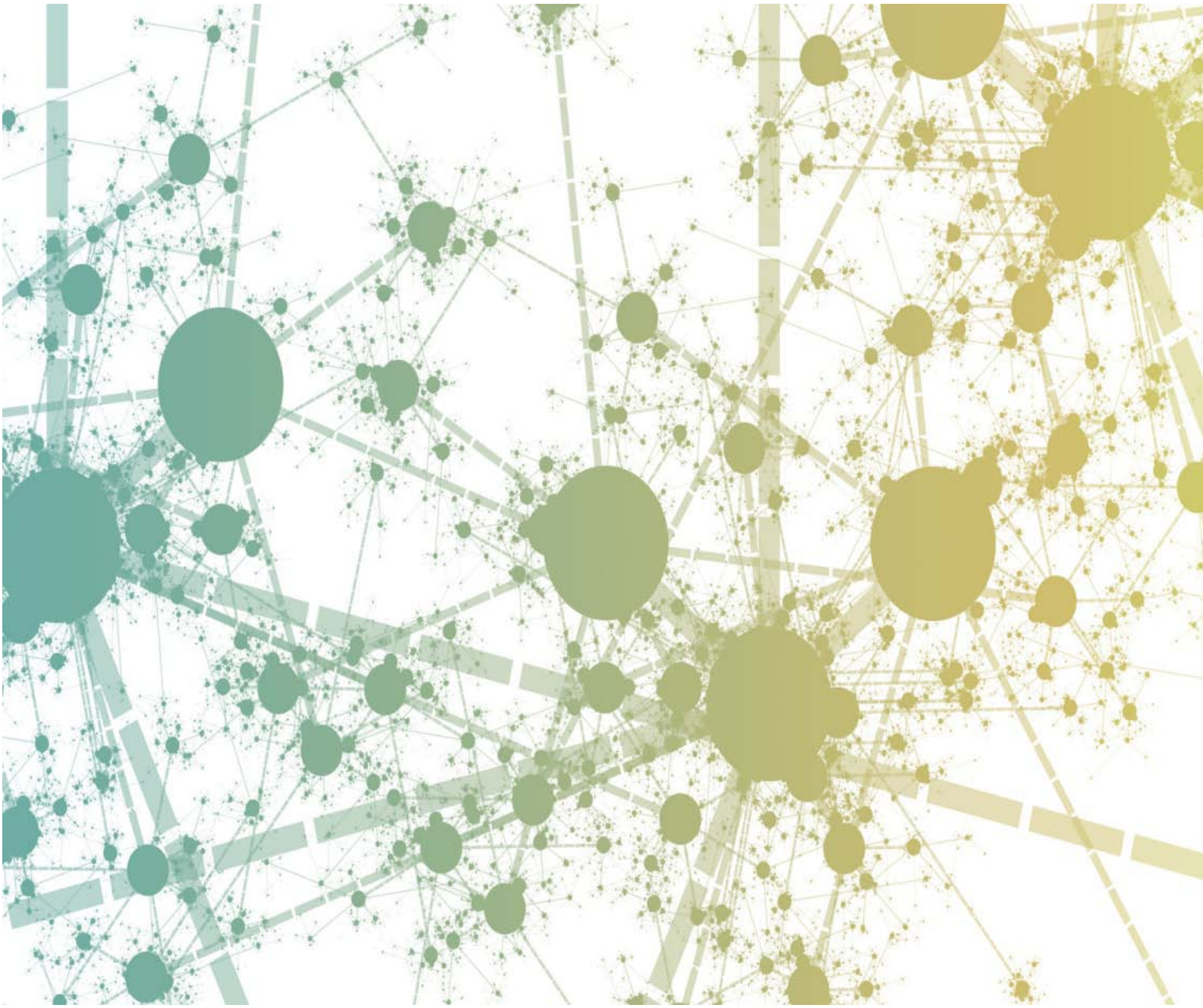
DIGITAL IDENTITY MANAGEMENT

Enabling Innovation and Trust in the Internet Economy



OECD

2011

DIGITAL IDENTITY MANAGEMENT

Enabling Innovation and Trust in the Internet Economy

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

Foreword

When the OECD Working Party on Information Security and Privacy (WPISP) initially explored the issue of digital identity in 2007, it brought together experts from government, industry, academia and civil society organisations across the OECD in a workshop in Trondheim, Norway. In the concluding session, the Chair of the workshop highlighted that the discussions revealed the confusion still surrounding digital identity management on basic questions such as "what are we talking about?" and "why are we talking about?" The discussions also highlighted the need for further analysis and research, for common understanding, and to identify policy directions.

This report on "Digital Identity Management of Natural Persons: Enabling Innovation and Trust in the Internet Economy" represents the culmination of four years of analytical work by the OECD between 2007 and 2011 to reduce this confusion and achieve a shared understanding among OECD government policymakers about digital identity management and its role in the Internet economy. After explaining what digital identity management is and why it is fundamental for the further development of the Internet Economy, it provides guidance to government policy makers for developing digital identity management strategies that support innovation across the public and private sectors while enhancing security, privacy and trust online.

The three annexes reflect the progress of the work since 2007 and provide more detailed information. The comparative analysis of "National Strategies and Policies for Digital Identity Management in OECD Countries" (Annex 1), developed in 2010-2011, provides a snapshot of the intense activity of governments in 18 OECD member countries to shape and implement public policies for digital identity. This analysis helped characterise digital identity management as a fundamental enabler for innovation in the Internet Economy and provided the essential knowledge base for the development of the policy guidance reflected in the main section.

The "Primer for Policymakers" on "The Role of Digital Identity Management in the Internet Economy" (Annex 2) was developed in 2008-2009 as a first attempt to clarify the main concepts related to digital identity and to cover simple questions such as what is the importance of digital

identity management, what are some illustrations of its usage and what are the main policy considerations. The discussions in the WPISP to address these fundamental questions revealed that much of the complexity surrounding digital identity management was generally related to the variety of facets of the subject matter (technical, organisational, legal, economic, policy), to the differences of perceptions between experts with different cultures and perspectives, and to an overarching confusion with respect to terminology.

Finally, the "Report of the OECD Workshop on Digital Identity Management" (Annex 3) summarises the discussions that took place at the very beginning of this process in the above-mentioned workshop which brought together various experts to explore the main policy issues surrounding digital identity management.

These reports have been developed by the OECD Working Party on Information Security and Privacy (WPISP) and declassified by its parent body, the Committee for Information, Computer and Communications Policy (ICCP) between 2007 and 2011. They benefited from input by member countries and by the Business and Industry Advisory Committee (BIAC), Civil Society Internet Society Advisory Council (CSISAC) and Internet Technical Advisory Committee (ITAC). They built on the expertise of the WPISP in the area of electronic authentication since 1998 and, more generally, on its work on security of information systems and networks and privacy protection.

Table of contents

Digital identity management for natural persons: Enabling innovation and trust in the Internet economy

Guidance for government policy makers

This report builds on the findings of the 2011 comparative analysis of national strategies for digital identity management in OECD countries. It represents the culmination of several years of work on digital identity management by the OECD Working Party on Information Security and Privacy (WPISP). It was prepared by the Secretariat (Laurent Bernat of the Directorate for Science, Technology and Industry) with Nick Mansfield, consultant to the OECD.

The report, which had the benefit of input from the OECD Network on E-Government, was declassified by the OECD Committee for Information, Computer and Communications Policy (ICCP) in October 2011.

Digital identity management is fundamental for the further development of the Internet Economy. This document makes a case and offers guidance to policy makers for developing strategies for the management of digital identity of natural persons. It is the culmination of four years of analytical work by the OECD Working Party on Information Security and Privacy (WPISP) on a major policy issue at the intersection of its activities on security of information systems and networks and on privacy protection. The guidance builds on the OECD Council Recommendation on Electronic Authentication[1] and responds to the Seoul Ministerial Declaration on the Future of the Internet Economy.[2] It is consistent with the 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security and the 1980 OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data.

The document explains why digital identity management is fundamental for the further development of the Internet economy. It highlights the need to address limitations in current approaches related to the complexity of credential management and the robustness required for high value services. It provides guidance to government policy makers for setting efficient framework conditions for innovation across the public and private sectors while enhancing security, privacy and trust in the Internet Economy.

Digital identity management can be approached from many perspectives. While recognising the importance, for example, of technology and of business process reengineering for successfully implementing digital identity management, this document focuses on the high level public policy concepts, reflecting the view that economic and social objectives should determine technical implementation rather than the reverse.

Identity management can be applied to human beings, business entities, devices or software applications. This guidance focuses on natural persons ("individuals") interacting with the information systems of public and private organisations ("service providers"[3]) through a digital network such as the Internet.

The first section introduces digital identity management from a public policy perspective as an enabler for innovation and trust in the Internet economy. The second section includes policy guidance for the development of national strategies for digital identity management.

I. Digital identity management is at the core of the Internet economy

Back in the mid 1990s, in the early days of the World Wide Web, the capacity for anybody connected to the Internet to access information, simply by clicking on hyperlinks, was revolutionary. However, within the span of a few years, another revolution took place: the possibility for individuals to establish interactions with remote computer systems which were able to take into account who they are in order to deliver information and services in a personalised manner.

This evolution of the Web from a publishing medium to an interactive platform for the delivery of personal services enabled electronic commerce, electronic government, and many other rich and diverse online interactions, from electronic health and electronic learning to social networks and the broader participative web. The possibility for individuals to establish a personalised interaction with, and to be recognised by, a remote computer system has been a major step. It has ushered in a decade of innovation, enabling Internet services to become pervasive, ubiquitous and increasingly essential in everyday life. It has transformed our economies and societies, serving as a building block for the Internet economy.[4]

How does digital identity management work?

The management of digital identity enables trusted remote interactions between an organisation and an individual.[5] Managing the digital identity lifecycle generally involves several processes[6]:

1. In order to be known by the system, the individual must first register with it and the conditions related to his/her identity or identity attributes must be checked so he/she can be provided with a set of credentials; this is the so-called *registration* or *enrolment* process.
2. Appropriate permissions and privileges to access the organisation's resources must be assigned to the individual, a process often called *authorization*.
3. To access resources, the individual makes an identity claim that can be verified: he/she logs into the system with the credentials provided during the registration process. This *authentication* process[7] establishes confidence in the user's identity.
4. The result of the authentication process is used in a process called *access control*, whereby the system checks that the individual has the appropriate authorisation to access the resource.
5. When the individual is not associated anymore with the system, a *revocation* process must take place whereby his/her credentials are rescinded.

Why is digital identity management essential for economic and social digital interactions?

These processes already exist in the physical world, but in many instances, we do not pay attention to their existence: for example, when we want to open a bank account and are asked to show credentials to prove our identity; when we use our employee badge to enter the premises of our employer's facilities; when we show an identity document to vote at national elections; or when we want to buy alcohol and have to prove our age. Identity management in the physical world helps address risks associated with human interactions and increases confidence between the parties interacting. It is therefore fundamental for economic and social life. The same is true online, where the lack of a demonstrable link between a physical person and a digital identity can create additional uncertainties that do not exist offline.

What is at stake from a public policy point of view is the development of effective and efficient digital identity management strategies to fully realise the economic and social potential of the Internet by migrating economic and social interactions online and unleashing innovation to create trust-based digital services.

What are the benefits of digital identity management to users?

Digital identity management is essential to the security of the organisation that grants access to resources in its information system. It is also essential to the security of the individual who accesses these resources, particularly when they belong or relate to him/her (*e.g.* money in a bank, or personal data such as a medical record). By offering security and privacy, digital identity management enables the establishment of a trusted relationship between remote parties.

Digital identity management does not offer a binary choice between full assurance or no assurance regarding the parties to an interaction. It offers a range of levels of assurance, as appropriate (*e.g.* low, medium or high). The rationale for selecting the level of assurance primarily includes its alignment with the level of risk carried by the interactions between the parties. If the level of assurance is lower than the level of risk, the parties are likely not to interact (*e.g.* a low level of assurance will not enable to secure a high value transaction). Reversely, asking individuals to provide too high a level of assurance might deter them from carrying out medium or low risk interactions, which do not seem to demand it. Indeed, in the physical world, we are used to being asked to prove our identity or to exhibit identity attributes when it is justified by the level of risk involved in a given interaction. Ensuring proportionality is even more important online because of the capacity of information systems to store identity information and transaction records indefinitely.[8]

Furthermore, in some cases, the delivery of services online enables a higher degree of privacy protection than what is possible offline. For example, it is difficult in the physical world to validate identity attributes like age or marital status without identifying an individual or to establish legally binding trusted offline interactions based on the use of pseudonyms. Such privacy protective mechanisms are however possible online.

Ensuring the highest level of privacy protection that technology enables, consistent with the appropriate level of assurance, is critical to further developing the market for online services, and in particular medium and high value ones.

What are the policy challenges?

While digital identity management has provided the access ramp to the online migration of offline services and to the creation of new digital services, there remains room for progress.

- First, many current digital identity management practices have limitations that may impede their continued positive impact on the development of the Internet economy.

  To interact with service providers, individuals have to register before they can start using a service and, each time thereafter, they have to be authenticated with the appropriate credentials created in the registration process (*e.g.* minimally, a login identity and a shared secret such as a password). As individuals increasingly register with a growing number of services, the complexity of managing ever more personal credentials becomes an impediment. It may create an unfair advantage for well-established service providers if users hesitate to join new alternative services to limit the total number of their credentials. Likewise, it can generate security weaknesses if users opt for easy-to-remember but weak passwords and/or reuse them across many services, creating a vulnerability in most of their accounts as soon as one is compromised. Users may also keep their passwords together in an insecure file or on a piece of paper, creating a "single point of failure" that an intruder can exploit.

- Second, many widespread digital identity management practices currently in use are not robust enough to support the development of higher value services which carry a higher level of risk.

  The number of offline services offered online has kept increasing since the early days of the Internet. However, a number of services are not yet available online because they require a level of assurance which is higher than what most digital identity management practices currently enable. Three main factors explain this situation:

  – A third party has often been considered to provide a high level of assurance regarding parties to an interaction. This third party, often called an "identity provider", is responsible for carrying out the registration of the individuals, for establishing their identity, and for issuing credentials. As the cost of these operations is relatively high, market forces do not seem to be sufficient for general high assurance identity providers to emerge, although there are some niche examples.

  – Moreover, to check an identity claim, high level of assurance services often require government "certified" information included in an identity card, driver's license, passport, social security card, birth certificate, marital status certificate, etc. Where no reliable mechanism exists to provide such elements online, the delivery of high level of assurance services requires

an offline manual process. This expensive step impedes the overall economic efficiency of the digital identity management process and the online migration of high value services as much as it prevents the creation of new digital services.

  - Finally, a circular situation exists whereby on the one hand, service providers are holding back from investing in new services until a critical mass of individuals use strong authentication credentials and, on the other hand, individuals are waiting for a critical mass of services that require strong authentication before they adopt the technology.

- Third, digital credentials providing a high level of identity assurance are not internationally recognised, preventing cross-border high value interactions.

What is the role of governments?

While many economic and social actors provide low, medium and high level of assurance credentials, governments are generally the primary issuers of the most trustworthy credentials for individuals' identity attributes such as their name, citizenship, date of birth, civil status (parenthood, marital status, etc.).

Although the form of these government issued credentials varies across countries, they generally enable high value public and private services offline. To migrate such services online and foster the blossoming of innovative digital high value services, market players need to establish end-to-end digital identity management processes. Therefore, the fact that a process or a tool provided by the government is not available in a digital form is currently a barrier which only governments can remove.

In addition, governments have the capability, as providers of essential online services to the whole population, to help generate a critical mass of high-value services and a critical mass of individuals equipped and trained to manage a high level of assurance credentials. Acting as model users, they can establish practices for themselves which can create the conditions for the emergence of user-friendly digital identity management solutions. Governments can take leadership and act as catalysts, promoting flexible policies for all stakeholders and creating favourable market and regulatory conditions for long term viability. Finally, governments also have a responsibility to ensure that digital identity management practices take advantage of technologies to enhance individuals' privacy where possible.

Governments are currently developing and implementing national strategies for the management of digital identity.[9] Making good policy choices today can positively influence the market in the long run and enable the further development of the Internet economy.

II. Policy guidance for governments

The principles below are based on the recognition that:

- Identity management is essential to provide trusted interactions between parties in the online and the physical worlds.
- Digital identity management is critical to the development of the Internet economy and brings considerable economic and social benefits by *i)* enabling innovative low, medium and high value online public and private services; *ii)* supporting the more efficient use of organisational resources; and *iii)* improving user convenience online.
- The development in the digital world of high-value trust-based economic and social activities that exist in the physical world is an important policy objective.
- Governments can facilitate high-value trust-based economic and social interactions online as providers of essential means for enabling high level identity assurance and as a driving force to help market players adopt consistent identity management practices.
- The development of identity management practices that support high-value services online should not replace their offline counterparts, so long as Internet access remains a challenge for some citizens.

Governments should adopt a clear national strategy for digital identity management

A clear national strategy for digital identity management is essential to the further migration of existing offline economic and social services to the digital world, to the creation of innovative online public and private services, and therefore to the continued development of the Internet economy.

It should aim to benefit the society at large, including businesses, citizens and the government, and minimise the risks that undermine trusted interactions online. The process for developing the strategy should be inclusive of all stakeholders with a view to identify and take into account their needs.

The potential long-term benefits to the broader Internet economy should be kept in sight

Governments should recognise the need for and the complexity of achieving long term objectives such as the migration online of public and private high-value services. They should clearly distinguish these long term objectives from short and medium term means to accomplish them. They should also avoid short term solutions which could impede the achievement of the long term goals. As identity management is a crosscutting area, involving many participants, and where small changes can have wide-ranging implications, a phased incremental policy approach involving all stakeholders may be needed to ensure long term success.

Where the national strategy is focused on e-government, policies should be designed to extend the benefits to the rest of the economy and society in the medium and long term, including by, as appropriate:

- Helping reach a critical mass of high value services based on high level of assurance mechanisms and a critical mass of individuals using high level of assurance credentials.
- Supporting a clear framework providing a degree of harmonisation for digital identity management at the national level.
- Promoting digital identity solutions that are sufficiently flexible to take advantage of future technical developments; Avoiding policies which can restrict or inhibit innovation within the broader Internet economy.
- Fostering interoperability of e-government digital identity with non-governmental identity solutions.

Existing offline identity management practices could be a natural starting place

Government identity management policies and practices are deeply rooted in countries' history, culture and style of government. Most government strategies for digital identity management can therefore consider building upon their existing identity management system, introducing evolutions where appropriate. For countries without established offline identity management policies and practices, the migration to the digital world is likely to be more complicated.

Where current offline identity management policies and practices are not considered effective, they should be improved as they are migrated online. For example, governments should take advantage of migrating

offline identity management practices online to improve privacy protection through encouraging the minimisation of identity data collection where it is not technically required to ensure an appropriate level of assurance.

Governments should recognise that the migration online of existing offline identity management policies and practices is likely to carry with it some of the same challenges that existed in the offline environment. For example, barriers to cross-border identity management will not be solved simply by migrating online. Similarly, digital identity management policies will have to address fraud and other malicious activities just like their offline counterparts.

E-government activities should be aligned with the national strategy

Digital identity management is a cross-cutting subject within the government. In order for a national strategy to be fully efficient, identity management policies and practices should be co-ordinated across the government, regardless of the specificity of each e-government activity and service.

A balanced digital credentials policy should be sought

The national strategy should aim to reduce or limit the number of digital credentials that individuals have to use across public and private sector services.

A balance should be found between the establishment of a unique universal credential for all digital interactions – which is sensitive for privacy reasons – and the multiplication of credentials that may impede usability. User convenience could be enhanced, for example, by encouraging the reduction of the number of credentials used for lower level of assurance interactions, by encouraging approaches where users have the choice of what credentials and level of assurance to use (so-called user-centric approaches), or by fostering the adoption of credentials providing a high level of assurance. The reduction of the number of credentials should not take place at the expense of privacy protection but should rather be based on privacy-friendly technologies.

Policies for digital identity management should ensure both security and privacy

The level of assurance regarding the identity of the parties involved should be based on an assessment of the level of risk in the transactions.

To establish trust, digital identity management practices and requirements should be proportionate to the level of risk in the interactions between the parties. The potential impact on privacy of digital identity management practices should be assessed and addressed as appropriate.

Digital identity management practices should respect legal privacy protection requirements. The development and implementation of digital identity management systems should include privacy protection, including data security, from the outset. Taking advantage of the potential for the technology to support both privacy and security, innovative technical protection measures should reinforce privacy protection requirements wherever possible, including through the use of pseudonyms where appropriate.

Governments should work together to enable cross-border digital identity management

The potential for digital identity management to facilitate high value e-government, e-commerce and other digital services across borders is impeded by various obstacles. Governments and other stakeholders should work towards reducing or minimising these obstacles. They should co-operate to further develop mutual recognition of national digital identity management approaches and to create the conditions for interoperability, for example through the use of regional and international standards.

Notes

1. This guidance should be considered in conjunction with relevant analytical reports listed in the references and in particular the comparative analysis of national strategies for digital identity management (OECD, 2011).

2. In the Seoul Declaration, ministers declared that, to contribute to the development of the Internet economy, they "will […] strengthen confidence and security, through policies that […] ensure the protection of digital identities and personal data as well as the privacy of individuals online." See OECD, 2008b.

3. The expression "service providers" relate to providers of services on the Internet and should not be confused with organisations which provide connectivity or access to the Internet.

4. OECD, 2008a, page 4. See also OECD, 2008b.

5. Third parties can also be involved, for example, when identity providers participate in the registration process.

6. Authorisation and access control processes can also be considered as belonging to "access management" rather than to "digital identity management".

7. The authentication process is further detailed in OECD, 2007a.

8. Practically, however, the assessment of the level of risk for an interaction depends on many factors including the value of the transaction, the context in which it takes place but also the amount of risk that the parties are accepting to take (*i.e.* "risk appetite"). It is therefore possible that the parties will disagree on what level of assurance is most appropriate or that similar transactions will require different levels of assurance when carried out by different parties.

9. See OECD (2011), National Strategies and Policies for Digital Identity Management in OECD countries, *http://dx.doi.org/10.1787/5kgdzvn5rfs2-en*.

References

On digital identity management and electronic authentication

OECD (2007a), "OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication". Available at *www.oecd.org/dataoecd/32/45/38921342.pdf*.

OECD (2007b), "Report of the OECD workshop on digital identity management. Trondheim, Norway, 8-9 May 2007". Available at *www.oecd.org/dataoecd/30/52/38932095.pdf*.

OECD (2009), "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Maker". Available at *www.oecd.org/dataoecd/55/48/43091476.pdf*.

OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. doi: 10.1787/5kgdzvn5rfs2-en.

Other

OECD (1980), "OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data". Available at www.oecd.org/document/20/0,3746,en_2649_34255_15589524_1_1_1_1,00.html.

OECD (2002), "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security". Available at *www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html*.

OECD (2008a), "Seoul Declaration on the Future of the Internet Economy". Available at *www.oecd.org/dataoecd/49/28/40839436.pdf*.

OECD (2008b), "Shaping Policies for the Future of the Internet Economy". Available at *www.oecd.org/dataoecd/1/29/40821707.pdf*.

Annex 1

National strategies and policies for digital identity management in OECD countries

This report is based on responses to the Questionnaire on National Strategies and Policies for Digital Identity Management (IdM) in OECD Countries circulated to the delegations of the OECD Working Party on Information Security and Privacy (WPISP) and to the OECD Senior Network of e-government Officials between December 2009 and June 2010 (Appendix III).

The report includes a detailed analysis, a list of references, country summaries (Appendix I) and a contribution by the Internet Technical Advisory Committee (ITAC) (Appendix II). It has been developed by the Secretariat (Laurent Bernat of the Directorate for Science, Technology and Industry) with expert input from Nick Mansfield, consultant to the OECD.

The Committee for Information, Computer and Communications Policy (ICCP) declassified this report at its 61st session on 16-17 March 2011.

Key findings

The following 18 countries responded to the 2010 OECD questionnaire on National Strategies and Policies for Digital Identity Management: Australia, Austria, Canada, Chile, Denmark, Germany, Italy, Japan, Korea, Luxembourg, the Netherlands, New Zealand, Portugal, Slovenia, Spain, Sweden, Turkey and the United States. All of them have or plan to develop a national strategy for Identity Management (IdM) or a set of policies which, taken together, represent such a strategy. They are at various stages of development and implementation.

The analysis of the responses focuses on governments':

- **Vision and strategy** for digital identity management. The vision describes the overarching objective of the government for developing their strategy, the intended future state that it wants to reach through the strategy. The strategy describes the main elements of the plan to realise the vision.
- **Policies** for digital identity management. The policies describe the set of tools (laws, plans, actions, etc.) developed to implement the strategy.

Vision and strategy

Vision: the main objectives for national IdM strategies are to realise e-government, to foster innovation in public and private e-services and strengthen cybersecurity.

For most countries, the overarching objective or vision for the development of a national IdM strategy is the realisation of electronic government. In addition to e-government, most countries also aim to foster innovation in the broader Internet economy, either explicitly or implicitly, either immediately or in the longer term. Two countries consider cyber-security as the fundamental objective for their strategy rather than e-government and/or the development of the broader Internet economy. Although their vision has a different focus, the strategy of these two countries does not

fundamentally differ from that of the other countries. Generally, however, innovation, e-government and cybersecurity can be identified in all countries' approaches. Variations are essentially related to the level where these dimensions are addressed (vision, strategy or policy). Fostering innovation in the broader Internet economy is a shared objective by a majority of responding countries but is not always explicitly mentioned as such. It can, however, be deduced from key aspects of their strategy and policies.

National IdM strategies aim to benefit businesses, citizens and the government. They are considered a key enabler for innovation in the public and private sectors: as they facilitate the generalisation of stronger electronic authentication, they enable higher value services that require a high level of security assurance to be offered. They are also expected to have economic benefits in terms of reducing costs and increasing productivity in the public sector and to foster usability of online services. Increased trust or assurance about identities online – or even bi-directional trust between parties transacting or communicating online – is also highlighted as a key benefit for all participants.

Strategy: the primary focus of national IdM strategies is the public administration with expected spillovers in the private sector.

The scope of all national IdM strategies encompasses public sector online services. Some countries favour a "universal approach", *i.e.* an approach that includes public/private sector use of digital credentials to support the broader Internet economy.[1] Others plan to extend to the private sector the use of digital credentials – or digital credentials' framework – established for the public sector. All national strategies address all layers of public administration, regardless of their level of autonomy. This aspect is often highlighted as a challenge.

Most countries recognise the leadership role of the government for better digital identity management in the Internet economy. The implementation of the e-government dimension of their strategy generally appears as a priority. However, the expected impact of these strategies on innovation extends beyond e-government to the broader Internet economy: governments can be seen as also willing to use the e-government side of their IdM strategies to try to foster identity management beyond e-government. Their strategies recognise, often implicitly, that the strong authentication market is limited by a circular situation: on the one hand, service providers are waiting for a critical mass of users to be equipped and informed in order to start investing in new services that require strong authentication and, on the other hand, users are waiting for a critical mass of services that require strong

authentication to be available in order to adopt the technology. Government can be seen as trying to break the resulting *status quo* by:

- Creating a critical mass of strong authentication users and services. The multiplication of e-government services that accept strong authentication credentials, and in several cases the distribution of digital credentials for strong authentication in the form of electronic cards, can potentially break the circular problem of strong authentication.
- Supporting a clear IdM framework to establish a degree of harmonisation for digital identity management at national level, thus reducing uncertainty for market players regarding which strong electronic authentication mechanisms to offer in order to participate in and benefit from a network effect, as well as potentially spurring investments and innovation.

