUCARIS: European Car and Driving Licence Information System http://www.eucaris.net/ (visited 18th July 2007)

mass of users to attract commercial service providers. If rolled out effectively the European eIDM standard could be world leading. This scenario depends heavily on technology and trust among participating governments and of the users in the system. To support this trust base the effective application of privacy enhancing technologies and data protection guarantees will play an important part.

There are a number of initiatives and drivers – discussed in the next chapter - that deliberately or implicitly try to counter the geographic and sectoral fragmentation, to endeavour for the establishment of one overarching pan-European eIDM framework.

CHAPTER 2

Key drivers for an interoperable pan-European eIDM framework

The benefits of one single pan-European eIDM framework are evident, even though the level of sophistication will largely depend on the policy priorities and the speed with which the system should be introduced. The least ambitious level would be the agreement on a single European identifier. There are a number of drivers of a common identifier in Europe that could counter the likely fragmentation of the European eIDM landscape.

The most direct and focused attempt to establish a common interoperable eIDM framework in Europe is the Large Scale eIDM Pilot (LSP)[3], which is under preparation in the Competitiveness and Innovation Programme (CIP - IST PSP) programme.[4] This initiative is a brave first attempt to address the lack of interoperability in Europe. The success of the Pilot, or better its ability to actually establish common standards and approaches; making national systems interoperable; and proving that such a Pan European (PE) framework may actually support real eGovernment services, will have a significant impact on the further outlook of the eIDM and Pan European eGovernment Services (PEGS) landscape in 2015.

Other attempts for a more shared approach may also lead to a different, perhaps more integrated outlook. Key drivers are likely to be:

1. the compliance requirements of EU governments under the Services Directive (SD)
2. the existence of more general ambition towards further European integration at the level of the citizen, and
3. Government transformation agendas and the pledge to reduce administrative burden in the EU by 25% by 2012.

Services Directive

An important driver is likely to be the Services Directive (SD). The SD aims at supporting a single market for services within the European Union. It is the first legal instrument that sets binding requirements for EU MS governments to develop eGovernment services by 2009, through its point-of-single-contact clause in article 8 of the Directive:

[3] A roadmap for eID for the Implementation of the eGovernment Action Plan available at: http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_table.pdf (visited 18th July 2007)

[4] Decision No 1639/2006/EC of the European Parliament and of the Council of 24 October 2006 establishing a Competitiveness and Innovation Framework Programme (2007 to 2013)

> "…ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities."

Thus, the whole process of fulfilling necessary formalities and procedures for establishing a business in another country has to be made possible by electronic means. For this a service provider would have to be identified and have its identity authenticated. For the effective applicability of the SD this would require the acceptance by the recipient public authority of the national ID of the service provider together with its supporting – nationally applicable - means of authentication. Though it is thinkable that for an intermediate time identification and authentication methods of the recipient country will be applicable this is likely to create further complications if the service provider wants to deliver temporary cross-border services from his new work location. Thus in the end a solution needs to be found where EU MS trust and apply each others eIDM systems.

The SD's legal reach is in the realm of Government to Business or G2B, and as such is not focused on enabling eGovernment service delivery to citizens. However, due to it's far reaching impact on the way public authorities will need to reorganise their 'customer' facing activities and underlying back office processes, it is likely to have spill-over effects to the area of services for citizens.

Further European integration at the level of citizens

As far as PEGS and a shared eIDM backbone can offer effective solutions to common problems they are policy instruments for further European integration. PEGS may provide a new impetus to European citizenship by allowing citizens to benefit more from the advantages of an integrated Europe.

The strength of this argument is largely dependent on the broader developments in Europe, around the European constitution and general perspectives on the role of the EU. It is also dependent on the level of trust that the pilot and more importantly, in general the participating public authorities are able to generate at the level of the EU citizen. eIDM may strengthen privacy protection, not withstanding certain public perceptions to the contrary. Trust and awareness are critical success factors, and they are also culturally determined and thus potential drivers of fragmentation and differentiation.

Countries currently lagging behind may actually make the difference in choosing one or other eIDM solution and thus generating sufficient critical mass for one common European approach, as they would be more open to European level guidance (based on best practice experience) than those countries that lead with national eIDM solutions, today. The integrationist logic and the underlying policy objectives of the open method of coordination (OMC) support such inclusiveness, as do the principles of cohesion that are fundamental to the EU.[5] Thus there is at

[5] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS; Working together, working better: A new framework for the open coordination of social protection and inclusion policies in the European Union COM (2005) 706, Brussels, 22nd December 2005 available at: http://ec.europa.eu/employment_social/social_inclusion/docs/com_2005_706_en.pdf (visited 18th July 2007)

least a strong impetus for not leaving those less advanced countries behind. How strong this influence will be and how it will finally affect a more integrated common pan-European eIDM system is still unclear.

Government transformation agendas and administrative burden reduction

People and businesses doing activities that involve administration in two or more EU countries - setting up a business, getting married, and registering a child's birth or the death of a relative - often face burdensome administrative barriers. Whereas the public authorities that manage the intake of non-nationals, face increased complexity and unexpected challenges, caused by misalignment of statuses, the lack of specific documentation and additional verification and authentication requirements. For instance: cross-border workers and mobile citizens often fall outside the prevailing national legal and social welfare systems. Thus identification, registration, monitoring and implementation require extra attention and create an additional burden for the relevant public authorities. Effective exchange of information between national administrations could potentially prevent a lot of duplication and errors. For the mobile citizen, receiving the support to which he/she is entitled proves to be very burdensome, if not impossible, today.

Moreover European policymakers have identified that administrative burden comes at a high cost and reducing the burden has thus become an objective in its own right, based on economic considerations.[6] In COM(2007) 23 final, the Action Programme for Reducing Administrative Burdens in the European Union,[7] presented on January 24 2007, a reduction target of 25 % is proposed, to be achieved jointly by the EU and Member States by 2012. This joint objective, which can only be attained on the basis of a shared responsibility and a common endeavour by the Member States and the European Institutions. Alongside the reduction target and priority areas, the Action Programme includes a list of fast track actions, which explicitly mention the effective deployment of e-services. Moreover, it is estimated that 40% of all national legislation is the direct or indirect result of European legislation,[8] thus the EU has a direct impact on the creation of administrative burden. This emphasizes that the reduction of the administrative burden is also a European issue. Besides, a reduction in one member state may affect the economies in other member states, in particular for PEGS.

How big the influence of this policy drive is for developing eID enabled PEGS is still to be seen, as the biggest incentives of national policymakers will be to achieve reductions in national administrative burden. The additional EU level may either be seen as an added layer of complexity to be treated with caution, or as a necessary issue to address in order to achieve the national objectives. It may also emerge as a common platform for European cooperation in eGovernment interoperability and a driving argument to establish a common European eIDM solution. It is expected that the success or failure of national large scale IT procurements and the political fall out of these, will also influence the 'appetite' for policy makers to engage in addressing the pan-European challenges.

[6] An assessment based on an extrapolation of Dutch data suggests that administrative costs may amount to circa 3.5% of GDP in the EU. Kox (2005): Intra-EU differences in regulation-caused administrative burden for companies. CPB Memorandum 136. CPB, The Hague.

[7] http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0023en01.pdf

[8] Review of the Dutch Administrative Burden reduction Programme, World Bank Group (2007)

Other likely factors

The finance sector is another area where many cross border eIDM initiatives are already deployed. Generally these are standards driven. There are 'back-end' finance systems like Society for Worldwide Interbank Financial Telecommunication (SWIFT) which run on a very restrictive architecture where the end-points of the network can be controlled but there are also industry led approaches based more clearly on standards, such as with the EMV Co Contactless Smart Card specification.[9] In Europe the development of a Single Euro Payment Area – SEPA - could be driving further development of European standards in payments.[10] SEPA will effectively remove all distinctions between domestic and transborder retail payments in the Euro zone and associated countries[11] by 2010. The European Central Bank is concerned that current suppliers of integrated payment solutions are American, Chinese and Japanese companies and it is urging European banks to develop their own standards. A single debit card for Europe would be a very important candidate for becoming a platform for eIDM related services. The Swedish eIDM example has shown the effectiveness of such a solution.[12]

Developments in law enforcement and policing like the European drivers licence[13] but also intensive data exchange through the Schengen Information System (and its successor SIS II and the Visa Information System), the International Civil Aviation Organisation (ICAO) 'e-passport' standard[14] are all expected to drive forward the integration and interoperability of electronic systems of government in Europe. How these will interact is uncertain; but it is likely that they will affect another.

Further important factors that will determine the actual development of PE eIDM are concerns about privacy and security, as well as the complexity of linking current national systems and the willingness to relinquish a certain level of national autonomy in this area.

[9] EMVCo 4.1 Integrated Circuit Card Specifications for Payment Systems Jun 2007 version 4.1 available at http://www.emvco.com/specifications.asp?show=3 (visited 18th July 2007)

[10] European Central Bank: Links on the Single European Payments Area (ECB 2007) avaiable at: http://www.ecb.int/paym/sepa/html/links.en.html (visited 18th July 2007)

[11] Iceland, Liechtenstein, Norway and Switzerland http://www.ecb.int/paym/sepa/html/vision.en.html

[12] Using bank cards for delivering public eID services: http://www.skatteverket.se/

[13] European Parliament Directive 2006/126/EC of the European Parliament and of the Council on driving licences 20th December 2006 available at: http://www.europarl.europa.eu/oeil/file.jsp?id=239192 (visited 18th July 2007)

[14] International Civil Aviation Organisation (ICAO) Standard for a Machine Readable Travel Documents 9303 (ICAO Montreal 2006) available at: http://mrtd.icao.int/ (visited 18th July 2007)

Summing up

Thus there are a number of critical factors determining the future outlook of eIDM and PEGS in Europe:

- Outcomes of the large scale pilot
- Levels of identity
- Ambitions: Quality of service
- Prevalence of trust

The key drivers behind these critical factors are: further European Integration, the implementation of the Services Directive, the stated ambitions on administrative burden reduction, and parallel private sector developments

CHAPTER 3 What eIDM enabled PEGS can be expected in 2015?

Different futures have different requirements. However, the cross-triangulation of outcomes of the various scenarios delivers certain robust predictions and also an analysis of eID requirements for 2015 and beyond and the likely supported services.

Today there is no clear business case for any specific PEGS for citizens. The Member States, being the main actors, currently do not have sufficient incentives to develop such services, as the demand is low and the barriers are high. Few people have real cross border needs and most of these can be dealt with in the margins of national systems and services. This negative cost-benefit ratio does not justify the effort of developing a full scale Pan European eIDM framework.

Nevertheless, borders matter less and less for the location of economic activities within the EU. ICT enables effective service delivery increasingly in a location independent way, and this development will continue over the years to come. By 2015 a number of PEGS are likely to be offered. The policy trajectories towards the emergence of such services and the development of supporting infrastructures and organisations are clearly set in motion. Many national initiatives are coming on line and attempts to integrate these within a European framework are becoming more concrete. An obvious example of the drive forward is the EC initiative to launch a large scale pilot on eIDM, but also a series of studies and projects like Modinis-IDM,[15] Privacy and Identity Management for Europe (PRIME)[16] and Future of Identity in the Information Society (FIDIS)[17] to research the feasibility of European eIDM and actual pilots in specific service areas like NETC@RDS.[18]

This drive forward is inspired and supported by a political ambition to develop a pan-European eIDM framework, which is spelled out in the Manchester Ministerial declaration and the eGovernment Action Plan. This political platform is fragmented as it does not come with clear

---

[15] MODINIS-IDM project website available at: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (visited 18th July 2007)

[16] Privacy and Identity Management for Europe project website at: https://www.prime-project.eu/ (visited 18th July 2007)

[17] Future of Identity in the Information Society (FIDIS) project website available at: http://www.fidis.net/ (visited 18th July 2007)

[18] Sušelj, M, Zuffada, R.; Netc@rds for e-EHIC - a Step Towards the Introduction of the European Health Insurance Card; eChallenges Conference and Exhibition 2005 available at: http://www.netcards-project.com/files/final%20conference/Paper_NETCARDS_FINAL_CONFERENCE.pdf (visited 18th July 2007)

mandates and leadership at the European level. This has lead to a portfolio of initiatives by the EC, the MS and also by industry. Some of which are developed in complete isolation, and which may drive or break the development of a full scale interoperable European eIDM backbone; or indeed remain as parallel infrastructures, thus foregoing clear potential for exploiting the obvious synergies and scale of a common system.

Where citizen-centric PEGS using some form of eIDM are likely to develop, this will be a bottom up process. Whatever the large scale pilot will produce there are certain services that will be pushing for PE solutions. These are particularly acute for healthcare services supporting mobility. In healthcare the European Health Insurance Card (EHIC)[19] provides a first platform - supported also by the NETC@RDS pilot - for further development of a European eHealth card containing essential health data and providing access to patient records, up and beyond its current function of "proof of insurance". The demand for cross border healthcare and the life saving potential of these and associated services are likely to drive their development.

BOX 1. Use Cases: Possible evolutionary introduction of full scale PEGS in Healthcare, driven by demand, critical mass and varying levels of complexity.

…what if there was one European market for healthcare?