To achieve this objective, IdM strategies lean towards reducing or limiting the number of digital credentials individuals have to use across a large number of services. Many countries also provide or plan to provide single sign-on solutions to access public sector services. In other words, most strategies can be seen as aiming to reduce either or both the number of digital *keys* or *credentials* Internet users have to manage and the number of digital *keyholes* or *gateways* they are facing when they try to access multiple government services online.

Strategy: National IdM strategies generally adopt an evolutionary approach based on existing offline identity regulations and practices rather than a revolutionary one.

All governments seem to automate and migrate their existing IdM business processes, they do not reengineer or reinvent them for the digital world. National IdM strategies reflect and respect national cultures, styles of government and offline identity management traditions. For example, all responding countries which have launched a national electronic identity card have actually migrated their existing paper-based national card. The voluntary or mandatory nature of the card was generally migrated as well. Countries which have a tradition of a national population register or an existing national identifier framework are using it as the basis for their digital identity management strategy, sometimes adjusting existing infrastructures to electronic use (*e.g.* networking or centralising existing population registers). There is no example of a country which has created a national identity card or population register without a pre-existing tradition. Countries which have other less centralised offline identity management practices develop decentralised or distributed approaches to digital identity management. This suggests that in

countries where offline identity management practices have never been centralised throughout history, solutions are likely to be more complex with the migration to the digital world.

Based on responding countries examples, one might conclude that strategic approaches; *i)* recognise the specificity of the country; *ii)* extend to the online environment the traditions, tools and processes that people are used to offline; and *iii)* help individuals to improve their efficiency online. The assessment of the cost and time required to successfully deploy national electronic identity cards is likely to be radically different in a country with a pre-existing national identity card framework to a country where there is no such tradition.

A related key conclusion is that there does not appear to be such a thing as a generic approach to digital identity management: identity management approaches are culture-specific and cannot be easily transposed or transported directly from one country to another.

Policies

Registration policies, *i.e.* the processes that establish the bond linking and legally binding a citizen to his or her electronic identity, are either centralised or decentralised and reflect how countries implement key aspects of their democracy. For example, countries where local layers of public administration are less autonomous tend to adopt a more centralised registration policy and, conversely, decentralised, federated or distributed approaches are found in countries where local layers of public administration are more autonomous. Confirming the evolutionary strategic approach highlighted above, digital identity management registration policies extend to the online world registration policies already established for offline interactions.

The nature of the challenges related to digital identity management interoperability, security and privacy and the characteristics of policies that address them depend on the centralised or decentralised nature of the registration policy. For example, IdM registration policy influences the level of interoperability that national policies can prescribe. In a country with a decentralised IdM registration policy, interoperability is promoted in the context of federation agreements. The common policy objectives are described independently of the possible technical solutions to achieve them and organisations participating in a federation agreement have the maximum flexibility regarding how to technically achieve the objectives. In contrast, countries following a centralised registration policy are more likely to adopt a relatively more prescriptive approach regarding policy and technical choices. Central registration policies raise privacy issues related to the use of a central population register, unique identifiers and, where relevant, national identity card frameworks. Decentralised registration policy provides each organisation

or jurisdiction with a high degree of autonomy with respect to the privacy protection measures it establishes. The level of privacy protection provided to individuals when interoperability is implemented depends on the trust agreements between the various participants in the federation. A single technical privacy protection solution cannot be imposed on participants in a decentralised policy framework. Just as for interoperability, participants are more likely to adhere to a set of privacy protection objectives and high level measures than to detailed policy measures or technical mechanisms.

Interoperability is mostly addressed from the technical perspective by responding countries. In some countries, IdM is included as part of the technical infrastructures developed for interoperability. Some respondents partially address interoperability issues within the public sector through a national e-authentication framework or national interoperability framework. Beyond the technical perspective, few other elements were provided on the scope and scale of changes that might be necessary at the legal or business process levels to achieve complete interoperability in identity systems across the public and private sectors.

As regards *security*, many countries have a policy to promote the use of Public Key Infrastructure (PKI). Most countries have established a digital signature legislative framework and many promote the development of a PKI market. The central and critical nature of the IdM function within the broader e-government infrastructure is not mentioned by respondents as requiring specific security policy attention.

With respect to *privacy*, all countries mention the application of their existing legal privacy protection framework as their main policy tool to protect privacy. Some countries implement strong privacy protection at the technical level ("privacy by design"). When biometrics are included in digital credentials, specific privacy safeguards are also implemented. Some countries consider data breach notification as one way to increase privacy and security awareness. Most countries do not consider the use of pseudonyms in their strategy and few countries provide details on certificates' suspension and revocation.

More generally, all countries recognise the key role of technical standards with respect to interoperability in general, and security in particular.

Policies for the *adoption of digital credentials* can be either voluntary or mandatory. Countries which have a tradition of mandatory offline credentials generally migrate that policy online. In other countries, the adoption of the digital credentials is voluntary. Governments have adopted a spectrum of ways, ranging from persuasion to coercion, to encourage or mandate the *use* of digital credentials by individuals and service providers.

Introduction

In November 2009, the OECD Secretariat circulated a questionnaire (*cf.* Appendix III) to delegations of the Working Party on Information Security and Privacy (WPISP) to gather information on their national strategies and policies for digital identity management. The main objectives were to illustrate and supplement the information provided in the report developed in 2008-2009 on *The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers* (hereafter "*Primer*")."[2] It also sought to analyse the commonalities and differences in national strategies for IdM[3], in policies for the implementation of these national strategies and in the challenges faced by governments.

Eighteen countries responded to the survey: Australia, Austria, Canada, Chile, Denmark, Germany, Italy, Japan, Korea, Luxembourg, the Netherlands, New Zealand, Portugal, Slovenia, Spain, Sweden, Turkey and the United States[4]. Respondents represent a good balance in terms of geography, population size, layers of government, diversity of cultures and styles of government. They also represent a sample of different stages of advancement with respect to development and implementation of IdM strategies, from preliminary reflection or early development stage to full deployment.

Following the analysis of the responses, Appendix I includes country summaries that have been developed to facilitate the analysis and provide a digest knowledge base enabling further exploration of each country's approach. These summaries are based on responses sent by countries[5] as well as additional research carried out by the Secretariat[6]. Resources used to prepare this report and cited by responding countries are listed, per country, at the end of this report. Appendix II includes a contribution by the Internet Technical Advisory Committee (ITAC) to the ICCP Committee in relation to digital identity management.

The scope of this report is limited to the management of digital identity of natural persons. With a view to ensuring a manageable output, the scope does not include specific aspects of digital identity management related to foreign nationals or to individuals as representatives of businesses and other organisations, cross-border aspects of identity management[7], and other issues such as the specific aspects of identity management frameworks for businesses or the deployment costs of digital identity management frameworks. When information on these dimensions has been provided by respondents, it is reflected in the country summary. It is however not taken into account in the analysis.

Analysis

This section includes an analysis of the eighteen responses received from OECD member countries to the questionnaire on national strategies for digital identity management, complemented by additional research. Responses received from countries included a large amount of information, the analysis of which is necessarily partial, reflecting only some aspects of the substance provided. This section follows the main structure of the questionnaire circulated to countries (National Strategies for IdM and Policies to implement the strategies).

National strategies for IdM

Vision

All responding countries have developed, are developing or are considering the development of a national IdM strategy. They are at various stages of development and implementation.

Although all responding countries have initiated action with regards to digital identity management, they are at various stages of development and implementation of their strategy (*cf.* Table A1.1). Some are considering the development of a strategy (Japan[8]) or have started to develop it (Chile, United States), some are finalising the development of their strategy (Canada, Luxembourg, Slovenia), some are initiating its implementation (Australia, Germany), some are following up on an initial experience (Denmark), some are quite advanced in the deployment of the main components of the strategy (Italy, Korea, Portugal, Spain, Sweden) and others are already operating a fully deployed strategy (Austria, Netherlands), and are continuously improving it.

Table A1.1 Estimated status of National IdM Strategy development and implementation

Stage	Development	Implementation
Not started or planning stage	Japan	Canada, Chile, Japan, United States
Early stage	United States, Chile, Slovenia	Germany, Australia, Luxembourg, New Zealand, Slovenia, Turkey
Ongoing	Canada, Luxembourg, Turkey	Austria, Denmark, Italy, Korea, Netherlands, Portugal, Spain, Sweden
Final stage	Australia, Germany	
Fully developed	Austria, Denmark, Italy, Korea, Netherlands, New Zealand, Portugal, Spain, Sweden	

Two countries consider cybersecurity as the fundamental objective of their strategy. For most other countries, the primary objective of the development of a national IdM strategy is the achievement of electronic government. However, in addition to e-government, most countries' strategy also aims to foster innovation in the broader Internet economy, either explicitly or implicitly, either immediately or in the longer term.

While most countries have an explicit focus on e-government, many strategies also include the management of digital identity in private sector transactions and aim to foster innovation in and growth of the broader Internet economy. This latter objective is generally less explicit in countries' responses and is sometimes only revealed by detailed analysis of the scope of their strategy (see Table A1.2) and other policy and implementation characteristics. The main indicator is countries' responses regarding inter-sections or relationships between government and private sector identity systems. In most cases, private sector use of digital credentials established by the IdM framework established by the national strategy is possible (see Table A1.2) either immediately (Austria, Denmark, Germany, Korea, Luxembourg, Portugal, Spain, Sweden) or in the future (Canada and Italy).

Security and cybersecurity are the primary objectives of two other countries in the development of their national IdM strategy, Australia and the United States. Australia focuses on identity security as the main objective of the national IdM strategy and places strong emphasis on the role played by identity security for Australia's national security and economic interests. The strategy recognises that identity security is vital in protecting citizens from the theft or misuse of their identities which often underpins terrorist and criminal activity, undermines border and citizenship controls and efforts to combat the

financing of crime and terrorism. The 2009 US Cyberspace Policy Review calls for a "cybersecurity-based identity management vision and strategy for the Nation" to encompass identity aspects of securing online transactions between businesses, individuals and governments.

Four observations can be made regarding these two exceptions:

It would be misleading to conclude that either or both countries ignore the role of IdM to foster e-government and the broader Internet economy. These two aspects are parts of their strategy but security and cybersecurity are the main overarching objectives or vision through which both strategies expect to reach these other goals. Similarly, it would probably be inaccurate to conclude that the other countries neglect security and cybersecurity as objectives of their IdM strategy: they are probably objectives as well but not stated as their primary goal.

The main distinction between Australia and the United States as compared to all others is the overarching nature of cybersecurity in the formulation of their strategies. There are also many differences at a more detailed level between their strategies and that of all other countries. They are, however, not necessarily a consequence of this overarching distinction and are more likely to stem from other factors such as national characteristics, history and style of government, as explained below.

The strategies of these two countries are led by high levels of government (Attorney General and White House) whereas other countries' strategies which focus primarily on e-government tend to be led by more specialised ministries and agencies.

As highlighted below, several countries have adopted the deployment of an electronic national identity card as a key building block in their IdM strategy. However, the overarching objective of their IdM strategy is generally not security and therefore their strategy is generally not led by the ministry responsible for security (*e.g.* interior), although this ministry often plays an important role in the development and implementation of the strategy.[9] The two countries whose strategy primarily serves a security objective have no plan for an electronic national identity card (they also have no tradition of a paper based identity card).

Finally, Korea has an interesting and unique approach. In addition to fostering e-government and innovation in the broader Internet economy, the Korean national strategy for IdM also aims to address growing concerns related to cyber violence. Korea has established an identification framework (based on the *i*-Pin) which aims to increase the responsibility of Internet users for their online behaviour while protecting individual freedom of speech and privacy[10].

Scope

National IdM strategies provide a framework within which participants can innovate.

IdM strategies aim to facilitate the generalisation of stronger electronic authentication thus enabling new public and private sector services (see Benefits section below) to be offered. The strategies aim to use the e-government side of their strategy to modify the current strong authentication market's *status quo* which deters the deployment of online services carrying a higher level of risk and which are also likely to have a high value.

Strong authentication mechanisms are expensive for service providers to deploy. Strong authentication can only be more generally adopted if the required investment by a majority of service providers is not too high and exponential network growth starts to appear to create a critical mass. However, market players do not know which strong authentication mechanism will ultimately initiate this network effect. As a result, they are caught in a circular (or "chicken and egg") situation whereby, on the one hand, service providers are waiting for a critical mass of users to be equipped and informed to use strong authentication in order to start investing in new services that require it and, on the other hand, users are waiting for a critical mass of services that require strong authentication in order to adopt the technology. National IdM strategies can be seen as an attempt by governments to break this circular problem by generating a critical mass of users and services through e-government services (and sometimes by distributing digital credentials themselves to the population) and by providing a degree of harmonisation for digital identity management at a national level that reduces uncertainty for online service providers regarding what mechanism to offer to benefit from a network effect.

The scope of IdM strategies always encompasses public sector online services. Some countries favour a "universal approach", *i.e.* encompassing public/private sector use of credentials to support the broader Internet economy. Others plan to extend the use of public sector digital credentials to the private sector – or digital credentials' framework. Most countries recognise the leadership role of the government for the generalisation of better digital identity management in the Internet economy. Government single sign-on services are only available or anticipated for public sector services, except in two countries where it also includes (or will include) private sector services.

While some countries keep private sector use of credentials – or credentials' framework– established by the IdM strategy as a possibility for the future (Australia, Italy), many others developed or are developing universal approaches with digital credentials for both public and private sector contexts ("universal credentials") (Austria, Canada, Denmark, German, Korea, Luxembourg, Portugal, Slovenia, Spain and the United States).

Austria, where "Citizen Cards" can be developed and offered by both private and public entities for both public and private sector transactions, is perhaps the best illustration of this approach. In Spain, both national electronic identity card's certificates and certificates issued by public and private sector certificate authorities can be used in public and private sector contexts. In Canada, although the federation model set out in the strategy enables public and private use of public and private credentials, the current focus is on e-government and the private sector aspects have not yet been fully assessed or defined. The United States' draft strategy explicitly focuses on transactions involving the private sector, individuals and governments. Other examples of universal public/private approaches include the Portuguese strategy where the single sign-on service extends to include private sector services and Denmark, where a universal single sign-on service is envisaged[11].

The Dutch strategy is limited to the public sector as a consequence of the strict regulation of the national identity number which cannot be used by the private sector. This is highlighted as a key challenge by the Dutch government. In New Zealand, the strategy focuses on public sector services but the government recognizes that an extension of some components to the private sector would require further assessment.

Table A1.2. Scope of national IdM strategies with regards to public/private use of credentials

Digital credentials can be used in:	
Public and private sector contexts (currently or in the longer term)	Australia*, Austria, Canada***, Chile, Denmark, Germany, Italy*, Korea, Luxembourg, Portugal, Slovenia, Spain, Sweden, Turkey, United States.
Public sector contexts only	Japan**, Netherlands, New Zealand.
Single sign-on is or will be available for:	
Public sector services	Australia, Austria, Canada, Chile, Luxembourg, Netherlands, Slovenia, Turkey.
Public sector services now and for private sector services in the longer term	Denmark, Portugal.
It is not considered	Germany, Italy, Korea, New Zealand, Sweden, United States.

Note: public sector refers to transactions between individuals, businesses or public sector bodies with public sector bodies (*i.e.* C2G, B2G, G2G).

* The use by the private sector of digital credentials established by the Italian strategy is being considered in the longer term. The use of the Australian national Document Verification Service by the private sector is being considered. Several IdM initiative targeting private sector (businesses) are carried out in Australia (see Country summary).

** Japan is at a very preliminary stage of the development of its strategy and only considers public sector credentials for the moment.

*** In the case of Canada, the framework enables private sector issued credentials to be used in public sector contexts and vice-versa. However, business models for private sector use of the framework still needs to be addressed.

One observation is that no strategy expresses the need for a single or global interoperable identity system. Each country develops its own strategy and implementation policies, applying international standards. Some countries participate in regional initiatives such as the EU STORK project for cross-border technical interoperability.

In general, responding countries seem to consider the implementation of the e-government dimension of their strategy as their priority.

This may be because they perceive that they have more control over government processes than they do as a wider market player. They may also consider that the development of IdM for e-government will be sufficient to create a critical mass of users and services that will modify the *status quo* for strong electronic authentication in the marketplace and impact on private sector IdM practices. The leadership role of the government for public and private sector IdM, when not explicitly acknowledged, is often implicit in most responses.

All national strategies address all layers of public administration, regardless of their level of autonomy. This aspect is often highlighted as a challenge.

In developing their national IdM strategy, all countries recognise the need to address the various layers of public administration in order for their strategy to be effective. For example, in countries with a federal system of government, the strategies cover the role of the federal government as well as the state or provincial level. In many countries, local levels of the public administration, such as municipalities, are also included in the scope of the strategy.

The need to address all layers of public administration is often highlighted as a challenge, for example in Canada, which follows a federated IdM approach, and Denmark, which notes the complexity of involving all participants including municipalities and their IT suppliers. In Italy, where regions and municipalities enjoy a large degree of autonomy, the slow adoption of a non-mandatory National Electronic Identity Card has led to the development of a National Service Card which is electronically compatible with the National Electronic Identity Card but lacks physical security features required for offline identity verification. This card is being deployed by regions and municipalities to enable access to regional and local e-government services. The adoption of this alternative card (33% of the population versus 3% for the national card) is such that it might be seen as an obstacle to the further adoption of the national card.

In one case, the legal protection of the national identifier was highlighted as an obstacle to a broad IdM strategy encompassing private sector transactions.

The Netherlands excludes private sector use of digital credentials created in the national IdM framework: the extension of the IdM framework to the private sector is strictly limited because the use of the "Citizen Service Number", a key component of the IdM framework, is restricted by law to the public sector. This highlights that the legal protection of the national identifier can become an obstacle to a broader IdM strategy encompassing private sector transactions, an issue which might be addressed by translating the legal protection of the national identifier into a technical protection, such as, for example, the solution adopted by Austria (see country summary).

Benefits

National IdM strategies aim to benefit businesses, citizens and the government. Strategies are expected to support innovation in the public and private sectors and to foster usability. Cost reduction and productivity gains generated by IdM for e-government are also often mentioned. Increased identity assurance for all participants is expected to foster the development and use of e-government and private sector services.

Benefits to businesses and governments are mostly economic: cost-reduction, productivity and efficiency gains. For example, in many cases, the pooling of authentication mechanisms or the availability of inter-operability frameworks reduces the cost of developing online services for smaller agencies and companies which are then able to keep their focus and resources on their core business. Most IdM frameworks create conditions for the provision of credentials that enable a high level of identity assurance. The diffusion of these credentials enables the development of new electronic services that would not be otherwise possible to offer (innovation). These include higher risk services such as the creation of a private enterprise online, including across borders, online car registration, and online crime reporting (Portugal). Interestingly, the two countries whose vision is focused on cybersecurity, Australia and the United States mention the reduction of fraud as another expected benefit for the government, but this is consistent with their overarching vision (the Netherlands also highlights the reduction of fraud as a benefit).

Benefits to citizens include the use of new online services that facilitate their relationship with the government and, more generally, enhanced convenience and usability of e-government services, for example by *i)* limiting the number of credentials users have to manage for their interactions with the government (*e.g.* Netherlands, Portugal, New Zealand, Sweden); *ii)* recognising a wide range of credentials through a federated approach (*e.g.* Canada, United States); *iii)* deploying national electronic credentials such as national identity cards or citizen cards (*e.g.* Austria, Denmark, Germany, Italy, Luxembourg), in some instances to replace sets of pre-existing credentials (*e.g.* Italy, Portugal, Spain); *iv)* implementing single sign-on services across government web sites where citizens are only required to authenticate once – generally on a government one-stop-shop portal or gateway– to access multiple government services (see Table A1.2). Other examples include the reduction of the requirements for citizens to provide documents issued by other agencies in order to benefit from a service (*e.g.* Slovenia). In most strategies, a digital signature created using a certificate issued by an accredited authority[12], has the same validity as a handwritten one, enabling citizens to interact with public services electronically.

The enhancement of trust and security within the citizen to government and to business relationship is often stated as one of the benefits to all participants.

Main components

Strategies include a large variety of key components.

Table A1.3 provides an overview of the main components of National IdM Strategies in responding countries.

Many countries provide or plan to provide single sign-on solutions to access public sector services (see Table A1.2).

One common objective is to reduce the requirement for users to log-in multiple times to access the various services provided by the same large-scale organisation (*e.g.* the public administration when considered as a single very large enterprise).

Table A1.3. Main components of national IdM strategies

Australia	• Standards for Registration, Enrolment, Security for Proof of Identity Documents, Integrity of Identity Data, Electronic Authentication, and Biometric Interoperability • National Document Verification Service (DVS) • Single sign-on to e-government services
Austria	• Universal* citizen card concept: framework for privacy-friendly credential that can be issued by public and private sector bodies. • Single sign-on to e-government services
Canada	• Foundational elements to define key concepts (*e.g.* assurance model, privacy code, trust model), • A framework defining a high-level structure and architecture as well as legal, privacy, security, identification trust and service experience requirements, • A service delivery component identifying pilot projects • A component supporting standards and guidelines
Chile	• Migration of the current national identity card to a universal* electronic card
Denmark	• Universal* PKI-based digital credentials for secure identification, digital signature, secure email. • Single sign-on to e-government services (possibly extending to the private sector).
Germany	• Migration of the mandatory paper-based identity card towards a universal* electronic identity card • Development of services for private use (secure email, proof of identity system and document safe). • Interoperable IdM infrastructure for e-government
Italy	• Migration of the non-mandatory national paper based card to a voluntary electronic card • Development of an electronic National Service Card (deployed by regions and municipalities) • Centralisation of municipality maintained residence registers
Korea	• Government PKI and promotion of private sector PKI • *i*-PIN framework
Luxembourg	• Certificate authority based on a Public Private Partnership with banks • PKI certificates for public and private interactions • One-stop-shop e-government portal • Migration of paper-based mandatory national identity card to a universal electronic card (future)
Netherlands	• Credentials to be used only for citizen to government interactions • Electronic identity card is under consideration

Table A1.3. Main components of national IdM strategies (cont'd)

New Zealand	• Various identity/authentication guidelines and standards, *i.e.* Identity Assurance Framework for e-government • Logon Service (one login/password per person for all participating government agencies) mechanism and Identity Verification Service for e-government.
Portugal	• Migration of the mandatory paper based identity card to a universal Citizen Card • Single sign-on identity provider for public and private online service providers • PKI certificates and services for public and private interactions • One-stop-shop e-government portal
Slovenia	• PKI for public and private sector transactions • Single sign-on for public sector
Spain	• Migration of the mandatory national identity card to a universal electronic national identity card • Promotion of public and private sector PKI (15 certificate authorities) • Validation platform for public and private sector PKI • National interoperability framework for the public administration
Sweden	• An agreement with selected private sector companies (banks) to foster PKI
Turkey	• Centralisation of citizens registers • E-government gateway • Plan for the migration of the paper based national identity card to a universal identity card.
United States	• A comprehensive identity ecosystem framework • An interoperable identity infrastructure aligned with the identity ecosystem framework

* Universal, in this report, means that it can be used in public and private sector contexts.

The implementation of a single sign-on service for e-government services sometimes occurs in parallel with the development of e-government portals or gateways (*e.g.* Australia, Austria, Denmark, Luxembourg, Netherlands, Portugal, Turkey)[13]. In Austria, the Government portal personalises the presentation of the various services available to take account of the individual's situation (*e.g.* profession, marital status, region, etc.). It includes an "electronic safe" for private documents, a reminder service and electronic delivery services. Stored data is protected but can be released by the citizen to specific applications to generate pre-filled forms. On the Danish Web portal, individuals can access the data collected about them by multiple public authorities, including tax services and the local municipalities, without logging-in several times.

Two exceptions may be noted. Germany does not consider single sign-on to e-government services for transparency reasons: personal data from online authentications may not be automatically forwarded to third parties. However tokens for individual single sign-on systems can be provided to the user on the basis of online authentication. New Zealand developed a Logon Service where individuals are provided with one set of login/password that works for all participating government agencies, although they can also use multiple logons for multiple services if they wish to. Single sign-on is not currently provided as users have to sign-on to each service, but it could be proposed in the future through a government portal.

Almost all national IdM strategies aim to reduce or limit the number of digital credentials that individuals have to use across a large number of services.

To simplify user experience and reduce costs for service providers, strategies aim to address the multiplication of credentials end users must manage to gain access to an increasing number of services online. Most strategies create a framework to facilitate the management of digital identity credentials or, more precisely, to promote the use of a limited number of digital credentials across a large number of services. However, this common high level objective is achieved through a variety of approaches across responding countries.

To use a metaphor, most strategies can be seen as aiming to reduce either or both the number of digital *keys* or *credentials* Internet users have to manage and the number of digital *keyholes* or *gateways* they are facing when they try to access multiple government services online.

Some countries develop innovative public identity services that can be used by the private sector.

Nevertheless, some countries develop innovative public identity services that can be used by the private sector to support economic and social activities. Germany provides an interesting example: although the strategy is a building block of the 2006 E-government 2.0 programme, it includes the development of innovative government identity services for public and private sector use such as long term document safe, registered email with possible use of pseudonyms and "proof of identity attributes" services whereby users can send proof of address and age by email. Portugal provides examples of innovative private sector benefits enabled by its citizen card such as opening a bank account online, signing private contracts and enabling authentication on private Web sites or workers assiduity registration.

Most countries have established a digital signature legislative framework and many promote the development of a PKI market.

For example Korea recommends the use of a digital certificate for e-commerce transactions above a certain value. Spain provides an interesting example of strategy addressing both e-government and the broader Internet economy with a universal national identity card framework and the stimulation of the PKI market. Although Spain has a dynamic PKI marketplace with 15 certificate authorities delivering certificates that can be used in both public and private sector contexts, the national card is used by the private sector to develop innovative services. For example, a bank modified its ATM machines to accept the national card and Cisco developed Virtual Private Network technologies based on the national card.

Approaches

Countries follow a migratory approach to identity management rather than a reengineering one. Governments aim to automate their existing business processes to reduce cost, improve usability and offer new services. At present, they do not aim to reengineer these business processes. IdM strategies are therefore evolutionary, based on adapting and extending existing identity practices, rather than revolutionary, involving the creation of something completely new.

In most cases, governments develop digital identity management strategies which extend existing offline identity management strategies to the online world. They do not try to reengineer digital identity management online as if nothing existed before or establish a completely new framework for digital identity management distinct or separated from existing offline traditions and processes. Most frameworks build upon the existing means for identity verification offline and extend or adapt them to the online world. They tend to minimize the creation of new processes that would imply new habits for citizens. Thus National IdM Strategies generally follow the principles of automation, migration and evolution of existing business processes (see Box A1.1).

For example, countries which have launched an electronic national identity card generally had a paper based national identity card for offline identity validation. Their initiatives are often presented to citizens as the migration and evolution of a paper card to an electronic card, thus enabling more services, more convenience and reduction of government costs. Spain, for instance, is migrating and extending its mandatory paper-based identity card to an electronic identity card which, in addition to providing the traditional offline identity verification, also enables electronic authentication online. Other similar examples include Germany, Italy, Luxembourg and Portugal[14].