First step: Pan-European eHealth provision

A elderly pensioner from Belgium who is on kidney dialysis wishes to visit his daughter who lives in Slovakia for an extended but finite period of time. He knows that due to the electronic European Health Insurance Card (eEHIC), he is able to do this without fear of not having access to the constant treatment he needs. The eEHIC allows citizens of the EU, EEA countries and Switzerland to receive medical treatment in another member state for free or at a reduced cost, if that treatment becomes necessary during their visit (for example, due to illness or an accident), or if they have a pre-existing chronic condition which requires care such as kidney dialysis.

By stipulating a common set of procedures across the MS, barriers to mobility for frontier, posted and migrant workers, tourists and visitors can be reduced – the intended impact being increased confidence to travel and increasing the competitiveness of Member States and Europe as a whole. The digitisation of this service is a natural extension of the EHIC which was introduced in 2004, but might require reconfiguration of back end processes and databases since the pan European benefits can only be achieved once seamless integration is accomplished, without manual translation of one data type on the EHIC to data types peculiar to that Member State.

Proposals from the European Standards body the Comité Européen de Normalisation (CEN) suggest that in an online version of this eEHIC a user access point would be complemented by a card status authority server which checks to see if the card has been revoked is fraudulent or might authenticate the healthcare professional.[20] Some verification of the validity of a card could

[19] European Commission: Employment Social Affairs and Equal Opportunities: Overview of European Health Insurance Card (European Commission, Brussels) available at: http://ec.europa.eu/employment_social/healthcard/situation_en.htm (visited 18th July 2007)

[20] CEN/ISSS Workshop on Interoperability of the electronic European Health

be undertaken where possible. At a simple level, the data on the card would need to be authenticated against data held in backend systems and the person presenting the token (this might be made more certain by the appropriate use of biometric data). Claims can be processed in a much speedier fashion due to the digitisation of EHIC processes.[21] This is not just about 'another card' but more importantly covers the standard representation of information, use of compatible meta information and suitable identifiers across institutions to allow backend databases to exchange information In this way the whole process of claims has been improved. By linking EHIC into eID it becomes possible to simply use a common eID to query this information rather than a token representing the system which is specific to it.

Second step: European electronic patient records

A citizen of the EU has healthcare records scattered all across Europe as she has worked in a number of different countries during her working life. Records relating to a rare disease she contracted as a child are in the country of her birth, whereas in another country there are records reflecting complications from the time she was pregnant. She might also have an allergy against penicillin, or be sensitive to certain other medication. As an emergency occurs doctors need to quickly find out her medical history to ensure that any subsequent treatments do not put her at further risk. Although she might possess some form of visual readable healthcare pendant describing some of the most essential information most data is kept in electronic patient files that include Multiple Resonance Imaging (MRI) scans, lab data, DNA profile, inoculations, prior treatments, etc. Furthermore a new set of issues are exposed when prescriptions are subsequently issued. It may be inefficient for the pharmacist to read a manually completed form and the process is open to fraud, error and duplication due to the insecurity of exchange of prescription information between doctor and pharmacist (which usually goes via the patient). The normal channels of the request of medical documentation are too slow and she cannot be repatriated in time.

In this case, identity must be absolutely authenticated and is a 'safety critical' concern. The provider of the medical history must be adequately assured that the request from the remote medical institution is for their patient and the response they subsequently provide is correct and tailored to the right individual. The use of biometric data would greatly assist in this manner, because they may be intrinsically linked to the content of the information exchange. eID could be used as a unifying catalyst for different data especially where this must be acquired from a number of disparate sources that might store their data differently or use non-standard meta information

The use of eID would allow more effective filters as the eID could be automatically anonymised to create a pseudonym which would disassociate the identity of the person from the data. This would have a significant knock-on effect in the area of medical research and large scale public

Insurance Cards (WS/eEHIC) Draft Business Plan v0.5 available at http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wseehicdraftbpv05.pdf (visited 18th July 2007)

[21] Communication from the European Commission on the European Health Insurance Card COM(2003)73 final ECOJ 27 February 2003 http://europa.eu.int/eur-lex/en/com/cnc/2003/com2003_0073en01.pdf (visited 18th July 2007)

health studies about potentially sensitive subjects.

Important trans-border issues that would need to be resolved include the standardisation of different measurements and values for prescriptions, treatment protocols and agreements on the use of equivalent licensed medicines (which may differ radically in MS). This may require the development of common specifications for medical data, treatment protocols (for example, what drug may be used when the prescribed drug is not available or is unlicensed). The real benefits and efficiencies come from rapid, seamless, and efficient access to content data (i.e. medical information) without the intervention of the patient. In that respect, the second or third level of eID would be the most beneficial, with more benefits (in terms of speed and efficiency) being seen, the more autonomously this process is conducted.

In the field of mobility there is the 'push' factor of the EU Treaty's goals to ensure the functioning of the Internal Market and free movement of people and labour. This is matched with a 'pull' factor of the increase in cross-border employment. The (latent) policy ambition to support work related mobility in the EU and the increased flows are likely to stimulate the demand for PEGS; like requesting work and resident permits on-line and even the portability of pensions and social welfare services. Having said that, the complexity of national social welfare systems is expected to be a strong barrier to their Pan European development. Alternatively a parallel European opt-in scheme could be envisaged, possibly next to national systems, to service the mobile worker/citizen. This is beyond the scope of eIDM alone and can only happen with strong political support, to overcome legal restrictions and subsidiarity concerns.

BOX 2. Use cases: Possible evolutionary introduction of PEGS related to (labour) mobility

…what if, labour and residence in Europe was supported by a pan-European eIDM system?

First step: Work permits and registration for mobile citizens

A French winegrower wants to extend his vineyards and hires a building company through searching specialist web sites where other vintners put up recommendations about companies they have found to be reputable. The building company soon begins work but while on site the foreman receives a visit from French immigration officials indicating that some of the workers are in possession of fraudulent identity documentation. They are actually foreign nationals from a third country outside the EU who have managed to acquire passports due to similarity in language and ethnic makeup. They get deported and the work stalls. The employer is held liable and is left in a state of legal uncertainty, affecting future employment of foreign EU nationals; and the vintner loses time and potential revenues.

A transparent and open labour market has beneficial effects for workers, customers and businesses in Europe. There is a large influx of skilled labour into Western Europe and the Services Directive - that is aimed at creating a single market for services within the European Union - promises to further reduce administrative and legal barriers to the delivery of services across Europe, making the need to address the links between identity and legitimacy of workers even more urgent. However it has proven to be difficult already today for "employers" to be sure of the legality of workers with origin from other European countries. Pan European eID would enable

citizens to (voluntarily) prove their legitimacy, employability and simplify the process of form filling for permits and necessary administrative activities.