Countries which do not have a tradition of national identity cards develop alternative approaches to introducing digital credentials. Sweden, for example, has a long tradition of offline identity verification carried out using bank credentials. The digital identity management strategy simply extends this policy online: banks selected through a public procurement process provide PKI certificates to citizens and validation services to the government. Denmark does not have a tradition of a national identity card, its digital identity framework provides an infrastructure for standardized and secure digital certificates that can be kept centrally in hardware, on a USB token or on a smartcard. Austria also does not have a national identity card tradition. It has developed a "citizen cards" framework defining minimal requirements for digital identity tokens to provide a secure and privacy-friendly signature device enabling qualified electronic signature as well as sector-specific identification and representation (to carry out legal transactions on another person's behalf). Austrian Citizen Cards can be developed and distributed by any public or private body such as the government, banks (on credit cards) and even telecommunications operators (SIM cards for mobile phones).

Where a national register or identifier (*e.g.* number) exists, it is generally used by governments as part of the new digital identity management strategy (*e.g.* in Austria, Denmark, Italy, Korea, Luxembourg, Netherlands, Portugal, Slovenia, Spain and Sweden). There is no example among respondents of a country which has created a completely new population register or unique identifier in order to support a digital identity management strategy. Countries which do not have a pre-existing register or identifier find alternative ways to support identity management at a national level. This is illustrated by Australia, Canada, New Zealand and the United States which are developing decentralised approaches that best suit their national features.

IdM approaches that are suited for the offline world cannot always be directly applied online. The migration process often requires adjustments and evolutionary changes. Sometimes, innovative components have to be designed to address specific challenges raised by the digital world or to take advantage of the digital context. For example, Austria and Italy had to centralise and the Netherlands had to network their population registers, which had all previously been kept by local municipalities, in order to facilitate the citizen card, national card or their unique identifier framework. In these countries, citizens traditionally registered at a local government office and continue to do so. However the information collected is now centralised enabling various electronic services to be offered by the central and local government. Thus, these countries have not established a completely new registration system to support e-government. Instead, pre-

existing registration processes have been adapted to enable these new services (see below, registration policy).

A further example is Australia where a document verification service is being implemented to enable agencies to perform real-time checks on the validity of documents presented by clients as proof of identity. Government agencies are also encouraged to follow an e-authentication framework that promotes the re-use of existing processes and practices to improve security, usability and cost efficiency. These approaches respect the decentralised tradition of Australia's style of government while enabling a more robust identity management system as the main objective of the Australian strategy.

Three observations can be made:

- Australia, Canada and the United States have the largest territory and the lowest population density of all respondents. Also, all three are examples of countries with a federal government system and favour a decentralised approach to digital identity management.
- In general, citizen cards or service cards are adopted by countries which do not have a tradition of a mandatory national identity card but do have a tradition of a national population register or identifier.
- A migratory approach is likely to carry with it the challenges that existed in the pre-existing environment. For example, cross-border challenges that existed with offline identity management will not be solved simply by migrating identity management online.

Box A1.1. The four stage journey of the migration of services online

The migration of services to an online environment, whether for electronic commerce, electronic government or any other form of business processing (*e.g.* intra-enterprise processes), is generally described as a four-stage journey:

1. Initially, organisations electronically publish information and forms that users can print, complete and submit in paper format. At that stage, there is no need to modify identity management approaches that follow the traditional paper-based method. The link between forms and users continues to be established on the basis of a signature on a paper form.
2. In the next stage, organisations provide a Web interface where forms can be completed online and submitted electronically. At this stage, some *electronic registration* method becomes necessary to link the form to the person or organisation completing it. In complex organisations such as governments or large firms, different electronic registration methods are often developed in parallel in the various entities (silos) of the organisation, for example each ministry in a government or each subsidiary in a multinational enterprise.

   As the number of online services increases, the number of electronic registration systems multiply and their complexity and cost increase. Eventually pressure starts to appear *i)* to streamline the development and maintenance of parallel vertical identity frameworks which become a source of unnecessary expenses and *ii)* to simplify access for end users who have to create and manage a growing number of credentials and may get lost in the proliferation of interfaces to access online services.
3. In the third stage, organisations decide to further *automate their business processes*. They identify common identity management elements within each domain and try to rationalise and share them to the extent possible. They adopt more comprehensive strategies for the management of identities online. Portals start to appear as well as single sign-on technologies. Organisations try to increase the number of applications users can access with a single credential.
4. In the final stage, organisations realise that innovative business processes can further reduce costs, improve users' experience and create opportunities to introduce new services with consequences that extend beyond the simple rationalisation of existing processes. This *business process reengineering* phase can be considered the final stage of the journey towards electronic services.

As regards identity management, all respondents have reached, in some area or another, the third stage of the evolution described above: the automation of pre-existing paper-based business processes which were established a long time ago[15]. No respondent has mentioned their intention to reengineer their business processes to achieve greater cost reductions (the above stage 4). It is likely that the cost and complexity of business process reengineering on a scale as a broad as the public administration are such that the automation of existing processes is seen as a necessary preliminary stage. In addition, the need to maintain –during a transition period– traditional paper-based infrastructures in parallel with the electronic ones prevents Governments from considering to reengineer their business processes whilst migrating their services online. Business process reengineering in the context of electronic government will probably only take place once the citizen base has fully migrated online and electronic services reach out to the whole population.

National IdM strategies respect the national culture, style of government and offline identity management tradition.

A deeper analysis of countries' geographic, administrative, political and historical specificities might find, for example, that countries with a longstanding practice of administrative centralisation would naturally rely on central population registers, countries with some historical experience of government abuse of population registration may be reluctant to adopt centralised schemes, countries with large territories probably provide more autonomy to regions and cities to compensate for the difficulty of communications with the central government, etc. (further discussion of centralised *vs*. decentralised registration policies are provided below). A striking example of the cultural nature of IdM practices is provided by Korea where the generalised use of an identifier stems from the limited number of last names in the population: only 274 last names are in use and almost half of the population shares the three most common Korean ones (Kim, Lee and Park). Unsurprisingly, the Korean identifier includes other identity attributes such as gender, date and place of birth to reduce the identity uncertainty that the first and last name alone might generate. A similar example is provided by New Zealand where government agencies designing online and offline identity authentication processes should take into account the fact that a person may adopt a name through usage and reputation (including, for example, adopting a spouse's name on marriage), and legitimately continue to use different names in different contexts. The migration of identity management online has to accommodate the fact that individuals may legitimately hold a range of documents that provide evidence of their use of their different names.

All these factors, and many others, form a specific and complex national equation that can help to explain why offline identity management policies vary across countries. Most of the variables of these equations are also valid for digital identity management and complemented by other technology-related parameters such as broadband penetration, pace of adoption of information technologies, etc.

Taking the example of countries which are successfully rolling out electronic national identity cards over a short period of time (*e.g.* Portugal, Spain), one could conclude that a fully federated approach to digital identity management could take longer to implement and, consequently, may not be an optimal policy. This view would, however, not take into account the fundamental fact that most countries which have successfully rolled out an electronic identity card over a short period of time are migrating their existing paper-based card infrastructure and rely on their existing population registers and management structures. The assessment of the cost and time required to successfully deploy national electronic identity cards should take

into account the effort and time that has historically been necessary to implement and operate the existing paper-based card infrastructure on which the new electronic card deployment will rely[16].

One may consider that a good strategic approach should recognise the specificity of the country, extend to the online world the traditions, tools and processes with which citizens are used to operate in the offline world, and improve their efficiency in the online context. Where offline identity management practices have never been rationalised or centralised historically, greater complexity is likely to emerge in migration to the digital world.

A related key conclusion is that there does not appear to be such a thing as a generic approach to digital identity management that could be applied regardless of the national context: identity management approaches are culture specific and cannot be easily transposed or transported directly from one country to another.

Policy: What policies support the strategy?

Developing and implementing a national digital identity management strategy covering an entire country's population is inherently complex and requires time. The nature, scale and complexity of challenges such as interoperability, security and privacy are related to the core objectives supporting the strategy (e-government, cybersecurity, broader Internet innovation). It is not realistic to target and address all core objectives and all challenges in parallel and with the same degree of priority. The more extensive the core objectives, the greater the number of challenges to overcome. Most countries probably try to strike a balance between objectives that match their broader national priorities and the challenges they can manage in the short term. They recognise that there are limits to what their policies can do to support their strategy: what is possible in the short term is not necessarily what they would like to achieve in the long term. Digital identity management at the national level is a journey.

The questionnaire included sections on interoperability, security, privacy and usability policies. The analysis of countries' responses helped identify their registration policy as well as their policy for the adoption and use of digital credentials as important aspects of their IdM approaches. The type of registration policy appeared as a key differentiating factor in the analysis of how national policies address each of these dimensions. This point is developed below more specifically in relation to interoperability and privacy.

Registration policy

National Identity Management strategies are based on either a centralised or decentralised citizen registration policy.

A citizen registration policy provides the basis for the bond and legal binding between the individuals and their electronic identity.

One can distinguish countries with a:

- Centralised registration policy generally based on a population register and, often, on a unique identifier (*e.g.* number) assigned to all citizens or residents,
- Decentralised registration policy, where each organisation is autonomous with respect to its registration policy. Several registration mechanisms coexist and interoperate within frameworks established by federation agreements.

Citizen registration policy is influenced by national history. The development of national IdM strategies has not led countries to reconsider their pre-existing citizen registration policy for offline identity management.

The choice of the citizen registration policy is likely to stem from many interrelated factors specific to each country including culture, style of government and history. Some countries have a longstanding tradition of maintaining a national population register (Chile, Denmark, Italy, Portugal and Spain) and identity number (Korea). As noted above, in other countries, population registers maintained at the local level were centralised (Austria, Germany) or networked (Netherlands) to be used for online identity management. In a third group of countries, there is no central population register and the citizen registration policy is based on a federated or decentralised approach. For example, each organisation is autonomous regarding its registration mechanism and adheres to a federation agreement that provides a trust model enabling interoperability of credentials across domains and single sign-on (Canada).

Table A1.4. Registration policies

Centralised	Austria, Chile, Denmark, Italy, Korea, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, Turkey
Decentralised	Australia, Canada, New Zealand, United States

The development of IdM Strategies has not led responding countries to change their citizen registration policy. Countries where the various layers of public administration are the most autonomous tend to adopt decentralised registration policies co-ordinated within federal agreements. Countries where local layers of public administration are less autonomous tend to adopt a more centralised registration policy. While no responding country has switched from one registration policy to another, some countries have modified some important characteristics of their citizen registration policy. For example, as noted above, population registers previously maintained at local level have been centralised (Austria, Italy) or networked (Netherlands). Overall, these elements confirm that current IdM strategies are more about automating and migrating existing processes rather than reengineering them, as highlighted above.

One conclusion might be that no citizen registration policy is better than another in the abstract because they have all been implemented within a specific historic, socio-cultural and political context. The registration policy of a country is deeply related to the country's style of government as it reflects the degree of autonomy within which each layer of the public administration can operate. It also reflects the country's history and culture, where for example registries of citizens might have appeared to support key public authority functions such as tax collection. And it can also be sensitive in countries where population registers have been historically used for illegitimate purposes by governments in the past or where there is a fear that such a situation could arise. In this regard, registration policies essentially reflect how countries implement key aspects of their democracy.

Policy for adoption and use of credentials

Adoption of the citizen credentials can be either voluntary or mandatory. Countries which have a tradition of mandatory offline credentials generally migrate that policy online. In other countries, the adoption of the digital credentials is voluntary. Governments have adopted various means, from persuasion to coercion, to encourage or mandate the use of digital citizen credentials by individuals and service providers.

Characteristics such as the voluntary or mandatory nature of the paper-based card are generally also migrated to the electronic card. Where paper-based identity cards are mandatory, electronic ones are often also mandatory, facilitating penetration in the short or medium term. *A contrario*, where the national electronic card is voluntary, its adoption can be slow (*e.g.* Italy): citizens do not automatically perceive the benefits of the electronic features of the card for themselves.

Governments use a wide range of means to increase usage by individuals and service providers, from encouragement to obligation. For example, Spanish citizens get entitled to tax refunds and receive them faster when they use the online tax services; Slovenia requires the use of electronic means to submit tax returns; in Korea, digital certificates are mandated by law for activities such as banking, stock trading and electronic commerce transactions above USD 260; the Danish government aims to require the use of the government provided digital credentials for e-banking and for public sector services.

As regards use by service providers, the Austrian framework encourages public and private sector organisations to provide Citizen Cards to individuals and provides open source modules to online service providers to facilitate the integration of the card to their online applications. Similarly, Portugal distributes a development kit to encourage the development of card-based applications. Adoption by private sector online service providers can also be encouraged by the creation of consultation forums such as the Digital Identity Management Forum in Korea. In the Netherlands, public sector agencies are mandated by law to use the DigID to provide online services.

Interoperability policy

All respondents, regardless of their registration policy, recognise the role of standards for technical interoperability and market competition and they encourage the use of widely recognised ones. However, IdM registration policy influences the level of interoperability that national policies can prescribe.

For example, in a country with a decentralised IdM citizen registration policy such as Canada, interoperability is promoted in the context of federation agreements. The common policy objectives are described independently of the possible technical solutions to achieve them. Organisations participating in a federation agreement have the maximum flexibility regarding how to technically achieve the objectives. In contrast, countries following a centralised citizen registration policy are likely to adopt a more prescriptive approach regarding policy and technical choices. For example, the Austrian government develops and provides open source software modules to simplify the development of "Citizen Card" compatible online services. In all cases, however, the role of regional and international standards for technical interoperability is widely recognised.

Where a specific technical solution is promoted by the government, such as in Korea with the *i*-PIN or Turkey with the national card, it is generally adopted as a national technical standard.

Countries which promote the use of PKI generally support PKI inter-operability through the establishment of a legal framework with a supervision mechanism and the recognition of standards (*e.g.* Korea).

Some countries develop technical infrastructures for interoperability that include IdM features.

This is, for example, the case with the German Secure Access to Federate E-Justice/E-government (SAFE) initiative, a technical framework for interoperable and safe usage of digital identities across administrative borders ("trust domains"). In Turkey, public bodies can access Identity Information Sharing System (KPS) through a virtual private network.

Technical infrastructures to promote interoperability in both the public and private sectors can also be developed by the government, such as with the Spanish @firma validation platform operated by the Ministry of Territorial Policy and Public Administration. This platform also aims to provide validation services across borders, mainly through the EU STORK project.

Most responses focused on technical interoperability. Few elements were provided on the scope and scale of changes that might be necessary at the legal or business process levels to achieve true interoperability across diverse identity systems, beyond the technical and across the public and private sectors.

At least two hypotheses might explain the lack of information regarding aspects of legal or business process interoperability:

- A bias in the survey exercise for example in the formulation of the questions; and/or
- A confirmation that since governments are essentially automating existing government business processes, few additional legal and business process mechanisms are required to support inter-operability.

Some respondents address interoperability issues within the public sector through a national e-authentication framework or national inter-operability framework.

For example, Spain developed a national interoperability framework to foster interoperability within the public sector. In Australia, the 2008 National e-Authentication Framework promotes the use of secure and interoperable electronic credentials in citizen- and business-to-government transactions and aims to assist agencies, jurisdictions and sectors in authenticating the identity of the other party to a desired level of assurance

or confidence. The framework does not mandate any particular approach but encourages interoperable e-authentication mechanisms so that individuals can expect similar authentication processes for transactions with similar assurance levels across all three tiers of government within Australia. To reduce cost and increase interoperability, federal agencies are encouraged to use the authentication infrastructure of designated lead agencies for government-to-government, business-to-government, or "people-to-government" authentication. New Zealand's e-government interoperability framework addresses interoperability of IdM systems.

Security policy

Although some respondents provided information on technical security measures for IdM, few details were provided regarding higher level security policy specific to IdM. One hypothesis is that IdM security stems from broader government information security policy and is not specifically addressed by governments at a policy level. This is, for example, the case in Australia where IdM security is addressed through the broader 2009 Australian Government Cyber Security Strategy, various legislative and regulatory security requirements, government standards and security manuals. Chile is similar in this regard.

An interesting observation is that the central and critical nature of the IdM function within the broader e-government infrastructure is not mentioned by respondents as requiring specific policy attention.

Many countries have a policy to promote the use of PKI.

Two groups of countries support PKI: countries which develop citizen electronic card frameworks (Austria, Germany, Italy, Portugal, Spain) and countries which develop PKI-based electronic credentials frameworks that are not necessarily card-based (Denmark, Korea, Luxembourg, Netherlands, Slovenia, Spain Sweden, Turkey). Most countries have adopted a legal framework to support PKI which includes supervision of certificate service providers.

Most countries have a policy to promote the use of digital certificates both for e-authentication and e-signature. Some also develop or promote related services such as time stamping (*e.g.* Portugal).

Few countries, besides Korea (which highlights this as a challenge) and Portugal, provide details on certificates' suspension and revocation.

Privacy policy

All countries mention the application of existing legal privacy protection framework as their main policy tool to protect privacy.

This includes for example the security of personal data, including sensitive data. Exceptions include Chile, where amendments to the privacy legislations are expected to address this issue and Turkey, where privacy is not specifically addressed.

Privacy Impact Assessments (PIA) are sometimes mentioned to be applied to government IdM systems (*e.g.* Australia, Canada, Luxembourg, New Zealand, and the United States). Korea is considering the modification of its Privacy Act to include an obligation for public agencies to perform PIA. The Dutch government and the Dutch privacy authority are also considering PIAs.

The role of the Data Protection Agency (DPA) as a provider of IdM guidance is sometimes highlighted, such as in Luxembourg, Portugal and Australia where the Privacy Commissioner issued privacy guidance on PKI.

Several countries mention the importance of data minimisation in relation to IdM. Government agencies in Canada are encouraged to comply with a Directive which addresses the proportionality of the personal information collected and requires the selection of "an appropriate set of identity data (such as personal attributes or identifiers) to sufficiently distinguish a unique identity to meet program needs, which is proportionate to identified risks and flexible enough to allow for alternative methods of identification, when appropriate".

Most countries do not consider the use of pseudonyms in their strategy.

Exceptions include Australia, in specific cases such as to protect the identity of victims of violence, Denmark which is considering it for the future, and Germany. The Netherlands plans to introduce the use of pseudonyms in its future IdM framework for business.

Privacy challenges and responses are, to a large extent, related to IdM registration policies.

Central registration policies raise issues related to the use of a central population register, unique identifiers and, where relevant, national card frameworks. Challenges include the protection of the number itself, and mechanisms to prevent its use to match individuals across multiple organisations where there is no legal basis to do so (unlinkability), inappropriate access to the central register database and to data stored on the card.

Privacy protection raises different challenges in countries that have adopted a decentralised registration policy. Since each organisation or jurisdiction has a high degree of autonomy with respect to the privacy protection measures it establishes to apply privacy laws, the level of privacy provided to individuals, when interoperability is implemented, depends on the trust agreements between the various participants in the federation. Just as for interoperability, a single technical privacy protection solution cannot be imposed on all participants in a decentralised policy framework. Again, participants are more likely to adhere to a set of privacy protection objectives and high-level measures than to detailed policy measures or technical mechanisms.

Some countries implement strong privacy protection at the technical level ("privacy by design" IdM approach).

Again, technical approaches to privacy protection vary according to the registration policy:

- Countries with a centralised registration policy are more likely to require specific measures to protect the national identifier, access to the population register, and the use of the national or citizen card when they have one. Technical privacy protection measures can be seen as an efficient way to address legal privacy issues and are also important to enhance trust in and acceptance of the IdM framework.

  In Austria and Germany, privacy protection is seen as a key feature of the card framework and the technical solutions that have been implemented to provide unlinkability based on the unique identifier (Austria) or to limit the transfer of data (Germany)[17] are particularly innovative. In Italy, the data stored in the central register is encrypted with the public key of the issuing municipality. In Korea, the whole *i-PIN* framework has been developed in part to limit the generalised use of the Resident Registration Number as the default identifier online which was leading to all sorts of abuse. An interesting and simple technical privacy measure is the obligation by the *i*-PIN agency to send an email to the individual each time his/her *i*-PIN number is used to identify him/her. In Portugal and Spain, biometric features are carried out using "match on card" technology which prevents the use of a central biometric database while protecting access to the data stored on card and enabling individuals to express consent in a secure manner for certain types of operations to be executed in the card (change of the PIN, renewal of the certificates). In Portugal, several sectoral identification numbers are available on the card to comply with the legal protection of the national identifier.

- In countries with a decentralised registration policy, privacy within a single decentralised local domain follows the same pattern as the centralised policy. On the one hand, decentralisation can be seen as inherently more privacy protective as there is no single point of privacy failure. But on the other hand, difficulties seem to arise when the identity data has to be transferred or shared with another domain in order to be used. Embedding privacy policy into technology in a manner that can be easily transferred or shared with another trusted domain (*i.e.* federated or otherwise linked) with, perhaps, different privacy policies, goes beyond simply being a technical challenge. One option, followed by Canada is to clearly state the privacy objective and leave the freedom to use any appropriate technical solution, thus side-stepping the technical difficulties and relying on audit of the objectives and other privacy tools to create an interoperable system. Another option, followed by New Zealand, is to embed strong privacy protections in solutions provided by the government to agencies.

When biometrics are included in digital credentials, specific privacy safeguards are implemented.

For example, the introduction of biometrics in the German identity card to enable its use as a biometric passport will include technical measures to restrict the use of biometrics to specific cases such as border control and prevent their use, for example, for e-authentication. The Portuguese and Spanish national cards both include biometrics but their use is limited by "match on card" technology.

Some countries consider data breach notification as a possible means to increase privacy and security awareness.

In addition to the United States, this is for example the case in Australia, Canada and Korea which are considering the introduction of data breach notification requirements.

User empowerment policy

Countries migrating their national paper-based identity card to an electronic card are generally aware of the user empowerment challenge. Although public acceptance for the electronic card is often relatively high due to the pre-existing paper-based card, citizens do not necessarily understand the potential benefits (and risks) related to electronic features of the card, such as digital signature and electronic authentication.

User awareness campaigns are often included in the broader cyber security awareness programmes (*e.g.* Australia, Canada, Denmark and Luxembourg). Some countries develop specific awareness raising campaigns, for example to support the adoption of citizen or national cards (*e.g.* Austria, Portugal, Spain) or identifiers (Korea). Most countries mention the registration or acceptation of the terms and conditions as a particularly suited moment to convey information about benefits and risks as well as privacy.

Usability is sometimes promoted through innovative applications such as the Korean Digital Identity Wallet system which enables users to log in to Web sites without filling in ID and password information. Austria considers usability and acceptance as key issues. The Austrian Citizen Card and the Danish NemID credentials are based on technologies that do not require users to install software on their computer, a important point for individuals who do not use their card often.

The Netherlands and Portugal have created a national helpdesk for identity fraud.

Notes

1. In the context of this paper, the term "universal" means across the public and private sectors rather than across countries.

2. See *www.oecd.org/dataoecd/55/48/43091476.pdf*.

3. In this report, IdM is the abbreviated form of digital identity management. Non digital identity management is explicitly referred to as "offline identity management".

4. In addition, the Mexican government has provided some information. See Appendix I.

5. Country responses have been posted on the WPISP Delegates' Workspace.

6. The work on "eID Interoperability for pan-European e-government services (PEGS)" carried out by the European "Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens" (IDABC) programme was particularly useful to complement information provided by European countries.

7. Several European countries mentioned the EU STORK project as a key initiative in this area.

8. In Japan, the Government has just begun to explore the possible development of an IT strategy including the establishment of an identity and of a numbering system to support electronic government.

9. There is a possibility that this consideration results from a bias in the way the questionnaire was circulated within the governments. This may also be a consequence of the fact that most countries follow a migration strategy where the ministry of interior keeps for the electronic national identity card the responsibility that it had for the paper-based national identity card and where responsibility and leadership for the electronic aspects are in the hands of the ministry whose objectives are served by the electronic features (*e.g.* e-government).

10. For more details, see the country summary for Korea in Annex 1. The Korean strategy also includes the promotion of the use of PKI with a public sector infrastructure and measures to encourage the private sector PKI market.

11. Denmark plans to extend its single sign-on solution to private sector services in the future, and at least to semi-public organisations (Railways) and general practitioners in 2010.

12. Often called "qualified digital signature" or "secure electronic signatures".

13. Respectively myhelp.gv.at and www.borger.dk.

14. An electronic identity card is also under consideration in The Netherlands.

15. It might however be possible that other government agencies than those involved in digital identity management are actually undertaking planning for or implementing significant business transformation that is reliant on the identity management strategy. This survey has not explored this dimension.

16. Such an assessment, or the methodology for such an assessment, would extend far beyond the scope of this study.

17. See country summary.

References

This section lists references cited by responding countries and other resources used by the Secretariat to prepare the report in addition to countries' responses to the OECD questionnaire.