European eID would allow to not only identify the status of workers, but also to link the identity to applicable labour legislation, and, when developed, the specific legal status of the individual with respect to the right to work within a country of the European Union. If a single authentic identity, certified as being 'correct' by a government agency could be used then the 'vicious cycle' that sometimes occurs (when a worker in a new country cannot obtain a work visa due to a requirement for evidence of a social security record, which in turn cannot be obtained due to a requirement for a valid work permit) can be broken. Also business would benefit from legal security and a reduction of compliance and liability costs. In particular for SMEs a service that would allow an effective and secure check, once and for all, would be beneficial in opening up jobs for workers from other EU countries. Finally, identity can be useful (and eID specifically) for citizens allowing them to do many of the administrative and workforce tasks in advance, via remotely accessible systems (perhaps over the Internet).

National registries of citizens could be queried using an authentic electronic source in the country of origin, this data could be exported to the destination country reducing data entry errors and reducing the potential for fraud. Work permits might also be linked to this data, which could, if properly implemented, help towards efficiency of the single market by allowing matches between expired and 'active' permits in each participating country (for example to see whether someone was trying to defraud the one or both Member States by claiming to work in two different countries). However, it has to be remembered that unlike social security (which is covered by the primacy of EU regulation) taxation is a bilateral agreement between two countries, so any eID system would need to be sensitive to this and capable of translating into a system design the different national agreements existing between two MS that have established such a bilateral arrangement.

<u>Second step: Work benefits</u>

A citizen of Portugal has been asked to move to set up a new branch office in Brussels. As this is a risky venture with the possibility that the office might close after a short while, he must ensure that the benefits that he has accrued under the UK system can be 'carried over' to the Belgian system and that he will not find himself in the unenviable position of not having worked long enough in the United Kingdom to be eligible for any benefits, nor having the required amount of service to be eligible to claim benefits in Belgium. Citizens when moving to work in a new country do not want to be burdened by extra worries about whether the social security scheme they have been paying into will cover them in the new country. It is important for them to have a degree of confidence that if they cannot find a job they are covered by the social security insurance scheme of their new country of residence. Equally, if they have built up a history of paying into a national insurance scheme and are posted by their employer, they do not want to loose this when they move.

In some member states, the provision of social security benefits may be on the basis of occupation and in others on the basis of residency. Entitlement may be based on amount worked or the completion of a certain number of year's residence. The provision of eID would help in making this process more efficient, by minimising the search and query time for matching eligibility and benefit history to citizens. This would help in making sure that the principle that citizens are only insured in one country at any one time is generally met. eID will be useful in ensuring that

contributor and receiver are matched. The more comprehensive data that can be contained on an eID system the better. In the instances where this data could be stored on a smart card (and backed up on the appropriate databases in the country of residence) this would enable, in effect, a 'benefits history' to be carried around by the citizen, thus speeding up the management of this information by allowing quick interrogation by the new country. Data would have to be validated by reference to another source but nevertheless this would greatly speed up the exchange of information.

The privacy and security issues for this use case revolve around measures taken to protect personal data in the electronic systems of the participating countries. As this is not a real-time application (in most instances) issues around reliability and availability of communications networks would be a lesser (but not unimportant) priority. If a token would allow a benefits history to be carried around by the citizen, then appropriate measures would need to be put in place so that this data could be modified only by authorised persons and risks of fraud be reduced.

Education may be a third area where PEGS could find sufficient PE demand and where the supporting organisational structures exist. However, the key element to cross-border educational services is the mutual recognition of courses, degrees and qualifications, which is a much larger co-ordination process (also known as the Bologna process).[22] Already many exchanges are possible without eIDM support. As qualifications also need to be transferred and demonstrated in person the 'e' aspect may not justify the development of a separate eIDM system. PEGS in educational areas are thus expected to emerge once a pan-European eIDM framework is in place.

Finally, PEGS are developing in well defined niches for specific tasks, such as the European standards for fully electronic tachographs for the transport industry.[23] In fact all PE government activities that are based on massive exchange of information, in particular those related to economic activities (the so-called "first pillar" of the EU) are likely to be subject to this development. Other applications in closed systems for relevant professional communities could be envisaged like eDoc standards[24] and centrally available land registration information for the notary profession[25]. PEGS towards businesses are likely to develop even faster than those towards citizens as direct economic gains easily justify and even urge the investments.

In the private sector, a number of cross-organisational and cross border developments are fast occurring. One of the most notable and ambitious is that of various measures which are being developed to implement Homeland Security Presidential Directive -12 (Policy for a Common

[22] Joint declaration of the European Ministers of Education The Bologna Declaration of 19 June 1999 European Higher Education Area available at: http://www.bologna-bergen2005.no/Docs/00-Main_doc/990719BOLOGNA_DECLARATION.PDF (visited 18th July 2007)

[23] E.g. see http://www.eu-digitaltachograph.org/

[24] E.g. see report of the eDoc Workshop, 18th April 2007, Brussels, Belgium (European Commission DG Information Society and Media, Brussels 9th May 2007

[25] E.g.: see http://www.kadaster.nl

Identification Standard for Federal Employees and Contractors).[26] Given the large number of federal agencies and departments affected by this policy (15 federal government departments all with numerous agencies) the deployment of eIDM on such a large, inter-organisational scale would hold many lessons for eIDM for PEGS.

[26] Bush, G.W.; Homeland Security Presidential Directive No 12 HSPD Subject: Policy for a Common Identification Standard for Federal Employees and Contractors (Washington DC August 27 2004) available at: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html (visited 18th July 2007)

CHAPTER 4

What would a pan-European eIDM framework serve?

PEGS hold the potential to provide a new impetus to European integration. They will enable the citizens of Europe to benefit from free movement of people and labour. Enabled by PEGS, people will be able to directly interact with PAs at European, national and local level, much as if they were interacting with their own home administration. This potential of delivering the benefits to the citizens and creating cross-border interaction with public authorities across Europe may also pre-empt the emergence of a pan-European Administrative space. Once it becomes easy to do PEGS transactions anywhere in Europe citizens and business are likely to find good use for it.

It requires leadership of the process towards the full scale roll out of PEGS for this to actually materialize. The current inertia of public authorities to invest in cross border and even Pan-European eIDM models, as well as to adjust legal legacy systems and coordinate organisational processes, still present a formidable barrier. Furthermore the business community is not eager to take the initiative or to support public approaches as long as the cost saving or revenue potential is not clear, and standards as well as concrete applications are not yet visible on the horizon.