- OECD (2007), "OECD Recommendation of the Council on Electronic Authentication and Guidance for Electronic Authentication", *www.oecd.org/document/7/0,3343,en_2649_34255_38909639_1_1_1_1,00.html*

European Union

- "eID Interoperability for PEGS", IDABC - *http://ec.europa.eu/idabc/en/document/6484*
- "Study on eID Interoperability for PEGS: Update of Country Profiles. Analysis & assessment report", IDABC, October 2009, - *http://ec.europa.eu/idabc/servlets/Doc?id=32521*
- "National e-ID card schemes: A European overview", Siddhartha Arora, information security technical report, Volume 13, Issue 2, May 2008, Pages 46-53.
- STORK programme - *www.eid-stork.eu*

Australia

- National Identity Security Strategy (NISS), *www.ag.gov.au/identitysecurity*
- Vanguard Secure e-Authentication Services, *http://vanguard.business.gov.au*
- Standard Business Reporting Program (SBR), *www.sbr.gov.au*
- Australian Government Online Service Point (AGOSP), *www.finance.gov.au/e-government/service-improvement-and-delivery/agosp.html*

- Office of the Privacy Commissioner's Guidance on PKI, *www.privacy.gov.au/materials/types/download/8809/6609*
- DVS Privacy Impact Assessments, *www.ag.gov.au/www/agd/agd.nsf/page/crimeprevention_identitysecurity*
- Australian National E-Authentication Framework, *www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html*
- Australian Government Cyber Security Strategy, *www.ag.gov.au/cybersecurity*.
- Gatekeeper Public Key Infrastructure (PKI) Framework, *www.finance.gov.au/e-government/security-and-authentication/gatekeeper/*

Austria

- "Austrian Country Profile - eID Interoperability for PEGS: Update of Country Profiles Study", IDABC, July 2009 - *http://ec.europa.eu/idabc/servlets/Doc?id=32296*
- "Giving an Interoperable Solution for Incorporating Foerign e-IDs in Austrian e-government", IDABC Conference 2005, 18 February 2005, Thomas Rössler, A-SIT - *http://ec.europa.eu/idabc/servlets/Doc?id=19404*
- "The Austrian Citizen Card - Concept and Cross-Border Approach", Herbert Leitold, A-SIT, London 20 April, 2006 - *https://online.tu-graz.ac.at/tug_online/voe_main2.getvolltext?pDocumentNr=43021*
- "Best Practice Catalogue - eGovernment in Austria", Federal Chancellery, 7/2008 *www.digitales.oesterreich.gv.at/DocView.axd?CobId=33428*
- Citizen Card Web Site - *www.buergerkarte.at/en*
- e-government portal - *http://help.gv.at and MyHelp.gv.at*
- Legal framework of eGovernment in Austria - *www.digitales.oesterreich.gv.at/site/6514/default.aspx*
- "Decree of the Federal Chancellor laying down conditions for equivalence under Section 6(5) of the E-government Act (E-government Equivalence Decree)" *http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=pisa_notif_overview&iYear=2009&inum=624&lang=EN&sNLang=EN*

- "Open source platform des Digitalen Österreich" - *http://egovlabs.gv.at* (in German)
- Centrum für sichere Informationstechnologie - Secure Information Technology Center *www.a-sit.at/de/allgemein/asit_en.php* (in German)
- Service center for citizens - *www.digitales.oesterreich.gv.at/site/6469/default.aspx* (in German)

Canada

- Pan Canadian Strategy for Identity Management and Authentication - *www.cio.gov.bc.ca/idm/idmatf/default.asp*
- Access Key - *https://cledacces-accesskey.gc.ca/a/eng/mc/*
- Provinces single sign-on interfaces:
  - British Columbia BCeID- *https://www.bceid.ca/*
  - Ontario One-key Service - *https://www.iaa.gov.on.ca/iaalogin/IAALogin.jsp*
  - Québec ClicSÉQUR *www.rrq.gouv.qc.ca/en/services/services_en_ligne/utilisation_securite_services/identification/Pages/clicsequr.aspx*
- Canadian Laws and Government policies, directives and standards:
  - Policy on Government Security- *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text*
  - Directive on Identity Management- *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577&section=text*
  - Federal Privacy Act- *http://laws-lois.justice.gc.ca/eng/P-21/index.html?noCookie*
  - Directive on Social Insurance Number *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342&section=text#cha5*
  - Operational Security Standard *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328*
  - Policy of Privacy Protection - *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text*

- Policy on Management of Information Technology *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755*
- Management Accountability Framework- Treasury Board Secretariat - *www.tbs-sct.gc.ca/maf-crg/index-eng.asp*
- Personal Information Protection and Electronic Documents Act (PIPEDA) *http://laws.justice.gc.ca/en/P-8.6/index.html*
- C-29 Safeguarding Canadians' Personal Information Act *www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4547739*
- Privacy Impact Assessment Policy - *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text*
- Guidelines for Privacy Breaches - *www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint-eng.asp*

Denmark

- "Danish Country Profile - eID Interoperability for PEGS: Update of Country Profiles Study", IDABC, August 2009- *http://ec.europa.eu/idabc/servlets/Doc?id=32303*
- "Digital Signature", National IT and Telecom Agency - *http://en.itst.dk/it-security/digital-signature*
- "eID/Authentication/Digital Signatures in Denmark", 8 July 2008, Nikolas Triantafyllidis / Charlotte Jacoby, Ministeriet for Videnskab Teknologi og Udvikling *www.open-standaarden.nl/fileadmin/os/presentaties/Kop08_pres_TriantafyllidisJacoby.pdf*
- "PKI for e-Gov. Experiences from Denmark", Allan Fisher-Madsen, Devoteam Consulting *www.arpt.dz/Docs/3Actualite/Communication/8-9_12_2009/Communications/Session2/S2P1eng.pdf*
- "eID and Authentication. Presentation for Forum Standaardisatie", Mikkel Hippe Brun, Center for Service Oriented Infrastructure, Danish National IT and Telecom Agency, Copenhagen, 8 July 2008 - *www.open-standaarden.nl/fileadmin/os/presentaties/Kop08_pres_HippeBrun.pdf*
- E-government portal - *http://borker.dk*

- EasyLog-In, ePractice.eu - *www.epractice.eu/en/cases/easylogin*
- EDAG3 - eDay 3 http://modernisering.dk/da/projektside/andre_projekter/edag3/ (in English) and *www.itst.dk/it-sikkerhed/digital-signatur* (in Danish).
- Danish Strategy for Single Sign-on for Public Web Sites- *www.modernisering.dk/da/projekter/brugerstyring/* (in Danish)
- Recommendations for guidelines for cross governmental IdM – roadmap and concept *http://modernisering.dk/fileadmin/user_upload/documents/Projekter/Brugerstyring/Retningslinjer_tvaeroffentlig_brugerstyring_1.0.pdf* (in Danish)
- OCES Certifikatpolitikker - *https://www.signatursekretariatet.dk/certifikatpolitikker.html* (in Danish)
- Netsafe Now! Campaigns - *http://en.itst.dk/it-security/netsafe-now-campaigns*
- NemLog-In and NemID disclaimers - *https://login.sikker-adgang.dk/fobslogin/visvilkaar.do* (in Danish)
- Danish Data Protection Agency's guidelines to be used if data is involuntarily published on the Internet - *www.datatilsynet.dk/erhverv/internettet/utilsigtet-offentliggoerelse/* (in Danish)

Germany

- "eID Interoperability for PEGS: Update of Country Profile study: German country profile", July 2009 - *http://ec.europa.eu/idabc/servlets/Doc?id=32302*
- "Abstract of the Core Concepts of S.A.F.E.: Standards for Federated Identity Management", *www.deutschland-online.de/DOL_Internet/binarywriterservlet?imgUid=d8710643-fa8a-9b11-d88e-f1ac0c2f214a&uBasVariant=22222222-2222-2222-2222-222222222222*

Italy

- "eID Interoperability for PEGS: Update of Country Profile study: Italy country profile", July 2009 - *http://ec.europa.eu/idabc/servlets/Doc?id=32311*

- "Rapporto eGov Italia 2010", December 2010, Minister for Public Administration and Innovation, *www.innovazionepa.gov.it/comunicazione/notizie/2010/dicembre/20122010-brunetta-rapporto-e-gov2010.aspx*

Japan

- The Realization of a Citizens-Oriented e-government of the New Information and Telecommunications Technology Strategies, Cabinet Decision of 11 May, 2010, *www.kantei.go.jp/jp/singi/it2/* (in Japanese)
- Promotion of the Utilization of Information and Telecommunications Technology in the New Growth Strategy - the Scenario for Restoring (a Vital Japan). Cabinet Decision of 18 June 2010, *www.kantei.go.jp/jp/singi/it2/denshigyousei/dai1/gijisidai.html* (in Japanese).

Korea

- Korea National PKI Status and Directions for Market Promotion, March 2009, JinSoo Lim, Korea Certification Authority Central, KISA *www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/vietnam09-tas/pdf/Doc7_Lim_PKI_kisa_korea.pdf*
- "The PKI Status of Korea and Cases of PKI Construction in Global Area", 8 November 2007, Korean Information Certificate Authority Inc. *www.apkic.org/WebSite/PKI2007/UpFile/File28.ppt*
- "Understanding Korea's Identity Verification System", Byeong Gi Lee, Commissioner, Korea Communications Commission, December 2009, *http://121.254.145.213/gisa_down.php?pfile=%2Fdata1%2Fftp%2Fgisa_download%2F20091206_%C2%FC%B0%ED%C0%DA%B7%E1_Identity+Verification+System+2009.12.+BGL.doc*

Luxembourg

- "eID Interoperability for PEGS: Update of Country Profile study: Luxembourg country profile", July 2009 - *http://ec.europa.eu/idabc/servlets/Doc?id=32283*
- LuxTrust web site. *https://www.luxtrust.lu*.

Netherlands

- "The Netherlands Country Profile - eID Interoperability for PEGS: Update of Country Profiles ", IDABC, July 2009 - *http://ec.europa.eu/idabc/servlets/Doc?id=32286*.
- "Presentation of DigiD" - *www.digid.nl/english*
- "DigiD", presentation by Gerrit Jan van 't Eind from ICTU at the 19th WPISP meeting on 4 October 2005
- "List of public sector services using DigiD" - *www.digid.nl/burger/over-digid/wie-doen-mee/*
- "The personal records database: for the authorities and for you. The Municipal Personal Records Database", Ministry of the Interior and Kingdom Relations *www.bprbzk.nl/dsresource?objectid=19176&type=org*
- "Bergerservicenummer - Frequently Asked Questions" - *www.burgerservicenummer.nl/veelgestelde_vragen/english_faq*
- "eRecognition for Companies" *www.eoverheidvoorbedrijven.nl/afsprakenstelseleherkenning/english/english.html*

New Zealand

- Identity Assurance Framework - *www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Publications-Identity-Assurance-Framework*
- E-government Interoperability framework - *www.e.govt.nz/standards/e-gif-3.3*
- Igovt Web site: *www.i.govt.nz*.
- Evidence of Identity Standard - *www.dia.govt.nz/Resource-material-Evidence-of-Identity-Standard-Index*
- Government Communications Security Bureau, NZ ICT Security Manual, February 2008 - *www.gcsb.govt.nz/newsroom/nzsits/nzsit-402-feb08.pdf*.
- Cross-Government Biometrics Group, Guiding Principles for the Use of Biometric Technologies for Government Agencies, April 2009. *www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Guiding-Principles-for-the-Use-of-Biometric-Technologies-Index*

- Office of the Privacy Commissioner Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist, Wellington, February 2008. *www.privacy.org.nz/privacy-breach-guidelines-2*

Portugal

- "eID Interoperability for PEGS: Update of Country Profiles study. Portuguese country profile. July 2009", IDABC - *http://ec.europa.eu/idabc/servlets/Doc?id=32289*
- "The Portuguese Citizen Card", Gonçalo Caseiro, presentation at the 16 Porvoo Group meeting, March 2010 *www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/9875BE23F60FBEB2C2257700001C21FF/$file/Portuguese_Citizen_Card.pdf*
- Cross-border digital signature in Portugal and Estonia (video) - *www.youtube.com/watch?v=4hNg5i4i3oU*
- "Portuguese Citizen Card", Maria Manuel Leitão Marques, 2007, *www.mj.gov.pt/sections/informacao-e-eventos/presidencia-portuguesa/ficheiros9831/maria-leitao-marques/downloadFile/file/e-IDCard_ejustice_final_-_maria_manuel.pdf?nocache=1191117229.93*
- Decree-Law 116-A/2006, Establishing the State's Electronic Certification System - Public Key Infrastructure and appointing the National Safety Authority as the national accreditation authority *www.anacom.pt/render.jsp?contentId=981438*
- "One stop shop. Easier, faster and cheaper. The Portuguese Experience", Luis Goes Pinheiro, 11 March 2010. - *www.oecd.org/dataoecd/55/62/44796252.pdf*

Slovenia

- "eID Interoperability for PEGS: Update of Country Profiles study. Slovenian country profile. July 2009", IDABC- *http://ec.europa.eu/idabc/servlets/Doc?id= 32292*

Spain

- "eID Interoperability for PEGS: Update of Country Profiles study. Spanish country profile. July 2009", IDABC - *http://ec.europa.eu/idabc/servlets/Doc?id=32280*
- DNI Electronico Web Site - *www.dnielectronico.es*

- "A new e-ID card and online authentication in Spain", Alexander Heichlinger and Patricia Gallego, *Identity in the Information Society*, Volume 3, Number 1, p.43-64 *www.springerlink.com/content/317530p4l1w00453/*
- "@firma – National Validation Authority for eID and eSignature Serv", 2010 *www.epractice.eu/en/cases/afirmaawards*

Sweden

- "eID Interoperability for PEGS: Update of Country Profiles study. Sweden country profile. July 2009", IDABC - *http://ec.europa.eu/idabc/servlets/Doc?id=32291*
- "Electronic Identity Management in Sweden: Governance of a Market Approach", Åke Grönlund, in « Identity in the Information Society », vol. 1/ 2008, vol. 3/2010, ISSN 1876-0678 *www.springerlink.com/content/m87277n29126411u/fulltext.pdf*
- "This is BankID", *www.bankid.com/en/What-is-BankID/*
- "BankID in Sweden. A National Identity and Security Infrastructure". Porvoo Meeting, 10 March 2008 *www.vaestorekisterikeskus.fi/vrk/fineid/files.nsf/files/205328912CB64B84C22574420041C356/$file/27_update_sweden.pdf*

Turkey

- "eID Interoperability for PEGS: Update of Country Profiles study. Turkey country profile. July 2009", IDABC - *http://ec.europa.eu/idabc/servlets/Doc?id=* 32294
- "The Central Civil Registration System (MERNIS)", 17 February 2009 *www.nvi.gov.tr/English/Mernis_EN,Mernis_En.html*
- "The Identity Information Sharing System", 12 February 2009 *www.nvi.gov.tr/English/KPS_EN,KPS_EN.html*
- "Information Society Strategy 2006-2010". State Planning Organisation. July 2006. *www.bilgitoplumu.gov.tr/Documents/5/Documents/060700_InformationSocietyStrategy.pdf*
- "Communiqué on Processes and Technical Criteria Regarding Electronic Signatures", Official Gazette ref 25692, 6 Janvier 2005. *www.tk.gov.tr/eng/pdf/Communique_on_Electronic_Signature.pdf*

United States

- "Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009 *www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*
- "National Strategy for Trusted Identities in Cyberspace. Creating Options for Enhanced Online Security and Privacy", Draft, 25 June 2010 - *www.dhs.gov/xlibrary/assets/ns_tic.pdf*
- "Identity Management Task Force Report 2008", National Science and Technology Council (NSTC) - *www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf*
- "Report to the President on Identity Management Strategy", National Security Telecommunications Advisory Committee (NSTAC), 2009 *www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf*
- "Federal Identity, Credential, and Access Management (FICAM), Roadmap and implementation Guidance", CIO Council, version 1.0, 10 November 2009 *www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf*
- Federal Information Security Management Act (FISMA) - *http://csrc.nist.gov/drivers/documents/FISMA-final.pdf*
- NIST Standards
  - "Electronic Authentication Guideline", NIST SP-800 63, April 2006 *http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf*
  - "Recommended Security Controls for Federal Information Systems", NIST 800-53, Revision 2 *http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf*
  - "Guide for the Security Certification and Accreditation of Federal Information Systems", NIST SP 800-37 *http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf*

Other

- Kantara Initiative - *http://kantarainitiative.org/*

Appendix I

Country summaries

This appendix includes summaries of countries' responses to the Questionnaire on National Strategies and Policies for IdM in OECD countries circulated in November 2009[1]. It also includes information from additional research made by the Secretariat.

Australia

The Australian National Identity Security Strategy sets standards for identity security in areas such as enrolment, document security and electronic authentication, and it establishes a real-time Document Verification Service (DVS) whereby agencies across jurisdictions can check the validity of documents presented by clients as proof of identity documents in real-time. The Australian Strategy is based on a decentralised registration policy where each agency is responsible for managing its own identity system. Several components of the strategy have been developed (*e.g.* guidance for identity data integrity) or implemented but not yet fully rolled out throughout all government agencies. To support interoperability, agencies are encouraged to follow a National e-Authentication Framework. The Australian Government has also agreed to a lead agency model for the provision of authentication services to government agencies. Single sign-on to e-government services is also being developed. Security and privacy are addressed through the Australian Government's Cyber Security Strategy and via existing legislation such as Australia's privacy legislation. In lack of a national identifier, the development of an alternative registration mechanism is considered as a key challenge.

National strategy for IdM

In 2007, Australia initiated a comprehensive whole-of-government cross-jurisdictional effort to develop and implement a National Identity Security Strategy. The Strategy is based on the recognition that false, stolen and multiple identities can underpin terrorist and criminal activity or under-

mine border and citizenship controls. The Strategy aims to develop standards for registration and enrolment, security for proof of identity documents, integrity of identity data, electronic authentication and biometric interoperability.

A key component of the Strategy is the development and implementation of a national Document Verification Service (DVS), a secure electronic, online system that can be used to check the validity of documents presented by clients as proof of identity documents in real-time. The DVS enables government agencies to check if a document has been issued by the issuing agency, if the details recorded on the document correspond to those held in the issuing agencies register, if the document is still valid (*i.e.* has not been cancelled or superseded), and if it has not been lost or stolen. The DVS may provide a useful tool to facilitate online enrolment.

The Strategy benefits from high-level leadership. It was adopted by the Council of Australian Governments, an entity chaired by the Prime Minister which comprises State Premiers, Territory Chief Ministers and the President of the Australian Local Government Association and which initiates, develops and monitors the implementation of policy reforms that are of national significance and require co-operative action by Australian governments.

The Australian strategy is based on a *decentralised registration policy*: there is no unique national identifier for Australian citizens, identity credentials are issued for specific purposes by each agency. Agencies are encouraged to follow a National e-Authentication Framework. The Australian Government has also agreed to a lead agency model for the provision of authentication services.[2] The current approach focuses on face-to-face enrolment with some services available online following registration.

Single sign-on to enable access by citizens to multiple government Web sites without repeatedly signing in is envisaged as part of the Australian e-government Strategy to access Federal Government Information and Services. This is to be available via australia.gov.au, the main gateway to government information across jurisdictions.

With respect to *relationships between the public and the private sectors*, on one hand, the DVS has been designed to be accessible by Australian Government, State and Territory agencies, and potentially by the private sector. On the other hand, and in the context of the above-mentioned lead agency model, two interrelated initiatives have been launched to enhance the security, simplicity and cost-efficiency of business to government transactions:

- Australia's Standard Business Reporting (SBR) program is a multi-agency initiative involving 12 federal, state and territory government authorities, principally revenue agencies. SBR was developed to simplify business-to-government reporting by using business software. The SBR program automatically pre-fills forms, provides a common reporting language based on international standards via a single secure online sign-on for users to all agencies involved.

- The VANguard platform, supported by the Department of Innovation, Industry, Science and Research has been developed to improve security of business to government transactions. The platform acts as a trust broker between business and government agencies to conduct transactions securely via a single entry point. VANguard allows business users to conduct transactions with multiple government agencies across jurisdictions using a single digital credential and it reduces the development and operational cost for each government agency of a dedicated identity silo, including for example PKI. This is largely achieved through the use of a range of digital credentials including Australian Taxation Offices' certificates. VANguard provides trust broker services for Australia's SBR.

Implementation of the strategy

A governance framework was set up to guide and develop the Strategy and the National Identity Security Co-ordination Group (NISCG) consisting of representatives from central agencies of the Australian and State and Territory governments, the Council of Australasian Registrars for Births, Deaths and Marriages, Austroads and the Privacy Commissioner was established as a high level group to co-ordinate and implement the National Identity Security Strategy.

Following a successful trial in 2006, the DVS is being progressively implemented, with more agencies planning to start using it in 2009-2010. Currently, passports, visas and drivers licenses are among the types of documents that can be verified using the DVS.

Interoperability of IdM systems is not a legal obligation in Australia. Future developments are likely to encourage interoperability through the use of international standards.

The 2008 *National e-Authentication Framework* promotes the use of secure and interoperable electronic credentials in citizen and business-to-government transactions and aims to assist agencies, jurisdictions and sectors in authenticating the identity of the other party to a desired level of assurance or confidence. This includes the deployment of electronic

credentials that are mutually compatible and conform to industry standards. The framework provides guidance on developing the processes and technology required to provide the desired level of confidence within the broader context of an agency's approach to identity and risk management. It does not mandate any particular approach but encourages interoperable e-authentication mechanisms so that individuals can expect similar authentication processes for transactions with similar assurance levels across all three tiers of government within Australia.

Federal agencies seeking to establish new online authentication capacity are required to use, unless a sound business case is made out, the authentication infrastructure of designated lead agencies for government to government, business to government, or "people to government" authentication. This is aimed at ensuring that costs both for government and non-government users are contained through better use of infrastructure and greater interoperability of systems.[3]

Information security and privacy are important themes in the Australian IdM Strategy. There are no specific instrument to address this. Rather, information security is mainly addressed through the broader 2009 Cyber Security Strategy and Government agencies are subject to various legislative and administrative requirements with respect to both security and privacy. Australian government agencies are also required to comply with various government standards such as the Protective Security Manual and the Australian Government Security Manual. The security of personal data is also regulated by the Privacy legislation.

In addition to threat and risk assessments carried out by security specialists, the security of IdM systems can be audited (*e.g.* by Federal, State and Territory Auditors-General).

Privacy Impact Assessments are undertaken by government agencies, following guidance issued by the Office of the Privacy Commissioner (now the Office of the Information Commissioner). The Office has also issued guidance related to privacy and PKI. For example, a Privacy Impact Assessment (PIA) developed with the assistance of the Office has guided the development of supporting processes and frameworks of the DVS. The system was designed to optimise privacy protection: requests to verify a document are encrypted and sent via a secure communications pathway through a "DVS hub" to the document issuing agency. No personal data is transferred from the document-issuing agency: the DVS only returns to the querying agency a "yes" response if the document matches information held by the issuing agency or a "no" response if the document details were not validated.[4]

There is no policy in Australia with respect to proportionality between the amount of personal information collected and the level of assurance required in determining the appropriate level of authentication.

Australia's identity management arrangements allow for the use of pseudonyms to protect the identity of certain persons such as the victims of domestic violence, those on witness protection programmes and law enforcement officers working under assumed identities.

Australia's Gatekeeper PKI Framework provides standards for the collection of personal information related to the issuance of digital certificates to individuals – where those digital certificates will provide a medium level of assurance. The National e-Authentication Framework provides a level of detail on the evidence of identity requirements based on risk for different levels of assurance.

There is no centralised policy with regards to identity attributes: each agency issues credentials to enable clients to access its services. Face-to-face enrolment is generally used for higher value services. Voice recognition is available on an opt-in basis by the agency facilitating social security services.

A set of *user awareness and education* initiatives within the framework of the Cyber Security Strategy promote online secure practices and encompass the benefits and risks of various identity management approaches. An *ID Theft Booklet* released by the federal Attorney-General's Department also helps to raise awareness of risks and benefits of Australia's identity management system by informing Australians about preventing and responding to identity theft. There are no specific obligations in Australia to inform clients or customers of incidents where there has been a loss or corruption of identity data or other data breaches. The Australian Government is, however, considering a recommendation of the Australian Law Reform Commission relating to data breach notifications.

Challenges

- In lack of a single national identifier, a key challenge is how citizens (and others) might enrol online to access services and benefits with an acceptable level of confidence about a person's identity. One issue to be addressed is to what extent information, including that relating to transactions, might be utilised to enable greater confidence in claims about identity. Australia's DVS may provide a useful tool in this regard and help to facilitate online enrolment.

Austria

The national IdM strategy provides a framework that enables public and private bodies to develop "Citizen Cards" that individuals can use as a means for qualified electronic signature, sector-specific identification and representation. Citizen Cards are issued by various bodies and can be used in public and private sector contexts. The framework is based on a centralised registration policy relying on national identifiers but includes robust privacy protection technical measures that prevent linkability based on the identifier. The IdM strategy also includes single sign-on to e-government services.

National strategy for IdM

In 2004, Austria introduced a comprehensive digital IdM strategy called "Citizen Card". Rather than a specific token, the Citizen Card is a technology-neutral framework which defines minimal requirements that a digital identity token needs to fulfill to provide a secure and privacy-friendly signature-creation device that enables *i) qualified electronic signature*; *ii)* "sector-specific" *identification* (see below); and *iii) representation,* whereby the holder can optionally carry out legal transactions on another person's behalf.

"Citizen Card" tokens can be considered as universal credentials that can be used in public and private sector contexts, issued by public and private sector providers and based on different technical solutions. Citizen Card tokens also enable single sign-on to public sector online services through *help.gv.at*, a one-stop shop to public administration online services.

Austria's IdM strategy is based on a:

- *Centralised registration policy* relying on the Central Resident Register (and Supplementary Register for non-residents) established in March 2002 which provides a unique number to all Austrian residents. Resident registers existed prior to 2002 but were kept by municipalities,
- Public Key Infrastructure (PKI).

The Austrian IdM strategy takes *privacy protection as a core design concept* at the legal, technical and procedural/operational level.

Implementation of the strategy

Citizen Card tokens are available as health insurance cards, civil servant service cards, mobile phones, professional cards such as notaries and pharmacists', student service cards and bank cards. Many national, regional and local applications require the use of a citizen card token (*e.g.* for e-reporting of certain crimes, application and access to pension records and child allowance, health insurance information, registration of a business, etc.) or support its use together with other methods (*e.g.* for tax declaration, e-banking, social security). The tokens can also be used for e-authentication in e-business contexts, to prevent tampering with electronic invoices, and to encrypt and sign personal documents.

In general, electronic identity tokens in Austria are prepared for being activated as a Citizen Card but the Citizen Card functionality has to be voluntarily activated by the holder, a process through which the actual user identity data is written on the token. The registration process requires personal appearance, for example at a registration office or at a post office upon reception of a personal registered letter containing an activation code. Where a trustworthy identity has already been established for an online application, this identity data can be used to register a Citizen Card without the need for the signatory to appear again personally. For example, citizens already registered at the TaxOnline application do not need to personally appear or be identified via a registered letter again to register a citizen card.

Identity data provided in the token includes a qualified certificate, a PIN derived from the Central Resident Register (CRR) signed by the Government as being linked to the individual, the name and date of birth of the individual and, optionally, data related to an electronic mandate provided to the holder by another individual. The qualified certificate enables authentication, the "identity link" enables unique identification.

Single sign-on is provided through the National Portal for e-government[5] where individuals using their Citizen Card token have access to personalised government services (*e.g.* taking into account their profession, marital status, region, etc.), an electronic Safe for private documents, a reminder service and electronic delivery services. Stored data is protected but can be released to specific applications to generate pre-filled forms.

The Austrian Strategy for IdM is supported by a legal framework which includes the E-government Act, e-government sector regulation, the Electronic Signature Law, regulation of the use of the Central Resident Register identifier, etc.

The Citizen Card concept is expected to facilitate the use of modern e-government services and to enable other innovative solutions and developments. Innovative IdM developments in Austria include qualified signatures based on a mobile phone which offer a comfortable alternative to smartcards. This project is a component of the European STORK project, to which Austria is a leading contributor, and which aims to establish a European electronic ID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national electronic ID.

The *security and privacy policy* of the Citizen Card framework aims to establish trust in the Citizen Card system and privacy has been addressed as a core design principle. The policy is based on a mix of legal (mentioned above) and technical measures that provide a strong protection to the CRR number and prevent public sector bodies to use, store and share the same identifier in their database across government sectors.[6] Concretely, the CRR number itself is never exposed. For the same individual, each organisation uses a different identifier cryptographically derived from the CRR number. This mechanism reduces complexity and cost as it is based on the central population register and avoids the multiplication of silo-based registration schemes. Moreover, it protects the "parent" national identifier (never exposed) and provides more protection to individuals against identity fraud by enabling the revocation of its encrypted "children" and the issuance of new ones, should encrypted identifiers be compromised. Finally, it technically prevents individuals to be matched across several organisations on the basis of their identification number (unlikability). Finally, a legal framework provides additional protections, for example by creating 26 public administration sectors which have to use different "child" identifiers.

In addition, the supervision of the main components of the framework is carried out by *i)* the Austrian Data Protection Commission which plays a critical role at the core of the system by operating the register of PINs (sourcePIN); *ii)* the Austrian GovCERT, operated by the department for Federal ICT Strategy of the Federal Chancellery, also responsible for the Citizen Card, which manages security breaches and cases of e-ID theft, analyses incidents and takes appropriate measures; *iii)* the telecommunications regulator (Telekom Control Commission) which supervises the qualified signature framework. These bodies are all subject to regular internal and external audits.

Finally, many Government Web sites as well as private organisations raise awareness about the Citizen Card. Specific information and assistance is provided by a Web site[7], on the e-government portal as well as by telephone and at a dedicated "brick and mortar" information center[8]. Individuals are informed about the process to revoke their token at the time of issuance.

Challenges

A key challenge for the development of the strategy is the mode of co-operation between all stakeholders involved in the Strategy as all levels of the public administration as well as private sector participants have a role to play and no one is in a position to provide binding instructions to the others. In 2005, the Federal Platform Digital Austria was founded to help co-ordinate a uniform e-government strategy. The platform involves public administration bodies at all levels, *i.e.* federal, provincial, municipal and local levels as well as businesses. All projects, strategies and guidelines, including the IdM strategy, are collectively planned, discussed, agreed and implemented in a co-operative and voluntary manner. This is a key success factor for Austrian e-government initiatives. As there is no national authority which has the competence to give binding instructions to all of the involved institutions, co-operation takes place on a voluntary basis, and recommendations from the Platform have therefore to be agreed upon during in-depth discussions amongst all stakeholders.