Leadership needs to be accompanied by effective governance of the process, with a firm hold on the principle of subsidiarity. The emergence of a European Administrative space is seen as against that principle by some, and much welcomed by others. The 'services driven' integration of the EU must not take the citizen and uninformed public authorities (PAs) by stealth. Even processes delivering potentially beneficial outcomes may backfire if they are not supported by effective governance guarantees and in full transparency. As indicated before, the success of any European eIDM depends largely on trust. Trust between PAs and trust of the citizens in administrations across the EU to defend their interests and rights, and to deliver concrete benefits, will also depend on the prevailing perceptions of the underlying policy processes.

A European eIDM framework is also expected to yield economic benefits; the assumption being that businesses will use such an overarching identification system to develop new services. Even a more fragmented landscape of different eIDM systems would probably enable or generate the development of sector specific services in areas of health care, tourism, employment services and possibly education. There is however substantial hesitation from the business community to proceed forward. The general attitude is characterised as 'wait and see'. If the public eIDM system proves to be effective and if the business opportunities from either cost saving or new revenue streams are apparent the private sector is likely to take a further, closer interest. For this to happen there clearly needs to be sufficient critical mass of users/consumers.

To get the private sector on board earlier in the process the PAs involved would need to work with existing standards, draw in the business community to understand their needs, and to involve it in the development of the system. Interactions of citizens with their governments are relatively limited in frequency and time. The great benefit of an active contribution and take up of the private sector rests in the increased utility of the PE eID for its customers, as private application would increase the frequency of use and the perceived benefits of a much wider supply of customer centric services. Obviously this would also increase the complexity of the system and may therefore push for a simple but resilient, secure and robust solution focused on identification only. A more fragmented approach would allow more sophisticated applications and vice versa: i.e. if the PEGS environment would be 'services and sector dependent', with underlying parallel eIDM systems, the advantage of scale and flexibility may be lost to the benefit of a more targeted and sophisticated approach.

In order to stimulate investment from the private sector, expected market size is an important element. When governments commit to specific standards and models (through standardisation bodies, or even through procurement) investment in those will be considered more attractive. Standards and models that should be taken into account to entice business involvement and to ensure more general applicability and thus greater opportunity for network effects to occur. In particular, care should be taken not to re-invent the wheel and use or reference existing common standards particularly those at mature stages of development promoted by the International Standards Organisation (ISO) and various regional standards groups. Where possible and appropriate, it would also be important to use other technologies or approaches that are emerging as de-facto standards. Examples include the Liberty Alliance standard for federated IDM architecture[27] and the SAML (Security Assertion Markup Language),[28] which seem to be the de facto choice for many national and organisational eIDM implementations.

In the private sector, a number of cross-organisational and cross border developments exist already today, and new developments can be expected. Also outside the EU interesting developments are taking place.[29] One of the most notable and ambitious is that of various measures which are being developed to implement HSPD-12 (Policy for a Common Identification Standard for Federal Employees and contractors).[30]

[27] Liberty Alliance Identity Federation Framework Specifications suite (Liberty Alliance Project) 25th March 2007 available at: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_complete_specifications_zip_package_25_march_2007 (visited 18th July 2007)

[28] Organisation for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee: Security Assertion Mark-up Language (SAML) version 2.0 (15th March 2005) available at: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security (visited 18th July 2007)

[29] For example see the vendor-led GlobalPlatform Standard for Smart Card Infrastructure Oveview available at: http://www.globalplatform.org/pdf/GP_Overview_June2004.pdf (visited 18th July 2007)

[30] Federal Information Processing Standard 201 Implementation Workshop on Personal Identity Verification (PIV) of Federal Employees and Contractors (National Institute of Standards and Technology, Washington DC 27-28 June 2005) available at: http://csrc.nist.gov/piv-program/workshop-Jun272005/index.html (visited 18th July 2007)

CHAPTER 5 Demands on the quality of the system

In order for a system to become acceptable and useful, there needs to be a broad opinion of its added value, and there needs to be sufficient trust and confidence. The first requires user involvement in the formulation requirements and development of services, the latter requires that there is a sufficient level of security and assurance that the systems will be available and protected against non-intended usage, in particular use that may compromise privacy or leave the information open to theft (i.e. "reliability").

Obtaining a degree of assurance of these elements means that they should be taken into account from the design phase onwards.[31] This complicates building the system, as users across the EU have different values and different levels of trust towards government services, yet building in an acceptable minimum level will be a precondition for its use. In order to convene specific requirements of citizens in some Member States, it seems to be unavoidable to build in different levels of reliability. However, in order to keep the system useable, it will be important to ensure that the number of levels is kept down to the lowest possible minimum.

In practical terms, the involvement of European Data Protection Supervisor (EDPS) and the European Network Information Security Agency (ENISA) in the development of the Large Scale Pilot (LSP) is a step forward that is the beginning of making this a reality. However, it is not enough: certain actions on harmonisation of national legislation will be unavoidable. Again, the LSP will encounter this in developing its services, and it is likely that valuable practical experience will emerge. Obviously, the level of sophistication of the system will go hand in hand with the preparedness to invest in this PE development.

[31] Flechai, I., Sasse, A.M., Hailes, S.M. V. Bringing security home: a process for developing secure and usable systems; Proceedings of the 2003 workshop on New security paradigms; ACM Press; Ascona, Switzerland; 2003 pp 49-57

CHAPTER 6 What actions would be required today to benefit developments in 2015?

Inertia at the level of PAs in Europe, but also of the private sector remains an important barrier to PEGS and PE eIDM development. Why commit funds and political (electoral) capital for services and systems that serve only limited constituents of citizens with some kind of cross-border profile or need?

For a real breakthrough there needs to be a political commitment beyond the pure utility of eIDM and PEGS for the citizens. The LSP sets the framework for such commitment, in a way that it brings stakeholders together and is expected to reduce barriers. It will need to define what services it will choose to test. Also it will explore what standards and models are available and which would be the most suitable to apply in view the provision of PEGS. Once effective solutions emerge political commitment to actual implementation is expected to grow. The same can be expected from other good examples at local, national and regional level, which may also remove barriers and increase the willingness of PAs to act.

Though it can be seen as a laudable first step, the current focus on the LSP is too limited given the various other platforms and avenues that could be explored and which are in fact being developed already. To avoid fragmentation, but also to ensure that the LSP process does not get overtaken by the developments triggered through legal obligations under the SD or those in specific sectors like health care, drivers licence, and also in the financial services and mobile telecom sectors, effective leadership is required. Such leadership should ensure a co-ordinated approach based on addressing the real needs of users, and facilitate a European application that is simple, secure, resilient, robust and effective. During the discussions with experts and stakeholders the dominant opinion was, given the urgency and the ongoing fragmentation, that the only feasible and possibly desirable option is to aim for one common European Identifier; one number based on existing national ID numbers, without authentication at the EU level.

This raises the issue of what security level would be required for accepting non-nationals to the system. Different countries have different security approaches. Some are based on Public Key Infrastructure (PKI) (e.g. Belgium) and others have a layered model that applies lighter security measures for less sensitive services (e.g. Germany, Netherlands). Either a common EU system is developed with accepted standards for a given set of applications or any PE application would most likely require the highest security level, which may still be PKI in 2015.

Much also depends on trust between PAs. Even the safest systems are worth little if the process of eID enrolment is fraught with inaccuracy and fraud. As this determines the quality of the data in the identification databases, the question remains whether the recipient country trusts the

practices of the state that has issued the eID.[32] Such trust depends – among others - on experience, cultural proximity, common understanding of norms and practices and the interoperability of technologies. It will be difficult to achieve this high level of trust among citizens of the EU 27 (and in 2015 possibly 30). Thus accompanying measures and guarantees are required that provide appropriate regress of assurance of fraud free enrolment and / or serious sanctions for inaccuracies and incompetence not to mention guarantees for liability and damages.

There is another important success factor that hinges on trust. Citizens need to trust that their information if safe and that neither government nor unauthorised third parties have access to this data. If this cannot be guaranteed or if the perception of abuse prevails – through actual breaches or false perceptions – the system will fail because of a lack of users.[33] This can be avoided by making the system mandatory. However, its forced introduction without public support will risk significant political backlash, endangering the whole endeavour. Thus alongside secure access, privacy needs to be build in from the start with the sensible use of PET/PEMs and its benefits and guarantees need to be communicated convincingly. User consent and clearly defined access rights are important elements. It should also be envisaged that the system decouples the eID from the personal data, which would allow usage of the (non-personalised) data for socio-economic and health research purposes.

It is assumed that the current demand for PEGS is limited[34], as the numbers of cross border active citizens seeking interactions or transactions with EU wide public authorities are low and their interactions infrequent. Other obstacles, as the requirement of face-to-face interactions with government and remaining administrative formalities would further limit the benefits of a PE eIDM to the citizen. To give policy makers a better grasp on what the true demand is and what perceptions prevail among European citizens towards eIDM, some form of data gathering exercise should be conducted. In the evaluation it needs to be explicitly considered that citizens will be better able to give an opinion on the impact of eIDM on existing services, than on the potential benefits of new services that never existed before.

In addition, the lacklustre demand could be partially overcome if other actors would have access to the PE eIDM backbone to support the development of their services, thus creating a multiplier and a network effect which would increase the overall value of the system. Therefore involvement of the private sector is expected to be a crucial factor, as it would increase the utility of the PE eIDM solution to substantially bigger groups of users by providing many more and diverse citizen or consumer centric services. However the private sector will only start considering the use of a public eIDM system if there is a sufficient critical mass of (potential) users as was elaborated before. The inherent chicken and egg problem could be overcome, if public spending could be applied to stimulate take up by the private sector.

---

[32] Jøsang, A., et al; Trust Requirements in Identity Management; Proceedings of the 2005 Australasian workshop on Grid computing and e-research - Volume 44 (2005) Australian Computer Society Inc pp 99-109

[33] Cyber Trust and Crime Prevention Project: Foresight Directorate, Office of Science and Technology; London; 2005 available at http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/Executive_Summary/Executive_Summary.html (visited 18th July 2007)

[34] Weehuizen, van Oranje: Pan-European eGovernment Services (PEGS) in perspective: function, forms, actors, areas, pathways and indicators. (2007)

Business involvement is also likely to be enhanced if existing and tested standards and models are applied. The level of trust in these are higher that in new public developments. One of the best examples of this is the EMV Integrated Circuit Card Specifications for Payment Systems a popular standard for credit/debit 'smart' cards.[35] Trust in the deployment of this system has been gained in no small part by long running public awareness campaigns and exhortations from banking groups[36] (such as the Association of Payment Clearing Services in the UK) as well as the commercial parties involved themselves. In addition market compulsion and a 'liability shift' helped to 'encourage' take up. Additionally, other national schemes are taking advantage of existing credit/debit card specifications (not necessarily the EMV specification) and building compatibility into national eID systems. The Malaysian MyKAD national eID card is perhaps one of the clearest examples of this which can run a number of applications such as eCash, transportation and credit and debit card facilities.

Additionally, many national eIDM schemes such as those in Estonia and Finland are clear in trying to justify the benefit to citizens by referencing the utility of using such schemes with private sector initiatives, financial services being the prime example across many national eIDM implementations across the globe. In Sweden electronic IDs are issued by the Swedish Post and mayor banks; using a commercial system for public use.

The plethora of standards, models, specifications, meta-languages and frameworks risks drowning practitioners in the total number of alternative and possibly incompatible approaches, leading to a loss of opportunity and effectively doubling the amount of work. To make sense of all these it should be considered to develop a clearing house or centre of excellence to communicate interoperability, interconnection and compatibility of the different standards and models, to provide an effective implementation oriented assessment of their applicability. One step further would be to set up a PE "knowledge centre" on identity management, and "virtual middleware" that would support the various different systems across Europe to interconnect by indicating or referencing which technical middleware would be appropriate to allow different eIDM systems to interconnect. ENISA, or an organisation like ENISA specific for PEGS could be such a centre of excellence. The "middleware" provider could be any (commercial?) trusted party.

[35] EMV 4.1 Integrated Circuit Card Specifications for Payment Systems Jun 2007 version 4.1 available at http://www.emvco.com/specifications.asp?show=3 (visited 18th July 2007)

[36] Outlaw News: "Chip and PIN hits credit card fraud, says APACS" Outlaw.com 7th March 2006 available at http://www.out-law.com/page-6705 (visited 18th July 2007)

CHAPTER 7 Conclusions and recommendations

General conclusions

Currently no real PEGS for citizens exist yet and no 'killer application' is expected for G2C services, though there is general agreement that some pan-European eIDM is desirable and expected in 2015. To breakthrough the current inertia leadership on the part of Member States and a better understanding of the key issues is required. We have argued that there are other incentives that may breakdown the current inertia. In addition to stated political commitments, the Services Directive puts a legal obligation to the MS to develop eGovernment services. The SD is obviously not focused on the citizen but on service providers; nevertheless the challenge that is raised for local PAs is likely to have a spill over-effect of services for citizens once the systems are in place. Burden reduction is also gaining momentum as a horizontal argument to support government reform and the introduction of eGovernment services at all levels.