The main implementation challenges include interoperability, in particular at the cross-border level, as well as usability and acceptance issues:

- To facilitate technical interoperability, the government promotes the use of widely adopted standards and provides open source modules to be integrated to online applications[9]. Use of foreign electronic ID is possible in Austria if "the application is provided with a qualified electronic signature which is linked to an equivalent electronic verification of that person's unique identity in his or her country of origin." Tokens of eleven countries have been decreed by the Federal Chancellor as electronic IDs equivalent to a Citizen Card token. Austria's participation in the European STORK project aims to address issues related to cross-border interoperability, in particular where e-IDs are not based on qualified signatures[10].
- To increase usability, the Austrian solution is based on technologies that do not require users to install software on their computer, a important point for individuals who do not use their card often.

Canada

The Pan-Canadian IdM Strategy focuses on the multi-channel delivery of government services across all layers of government ("jurisdictions"). It is based on a decentralised registration policy and on a federated trust model where participants keep the maximum operational autonomy. The nature and provision of credentials is fully decentralised. Single sign-on will be provided on the basis of federation agreements. Canada has also established a National Committee on Identity Management with public and private players currently focusing on standards and which could potentially address other aspects in the future. Most of the characteristics of and challenges raised by the strategy's implementation policies are related to the decentralised nature of the Pan-Canadian IdM Strategy: the interoperability of credentials within and across public and private sector IdM systems is based on federation agreements; IdM frameworks operate under existing legal requirements (*e.g.* on privacy); each institution is responsible for the type of credential, for the choice of identity data to be used, of the level of assurance to be provided, as well as for the information provided to users regarding benefits, risks and incidents. Challenges relate to inconsistencies across the various jurisdictions regarding legal requirements, languages and accessibility. Uncertainty with respect to business models for private sector use of the framework still needs to be addressed.

National strategy for IdM

The Canadian IdM strategy focuses on the *delivery of government services* at federal, provincial, territorial and municipal levels ("Pan-Canadian strategy")[11]. In contrast with the definition of IdM in the OECD Primer, the strategy covers offline and online identity management (*e.g.* multi-channel delivery of services including telephone, in person, Internet and mail). It aims to support a seamless and user-centric service delivery experience to citizens and businesses when they are interacting with all levels of government, where they can enjoy "simple, convenient and protected access to multi-jurisdictional (federal, provincial, territorial) services in a manner they choose and control" and where "all governments in Canada are trusted, collaborative leaders in citizen-centered service delivery".

The development of the strategy is the government's response to the multiplication of non-standard authentication frameworks implemented by various jurisdictions which creates obstacles for collaboration between them and increases cost. Expected benefits include convenient, secure and privacy-friendly access to services for users, maximized use of resources and improved efficiencies for participating organisations; reduced costs, improved transparency and increased client satisfaction for the Government.

The Pan-Canadian Strategy is based on a *decentralised registration policy,* where federated organisations trust each others' assurances of identity and operate in an environment that supports the use of client-chosen credentials provided by multiple providers across multiple jurisdictions, via multiple service delivery channels, irrespective of the technology used. Thus there is no centralised identity authority in Canada. The authority to identify individuals is prescribed by the legislative provisions that are specific to a jurisdiction or to a department responsible for administering the legislation (*e.g.* Canada Revenue Agency administering the federal Income Tax Act). The strategy is designed to work in the current legislative framework. The responsibility for identity management (and the relevant authorities) will continue to remain with the individual departments.

The strategy includes four major components: *i)* foundational elements to define key concepts (*e.g* assurance model, privacy code, trust model); *ii)* a framework defining a high-level structure and architecture as well as legal, privacy, security, identification trust and service experience requirements, *iii)* a service delivery component identifying pilot projects; and *iv)* a component supporting standards and guidelines.

The strategy addresses the separation of *credential assurance* from *identity assurance* that enables a phased incremental approach where a network of government organisations and commercial enterprises federate credentials in the shorter term and identity in the longer term; multiple levels of assurance; citizen-centric design based on a sufficiently large choice of credential service providers; risk based approach balancing the need to attract federation partners while mitigating the risks; cost efficiency; technology neutrality to enable credential providers to enter the federation regardless of the technology and to allow for the evolution of the technology; autonomy of identity and credential management services.

Single sign-on is also a key goal and will be enabled through the federation of credentials as issued by a provincial, territorial or federal jurisdiction and eventually commercial providers. Over the longer term, users will be able to use their credential of choice to enable single sign-on to access government services. Once a user's credential has been validated, it will be possible to redirect her seamlessly to other programmes or services without re-challenging her. As a result, once authenticated, she will be able to easily access services having the same assurance level or lower.

The strategy promotes the use of open industry standards within federation agreements to foster interoperability. It encourages competition within the industry to provide the most cost-effective solutions and stimulate innovation. For example, the government described, as a best practice (not

yet as a policy instrument), the interfaces between relying parties (such as departmental portals and applications) and credential assurance providers.

In addition to the Pan-Canadian Strategy, some departments of the federal Government have developed bilateral arrangements to harmonise existing methods of identity management. Access Key, a unique electronic credential that allows citizens to communicate securely with online enabled government programs and services, is a single sign-on approach used by some government programmes and services.

This strategy is currently being finalised, and its implementation is at a planning stage with the identification of pilot projects to test and demonstrate the concepts. Implementation is planned to be incremental.[12] The first phase focuses on the development of standards-based "anonymous" credentials at a given level of assurance (Level 2 or Level 3) and on the federation of credentials across jurisdictions.

In addition to the strategy described above, Canada has established a national committee on identity management (NCIM) which provides both public and private sector members with a forum to co-ordinate views/ comments feeding into international standards development (*e.g.* ITU, ISO), and exchange information and developments on identity management policy and standards-related issues. Going forward, it is expected that the Committee's work will evolve beyond standards in such a way that it will play a key advisory role in terms of the formulation of Canadian positions and input to policy-level work (domestic and international).

Implementation of the strategy

The government is developing a federation model that will enable multiple credential providers and acceptance of credentials from other authoritative parties such as federal government, provincial/territorial governments, municipalities, and commercial partners. This approach will enable private sector issued credentials to access public sector online services and vice-versa. However, various industry sectors (*e.g.* financial) have adopted proprietary and non-interoperable approaches to IdM. While there have been discussions aimed at pursuing a federated and co-ordinated approach within the private sector (including public/private sector partnerships), to date, none have led to any concrete outcomes.

There is no specific legislation for IdM in Canada. The strategy and its implementation is based on existing legislation, such as, for the private sector, the Personal Information Protection and Electronic Documents Act (PIPEDA), and for the public sector, the federal Privacy Act. Canada's

Criminal Code and its new identity-related offences is also an element of the legislative framework.[13]

A set of policies, directives and standards support security, privacy and interoperability of identity management between federal institutions. [14] One example is the Privacy Impact Assessment Policy[15] which requires that privacy principles are taken into account when there are proposals for, and during the design, implementation and evolution of programmes and services that raise privacy issues. Institutions must include the results of the Privacy Impact Assessment (PIA) in the body of the submission or the project brief, where applicable, to get the Treasury Board's approval for their project, including a summary of the actions taken or to be taken to avoid or mitigate the privacy risks, if any, as per the Privacy Impact Assessment. The use of PIAs in the private sector is recognised as a useful tool for the development of IdM systems although it is not a requirement under PIPEDA. Another example is the Directive on Identity Management[16] which addresses proportionality of the personal information collected and requires federal government departments to select "an appropriate set of identity data (such as personal attributes or identifiers) to sufficiently distinguish a unique identity to meet programme needs, which is proportionate to identified risks and flexible enough to allow for alternative methods of identification, when appropriate." It remains a departmental responsibility to define the necessary amount of personal information (*i.e.* identity data) and the level of assurance required. Finally, the Directive on Social Insurance Number which restricts the collection, use and disclosure of this identifier by a government organization is also relevant[17].

IdM systems will be monitored according to the Treasury Board Secretariat (TBS) Management Accountability Framework[18] which sets out the Treasury Board's expectations of senior public service managers for good public service management. Federal departments' performance would be monitored according to the requirements set out in the Directive on Identity Management.

It is the responsibility of each federal institution to inform users of the benefits and risks, and of any incidents, within the existing Policy of Government Security and Guideline for Privacy Breaches[19].

Challenges

The main challenges relate to inconsistencies between the various jurisdictions with respect to: *i)* legal issues regarding accountability, liability and privacy, as there is no broadly accepted framework that directly addresses identity management; *ii)* language requirements, as the federal government is required to use both official languages whereas not all

provinces have this requirement, leading to increased costs and non-compliance; and *iii)* accessibility and common look and feel across jurisdictions. Other challenges relate to cost, consistency of user experience, and the uncertainty of commercial business models which are compounded by unresolved legal issues related to accountability and liability. Finally, there are challenges associated with the need for many levels of stakeholder involvement in the development of the most appropriate standards and technologies.

Chile

The IdM strategy of Chile is based on the migration of the current paper based national identity card to an electronic card[20]. The planned card is seen as a driver for innovation. The current practice relies on the wide use by public and private sector bodies of a national identity number established in 1969, originally for tax purposes. Electronic authentication based on this number associated to a password is common practice in Chile. In the health sector, biometric fingerprint identification is also available although not extended to the whole health system.

National strategy for IdM

The Civil Registry and Identification Service (SRCeI), within the Ministry of Justice, is responsible for the management of identification data.

The planned electronic identity card is seen as a driver for innovation. For example, although no decision has been made regarding such potential innovations, it could carry medical data or be used as a payment mechanism (*e.g.* in the public transport system). The government is also considering adding digital certificates for electronic authentication in the card. Finally, single sign-on is also envisaged for transactions with the public sector.

The strategy envisions the use of the citizen identification as the sole input, to access any government information thanks to the planned enhanced interoperability of public agencies information systems. The Civil Registry and Identification Service joined the "Platform for Interoperability of State" Project which is working to standardize the use of data and metadata and which fostered the use of digital certificates for authentication across public services.

As regards security, a specific regulation for Information System Security[21] is in place and an Information System Security Regulation led by Ministries of Internal Affairs and Finance and which will include IdM, is being deployed at the government level. A security committee, chaired by the Director of SRCeI, defines rules and security audits applied to the

management of identity data. Additionally electronic signature certificates are used for the operation of the service.

The law that created the SRCeI includes safeguards to protect personal data. A privacy policy defined in the organic law of SRCeI and by the Security Committee details measures to ensure the protection of personal data. Nevertheless, no agency is responsible for the enforcement of privacy protection in the context of IdM. An amendment to the Transparency Law is being discussed in Parliament to entitle the Transparency Council to ensure the protection of personal data. In practice, the SRCeI never delivers data to public or private institutions but rather provides validation to queries. For example, the SRCeI validates (or not) queries from the Health System about names and data from beneficiaries by sending simple positive or negative responses. Each public or private sector body define their own privacy policy.

Finally, the government recognises the need for public awareness in the context of the deployment of the planned electronic identity card.

The main challenges of identity verification systems in electronic forms are not technical, since this is a problem largely solved by the industry. The Civil Register and Identification Service is capable of providing electronically, for example based on a fingerprint, the match score of that fingerprint compared to the one stored. It is up to the receiving end to determine whether the match is acceptable or not. However, current implementation systems imply a latency exceeding the standards of current banking systems.

Challenges

The main current challenge is the incorporation of enhancements to the identity card and passport. These include improving safety standards and the incorporation of a chip including both a protected area and an open area where personal data could be stored. The new identity card is expected to be operational by 2012.

Denmark

The Danish IdM strategy aims to provide individuals with digital credentials for public and private sector online transactions as well as single sign-on for e-government services, possibly extended to private sector organisations in the future. It is based on a centralised registration policy for digital credentials.

National strategy for IdM

The Danish IdM Strategy aims to provide individuals, businesses and public authorities with digital credentials for secure identification, digital signature and secure email in public and private sector online contexts, including for access to web-based public sector services and all Danish banks (EasyID, or NemID in Danish). It also includes a single sign-on solution for public sector Web sites (EasyLog-In, or NemLog-In in Danish).

NemID relies on a *Public Key Infrastructure* built upon a *centralised registration policy*: identification is based on a unique personal number assigned to all inhabitants in Denmark by the national central personal register which has existed since 1968. Denmark does not have an identity card tradition but uses a combination of social security card and driver's license, passport or banking card[22]. Thus, the framework does not aim to establish a national electronic identity card but provides an infrastructure for standardized and secure digital certificates that can be kept centrally in hardware, on a USB token or on a smartcard. The certificate contains the name of the person and a reference to the person's personal identification number. NemID digital certificates are provided for free to all citizens and for the first three employees in enterprises.

NemLog-In single sign-on *benefits* for individuals include easy access to public services through a personalised web portal[23] where they can access their own data collected by multiple public authorities, including tax services and the local municipalities, without logging-in several times. The main benefit for public authorities is a cheaper, simpler and faster process to create new identity-based services on the web portal and other digital services.

NemID is the second phase of the Danish digital signature initiative (OCES) which started in 2003 and as of January 2010 resulted in a penetration of over 33% of the adult population[24] with over 120 public sector agencies offering more than 200 services and 33 private sector organisations offering more than 50 services. The objective is that by November 2010, all self-service public sector services to citizens requiring secure authentication must use only NemID and NemLog-in. Today the EasyLog-in infrastructure is implemented in 22 cross-governmental digital services, which the citizens can access through single sign-on.[25] As of October 2010, all public sector services must use digital certificates for access and all citizens can require that all communication from the public sector is digital.[26] The Government aims to provide NemID cards to all the population.

In 2009, EasyLog-in handled on average 10 000 unique users per day. The system peaked in the spring 2009 with 400 000 logins and 110 000 unique users during one day (for an overall Danish adult population of 4.2 million people).[27]

Implementation of the strategy

The implementation of the strategy relies on a common security infrastructure between the public (central government, regions and municipalities) and financial sectors.

NemID credentials are based on a national standard using the national identification number. NemID uses certificates provided to individuals after a face-to-face identification step, for example in a bank, or registration by presentation of an identity document obtained by face-to-face identification. Although they are not technically "qualified certificates", they provide a strong level of assurance. NemID digital signatures can be generated from any device connected to the Internet and capable of running a Java applet downloaded from the Internet, without dedicated hardware (*e.g.* card reading) or software being required (unlike for OCES). NemID uses two factor authentication: users logon to a registered web service which establishes a secure connection to a central server at the Certification Authority (DanID), then authenticate using a login and password as well as a challenge/response one time password taken from a plastic card.

While OCES and NemID credentials can be used in public and private sector contexts, NemLog-In is restricted to public sector organisations. However, its technical model is based on an open federation, enabling public and private organisations to join, leaving a possibility to extend NemLog-In to private sector in future.[28] One challenge for the Government in 2010 will be to enable semi-public sector organisations such as government-owned corporations (*e.g.* Danish Railways) and general practitioners to use the public sector single sign-on solution.

Essentially domestic, the strategy is based on open international standards and standard products to facilitate interoperability and cross-border implementation.[29]

The broad adoption of NemID is expected to be stimulated by the requirement to use it for e-banking and to use both NemID and NemLog-In for public sector services by 1 November 2010.

The Strategy is supported by a *legislative framework* addressing the use of the central personal register and electronic signatures (consistent with the European Directive). Danish legislation has been modified several times, for

example to modify laws requiring a paper based signature or to regulate the use of electronic health records.

Security and privacy for the issuance of digital certificates is regulated by the National IT and Telecom Agency. The Agency issues certificate policies[30] which refer to the Danish data protection law. Certificates contains only an ID number and optionally the name and email address of the individual. The single sign-on service only stores information on log-in sessions and access to logs is limited. The use of pseudonyms is being considered in the context of the tender for the next four years' solution. The authentication service is designed so that only relevant information is made available rather than all the attributes in the directory. The use of attributes are regulated on a "need to know" basis.

The Danish law implements a supervisory and auditing scheme for qualified certificates. For NemID certificates, an agreement between the CA and the National Telecommunication Agency (OCES standard agreement) sets out auditing and reporting requirements which are inspired by the legislation on electronic signature.

NemID will be advertised commonly by the public and financial sectors. Security awareness is addressed within the broader security awareness raising campaign carried out by the National IT and Telecom Agency.[31] A web site is available for users of OCES and NemID digital credentials.

In case of security incidents, the Certificate Authority must revoke related certificates. Users have to accept terms and conditions prior to using NemID credentials. Users of NemLog-In have access to a short Terms and Conditions page which gives details about the privacy policy. [32]

Challenges

The main challenges faced for the development of the strategies are: *i)* the need to invest resources to select or develop the most appropriate standards and technologies is a challenge in an area where the technologies and concepts are not yet mature; *ii)* the difficulty to attract resources as IdM is often considered as a minor issue in most digital projects; *iii)* the lack of knowledge about IdM in government agencies, challenging the establishment of a dialogue with experts on the development of IdM initiatives; *iv)* confusion regarding cross-organisational IdM versus intra-organisational IdM that confuse stakeholders.

Implementation challenges include the involvement of many government agencies, local governmental organizations, and their IT suppliers, stakeholders' learning curve to integrate IdM solutions in their applications, interoperability issues related to digital signature, in particular regarding trust

and liability on the legal side and semantics and standards on the technical side.

Germany

The German IdM Strategy is based on i) the migration of the mandatory paper-based identity card towards an electronic identity card providing individuals with a universal token for authentication on the Internet for e-government and e-business communications; ii) certified "citizens portals" to enable secure email, identity verification services and document safes; and iii) a technical framework for interoperable and safe usage of digital identities across administrative borders (SAFE). However, as a unique identification number is not allowed by the Constitution, individuals are identified by a set of attributes, and identification numbers are sector-specific. Thus the Germany strategy is based on a centralised registration policy which does not rely on a unique identifier.

National strategy for IdM [33]

The national strategy for IdM in Germany is based on a centralised registration policy relying on citizens' registers of residence maintained by municipalities. As the German constitution does not allow for the creation of a unique personal identity number to be used across all services, individuals will be identified by a combination of attributes such as first and family names and date of birth. Sector-specific identification numbers are used in areas such as tax, health and pension.

With the replacement of the current paper-based identity card with a contactless smart card (nPA for "ePersonalausweis"), the government aims to provide a universal token for strong authentication on the Internet for e-government and e-business. Although it will be possible to use the card for electronic signature, certificates will not be provided by default and will have to be uploaded once the card is in the hands of the holder. Like the current paper card, the nPA will be mandatory for all citizens aged 16 or above.

With the De-Mail concept, the government aims to create the conditions for the development of government-certified identity services by the private sector such as:

- *Secure email services*, enabling citizens to open "De-mail" accounts to send and receive email with a high degree of assurance regarding the link between the email address and the individual behind the address. This will enable communications similar to registered letters in the offline world. In addition, the framework will provide

the possibility for individuals to use pseudonyms in their communications with the legal certainty that under specific and narrowly defined circumstances, such as a legal dispute, real identities can be disclosed.

- *Identity services* to enable users to prove identity features. For example, a user might generate a certified proof of address or age and send it from her De-mail to another De-mail address.
- *Document safe* to securely store key documents in the long run.

The German strategy does not include single sign-on for transparency reasons (personal data from online authentications may not be merely forwarded to third parties). But tokens of single-sign-on systems can be provided to the user on the basis of online authentication.

The Secure Access to Federate E-Justice/E-government (SAFE) initiative is a technical framework for interoperable and safe usage of digital identities across administrative borders ("trust domains"). Its goal is to define open, interoperable and internationally standardised interfaces for the participants in e-justice and e-government that allow secure access to communication services as well as secure and reliable electronic communication. It includes secure registration, authentication and authorisation as well as storage of communication participants. The standard is open and allows for single sign-on solutions for accessing different services with the same digital identity. The base concept, initially developed for e-justice, can be customised by other e-government applications, generating an expanding pool of interoperable e-government services with a common registration and authentication interface.

These components are building blocks of the E-government 2.0 programme adopted in 2006 and implemented by the IT Commissioner of the Federal Government established in 2007 to co-ordinate all e-government activities in co-operation with relevant institutions at federal level.

Implementation of the strategy

Interoperability is a key characteristic of the strategy. One of the main objectives of the IdM strategy is to provide a universal token for electronic authentication on the Internet (nPA) for e-government and e-business transactions and an interoperable IdM infrastructure for e-government (SAFE). The nPA strategy was decided in 2005 and a general concept was published in 2008. An ID Card Act was adopted by the parliament in February 2009, pilots were initiated in 2009 and nPA was officially launched in November 2010. Germany participates in the EU Stork project. nPA specifications are planned to be in line with CEN and ISO standards.

The implementation of the SAFE concept started in 2009 for e-justice with production rollout scheduled in 2010. SAFE is based on OASIS and W3C standards. It is a platform independent framework which is open to various registration and authentication methods. It will be brought into the European Commission's project "Distributed Identity Management" (DIM) as a baseline for implementing an authentication system in the future EU E-Justice Portal.

Legal privacy protection is provided by the Federal Data Protection Act which implements the EU Directive 95/46/EC. The government followed a "privacy by design" approach for the development of the nPA and privacy protection is seen as a key feature of the card framework.

The nPA provides several important security and privacy protection mechanisms: *i)* the Internet authentication function is restricted to services that have been awarded special "entitlement certificates" beforehand, thereby providing a high level of assurance to the individual regarding the identity of the connected service; *ii)* attributes are provided upon users' consent and only when they match a predefined list of attributes included in the provider's entitlement certificate, thus offering a proportionality mechanism. In addition, users are able to check off the transfer of certain data. *iii)* the provision of data from the card is protected by a mandatory user PIN and strong end-to-end encryption secures the exchange of data; *iv)* data fields provided by the card include pseudonym and yes-no responses regarding age limit and address information; *v)* consistent with the interdiction of a unique identification number, it is explicitly forbidden to use the document number included in the card as an identifier; and *vi)* the card contains a set of attributes including biometric data (digital image and, optionally, two fingerprints) that enable to use it as a travel document within the EU. However, biometric data will be technically secured to be used only in specific authorised contexts (*e.g.* border control), excluding e-authentication.

The use of a contactless RFID chip for nPA has raised concerns in Germany. A special protocol has been designed and internationally standardised to enable secure communications from the card terminal to the nPA.

Auditing controls are foreseen through certification procedures for hardware and software components. The data protection framework, including supervision by the privacy regulator, applies to the electronic identity card.

Information regarding the benefits and risks of the IdM system are provided to users upon registration. A hotline is available for users who have lost their ID card.

Challenges

Challenges highlighted by Germany include open infrastructure character, security, privacy, usability and the need for an interdisciplinary approach (technology, organisational, law).

Italy

The Italian national strategy for IdM is based on the migration of the existing paper-based national identity card to an Electronic Identity Card (EIC) intended for all citizens and on a National Service Card (NSC) which aims to satisfy specific e-government needs. Both cards have similar and compatible electronic features which enable electronic authentication to e-government services, and, optionally, digital signature. However, the service card, which is developed by regions and municipalities do not include physical security features required by a national card used for offline identity verification. The Italian strategy is based on a centralised policy where registers maintained by municipalities are centralised at national level and the fiscal code is a unique identifier across public sector databases.

National strategy for IdM[34]

The Italian IdM strategy is based on the deployment of national non-mandatory Electronic Identity Cards (EIC) and National Service Cards (NCS) to provide access to e-government services and enable digital signature. The most recent reform[35] of the legal framework, the so-called "Digital Administration Code", confirms eID through EIC and NSC, letting Public Administrations deploy other tools of identification, as long as these tools allow the identification of the person requesting the service. The main drivers of the Italian IdM strategy are related to a better use of government resources. The use of both cards for private sector transactions is being considered and collaboration agreements with private sector are under elaboration.

Launched in 2001, the EIC aimed to replace the identity card initially established in 1931. It was designed to enable offline identification of individuals similar to its paper-based predecessor, while offering, in addition, electronic authentication to e-government services. However, as adoption pace of the EIC was relatively slow, it was decided to roll out the NSC to enable access to online services that had been developed for the EIC, to users who did not yet have the EIC. The main difference between the two cards is that the NSC does not include offline security features such as holograms and pictures and therefore cannot be used as an offline identification card. All public sector organisations providing online services

have to accept the EIC card although they can provide other means of e-authentication such as with the NSC or other mechanisms. Some regions have distributed NSCs under another name (*e.g.* "Carta Regionale dei Servizi" in Lombardy).

Interoperability between the two cards is ensured by way of a common set of requirements issued by the Ministry of Internal Affairs. For example, an NSC issued by a region can be used to authenticate online services offered within that region and services offered by national public sector bodies. Both cards hold a digital certificate for authentication and can optionally hold another certificate for electronic signature. Users have to be equipped with a card reader and dedicated software to use the card. The delivery of cards requires the physical presence of the individual. The cards enable standard services provided by national or local authorities in full autonomy. They also enable services that require further data to be uploaded onto the card by municipalities.

A key characteristic of the Italian context is the large degree of autonomy of the various layers of public administrations, from the national government to municipalities including provinces and regions. While the central state has full competence in relation to technical co-ordination of administrative data and thus designs ICT standards to be used at national and local levels, regions, in matters where they have competence, have decision power over the creation and implementation of applications and platforms. Regions, provinces and municipalities are autonomous in the development of e-services, following centrally adopted standards. Thus co-ordination is a key challenge, taken up at national level by the National Agency for Digitization of Public Administration – DIGITPA (former National Centre for IT in the Public Administration – CNIPA) which is attached to the Prime Minister.

Implementation of the strategy

Although the EIC was launched in 2001, only 2.5 million Italians had one in 2010 while 20 million had an NSC[36]. In 2006, the government decided to stop the production of paper-based ID and replace them progressively with EICs. However, the application of this directive by municipalities, which control the process at operational level, has not been optimal. As a result, it is likely that both the EIC and NSC will coexist in the long run. Legally, public authorities must provide EIC- and NSC-based authentication and can also provide other authentication mechanisms (*e.g.* login/password).

Interoperability is a key characteristic of the identity card framework, both at legal and technical levels. Technical interoperability is ensured through compliance with a set of international and national standards. However, interoperability across borders is limited, but Italy actively participates in the EU Stork project. Legal interoperability stems from the adoption of a Code of Digital Administration in 2005, updated in 2009 and 2010. The National Agency for Digitization of Public Administration (DIGITPA) plays a key role for the governance of the interoperability framework and for the dissemination and encouragement of the use of standards, norms and service agreements.

The security of the "public system of connectivity" is addressed by the co-ordination of Central and Regional CERTs, implementation bodies and through the joint development of methodologies for preventing, monitoring, managing and analysing security incidents and ensuring consistency across the system. A "management centre" is responsible for the PKI and acts as the registration and certification authority. The code of digital administration covers security aspects such as the development of contingency plans in case of disasters.

While no specific *ad-hoc* policy has been adopted for data protection of public sector IdM systems, the digital administration code was issued after auditing the privacy authority and joint interoperability guidelines will be developed with the Privacy Authority. Although the Fiscal Code acts as a unique identifier for the exchange of personal data across government agencies, each record stored in the central database to facilitate exchange of citizen data between municipalities and other public authorities is encrypted with the public key of the issuing municipality. The digital certificate stored in the cards to enable authentication contains a hash of a personal data file rather than the holder's personal data itself. Such data can only be retrieved with explicit permission. Access to the chip is controlled by PIN code, network operations are encrypted. If another certificate is included in the card for digital signature, a different PIN is required to access it. Additional data can be stored on the card such as biometric and health-related information, but the consent of the holder is required.

The Italian data protection authority supports the concepts of "privacy by design", data minimization and privacy impact assessments in the context of IdM systems and electronic authentication solutions. Following an investigation of the Italian Tax Register which pointed out several data security shortcomings (*e.g.* poor capabilities to monitor inappropriate access and lack of measures to protect the database), in 2008 it adopted a decision which set forth requirements to be applied to security and authentication systems. The Italian data protection authority discourages the use of the tax identifier as a national PIN.

Most information about benefits of the card is provided to users by the issuing administration. Security advice and information regarding procedures in case of incidents are also often provided at time of issuance.

Challenges

The large degree of autonomy of many Italian public administrations, whether jurisdictional (regions, cities) or sectoral (*e.g.* health) creates a key governance challenge for a system mostly aimed at interoperability and a model of shared technical rules. Another challenge is raising awareness of citizens which is seen as an opportunity to address the relationship between e-government IdM and the private sector.

Korea

The Korean strategy is based on a dual public and private sector PKI for the provision of digital credentials to individuals and on the establishment of a technical framework (i-PIN) to better protect the online use of the national register number and enhance Internet users' responsibility while preserving freedom of speech. The broad adoption of digital certificates is promoted by a policy or recommendation to use them for Internet banking, online stock trading and online shopping transactions above USD 260. Both PKI and i-PIN are based on a centralised registration policy relying on the Resident Registration Number.

National strategy for IdM

Several characteristics of the Korean context have to be taken into account to understand the Korean IdM Strategy. First of all, there are only 274 last names in use in Korea and the three most common (Kim, Lee and Park) account for nearly half of the population. Naturally, this situation creates a challenge for identification processes in public and private contexts, whether offline or online. One of the consequences is that Korea has developed a national identity card and a central resident register. All Korean residents are assigned a unique number, the Resident Registration Number (RRN), a meaningful 13 digit number including gender, date and place of birth. Another characteristic of the Korean context is that this number has been widely used online, both for private sector and public sector interactions, including for registration to Web sites, posting information online, online payment, and identity check.

In this context, since 1999 the Korean IdM Strategy encourages the use of digital credentials based on PKI and, since 2005, of a secure digital identifier, the *i*-PIN. Both components of the Korean IdM strategy are based on a *centralised registration policy* relying on the RRN.

The promotion of digital credentials by the governments is based on:

- Two Public Key Infrastructures: the National PKI (NPKI) which enables the use of digital certificates for private sector transactions and the Government Public Key Infrastructure (GPKI) for transactions within the public sector.[37]
- The recommendation to use digital certificates (NPKI) for any financial services such as Internet banking, online stock trading and online shopping transactions above USD 260.

In parallel, the government developed a secure online identifier system, the *i*-Personal Identification Number (*i*-Pin) to respond to a double challenge: *i)* the overuse of the RRN online without appropriate protection which led to a considerable increase in identity theft. The *i*-PIN aims to provide a means for secure identification of individuals online based on the RRN but without compromising it; *ii)* growing concerns that emerged regarding an increase in privacy violations, defamation, cyber violence, and offenses online. While recognizing the considerable benefits of the Internet for the individuals and the Korean society, a heated debate took place in 2002 about how to tackle negative consequences of aggressive behaviour online. Ultimately, the Parliament voted almost unanimously for the development of an identity verification framework which aims to prevent Internet users from abusing online anonymity by imposing some responsibility on users[38]. The *i*-PIN is the key component of this framework as it provides a simple and secure way to reveal the identity of a user without requiring such identity to be exposed to the public.

The *i*-Pin system provides a high degree of certainty to the web site with respect to the identity, age and gender of the end user without compromising the RRN while still using it as a key element for identification, and without requiring the real identity of the user to be exposed to the public.[39] It can be used to access e-government services. It has to be used for private sector web sites with a minimum of 100 000 visitors per day.

Implementation of the strategy

The strategy is based on a legislative framework including the 1999 *Electronic Signature Act* which sets forth a framework for the use of electronic identity credentials for e-commerce and electronic documents,

and the 2002 *E-government Act* for the promotion of governmental digital certificates.

NPKI certificates are issued by five private sector accredited Certificate Authorities (CA) and GPKI certificates by the Ministry of Public Administration and Security (MOPAS). Korea Internet & Security Agency (KISA) is the Root CA. NPKI certificates are provided for free when used in a specific area (*e.g.* e-commerce, banking, stocks). All-purpose certificates are provided for a small annual fee of USD 4. While the Government Certification Management Authority acts as root CA in public areas, the Korea Local Information Research & Development Institute provides GPKI certificates to civil servants.

The number of digital certificates delivered is 23.6 million as of October 2010

Intersections or relationships between government and private sector systems (GPKI and NPKI) are enhanced by a Certificate Trust List (CTL). While the CTL mechanism is operational and does not raise specific issues, it required a long and difficult process to reach an agreement regarding who will operate the CTL and how to renew a certificate under the CTL system. The "Framework for internet-Personal Identification Number Service" and the "Message Format for *i*-PIN Service" have been adopted as national standards in 2005 to enable the use of *i*-PIN in both sectors.

Innovative developments include a *User Control Enhanced Digital Identity Wallet System* enabling users with a Digital Identity Wallet to log in to websites without filling in ID and password information. A pilot test service enabling the use of *i*-PIN with a Digital Identity Wallet is now underway.

Korea encourages the *interoperability* of electronic identity credentials by monitoring Root CA and accredited CAs to make sure they comply with interoperability requirements. The Electronic Signature Act was modified to introduce an obligation for private sector to comply with the NPKI standard. Twenty-four norms for safety and reliability of a PKI certificates have been adopted.

In addition, the Digital Identity Management Forum was founded in 2008 to enhance the interoperability of IdM, to share information and knowledge of the technology and standards of IdM, to gather various opinions from the private sector, and to deliver precise and explicit opinions to policy makers. Finally, Korea is developing a way to interoperate *i*-PIN and electronic certificates.

With respect to information security, key length and hash algorithms have been upgraded. The Korea Communications Community (KCC) enacted the technical and operational mandate for protecting Private data, which describes the provisions to be observed by all companies with respect to consumer data, with possible fines up to USD 1 000. KISA annually investigates the security measures of the five accredited CAs and the Authentication Agencies who issue ID and passwords for *i*-PIN.

Regarding privacy, the *i*-PIN framework has been established as a privacy protection measure to secure the resident registration number. However, the fact that the *i*-PIN framework systematically provides the web site with the real name, gender and age of the user with a high level of assurance could be seen as a potential privacy threat.

Korea is considering the modification of the Act on the Protection of Personal Information Maintained by Public Agencies to include provisions for all public agencies to perform a privacy impact assessment. The Act on the Promotion of Information and Communications Network Utilization and Information Protection requires e-government systems as well as e-commerce systems to encrypt the storage of some identity attributes such as the resident registration number, bank account number, etc.

Awareness raising for *i*-PIN and digital certificates is promoted by the dissemination of manuals and animation materials that help the public understand how to issue and operate *i*-Pin and by conferences and campaigns.

i-Pin theft is prevented by the obligation for the agency managing the *i*-Pin to notify users by email whenever their *i*-PINs are used to identify them. Korea is also considering introducing data breach notification for Internet service providers.

Challenges

Korea developed a Certificate Trust List (CTL) mechanism to enable interoperability between NPKI for private sector and GPKI for governmental sector. This system, operating since 2002, did not raise particular technical problems but it was difficult to establish and in particular it took long time to reach an agreement regarding aspects such as who will operate CTL and how to renew an electronic certificate based on PKI with the CTL system.

Japan

Although Japan does not have an IdM strategy, the manifesto of the Democratic Party of Japan (August 2009) states that the possibility of "introducing a unified serial number system for both taxation and social security to facilitate monitoring of income" will be examined. A Cabinet decision of 18 June 2010 states that a study has been launched regarding the introduction of a citizens ID system that would both ensure the protection of personal information and maintain consistency with the study for a system for social security and tax numbers.

The Government of Japan has just begun to investigate the establishment of an IT strategy under the new administration and will also examine the relationship between the establishment of IDs, which is needed to promote electronic government, and the number system. A Cabinet decision of 11 May 2010 mentioned the introduction of a citizens ID system by 2013 as the common base of e-government enabling the linking of data between central ministries and local governments, consistent with the protection of personal information and the exploration of systems for common numbers for social security and tax.

In order to improve information security in all Japanese government agencies, central government agencies have to comply with "Standards for Information Security Measures for the Central Government Computer Systems" which includes a chapter on Identity Management. Compliance is evaluated by inspections from the National Information Security Center.

There is no dedicated policy with regards to the protection of privacy in relation to IdM systems so far.

Luxembourg

Luxembourg's current IdM strategy of is based on the use of PKI certificates issued by a certificate authority based on a public-private partnership between the government and private sector companies (LuxTrust). The strategy relies on a centralised registration policy based on a central register, a unique identification number and a mandatory paper-based identity card. Future plans include the distribution of national identity cards containing embedded electronic data, including biometrics, to be used for public and private sector digital interactions.

National strategy for IdM

The current national IdM strategy of Luxembourg aims to increase security in e-commerce and e-government transactions. It is based on PKI certificates delivered by LuxTrust, a certification authority established in 2005 on the basis of a public-private partnership between the government and key business actors such as financial institutions. The status of LuxTrust enables close co-operation with financial institutions and is overseen by the official financial supervisor (Commission de Surveillance du Secteur Financier – CSSF). LuxTrust provides PKI certificates on smart cards and USB tokens. It also provides "signing server certificates" which generate one time passwords either via SMS messages or by using a dynamic authentication token. Registration requires a face to face relationship with one of the banks recognised by LuxTrust as registration authorities.

PKI certificates enable access to public and private sector online applications and digital signature of documents and email[40]. With LuxTrust PKI certificates, individuals can log in to a unique counter for citizen-to-government interactions called "de Guichet" to carry out a large number of formalities online. Private sector services using LuxTrust certificates are mainly offered by banks and financial institutions.

The government maintains a *centralised identity registration framework* based on *i)* a central register ("répertoire général") established in 1979; *ii)* a unique identity number which contains the individual's date of birth and gender and the use of which is limited by law to public sector and, in some contexts, social security organisations, and *iii)* since 1939, a mandatory paper-based identity card for all citizens over the age of 15.

One of the government's objectives is to issue an electronic national identity card containing embedded data, including biometrics, to be used for public and private sector digital interactions.

Implementation of the Strategy

Interoperability is supported by including relevant stakeholders in the working groups involved in issues related to dematerialisation of documents, archiving and digital signatures and by relying on international standards. Luxembourg is preparing cross-border interoperability by participating in the European Stork project.

The design of government IdM systems was based on security and privacy impact assessments. Governmental IT projects are submitted to an independent internal security team whose policies are based on ISO 2700x standards. External audits are carried out regularly and the IdM system is audited and accredited against several ETSI standards by the national

standards and verification body[41]. Every major e-government project is submitted to specific external intrusion tests before going into production.

The IdM system was designed following the recommendations of the national data protection committee and complies with the national data protection law. The strategy is based on strong authentication and does not authorise the use of pseudonyms. Few attributes are included in the certificates (first name, last name and nationality).

Awareness campaigns are carried out to inform citizens about the benefits of IdM. Information on risks is provided to citizens through a security awareness portal (*www.cases.lu*). In case of an incident, the IdM policy includes a mechanism for the revocation of the credentials and notification of the individual.

Challenges

Key challenges include the provision of secure solutions in a rapidly changing technical environment, data privacy, interoperability and legal environment. The key to an efficient deployment lies not so much in the distribution of a large amount of electronic credentials but in their extensive use by citizens through well-designed interoperable applications.

Netherlands[42]

The Dutch IdM strategy aims to reduce cost and complexity of e-government services, fight fraud and increase simplicity for end users. It includes the provision of digital identity credentials to citizens and businesses for electronic authentication to public sector applications with several levels of assurance. It is based on a centralised registration policy relying on a centralised population register.

National strategy for IdM

The Dutch IdM strategy is based on DigiD, a national digital identity and authentication mechanism for electronic transactions of citizens and entrepreneurs with public agencies. DigiD provides citizens and residents with digital credentials to be used for their relationships with the Government and for single sign-on to e-government services. It results from a collaborative effort across ministries and local authorities to streamline the implementation of e-government.[43] The Ministry of the Interior and Kingdom Relations oversees the programme and the Ministry of Economic Affairs is responsible for the IdM strategy with respect to business-to-government.

DigiD is based on a *central registration policy* relying on a central population register which provides a unique "citizen service number" to all citizens and residents[44] and on a trade register, which provides businesses with a company number. The Dutch population register was established in 1994. It is hosted by each municipality but connected by a national secured network, managed by an agency of the Ministry of Interior, to prevent multiple registrations for the same individual. The register contains personal information such as the name, date of birth, gender, place of residence and nationality and since 1 April 2010, all Government agencies have to use it to obtain the personal data they need. From the citizen's practice perspective, nothing has really changed: they still have to provide information at a local office as in the past. Thus the Netherlands have not established a completely new registration system to support e-government. Instead, pre-existing registration processes have been modernized to enable new services.

The objective is that DigiD becomes the only authentication system used in public administration to deliver electronic services to citizens. However, DigiD does not fully address the needs of business-to-government interactions as it can generate only one code per company. A programme called "eRecognition for Companies", led by the Ministry of Economic Affairs and based on a public-private co-operation, aims to establish an infrastructure to accommodate the need for different levels of authorisation that may arise within companies and institutions. This solution, based on an agreements scheme, could also be used for business–to-business interactions.[45]

As the use of the citizen service number by the private sector is strictly forbidden by law, the extension of DigiD to the private sector is challenging. Reciprocally, the use of private sector IdM applications in a public sector setting is also difficult. Nevertheless, organisations legally identified as fulfilling a public sector role (*e.g.* some private sector hospitals) can use DigiD.

DigiD currently provides two levels of assurance: username/password (DigiD Basic) and username/password with SMS verification (DigiD Medium). The username/password combination is issued after a check against a population register. An electronic identity card to be used for a third level of assurance is currently under consideration. Benefits for the government include lower costs, better and more efficient service to customers, fraud control, benefits for end users include trust, ease of use and accessibility.[46]

Above 6.7 million citizens have created a DigiD for a population of 16.8 million (39% penetration rate), with 56% using DigiD Basic and 46% using DigiD Medium. 17 million successful authentications have been carried out in 2008.[47] A large number of public administrations participate in DigiD[48],

including central administrations, provinces, regions, hundreds of municipalities, healthcare institutions, health insurers and police departments. Many services are available including the submission of online applications for child benefit allowances and statutory old age pensions, digitally signing a tax declaration, requesting a copy of the municipal personal records database, applying for various permits, notifying a change in address, paying municipal taxes, paying parking fines, etc.[49]

Implementation of the strategy

With respect to eRecognition for companies, the main challenges are related to legal issues, to existing IdM systems in use in some government agencies for interactions with companies that will have to be replaced, and to the establishment of a sufficiently critical mass of services for companies to be interested in joining the agreements scheme.

Interoperability is an essential aspect of eRecognition for companies since it aims to provide access to all government agencies with a single token compatible with the eRecognition scheme. eRecognition for companies also provides for cross-border interoperability within Europe. This programme supports the use of open standards and open source. The final agreements scheme is expected to be adopted as a standard by the Dutch standardization council.

As in other countries, a legal framework supports the implementation of the Dutch IdM strategy, including in the area of e-signature, protection of privacy and with respect to the use of the citizen service number.

The level of assurance required for the use of DigiD is related to the type of service provided to the citizen. eRecognition for Companies offers several levels of security, from a username/password combination to PKI based solutions. In the scheme, providers make arrangements on the use of security standards, protocols and liability.

With respect to privacy, the privacy framework applies to IdM. Privacy Impact Assessments are being looked into by the government and the Dutch data protection authority. A key concept is to avoid the use of sensitive personal data in the IdM system used for business–to-government communication. Very little personal information is required for the eRecognition for companies programme and the use of pseudonyms for company workers is possible. The use of the Citizen Service Number is regulated.

DigiD is subject to yearly internal, as well as external, reviews. Furthermore, public scrutiny is a strong driving force for quality control. The parties working together in the network of eRecognition for Companies will set up a system for certification.

DigiD was introduced several years ago via media announcements and is well known to the general public. Users are informed about the usage of their data and related risks and about their rights and duties during the registration process. A national helpdesk on Identity Fraud is available for the citizens. The provider of means of eRecognition for Companies has the obligation to inform users in case of corruption of the data. Liability is partly arranged in laws and will partly be subject to the arrangements between the parties in the network of eRecognition for Companies. At the moment these arrangements are under construction.

Challenges

The use of the Citizen Service Number is strictly regulated to limit its use to the public sector and it is the unique and only identifier that government bodies have to use to provide services to citizens. The possibility to use private sector IdM applications and credentials for public sector services as well as the use of public sector credentials for private sector services is therefore a challenge.

Legacy problems are also challenging: some governmental agencies have their own IdM systems in use for companies that they will have to replace.

The widespread use of eRecognition for companies will start when enough governmental agencies will have migrated their services online. During the first years the challenge will be to seduce companies to make use of it. This implies that the private sector will be reluctant to take its part in the agreement's scheme because the business case for them may only be positive once use is widespread.

New Zealand

New Zealand's identity management strategy is based on a set of policies and initiatives for public sector agencies to manage their identity assurance processes more effectively and in a more co-ordinated manner, with a view to facilitate the delivery of Government's services in the online environment. These include an Identity Assurance Framework for Government, a "Logon Service" allowing individuals to use the same logon details to access all participating government online services and an "Identity Verification Service" allowing individuals' identity to be verified

by participating government service providers via the Internet. Privacy protection and the security of personal data are integrated into the design of these technical solutions, ensuring compliance with the 1993 Privacy Act. Interoperability is addressed through the use of international standards. New Zealand's approach is based on a decentralised registration policy where each agency is responsible for determining the appropriate level of identity assurance for its online services.

National strategy for IdM

New Zealand's strategy for digital identity management is based on the government's recognition that agencies could manage their identity assurance processes more effectively and in a more co-ordinated manner, to the extent permitted under the existing law. The general approach is decentralised, whereby agencies are responsible for determining the level of identity assurance that is necessary when providing their services to individuals, and a range of documents are generally accepted to verify identity, where necessary. The government supports agencies with a range of policies, standards, and guidance material such as the 2008 Identity Assurance Framework for Government (IAF)[50] which encompasses agencies within the public sector and also other agencies with an interest in identity assurance. It supports "citizen-centric" services and the reduction of the amount of identity information held by agencies, through the use of real-time verification processes.

In 2003, the government designed an all-of-government authentication solution, taking privacy and security as key considerations, to allow users to have a single username and password to access a variety of government services across many agencies[51] ("igovt Logon Service", launched in 2007), and to verify their identity securely online when accessing these services (igovt Identity Verification Service – IVS, launched in 2009). At present, eligible applicants enrol in person for an electronic identity credential containing minimal identity information ("igovt ID"), their photo and personal details are compared against a passport or citizenship record held by the Department of Internal Affairs. "igovt IDs" are currently only able to be used in connection with one agency's online service. A user logs onto that service's website and enters a code that is sent to the user's mobile phone. The user may then choose to consent to the release of the information that makes up his or her igovt ID, *i.e.* full name, date of birth, place of birth and gender, to the agency to verify identity. It is expected that legislation would be enacted to support the future use of the igovt IVS by a wider range of individuals and agencies.

igovt initiatives are aimed at public sector services and their extension to private sector to foster the development of new online products and services would require further assessment. Access by private sector agencies to individuals' identity information held on government agencies' systems may occur only to the extent permitted by law. In some instances, there are specific legislative provisions governing the disclosure between government and private sector agencies of personal information for certain purposes such as to support the delivery of health or welfare services.

The government has also developed a Data Validation Service which can immediately confirm whether identity data entered by users is consistent or not with authoritative record in the database held by the Department of Internal Affairs. This can include details on citizenship, passports and births, deaths and marriages databases and registers. This system will be extended to private sector organisations which meet strict security, privacy and integrity criteria as a way of confirming identity and reducing costs. It is not proof of identity in itself, nor is it conclusive proof that the document is valid since a true set of data on a counterfeit document could be overlooked by an inexperienced operator. The role of the Data Validation Service is to support the gathering of a number of pieces of corroborating evidence to prove identity where presentation of documents is part of the business process.

Implementation of the strategy

Interoperability of e-government identity management systems is achieved through the 2002 E-government Interoperability Framework (e-GIF) which is mandatory for core government agencies, recommended for the public sector and encouraged for local government. The igovt Logon Service and IVS are both interoperable and supported by open standards. In respect of identity verification, the e-GIF includes the Evidence of Identity Standard, a good practice risk-based standard for government agencies when verifying identity online or offline.

The Privacy Act 1993, including the regulatory role of the Privacy Commissioner, applies to IdM systems. The Privacy Commissioner can receive complaints from individuals, investigate the matter and resolve it through conciliation, mediation or by making recommendations. Security provisions are included in the Privacy Act which controls how agencies collect, store, use, disclose and give access to individual's identity information or other personal information, including regulating the use of unique identifiers that agencies assign to individuals' information.

The NZ ICT Security Manual contains policies about how ICT security for the New Zealand Government is managed, implemented and documented. It also includes ICT security standards, principles and advice relating to specific aspects of ICT systems, such as hardware, software and access control.

The igovt services are designed, implemented and deployed in a security and privacy conscious manner, compliant with the ICT Security Manual, covering all aspects of their life cycle, including their ongoing operation and administration. The igovt services have been designed in a privacy-protective way, in consultation with the Privacy Commissioner. They require neither a physical card nor a unique identifier. There is a separation between the logon and identity verification processes, and between those processes and the transaction that an individual undertakes with an agency. An individual's identity is authenticated with each authorised agency using an identifier that is unique to that agency. There is no common unique identifier through which any agency can find out what services an individual has been accessing through another agency. While the Department of Internal Affairs holds a record of all agencies where an individual has used his or her electronic identity credential, the Department does not record which specific services an individual has accessed at each agency. Individuals can check their personal information before it is sent to an authorised agency, and have control over whether or not it is sent. Only the minimum amount of identity information is transmitted to the agency. No biometric information, including the individual's photograph, is sent to an agency to authenticate the individual's identity. Individuals can also monitor how their personal information has been accessed and used and, if they detect misuse, report this for investigation by the Department of Internal Affairs. As an individual's identity is authenticated to a high level of confidence when creating an igovt ID, and because of the secure way it is used, the risks of other people impersonating the individual are reduced.

The Privacy Commissioner encourages agencies to undertake Privacy Impact Assessments for significant new initiatives involving the handling of personal information. Privacy Impact Assessments for the igovt Logon Service and IVS have been undertaken by independent assessors, and will continue to be undertaken periodically. The recommendations made in those Privacy Impact Assessments have been given effect in respect of the design, architecture and operation of the igovt services.

The igovt logon service and IVS have both been developed in compliance with the above mentioned Evidence of Identity Standard. Many agencies' services are integrated only with the Logon Service, which means that users are able to transact pseudonymously for those services.

In general, the collection, storage, use and disclosure of any type of identity attribute, and unique identifier associated with that information, must comply with New Zealand's Privacy Act 1993. In some instances, particular laws govern the certain types of records containing identity information, unique identifiers and biometric information. In 2009, a cross-government group of agencies issued guidance material to inform agencies' decision making when considering biometric technologies for identity-related business processes. In designing online and offline identity authentication processes, agencies should take account of the fact that in New Zealand, a person may adopt a name through usage and reputation (including, for example, adopting a spouse's name on marriage), and legitimately continue to use different names in different contexts. Indeed, individuals may legitimately hold a range of documents that provide evidence of their use of their different names.

External security and privacy specialist organisations undertake regular audits, reviews and tests. Measures to protect personal data taken by agencies vary depending on the identity management system, depending on what is reasonable in the circumstances. Audit and event logs are kept and are regularly monitored for anomalous entries.

Each agency is responsible for raising awareness regarding the benefits and risks of its identity management system. The Department of Internal Affairs intends progressively to make people aware of the benefits and risks of using the igovt services. Services based on the igovt framework provide their users with help desk contact details. Users are able to view their personal details online, including information about where their logon and igovt ID has been used, and who has accessed their personal information. In 2008, the Privacy Commissioner issued voluntary data breach guidelines to assist agencies deal with incidents of unauthorised access to or collection, use or disclosure of personal information.

Challenges

The creation of new arrangements (whether through new or existing legislation) for sharing individuals' personal information between government agencies, or between government and private sector agencies must ensure that public trust in government is not undermined. This has been a key consideration in the design of the igovt services.There are also practical challenges involved with the implementation of an e-authentication solution across government, due to the variety of types of personal information held by different agencies for different purposes. In practice, personal information relating to the same individuals is often inconsistent and, in some cases, of poor quality.

Portugal

The main driver for the Portuguese national IdM strategy is the modernisation of the public administration towards user-centric processes and services. The strategy focuses on the Citizen Card project, which consists in the replacement of several public sector traditional cards with a single smart identity card enabling in person, Internet and telephone based authentication as well as digital signature, both in public and private sector contexts. The card is seen as a driver for innovation enabling new public and private sector services. A single sign-on identity provider is being established to enable public and private sector to offer authentication from a common and central point based on the Citizen Card. The framework is based on a centralised registration policy relying on the pre-existing population register.

National strategy for IdM

The Portuguese national strategy for IdM is based on the Portuguese Citizen Card project (Cartão de Cidadão), a physical and electronic mandatory document which allows citizens to identify themselves physically and electronically and to legally produce a valid e-signature. The card aims to replace the former mandatory paper based national identity card in place since 1914. It is based on a centralised registration policy using the national population register. Although it can be used in public and private sector contexts, its primary objective is to contribute to the development of a more user-focused, integrated, convenient and effective public administration including through new customer-oriented advanced services and less interactions related to citizens' identification. The card puts together in a single document several national identification documents (identity, health, tax and social security cards), supports safe electronic interactions between the government, citizens and private entities and it encourages dematerialisation and simplification of public administration's procedures. It is instrumental in achieving the objective of placing companies and individuals at the core of the government's modernisation process.

The Portuguese IdM strategy supports strategic modernisation objectives such as *i)* enhancing security of identification processes; *ii)* introducing legal equivalence of electronic authentication to traditional in-person identification methods thus fostering dematerialisation of processes and documents; *iii)* alignment with EU requirements for citizen identification; *iv)* simplifying citizens interactions with public and private organisations by combining authentication and signature mechanisms; *v)* fostering the use of electronic services; *vi)* improving the delivery of public services by aligning technological and organisational modernisation processes; *vii)* rationalising resources, means and costs for all stakeholders.

Citizens can authenticate themselves to public administration portals and sites using the Citizen Card and the government is implementing a Single Sign-On Identity Provider for public and private sector organisations which will provide a common and central point of authentication for citizens, based on the Citizen Card.

The overall management and business operation of the Citizen Card project falls under the responsibility of the Agency for Public Services Reform (AMA) and Institute of Registries and Notaries (IRN).

Implementation of the Strategy

The Citizen Card was launched in 2007 and granted to all citizens[52] from the age of 6 years old. in December 2010 4.2 million cards had been distributed to the population and 39% of citizens opted to activate the e-signature. It costs EUR 15 (in December 2010).