Any public eIDM system would benefit tremendously from active private sector involvement. If commercial services would be provided based on the public pan-European eIDM backbone this would significantly increase the utility and therefore the value of such a system. Public services alone are not likely to create the demand pull required to develop the system. At the same time business is not likely to get involved if there is insufficient critical mass of users. Public authorities must be aware of the risk of a vicious circle which could lead to paralysis and parallel developments. To engage the private sector current developments must be actively taken into account and available standards should be applied where possible. Close engagement of key commercial stakeholders may enable a virtuous circle of increased use – more services - more users – more support – more political and economic benefit.

As a general condition for any scenario and any future eIDM system in Europe trust is an important precondition. Security and privacy enhancing technologies, and effective data protection rules are essential and need to be integrated in the system from the start.

Recommendations

- The European Commission should:
    1. Plan and commission a large scale, statistically valid, **survey of attitudes** of European citizens and consumers to pan European eID and the likely PEGS that this system would support. As this concerns future services and the demand may be latent as well as explicit, we recommend using stated preference modelling techniques to fully grasp the potential demand for such services.
    2. Conduct a **scoping exercise** to identify how other common systems like the Euro have dealt with divergent participating standards
    3. Include eID usage for PEGS in **the IDABC eGovernment Fact sheets** (http://ec.europa.eu/idabc/en/chapter/203) and start including PEGS in eEurope benchmarking exercise to follow up on the political ambitions that have been clearly stated in the Manchester Ministerial declaration, but so far have not been followed up.
    4. Execute a **mapping exercise of the different frameworks** of user identity information and determine their use within the PE public context; or at least coordinate and centralise the various ongoing national and European mapping initiatives.

- The Large Scale Pilot should be designed to:
    1. **take into account as many different models**, specifications, meta-languages and frameworks as possible
    2. focuses 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**
    3. Research the possibilities of supporting business development and active private sector involvement through **measures to increase user demand**;

- Member States and the European Commission, should:
    1. Allocate, after the completion of the LSP, some investment or grants to **stimulate take up by the commercial sector** and assess the impact of such measures under current state aid rules.
    2. Undertake a feasibility study to identify what would be the most appropriate vehicle to act as an **eIDM clearing house** or virtual middleware repository

Glossary

EDPS – European Data Protection Supervisor

eIDM - electronic Identity Management

ENISA – European Network Information Security Agency

G2B – Government to Business services

G2C – Government to Citizen services

ICAO – International Civil Aviation Organisation

ISO – International Standards Organisation

LSP – Large Scale Pilot

OMC – Open Method of Co-ordination

PA – Public Administration

PE – Pan European

PEGS – Pan European eGovernment Services

PEM – Privacy Enhancing Measure

PET – Privacy Enhancing Technology

PKI – Public Key Infrastructure

SAML – Security Assertion Markup Language

SEPA – Single Euro Payment Area

SD – Services Directive

SIS – Schengen Information System

SME – Small to Medium Enterprise

UCE – Unsolicited Commercial Email

VIS – Visa Information System

REFERENCES

Reference List

Bush, G.W.; Homeland Security Presidential Directive No 12 HSPD Subject: Policy for a Common Identification Standard for Federal Employees and Contractors (Washington DC August 27 2004) available at: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html (visited 18th July 2007)

Cap Gemini: Study on Stakeholder Requirements for pan-European eGovernment Services (final report, ranking and description of PEGS, 2005)

CEN/ISSS Workshop on Interoperability of the electronic European Health Insurance Cards (WS/eEHIC) Draft Business Plan v0.5 available at http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wseehicdraftbpv05.pdf (visited 18th July 2007)

Djordjevic I. and Dimitrakos T., A note on the Anatomy of Federation BT Technology Journal on Identity Management Vol. 23 No 4 October 2005 Identity Management (BT Research, Ipswich) Springer 2005

EMV Co. EMV 4.1 Integrated Circuit Card Specifications for Payment Systems Jun 2007 version 4.1 available at http://www.emvco.com/specifications.asp?show=3 (visited 18th July 2007)

European Commission History of the European Health Insurance Card Project available at http://ec.europa.eu/employment_social/healthcard/coinexpert_en.htm (visited 18th July 2007)

European Commission: The Community provisions on social security - Your rights when moving within the European Union: Update 2004 available at: http://ec.europa.eu/employment_social/publications/2005/ke6404022_en.pdf (visited 18th July 2007)

European Commission; COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS; Working together, working better: A new framework for the open coordination of social protection and inclusion policies in the European Union COM (2005) 706, Brussels, 22nd December 2005 available at: http://ec.europa.eu/employment_social/social_inclusion/docs/com_2005_706_en.pdf (visited 18th July 2007)

European Commission; Communication from the European Commission on the European Health Insurance Card COM(2003)73 final ECOJ 27 February 2003 europa.eu.int/eur-lex/en/com/cnc/2003/com2003_0073en01.pdf

European Council; COUNCIL REGULATION (EC) No 1408/71 of 14 June 1971 on the application of social security schemes to employed persons, to self-employed persons and to members of their families moving within the Community available at: http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1971/R/01971R1408-20060428-en.pdf (visited 18th July 2007)

European Council; COUNCIL REGULATION (EEC) No 574/72 of 21 March 1972 laying down the procedure for implementing Regulation (EEC) No 1408/71 on the application of social security schemes to employed persons, to self employed persons, to self-employed persons and to their families moving within the Community available at: http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1972/R/01972R0574-20060228-en.pdf (visited 18th July 2007)

European Parliament: European Parliament Directive 2006/126/EC of the European Parliament and of the Council on driving licences 20th December 2006 available at: http://www.europarl.europa.eu/oeil/file.jsp?id=239192 (visited 18th July 2007)

European Parliament; Decision No 1639/2006/EC of the European Parliament and of the Council of 24 October 2006 establishing a Competitiveness and Innovation Framework Programme (2007 to 2013)

Financial Crimes Enforcement network (FINCEN) Aspects of Financial Transactions indicative of terrorist funding SAR Bulletin January 2002 available at http://www.fincen.gov/sarbul0201-f.pdf (visited 18th July 2007)

Flechai, I., Sasse, A.M., Hailes, S.M. V. Bringing security home: a process for developing secure and usable systems; Proceedings of the 2003 workshop on New security paradigms; ACM Press; Ascona, Switzerland; 2003 pp 49-57

Information Assurance Advisory Council Position Paper on Identity Assurance (IdA) - Towards a Policy Framework for Electronic Identity; IAAC; Cambridge 2006; p1 available from http://www.iaac.org.uk/Default.aspx?tabid=105 (visited 18th July 2007)

International Civil Aviation Organisation (ICAO) Standard for a Machine Readable Travel Documents 9303 (ICAO Montreal 2006) available at: http://mrtd.icao.int/ (visited 18th July 2007)

Joint declaration of the European Ministers of Education The Bologna Declaration of 19 June 1999 European Higher Education Area available at: http://www.bologna-bergen2005.no/Docs/00-Main_doc/990719BOLOGNA_DECLARATION.PDF (visited 18th July 2007)

Jøsang, A., et al; Trust Requirements in Identity Management; Proceedings of the 2005 Australasian workshop on Grid computing and e-research - Volume 44 (2005) Australian Computer Society Inc pp 99 – 109

Kox (2005): Intra-EU differences in regulation-caused administrative burden for companies. CPB Memorandum 136. CPB, The Hague.