The government considers the Citizen Card as a driver for innovation as it enables the development of new services which would not be possible without it. Flagship applications include creating a company,[53] registering a car, and reporting a crime online.[54] Citizens can also access the citizen portal[55] for example to change their address, and access regional e-services.[56] Since December 2009, eProcurement platforms are dematerialised and use citizen cards and certificates. The card can also be used for authentication to information systems of specific organisations.[57] The card is also used in private sector contexts, for example to support bank services such as the opening of a new bank account, or to sign private contracts, enabling authentication on private websites or workers assiduity registration

The card includes a large range of security features which enable its use in various contexts and foster the deployment of new services. They include PKI services with revocation functionalities, time stamping services, legally valid digital signature and multichannel identity authentication, *i.e.* in person with "match-on-card" biometric authentication (where the biometric match is taking place on the card), by phone with a one-time password generated with the card, by Internet using the card's digital certificate. Confidentiality and integrity are provided via a contact chip with information storage and cryptographic processing capacity.

The use of international standards is considered as essential to ensure interoperability, market competition for services around e-ID and to encourage cross-border applications. Standards are promoted in all projects developed by the Agency for the Public Services Reform (AMA). The Citizen Card implements several ISO, CEN, ICAO and other standards. For example, it enabled Portugal to sign bilateral agreements with Belgium,

Estonia and Spain to allow citizens of one country to create a company online in another participating country using their national citizen card (Portugal participates in the EU STORK project).

To encourage the development of card-based applications, development cards are available and a development kit can be downloaded online.

Interoperability of government's IdM systems at national level is enabled by the "Electronic Certification System of the State" (SCEE) which constitutes a hierarchy of trust that guarantees security and strong electronic authentication within the public administration and with citizens and private companies. The SCEE operates independently from other PKI, whether private or foreign, but allows interoperability with the infrastructures that fulfil the necessary authentication requirements. All IdM infrastructures depend on the same national root and follow a similar policy. The Citizen Card is the largest branch (in terms of number of certificates issued) of the SCEE hierarchy. The SCEE is managed and monitored by the Management Center for the Electronic Government Network (CEGER)

Finally, interoperability is also supported by a legal framework which defines the regulatory requirements that all electronic ID certification systems must comply with (Decree-Law 116-A/2006) and which makes the use of the Citizen Card authentication and signature mandatory for public services providing e-services to citizens (Ministry Council Resolution n°109/2009).

The National Security Agency (Autoridade Nacional de Segurança) is responsible for verifying compliance with security requirements by the Certification entities. Audits are also carried out by external and independent auditing teams. All systems and processes used by the public administration for issuing and managing citizen cards are authenticated and registered to enable third party audits.

With respect to privacy, the Citizen Card was designed to comply with the legal interdiction to share identifiers and data across public services. Thus the data stored on the chip includes the national identity card number, social security number, tax number and health user number instead of one cross-cutting number. Information about the individual is kept separately in the database of each body involved in its use. The card also includes two certificates, one for e-authentication and one for e-signature, biometric attributes (picture and fingerprint) that enable match-on-card biometric verification, guarantying privacy by not permitting access to any personal data without the individual's express consent, or other data printed on the card such as full name, gender, place and date of birth, name of parents, height and nationality. The card is activated by the citizen upon reception of

a PIN letter. The policy and the law have been reviewed by the National Data Protection Authority.

The Citizen Card is highly accepted by citizens but the government recognises the need to promote electronic services and explain the advantages of the card such as simplicity and confidence. The government organises communication campaigns to promote the card and, when they receive their card, individuals are asked to sign a document that provides information about its major benefits and risks. Citizens can report incidents to a 24/7 support service which can manage identity suspension/revocation in real time.

Since July 2010, the Portuguese Citizen Card can also be used for authentication to the major European e-government portals. Interoperability was accomplished in the context of the European STORK project that established a European eID Interoperability Platform.[58]

At a national level, Portugal is currently extending its national eID platform in order to allow additional attributes ("citizen roles") to be accessed using the Portuguese Citizen Card, for authentication and signature purposes – for example "engineer role", "public servant role", "company CEO role", "teacher role", "medical doctor role", among others. This service is expected to be available, in pilot phase, during 2011.

Challenges

Challenges include:

- Horizontal political support for the overall management and business operation of the Citizen Card was a key strategic challenge.
- Putting into practice the interoperability concept. The legal constitutional barrier to centralise the identification system preventing the use of a single identification number was overcome by the adoption of identity federation, communication through web services (WS* standards), secure cryptographic messaging and other interoperable standards to enable interactions between different information systems platforms. Interoperability relies on the use of identity federation through the Portuguese National Interoperability Platform as well as eID open standards.
- Functional and business process optimisation along all the workflows that support the main Portuguese identification systems: improving data quality not only in identification processes but mostly developing new opportunities to dematerialise processes using e-ID potential.

- Awareness raising and communication about the services, although penetration and acceptance of the citizen card is very high.

Slovenia

The national strategy for IdM in Slovenia aims to generalise digital certificates for electronic authentication and signature. It is driven by the e-government strategy which aims to deliver better government services with fewer resources. The framework is based on a central registration policy relying on the personal registration and tax numbers for the private sector and on a standalone centralised identity database for the public sector.

National strategy for IdM

The strategy for IdM in Slovenia is driven by the implementation of the 2008 e-government Strategy which aims to foster the delivery of better government services with fewer resources. Key concepts to reduce cost and increase quality and uniformity of services include the development of a shared infrastructure and the reuse of modules. A key direction is the limitation of the number of credentials that citizens have to use to access e-government services by providing common electronic signature and authentication mechanisms with certificates and username/password. One important building block is the implementation of the "authentic source" principle whereby users should not be requested to provide the same information twice: information should be stored in a single authentic source after the first request and other e-government services should tap into this source instead of requesting the information again from the user. A new action plan implementing the e-government Strategy was adopted in April 2010. The development of an electronic identity card has been planned since 2003 but suspended several times.

With respect to credentials, the strategy is based on the availability of digital certificates for public and private sector transactions. There are three private sector registered certificate service providers and one public sector provider in Slovenia. Qualified certificates issued by any of these four registered providers can be used to access e-government services. Some banks accept only certificates from the public sector or from the provider operated by banks.

Single sign-on is included in the action plan for e-government in order to support the concept of one-stop-shop e-services accepting multiple credentials based on different technologies and devices but privacy and security aspects have not yet been fully analysed. Companies can already

use one-stop-shop access to nine institutions and e-social security services aim to integrate up to 22 services.

Identity Management is also addressed on a sectoral basis, namely for local e-government, e-health and e-justice.

Implementation of the strategy

In order to stimulate adoption of electronic identity management by citizens, the government required using electronic means to submit tax returns[59].

Security requirements for certificate service providers are defined in a series of decrees and privacy requirements are established in the Personal Data Protection Act. Inspections of certificate service providers are carried out by the Ministry of Higher Education, Science and Technology and can also be carried out within the framework of an accreditation scheme which was not brought into force yet.

Slovenia is a member of the EU Stork Project and supports the model of interoperable electronic ID mutually recognised in EU member states. The Slovenian Electronic Commerce and Signature Law includes mutual recognition as a means for integrating the Slovenian economy into the international economy.

Slovenia has developed a national interoperability portal and maintains an inter-sectoral working group to facilitate technical, semantical, legal and organisational interoperability. Certificate service providers are responsible for the technical solutions they provide and can offer different types of smart cards and middleware. While there are no legal obligations or limitations regarding compliance of certificates with standards, legal oligations are likely to be established in the future to support new solutions.

Interoperability implementation challenges are related to strict privacy protection provisions for public sector agencies. While private sector certificate providers can use the tax or personal registration number to map a certificate to its holder's data, the public sector certificate provider is required to use a specific certificate serial number and the Ministry of Public Administration has to keep all personal data in a standalone database. This discrepancy between public and private sector make it more difficult for private operators to support certificates from all providers.

Regarding cross-border aspects, two pilot projects addressed technical and semantic interoperability through the use of international standards and highlighted a number of technical difficulties. They also helped identify organisational and legal interoperability arising from the exchange of

information from national registers between different countries as a more difficult challenge to overcome.

Finally, the last challenging area relates to the complexity of identity management for users.

Challenges

A key challenge is the need for a critical mass of users and services in both the private and public sectors to foster adoption and use and therefore return on investment. The government is facing this difficulty for example as it plans to generalise the use of mobile-based certificates.

National and cross-border interoperability are seen as key challenges for IdM.

Spain

The Spanish national IdM strategy is based on the provision by the government of an IdM infrastructure to foster the development and use of public and private sector electronic services and facilitate e-inclusion. The strategy promotes the use of qualified PKI certificates both by the provision of a mandatory electronic national identity card (Documento Nacional de Identidad Electrónica) replacing the paper-based card and by the establishment of a legal framework for electronic signatures and for its use in the public sector. The framework is based on a centralised registration policy relying on the national register number which is included in all qualified certificates. Interoperability issues are addressed by a validation platform for digital certificates and electronic signatures and by a national interoperability framework for the public administration.

National strategy for IdM

With more than 19 million "Documento Nacional de Identidad" (DNI) delivered between 2006 and 2010 and 500 000 cards being issued monthly, the Spanish national electronic identity card can be seen as the first pillar of the Spanish national IdM strategy. The card is mandatory for all citizens over 14 and replaces the paper-based identity card initially created in 1944. The electronic card is being smoothly deployed and rapidly adopted, probably as it is perceived by individuals as a natural evolution of the paper one. It includes a qualified certificate for strong electronic authentication of the identity of the holder and another one for electronic signature of documents which provides the same legal validity as a handwritten signature. Issued by the Police Directorate in the Ministry of Interior, the card is also a secured physical document used for the verification of identity

and citizenship offline. The national register number assigned to all citizens is printed on the card and included in its qualified certificate.[60] This number is also included in all other qualified certificates issued in the country.

Nevertheless, the card should not be seen as the only or main element of the framework. The strategy is also supported by a legal framework including:

- The 2003 e-signature law[61] which transposes the European Directive 1999/93 on a Community Framework for Electronic Signatures. It establishes a voluntary accreditation scheme for certificate service providers without prior authorisation and assigns the responsibility for the supervision to the Ministry of Industry and Trade. The law defines three levels of digital identity: electronic signature, advanced electronic signature and qualified electronic signature (advanced electronic signature based on a Secure Signature Creation Device or SSCD). The law also allows public administrations to define their own requirements for the use of digital identity in e-government services.
- The Citizens' Electronic Access to Public Services Law[62] adopted in 2007 to foster the deployment of e-services in the public sector. The law defines the legal requirements of the Spanish Public Administration Digital Identity System, including the use of electronic identities by citizens, public employees and public administrations for e-government services. It recognises the right of citizens to use their electronic identity card in any Spanish e-government service and the obligation of public administration to accept advanced signatures based on qualified certificates. In practice, administrations can choose to ask for a simple electronic signature (*e.g.* a password) or an advanced electronic signature. Both authentication mechanisms can coexist.

The Spanish market for digital certification is relatively dynamic with more than 15 public and private commercial certificate service providers. Public administrations must accept qualified digital certificates regardless of the public or private nature of the issuing service provider. Qualified certificates delivered by private service providers are used in private sector contexts and are equally accepted for e-government applications and interactions with public administrations. Conversely, national identity card's certificates can be used for private sector applications.[63] One bank allows its clients to be identified by their national identity card when they require financial services online and it is adapting its ATM machines to accept identity cards instead of traditional bank cards. Interestingly, Cisco has

developed a system to allow users to be identified in companies' Virtual Private Networks with their national identity card.[64]

The third pillar of the strategy addresses interoperability issues raised by the various types of certificates available and multiplicity of certificate service providers. It includes:

- A national validation platform called "@firma", established in 2006 to tackle interoperability issues raised by the high number of qualified certificates in circulation. Operated by the Ministry of Territorial Policy and Public Administration, @firma carried out more than 14 million validations in 2009 (against 880 827 in 2006). The platform validates certificates and signatures issued by 13 certification authorities, it can handle more than 100 types of qualified certificates including those included in the national identity card. Its main clients are public administrations which use it to validate certificates used by citizens in their e-government applications. It also provides time stamping services and an e-signature client program that allows citizens to sign documents in various e-signature standards before submitting them online. It is planned that @firma will in the short term recognize certification authorities from other EU member states such as the Portuguese identity card and, in the medium term, will validate qualified certificates from authorities included in the EU Trusted List of Certification Service Providers.[65]
- An interoperability framework which establishes that public administrations will have a policy for electronic signature and certificates and that the General Administration of the State will define a policy for authentication and mutual recognition of electronic signatures to be used as a reference by other public administrations. The framework covers best practices for certification service providers and validation platforms and plans the development of a technical interoperability guide. Security is addressed in the National Security Framework. In practice, interoperability is addressed through the use of international standards and norms, including X509, SOAP, WSS, WS-I, XML, SSL and OSCP.

Implementation of the strategy

The strategy is seen as a driver for innovation in particular with respect to fostering cross-border electronic authentication and thus enabling or facilitating new services or the expansion of existing services to new markets. For example, an agreement signed recently with Portugal enables

Portuguese electronic identity cards to be validated in Spain for Spanish e-government services. Further, @firma is expected to support the validation of certificates issued from other countries' providers, potentially all EU Member States Trust Lists. In addition, Spain participates in the EU STORK project for electronic identity card cross-border interoperability within the EU. The project aims to use @firma validation services to enable Spanish citizens holding a digital certificate from a provider recognised by the Spanish Ministry of Industry to get access to other European e-government services in a transparent manner. Reciprocally, Spanish administrations will be able to identify foreign citizens by means of their national electronic identity card or qualified certificates.

As regards security, a proposal on assurance levels for electronic identity credentials setting three levels of assurance has been developed. In the private sector, it is the responsibility of the service owner to permit more or less rigid authentication methods, except when the law requires the use of electronic signatures. All e-government services must recognise the new electronic identity card which is therefore likely to become the standard solution for e-authentication in public sector contexts. The identity card's has been certified as a Secure Signature Creation Device against the Common Criteria by the Center for Cryptology. Access to the certificates requires the use of a PIN code and/or fingerprint match. Validation services provided by @firma are available to all eGovernment services of the country through the Private Administrative Network for Spanish Administrations (Red SARA) that interconnects all public bodies and offers encrypted channels. It can also exceptionally be offered temporarily over the Internet but all requests have to be signed. All @firma responses are signed for integrity and non-repudiation purposes. @firma is being certified by the National Center for Cryptology against the Common Criteria as Validation Authority compliant with EAL2+ level.

@firma is subject to auditing requests from public authorities or customers. Validation requests and responses and other actions performed by @firma as well as business and error alarms are logged in the central database of the validation platform. Logs are internally signed by the platform every day and can be used for auditing with guaranteed authenticity and integrity of the information they contain.

As regards privacy, the whole framework complies with data protection principles. Qualified certificates contain only the full name and national identity number of the holder. According to the data protection and e-signature laws, each time a citizen uses a certificate for authentication purposes, she is providing implicit consent to disclose the personal data to the e-government application. E-government applications must comply with the data protection law regarding how they handle this data. The validation

platform removes from its logs any personal data contained in the verification of the certificate. Privacy principles and rules that e-government applications have to follow for compliance with privacy legislation are also set out in the national security framework. Biometric data can only be requested at controlled points of access and relies on "match-on-card" technology. The national identity number included in all certificates can be disclosed to any e-government application. Other personal attributes can only be disclosed and exchanged between public administrations with user consent.

The government recognises that citizens use e-government services when they are appealing and useful to them. For example, the main reason at the beginning for the uptake of qualified certificates in Spain was to get a tax refund in a shorter period of time when the citizen was entitled to it according to the tax declaration. Several initiatives are under way to promote the use of the national identity card in a secure way: at the issuance point (police stations), citizens are instructed on how to use the identity card, a major awareness campaign has been launched in Spanish media, thousands of card readers have been distributed to citizens, several web sites are informing citizens on how to use the card.

Challenges

The most challenging aspects of the national strategy are:

- The lack of understanding regarding the possibilities offered by the electronic identification. Public awareness campaigns and efforts to increase the usability of the electronic identity card are essential.
- Electronic identity for foreigners. Participation in the European STORK project will facilitate the recognition of foreign credentials by Spanish e-government services.

At a more operational level, challenges include:

- The great variety of standards and technical norms, especially for smart-cards, which makes the integration of eID solutions extremely challenging.
- User-centric identity frameworks provide technical solutions to help users easily register with and sign on to web-based services. However, these frameworks alone cannot solve the human problem of establishing and maintaining trust. Convergence between user-centric and established federation standards and the incorporation of merged functionality into products are needed to bring user-centric identity management functionality to the mainstream.

- Although there is great demand for the recognition of governmental electronic identity credentials in commercial applications, the lack of proper and simple routines that can cover many different solutions explains why few private sector service providers support cross-border activities. Although public electronic identity credentials meet many of the private sector needs, business models and propriety solutions still complicate, or even prevent, development and common deployment.
- The private sector in some cases lacks the organisational and technological frameworks for electronic identity services. Instead, it is willing to use the solutions accepted and supported by the public sector, and also wants the public sector to handle an infrastructure that meets its need for flexibility. Public Sector Quality Authentication Assurance models could play an important role, as long as the Service Provider can rely on the mapping carried out by each national organisation.
- Open or closed electronic identity systems are an important issue to the private sector, not from a security point of view but because of practical routines. As long as there are practical routines in place, the private sector could accept the same electronic identity services as the public sector, but there is a need for a simple and stable routine to access electronic identity services. These services need to include entity authentication as well as digital signatures like signing data by natural persons and legal persons, or representatives of legal persons.
- Business models are very important to the private sector and should be subject to further studies in each member country. It is important to provide flexible solutions in this regard.

Sweden

The Swedish national strategy for IdM is a subset of the e-government strategy which aims to enhance the productivity and efficiency of public sector agencies and to boost the development capacity and innovative potential of society. It does, however, provide an IdM framework for both public and private bodies. Following a long tradition of identity credentials being provided by banks, an agreement between the government and a set of four companies selected through a public procurement process establishes a framework to encourage the provision of PKI certificates to citizens and of validation services to government bodies. This framework, which is being revised, benefits public and private sector IdM. The strategy does not

include single sign-on but all agencies accept electronic credentials from these selected companies and users are exposed to the same user interface regardless of the agency requiring identification. The strategy relies on a centralised registration policy: certificate service providers access the population register to provide their services.

National strategy for IdM

According to the current approach, a public procurement process selected four commercial certificate service providers: a bank (Nordea Bank), a bank consortium (BankID), a telecommunications operator (TeliaSonera Sweden) which co-operates with a Swedish bank and Steria, an IT security company. The customers of the first three companies cover most of the Swedish population. According to the framework agreement between them and the government, these companies issue digital certificates to users and provide validation services to public authorities. As individuals are generally already engaged in a trust relationship with the service providers, the acceptance level is relatively high. These digital certificates can be used in public and private sector contexts. Online providers (relying parties) pay for the verification services and market players cover the cost of the production of the certificates. This market model was chosen because it was assumed that competition among providers would reduce costs, that relying on existing companies would enable fast and cheap deployment to citizens and that the government would avoid a large upfront investment. [66] There is no government root Certificate Authority in Sweden.

According to figures available in 2009, approximately 2.5 million users have a digital certificate in Sweden, almost one million used it to submit their income tax declaration in 2009 and around 1.5 million public and private transactions rely on it every month.[67] In 2010, one of the selected services issued by 10 banks, BankID, claimed 75% of the market with more than 2 million users and over 400 public and private sector services recognising BankID.[68]

The IdM Strategy relies on the population register and on the personal identification number. The register which used to be maintained by the church since the early 17th century has been maintained by the National Tax Board since 1991. The personal identity number which includes the date of birth and birth number is assigned to all registered individuals and started to be used in 1974 as the key to every public record and many private ones. Sweden has also a long tradition of identity cards distributed by private organisations that contains this number.

The strategy supports two types of credentials: a soft token in the form of a file that individuals can download to their computer and a hard one, generally a smart card. Both enable authentication and e-signature via two digital certificates. The soft token is used in almost all transactions. The first hard token is the "National ID card prepared for e-Legitimation" (NIDEL) which has been issued by the police since 2005 and has been developed to enable identification in the context of the Schengen Treaty. It includes a chip but does not however carry a certificate at this stage. As of October 2009, 290 000 NIDEL cards had been issued. The second hard token is the card issued by the Tax Authority since June 2009 which can optionally carry a certificate issued by one of the four providers (Telia) and was developed to provide an identity document to as many people as possible, including people above the age of 13 and non-Swedish residents. All providers of soft and hard tokens follow the same technical specifications. Certificates include a public key, first and last name, personal identity number, date of validity of the public key, serial number, name of the issuing company and signature of the certificate provider.

Other forms of e-authentication are available in e-government applications such as login/password or two factor authentication (login/password + SMS message). Each service provider decides on the authentication solution to offer.

The legal framework supporting this approach includes a law on qualified electronic signatures which implements the European Directive 1999/93.[69] The law recognises advanced and qualified electronic signatures but only advanced signatures are available to individuals in Sweden. Besides electronic signatures, the law does not cover digital identity as such which is legally addressed only in the regularly renewed public procurement contracts. In 2008, a report from the Swedish Administrative Development Agency ("Verva") suggested to establish a new legal framework to regulate digital identity including functional requirements and the obligation to comply with European security standards. The framework would be applicable to public and private sector applications. A new agency would co-ordinate certificate providers and public sector bodies and act as a European contact point.

Certificate service providers which issue qualified electronic signatures must comply with security requirements and are supervised by the Post and Telecom Agency (PTS) which also maintains an e-signature advisory and discussion group with representatives from all interested parties. The Swedish privacy regulator, the Data Inspection Board, oversees the security of personal data used in IdM systems.

The Strategy underlines the need to use standards. However, inter-operability between the four providers is provided to the extent that online services accept all the credentials they offer. When some local and regional bodies limit access to credentials issued by one or two providers, inter-operability cannot be guaranteed. The new strategy proposes the implementation of a federation system whereby different identity providers can interact to enhance the usage of identities across domains. This will require additional legislation to be adopted.

Providers of e-services are responsible for informing users about regarding risks and benefits of their services, including IdM.

The current strategy is being reviewed. The Action plan for e-government adopted in June 2008 emphasises electronic identification as essential for trust and for the dialogue between government, citizens and businesses. A Delegation for e-government has been established within the Ministry of Finance with the representatives of 13 key public authorities to develop a strategy to enhance e-government efforts, to co-ordinate various IT projects, to examine possible concerns for citizens and companies and to assist in international questions. A report is expected by 2014. The new strategy will propose the establishment of a co-ordinating function for e-identification, electronic signatures and related services. An independent board with statutory decision making powers and the power to issue regulations would be set up within the Swedish Tax Agency. The board would supply services against payment, *e.g.* e-identification, electronic signatures, seals, etc., to affiliated government agencies and local government authorities. It would also provide support for a corresponding development in the business sector. Solutions here would need to include under-age users and/or those who do not have a personal identity number. The board would be required to direct and control the procedures used by issuers of electronic credentials so that, for example, personal identity numbers are only disclosed to agencies and other actors entitled to this information. The concept of e-service identification would no longer require the use of the personal identification number. Businesses and public bodies would be able to obtain credentials for their employees and contractors. As noted above, the new framework would support a federated model.

Challenges

Despite the success of the strategy so far, there are some challenges such as:

- Costs for the relying parties.
- Lack of flexibility of the overall model leading to some technical problems.

- E-authentication from public computers and from the workplace.
- Usability.

Turkey

The Turkish Strategy for IdM is based on the promotion of digital certificates and, in the near future, on the deployment of an electronic identity card. It includes: *i)* a centralised civil registration system (MERNIS); *ii)* a legal framework for electronic signature; and *iii)* an e-government gateway providing single sign-on. Future plans include the migration of the current paper-based identity card to an electronic identity card enabling secure electronic authentication for public and private sector services. The Turkish strategy is based on a centralised registration policy relying on the Turkish identity number.

National Strategy for IdM

Turkey has a long tradition of civil registration, dating back to the first census in 1904. Since the proclamation of the Turkish Republic in 1923, civil registration has been subject to many changes, the last of which was the establishment of a central civil registration system called MERNIS in 2000 to increase the speed and efficiency of public services and ensure secure and up-to-date access to personal information. MERNIS collects in real time changes made to citizens' civil status by 966 civil registration offices spread throughout the country. Its content, more than 130 million personal data files as of January 2009, is shared with over 2 500 public bodies for administrative purposes as well as some private sector organisations, subject to the limitations in the respective access protocols.

Since 2005, over 3 000 public and private bodies no longer need to request copies of civil records or domicile address certificates from citizens. They can access this information directly from the Identity Information Sharing System (KPS) via a virtual private network, whether through web sites[70] or web applications[71]. Access is subject to the conclusion of a bilateral agreement with the General Directorate of Civil Registration and Nationality.

The Turkish IdM strategy is also supported by a legal framework for electronic signature adopted at the beginning of 2004[72] and put into force in the middle of the same year which gives the same legal value to e-signatures generated with qualified electronic certificates as to handwritten signatures. Providers of qualified electronic certificates are legally liable for ensuring that the identity of the holder is determined in a reliable and secure manner. Four certificate service providers operate on the Turkish market and mobile

telecommunications operators introduced mobile e-signatures based on qualified electronic certificates, a service which is currently used in electronic banking applications for identity verification. As of June 2010, approximately 251 000 qualified electronic certificates had been sold, 105 000 of which were used for mobile electronic signatures.[73]

Since 2008, citizens can access a gateway to e-government services which provides a single sign-on mechanism and central authentication mechanisms that government services can rely on. This single sign-on solution offers authentication based on: *i)* a combination of identity number and password; *ii)* an electronic signature; *iii)* a mobile signature; and *iv)* in the future, the electronic citizenship card (see below).

The Turkish Information Society Strategy 2006-2010 envisages replacing the current paper-based identity card with an electronic "Republic of Turkey Identity Card" which will enable secure electronic authentication for public and private sector services. The card will enable authentication based on the combination of the Turkish identity number and a password or on a biometric, depending on the services' requirements. The pilot project on electronic identity cards implemented in the Bolu province was completed in November 2010 and country wide implementation and replacement of the paper-based identity card is expected to start in late 2011/early 2012, subject to the relevant decision to be delivered after the evaluation of the outcomes of the pilot The card will be issued by the General Directorate of Civil Registration and Nationality. It will contain identity information as well as fingerprints. It will only be used for identification and authentication. A Prime Minister Circular sets out the implementation details of the card project and prohibits public agencies from developing independent smartcard projects.[74]

Thus the Turkish IdM strategy encourages both the use of digital certificates and of the planned electronic identity card for electronic authentication. Qualified certificates issued by authorised service providers can be used to access public and private sector electronic services. Public and private bodies will be able to use the electronic card for controlling access to their services. The new electronic identity cards issued in the piloting phase were tested in hospitals, pharmacies and social security offices in the Bolu province.

The Turkish IdM strategy is based on a centralised registration policy: since 2000, all citizens are allocated a unique "Turkish Republic Identity Number" to resolve problems related to homonyms, provide fast and efficient identification, register all civil events from the moment of birth, and provide fast and efficient services to users of public services by ensuring efficient exchange of identity information among public institutions and

agencies. A Prime Minister Circular obliges all public agencies to attach this number in every relevant document (driver license, passport, forms, etc.) and to associate their relevant electronic record with this identifier. Public sector IT systems should use this number to enable electronic data exchange with the MERNIS database.[75]

Implementation of the strategy

As regards security, the electronic identity card contains a contact chip for national applications and a contactless chip for ICAO applications with a national operating system developed by the National Research Institute of Electronics and Cryptology (UEKAE), an affiliate of the Scientific and Technological Research Council of Turkey (TUBITAK) who is responsible for the execution of the pilot phase of the project. The contactless chip will not be used for generic identity authentication in daily business processes. The contact chip, designed by UEKAE, respects a number of international security standards and has a security level of EAL5+. The card may be read with standard smartcard readers or more sophisticated devices enabling fingerprint authentication and database connection to confirm the card validity. The design for the electronic identity card reader will be published as a Turkish standard by the Turkish Standards Institute. The security of e-signature applications complies with international standards as defined in the Communiqué on Processes and Technical Criteria Regarding Electronic Signatures.