Liberty Alliance: Liberty Alliance Identity Federation Framework Specifications suite (Liberty Alliance Project) 25th March 2007 available at: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_complete_specifications_zip_package_25_march_2007 (visited 18th July 2007)

MODINIS-IDM; A roadmap for eID for the Implementation of the eGovernment Action Plan available at:

http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_table.pdf (visited 18th July 2007)

Office of Science and Technology, HM Government; Cyber Trust and Crime Prevention Project: Foresight Directorate, Office of Science and Technology; London; 2005 available at http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/Executive_Summary/Executive_Summary.html (visited 18th July 2007)

Organisation for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee: Security Assertion Mark-up Language (SAML) version 2.0 (15th March 2005) available at: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security (visited 18th July 2007)

Sušelj, M, Zuffada, R.; Netc@rds for e-EHIC - a Step Towards the Introduction of the European Health Insurance Card; eChallenges Conference and Exhibition 2005 available at: http://www.netcards-project.com/files/final%20conference/Paper_NETCARDS_FINAL_CONFERENCE.pdf (visited 18th July 2007)

Weehuizen, van Oranje: Pan-European eGovernment Services (PEGS) in perspective: function, forms, actors, areas, pathways and indicators. (2007)

World Bank Group Review of the Dutch Administrative Burden reduction Programme, (2007)

Appendix A: Workshop: Setup, scenarios, participants

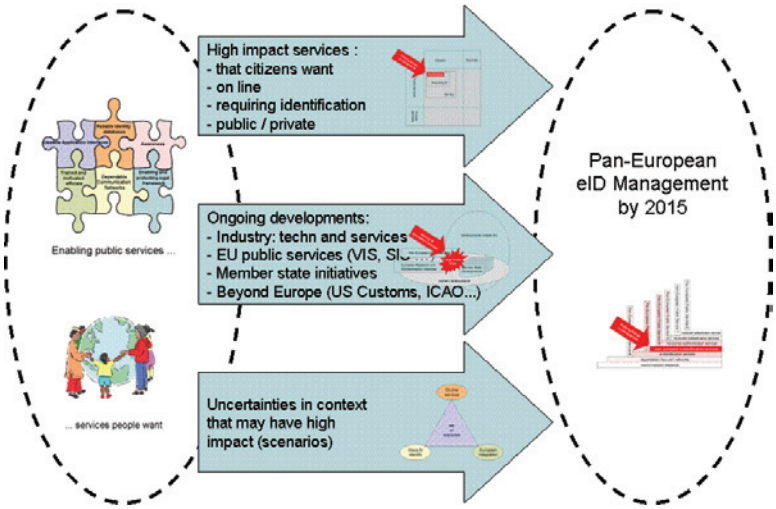
Set-up of the workshop

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



Presenting the scenarios

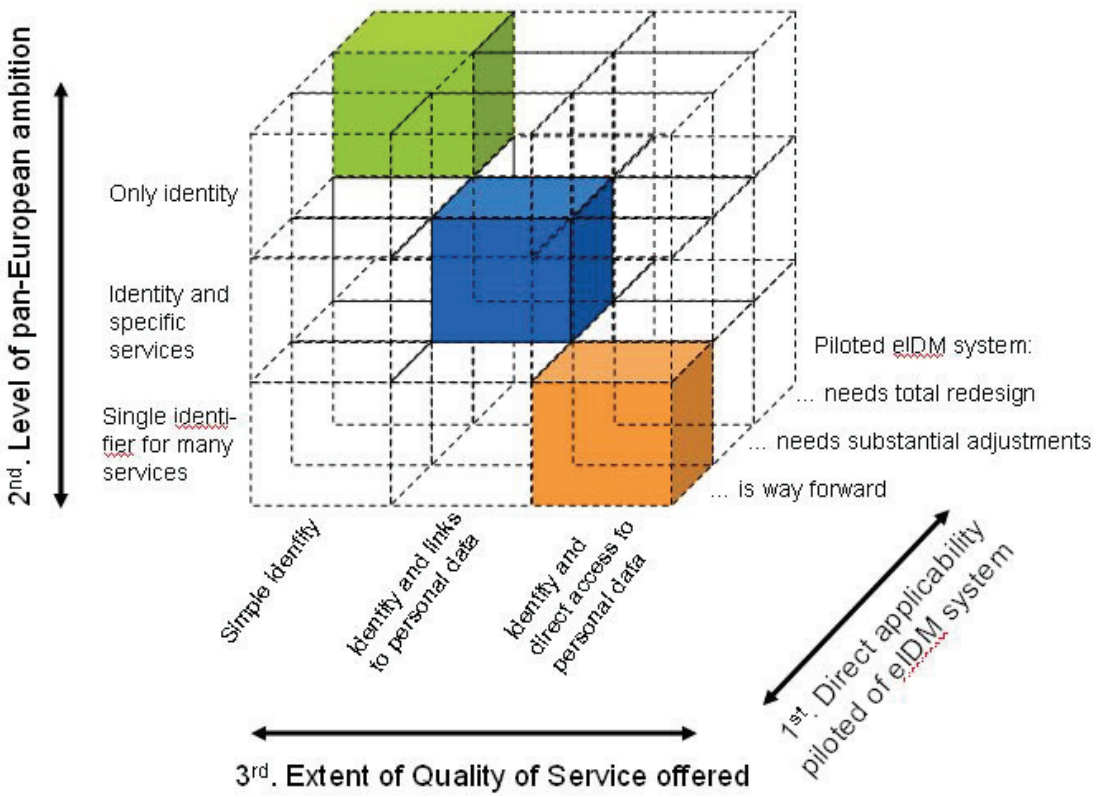
In order to explore future options from several perspective, three scenarios were presented by Maarten Botterman as starting point for the discussion in three subgroups of the participants to the meeting. In preparation of the scenarios we assumed that the current policy initiatives, as announced by 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.

The 3 scenario's

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.

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.

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.

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.

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)
- Hendrik Tamm (Project RISER)
- Lorenzo Gaston (Gemalto / CEN)

Participants

The workshop comprised of 39 participants (full list below), of which there were:

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

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