As regards privacy, personal data in MERNIS is only shared with relevant public and private sector agencies, subject to the limitations contained in the respective access protocols. The public body in charge of the management of the system is liable for protecting the data from unauthorized access. In the new electronic identity card, biometric data is only stored in the card (rather than centrally) and technical protections are preventing retrieval. Qualified certificates do not cover sensitive personal data. The private key used for e-signature is stored on a smartcard based signature creation device with an EAL4+ security level.

Interoperability is provided at three levels: *i)* by the e-government gateway for e-authentication across all e-government applications; *ii)* by international standards and specifications for electronic signatures and qualified electronic certificates as set by the regulatory authority;[76] *iii)* by the planned electronic card which public and private sector services will be able to accept and that citizens will be able to use with the appropriate readers. The card itself complies with international standards. Standardisation of the card readers for specific functionalities is expected to address interoperability issues. A Guide for Interoperability which provides guidance

for public administrations with regards to standards and specifications to be used in their e-government project has been issued in 2005 and revised in 2009.

Challenges

The main challenge is to convince all public agencies to adopt a common IdM system and policy and to manage and overcome resistance from agencies to discard their pre-existing IdM systems, replace their specific identifiers with the Turkish Republic ID number and reject plans for specific smartcard based authentication tools particularly suited for their own business.

Another challenge is to convince private service providers that authentication mechanisms implemented by a public agency are reliable and secure. The e-government Gateway, for example, has a built-in single sign-on solution but banks, who provide money transfer services for e-government services requiring financial transactions, use their own authentication mechanism and do not trust the Gateway's single sign-on mechanism. Establishing a trust environment through authentication mechanisms based on determined standards and legal clarity regarding liabilities in using these authentication systems is key.

United States

Following up on its 2009 Cyberspace Policy Review which called for a "cybersecurity-focused identity management vision and strategy" that "addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation", the US government has released a draft "National Strategy for Trusted Identities in Cyberspace" in June 2010. The strategy supports the overarching vision of individuals and organisations utilising secure, efficient, easy to use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation. Key aspects include the concept of an ecosystem of interoperable identity service providers and relying parties (identity ecosystem) where individuals have the choice of different credentials or a single credential for different types of online transaction. Guiding principles include secure, interoperable, privacy friendly, voluntary, usable and cost efficient identity solutions. The US approach to identity management is based on a decentralised registration policy and on a federated identity model. It is at an early stage of development.

National strategy for IdM

President Obama's 2009 Cyberspace Policy Review called for the development of "a cybersecurity-focused identity management vision and strategy" that "addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation" (near term action item 10).

An interagency working group has been established and has had active engagement with industry during development of the strategy.[77] This process draws on recommendations included in broader reports.[78] It is also undertaken adjacent to related legislative efforts, such as the Data Accountability and Trust Act, which is currently being discussed at the US Congress.

On 25 June 2010, the White House released a draft "National Strategy for Trusted Identities in Cyberspace" and called for public comments. The strategy focuses on how to establish and maintain trusted digital identities as a key aspect for improving the security of online transactions. It encompasses transactions involving the private sector, individuals and governments and it addresses the international nature of many of these transactions. Thus the draft strategy, like the review, targets activities of the Nation as a whole, including both public and private interests and considers the role of the government as to address the safety and economic needs of its people.

The strategy supports the overarching vision of individuals and organisations utilising secure, efficient, easy to use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation. It builds upon four guiding principles which state that identity solutions will be *i)* secure and resilient; *ii)* interoperable at technical, semantic and policy levels; *iii)* privacy enhancing and voluntary for the public; and *iv)* cost-effective and easy to use.

The establishment of a national identification card is explicitly excluded in the draft strategy in favour of an ecosystem of interoperable identity service providers and relying parties (identity ecosystem) where individuals have the choice of different credentials or a single credential for different types of online transactions. Individuals should have the choice of obtaining identity credentials from either public or private sector identity providers, and they should be able to use these credentials for transactions requiring different levels of assurance across sectors. In the identity ecosystem, individuals, organisations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities. Several disparate organisations and individuals function together and fulfill unique roles and responsibilities governed by an overarching set of standards and rules. Individuals interacting with services that do not require

strong identification and authentication remain anonymous. This approach relies on a decentralised registration policy where organisations accept third party credentials from external parties.

To increase ease of use and reduce costs, the strategy supports federated identity solutions, fosters the elimination of silos that require individuals to maintain multiple identity credentials and encourages service providers to perform usability studies. Individuals will benefit from increased security, privacy, confidence, efficiency, easy to use mechanisms based on existing infrastructure components (cell phones, smart cards, computers) and choice. Organisations would benefit from fraud reduction, reusable infrastructure, lower implementation costs, and the minimisation of help desk and other burdensome processes. Public and private organisations would also benefit from increased innovation potential as the identity ecosystem would enable new higher risk services, including smart grid and health IT deployment.

The draft strategy benefits from high-level leadership (White House). It sets nine high priority actions such as the designation of a federal agency to lead the public/private efforts associated with advancing the vision, the development of a public/private implementation plan, the expansion of government services, pilots, and policies and further work to implement enhanced privacy protections.

Implementation of the strategy

The development of the strategy is only at a preliminary stage but a number of implementation policy directions are included in the draft strategy.

Interoperability is an important aspect of the draft strategy but it would be premature to assert which systems will be interoperable. As a general principle, interoperability and relationships between government and private sector systems is encouraged where appropriate; however, it will not be mandated across the board. As means of an example, the administration's Open Government initiative, which requires low correlation between a true and online identity, has benefitted from private sector interoperability efforts so that users wouldn't be required to establish a new identity/password specifically for this application. The draft strategy encourages non-proprietary standards and modular solutions to foster flexible, reliable and reusable systems.

Within the Federal Government, guidance and standards are being established which will help establish and track specific performance metrics. The United States also engages in international standards activities such as the Kantara Initiative, the standardization sector of the International Telecommu-

nication Union (ITU-T), and the International Standardization Organization (ISO), etc. These standards activities are key enablers for interoperability.

Several existing legislative and regulatory requirements are related to Federal Government identity management such as:

- The Privacy Act of 1974, which protects certain Federal Government records pertaining to individuals. In particular, the Act covers systems of records that an agency maintains and retrieves by an individual's name or other personal identifier (*e.g.* social security number).
- E-government Act of 2002, which intends to enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer (CIO) within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.
- Electronic Signatures in Global and National (ESIGN) Commerce Act of 2000**,** which was intended to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

There are sector-specific requirements for certain types of sensitive data (*e.g.* financial records, medical records, tax records, telephone toll records (customer proprietary network information – CPNI) With respect to at least one of these categories (CPNI), there are specific regulations from the telecommunication regulator (Federal Communications Commission) about when telephone companies can provide this information and what level of identity assurance is required to avoid pretexting which had been a problem.

Specific security policies and guidelines for the online IdM strategy have yet to be determined. Nevertheless, the strategy sets security and resilience of identity solutions as a guiding principle. Security includes strong cryptography, use of open security standards and auditable security processes. Currently, federal IdM systems adhere to strict security policies which vary significantly by application and by the type of security necessary for the information involved. Each IdM system is designed individually depending on its intended purpose, and as a result, the security policies for each system are often unique. For example, Homeland Security Presidential Directive (HSPD) 12- requires that all Federal Executive Departments and Agencies implement a Government-wide standard for secure and reliable forms of identification for employees and contractors, for access to Federal

facilities and information systems and designates the major milestones for implementation. The security of the applications involved in HSPD-12 implementation involves not only the physical security of the identification cards used, but also the general security of the background architecture.

As regards the government related systems, which is a subset of the strategy's scope, auditing controls will be designed according to the purpose of the individual application. The privacy, certification, and accreditation policies for these applications will be specifically tailored. Regarding Federal systems, Title III of the E-government Act, entitled the Federal Information Security Management Act (FISMA)[79] requires each federal agency to develop, document, and implement an agency-wide programme to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA requires security certification and accreditation of information systems to enable more consistent, comparable, and repeatable assessments of security controls in Federal information systems. These requirements can be found in NIST SP 800-37.[80]

Privacy Impact Assessments (PIAs) are conducted by Federal agencies to implement the principles established by the E-government Act and the Privacy Act. The goals inherent in federal PIAs will be adapted to online IdM, but the exact method has not yet been determined.

The draft strategy emphasises privacy enhancing and voluntary identity solutions. Identity solutions should preserve the positive privacy benefits of offline transactions while mitigating some of the negative effects. It calls for the full integration of the eight Fair Information Practice Principles (*i.e.* reflected in the OECD privacy principles) in the identity ecosystem as a key objective to achieve trusted identities in cyberspace. Examples of privacy approaches supported by the strategy include the creation and adoption of privacy enhancing technical standards that allow minimization of the personal data transmitted and of the linkage of credential use among and between providers; the communication of individuals' choices regarding the use of their data to all subsequent data holders; the limitation of personal data retention time; the possibility for individuals to access, correct and delete their data; auditable records regarding privacy protection and compliance with applicable standards, laws and policies.

Voluntary participation by individuals and organisations is a key concept whereby the Federal Government will not require organisations to adopt specific solutions nor require individuals to obtain high assurance digital credentials if they do not want to engage in high risk online transactions with the government. The identity ecosystem should encompass

a range of transactions from anonymous to high assurance and allow the individuals to select the credential he or she deems most appropriate for the transaction, provided it meets the risk requirement of the relying party. Thus the US government recognises the concept of proportionality between the amount of personal information collected and the level of assurance required in determining the appropriate level of authentication. Currently, the Privacy Act requires federal agencies to provide an explanation of "what information is to be collected" and "why". The Privacy Act only allows collection of personal information that is "relevant and necessary." A similar concept is found in NIST SP 800-63, which is used for Federal systems and is being utilised by international standards development organisations like the Kantara Initiative and is the basis of a joint standards project between ISO and ITU-T.

In Federal systems, high-level privacy notices including statements about what happens in the event of a data breach are required. Federal PIAs are also publicly posted on the Internet. The Federal Government is developing a national cybersecurity awareness campaign that will likely address identity management issues. How this principle will be adapted to the broader online IdM sphere has not yet been determined. Currently, requirements for notification differ by sector and by state. Forty-four states have breach-notification laws that require entities to notify residents of those states if any are affected by breaches of personally identifiable information. The laws vary by state. Some require the breached entity to also inform a state agency, such as the attorney general's office, if a breach occurs, which makes it easier to track breaches. The notification method may also differ depending on the type of data. This is an area of current research while the online IdM strategy is being developed.[81]

Challenges

The most challenging issues for the development of the US national IdM strategy are *i)* the identification of an approach that mutually benefits security and privacy concerns, *ii)* the collaborative policy development process required by the federal system of government and the involvement of the private sector. Other challenges are related to:

- Privacy: the approach must protect privacy and be perceived as "privacy enhancing" or it will fail; it must be flexible, and enable anonymity as appropriate; significant amounts of data can be liable to breach; there is a potential for procedural mistakes, there are legal differences between federal, state and at cross-border levels.

- Voluntary: the form of voluntary trusted assertion of identity that allows authentication of identity should be as acceptable and desirable as a credit card and not be seen as a required "national identity card" to be carried at all times, because that could be problematic in the United States.
- Interoperability: the approach must enable interoperability to avoid unnecessary incompatibility across systems and increased costs.
- Security: All forms of cyber threats have to be considered and the solution must be risk-based and promote the highest level of integrity corresponding to the risk, for example using strong cryptographic algorithms/protocols and no backdoors.
- Scaling: the framework needs to scale to population and minimize costs.

Appendix II

Contribution from the Internet Technical Advisory Committee (ITAC)[82]

Technologies have historically interacted with user identities and their associated personal data through a centralized approach that can secure the borders around the access to, and use of, services and data. Expanding this approach to link multiple centralized systems enables the re-use of user identity credentials among them, and similarly provides methods for accessing linked resources and data. The growing use of distributed solutions and multiple interaction points, however, has further expanded this approach to enable the use of decentralized identities with access to multiple repositories of associated personal data.

Supporting this change in focus are emerging solutions such as OpenID,[83] IMI,[84] OAuth,[85] and UMA.[86] Technologies such as these enable the user to control the release of specific personal data within a given context. While their details vary, they adhere to privacy-respecting patterns in which only the minimal amount of data is passed between parties under the control of the user, in order to satisfy a given transaction. Some of this work is taking place within well established standards bodies (*e.g.* OASIS,[87] IETF[88]), while other work is being developed within various open technical communities (*e.g.* OpenID Foundation,[89] Kantara Initiative[90]).

In more secure environments, specifically those in which higher levels of identity assurance are required, controlled use of personal data flow can be achieved by distributed solutions supporting technologies such as X.509/PKI,[91] SAML[92] and XACML.[93] While these solutions require more sophisticated deployments and in some cases closer integration between parties, they often enable flexible controls that may be necessary within some regulated environments (*e.g.* healthcare, banking, etc.). To ensure technical and regulatory compatibility, many organisations choose to leverage the defined commonalities by joining an identity management federation such as InCommon,[94] eduroam,[95] Janet(UK),[96] and STORK.[97]

In addition to solutions that are specifically related to identity management and associated personal data, there is a rich set of technologies that enhance security and privacy as well as improving overall confidence in the system. For example, when they are employed as part of a solution, DNSSEC,[98] DKIM,[99] and TLS[100] significantly increase trust within the system by providing assurance that distributed servers are communicating with the intended destination before transferring personal data. Distributed trust models such as the one put in place by the OIX[101] also help to engender trust between identity providers and relying parties.

Beyond the technical specifications and related solutions, there are programs focused on addressing regulatory environment that support them. These include the work funded by the Seventh Framework Programme[102] such as PrimeLife[103] and SWIFT[104]. Also of interest is the newly proposed Privacy Management Reference Model[105] at OASIS as well as ongoing engagement with policymakers within the Privacy and Public Policy Work Group[106] at the Kantara Initiative. Work such as this helps bridge the divide between technology and the environment in which identity solutions are deployed.

Appendix III

Questionnaire on national strategies and policies for IDM in OECD countries

This questionnaire was circulated to OECD delegations between December 2009 and May 2010.

I. National strategy for IdM

1. Do you have, or are you planning to develop a **national strategy** for IdM? If yes, please provide details, as appropriate, including on its **scope**[107] of coverage on and on the **rationale** or business case advanced for IdM (*please refer to Section 1.1 of the Primer on the "Importance and benefits of IdM").* Please highlight any aspects of the strategy that reflect issues addressed in the OECD Recommendation on e-authentication[108].
2. In your experience, which **substantive issues** are the most challenging to address when developing a national IdM strategy? *(please refer to Section 5 of the Primer)* Please provide details, as appropriate.
3. Does your national strategy address electronic **identity credentials**? Please provide details, as appropriate.
4. Does (and how does) your national strategy address **intersections or relationships** between government and private sector systems? For example, does it address the use of government issued electronic identity credentials to access private sector online services and *vice versa*? How does your strategy address areas where the private sector plays a part in the delivery of government services such as health or welfare, and *vice versa?* Please provide details, as appropriate.
5. Does your national strategy encompass **single sign-on** (*i.e.* where users log in once and gain access to all systems without being prompted to log in again) or **single e-authentication** approach? If yes, in what contexts? Please provide details, as appropriate.

II. Policies for the Implementation of your Strategy

Across this section, please provide **substantive examples** to illustrate your responses. In addition, please provide details regarding intersections or relationships between government and private sector IdM systems, where appropriate.

6. In your experience, which **challenges** are the most difficult to address in the implementation stages of your national strategy, including in the case of **intersections or relationships** between e-government IdM and the private sector? Please provide details, as appropriate.
7. How is your national IdM strategy intended to foster **innovation?** (*e.g.* new products, new processes, new types of co-operation, etc.)? *(please refer to. Section 4.1 of the Primer)*

Please provide details, as appropriate.

Interoperability

8. If your national strategy allows for or encourages **interoperable IdM**, how is this aspect implemented? Please provide details, as appropriate.
9. To what extent do you employ or encourage the use of **standards, norms or good practices** for interoperability of IdM systems?
10. Please provide details, as appropriate.
11. Is there **legislation or regulatory requirements** in place in your country to support interoperability of IdM systems? (*e.g.* regarding levels of assurance for authentication, specific sectoral security requirements, privacy, national identifiers, e-signature, liability, …).

Please provide details, as appropriate.

Security

(Please refer to section 5.3 of the Primer)

12. What is your policy with regards to the **security** of IdM systems and how is it enforced?
13. Please provide details, as appropriate, including measures taken to ensure the robustness of e-government IdM systems.

14. How do you ensure the **security of personal data**, including particular measures for sensitive personal data that is utilised in IDM systems?

Please provide details, as appropriate.

15. What role is foreseen for **auditing controls** to verify that your IdM systems are working as intended? How do you ensure that the security of e-government IdM systems is **appropriate and fit for purpose**?

Please provide details, as appropriate.

Privacy
(Please refer to section 5.4 of the Primer)

16. Do you have a policy with regards to the protection of **privacy** in relation to IdM systems?

If yes, please provide details, as appropriate.

17. What role is foreseen for **privacy impact assessments** for IdM systems? To what extent do privacy impact assessments affect the architecture, design and choices of IdM systems?

Please provide details, as appropriate.

18. Do you have a policy highlighting the need for **proportionality** between the amount of personal information collected and the level of assurance required in determining the appropriate level of authentication[109] (*e.g.* does your policy encourage the use of pseudonyms or other means of providing a relative level of anonymity to individuals)?

If yes, please provide details, as appropriate.

19. What is your policy with regards to identity **attributes** (*e.g.* name, social security number) which can be used for electronic authentication to e-government systems? Are **particular identity attributes** (*e.g.* national security number, biometrics) protected?

Please provide details, as appropriate

User empowerment
(Please refer to section 5.2 of the Primer)

20. How are end users/citizens made aware of the benefits and risks of using IdM systems?

Please provide details, as appropriate

21. In the instance of an incident (*e.g.* loss or corruption of identity data or credential), how are users/citizens informed? Are they made aware of who is accountable for what?

Please provide details, as appropriate

Notes

1. In addition to the countries included in the survey, Mexico provided some information regarding its National Identity project initiatied in 2003, under the leadership of the Ministry of Interior and with the National Population Register (RENAPO) as the agency in charge of the project. This project aims to develop a single national identity card supported by a national database of secure identification and free of duplicates. It will include information on the legal identity, the existential identity as a record of the individual, and biometrics data (fingerprints, facial features and iris recognition). Co-ordination is taking place with agencies and ministries as regards for example the National e-government strategies, the National Interoperability Framework and the Citizen Portal.

2. The lead agencies are the Australian Taxation Office (ATO) and the Department of Innovation, Industry, Science and Research (DIISR) for the joint provision of Business to Government (B2G) and Government to Government (G2G) authentication services; and the Department of Human Services (DHS) for the provision of People-to-Government (P2G) authentication services.

3. See *www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html*

4. For more details, see DVS Privacy Impact Assessments.

5. *myhelp.gv.at*

6. The unique 12 digit CRR number is never used directly. Instead, a "SourcePIN" number is cryptographically derived from the unique CRR number attributed to each Austrian resident. The link between the sourcePIN number and the individual is established by an electronic signature from the sourcePIN Register Authority which is the Austrian Data Protection Commission. However, the law defines 26 government sectors and requires that each of them uses a different identification number. So government agencies cannot use the SourcePIN identifier directly either. Instead, they are provided with a sector-specific PIN (ssPin), specific to each government sector, and cryptographically derived from the SourcePIN number. Authorities do not have access to ssPINs from other sectors and they do not know the sourcePIN from which ssPINs can be calculated for other sectors. The use of 26 ssPIN numbers by the government, one per government sector, and which cannot be related together, prevents cross-sector identification and tracking

of individuals. In other words, this mechanism is based on a single unique identifier per individual but uses cryptography to recreate identification silos for privacy purposes. Finally, the same process can be applied for private use, each company being treated as a specific additional sector. See IDABC and *http://ec.europa.eu/idabc/servlets/Doc?id=19404* and *https://online.tu-graz.ac.at/tug_online/voe_main2.getvolltext?pDocumentNr=43021*

7. *www.buergerkarte.at*

8. *www.digitales.oesterreich.gv.at/site/6469/default.aspx*

9. See: *egovlabs.gv.at*

10. The Federal Chancellery and the Graz University of Technology are partners in the project consortium. See *www.eid-stork.eu*

11. Pan-Canadian Strategy for Identity Management and Authentication was developed in 2007. See: www.cio.gov.bc.ca/idm/idmatf/default.asp. Work has been carried out since its publication. Canada is preparing a paper as an update to this strategy which should be ready for consultation early in 2011.

12. The individual strategies of provinces and territories are not yet formally aligned or integrated with the strategy of the federal government. For example, British Columbia has BCeID (https://www.bceid.ca/) Ontario has the One-key Service *https://www.iaa.gov.on.ca/iaalogin/IAALogin.jsp* Quebec has clicSÉCURE: *www.rrq.gouv.qc.ca/en/services/services_en_ligne/utilisation_securite_services/identification/Pages/clicsequr.aspx*

13. The federal Privacy Act, see *http://laws-lois.justice.gc.ca/eng/P-21/index.html?noCookie.*

14. Operational Security Standard: Management of Information Technology Security (*www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328*), Policy on Government Security (*www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text*), issued under the FAA, the Directive on Identity Management (*www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577&section=text*), Policy of Privacy Protection (*www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510&section=text*) Policy on Management of Information Technology (*www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755*)

15. *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text*

16. *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577&section=text*

17. The Directive on Social Insurance Number, see *www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342&section=text#cha5*

18. *www.tbs-sct.gc.ca/maf-crg/index-eng.asp*

19. *www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint-eng.asp*

20. The current card includes the following information: name, date of birth, gender, signature and fingerprint.

21. NCh 2777, by the National Normalization Institute

22. eID interoperability for PEGS : Update of Country Profile Study. Danish country profile. August 2009, p. 9.

23. *my page* at *ww.borger.dk*

24. 1 592 756 digital certificates (1 318 895 personal certificates, 265 061 employee certificates in 90 000 enterprises/government organisations, 6 533 enterprise certificates, 2 267 function certificates

25. *www.epractice.eu/en/cases/easylogin*

26. See *www.arpt.dz/Docs/3Actualite/Communication/8-9_12_2009/Communications/Session2/S2P1eng.pdf*

27. *www.epractice.eu/en/cases/easylogin*

28. *www.open-standaarden.nl/fileadmin/os/presentaties/Kop08_pres_HippeBrun.pdf*

29. NemID is based on a national standard based on ETSI (European Telecommunications Standards Institute) standards. NemLog-In is based on SAML.

30. *https://www.signatursekretariatet.dk/certifikatpolitikker.html*

31. *http://en.itst.dk/it-security/netsafe-now-campaigns*

32. *https://login.sikker-adgang.dk/fobslogin/visvilkaar.do*

33. Most of the information provided in this section reflects the IDABC country profile, referred to as a key resource in the German response to the questionnaire.

34. Many elements have been taken from the IDABC Italy country profile, in addition to the response provided by Italy.

35. Legislative Decree 235/2010, published in the Italian Official Journal of 10 January 2011.

36. In addition, 3.7 million use digital signature. See "Rapporto eGov Italia 2010" – chapter 1" - *www.innovazionepa.gov.it/comunicazione/notizie/2010/dicembre/20122010-brunetta-rapporto-e-gov2010.aspx*

37. See *www.apkic.org/WebSite/PKI2007/UpFile/File28.ppt*

38. "Understanding Korea's Identity Verification System", Byeong Gi Lee, Commissioner, Korea Communications Commission, December 2009, *http://121.254.145.213/gisa_down.php?pfile=%2Fdata1%2Fftp%2Fgisa_download%2F20091206_%C2%FC%B0%ED%C0%DA%B7%E1_Identity+Verification+System+2009.12.+BGL.doc*

39. In practice, two steps need to be considered:

Creation of the i-PIN *identity*: the first time a user wants to use the *i*-Pin system, she has to create an *i*-Pin identity through one of the four *i*-Pin providers which are operating on the market as semi-public companies. The process requires a two factor-authentication mechanism where *i)* the user provides her name and RRN, which are checked against the RRN registrar by the *i*-Pin provider and *ii)* the user validates one's real identity by providing one of these: a secret number sent to oneself via an SMS message, credit card information and its PIN number and a PKI authentication. At the end of the process, the user is provided with a unique *i*-Pin identity of her choice (like a pseudonym) associated to a password. This *i*-Pin identity can then be used on Web sites to provide a high level of assurance regarding the identity of the person without requiring the provision of the RRN.

Use of the i-PIN *identity:* when the user wants to create an account on a Web site, she first provides her *i*-Pin identity and password. The web site checks the *i*-Pin identity with the *i*-Pin provider. The *i*-Pin provider returns either *i)* a negative response if the *i*-Pin identity does not exists, does not match the password or has been revoked, *ii)* the name, gender and age of the user if the *i*-Pin credentials are valid. In the latter case, the user is invited to create an account on the Web site with a username and password dedicated to the site.

Unlike the direct use of the RRN, if the *i*-Pin identity is compromised, the user can request its revocation and the issuance of a new one.

40. See "Which LuxTrust product do I need for a particular application?". *https://www.luxtrust.lu/solutions/choix/choix?setLocale=EN*

41. Institut Luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ILNAS

42. See "eID Interoperability for PEGS: Update of Country Profiles study The Netherlands country profile - July 2009", IDABC, European eGovernment Services, *http://ec.europa.eu/idabc/servlets/Doc?id=32286*.

43. National Implementation Programme Service Delivery and eGovernment.

44. About the register, see: "The personal records database: for the authorities and for you", Ministry of the Interior and Kingdom Relations, *www.bprbzk.nl/dsresource?objectid=19176&type=org*. About the Citizen Number, see "Burgerservicenummer - Frequently Asked Questions", *www.burgerservicenummer.nl/veelgestelde_vragen/english_faq*.

45. See IDABC and *www.eoverheidvoorbedrijven.nl/afsprakenstelseleherkenning/english/english.html*.

46. DigiD, presentation by Gerrit Jan van't Eind at the 19th meeting of the OECD Working Party on Information Security and Privacy (WPISP) on 4 October 2005.

47. IDABC, p. 7.

48. For a list: *www.digid.nl/burger/over-digid/wie-doen-mee/*

49. *www.digid.nl/english*

50. Many of the principles underpinning the IAF reflect those in the *OECD Guidance for Electronic Authentication*, including ensuring security, privacy and usability, and managing risk.

51 . Individuals can also use choose to use several igovt logons for several services because these logons are pseudonymous. If they choose to have only one igovt logon, it can be used with all participating agencies, among which there will be some agencies that link the logon with an enduring "account" or customer record for the purposes of doing business with just that agency. There is currently no "all-of-government" account.

52. It is also granted to Brazilian citizens covered by the Treaty of Porto Seguro.

53. More than 10 000 companies have been created using this system, saving more than EUR 20 million.

54. Respectively *www.partalempresa.pt*, *www.automovelonline.mj.pt* and *https://queixaselectroncias.mai.gov.pt*.

55. *www.portaldocidadao.pt*

56. For example *www.riac.azores.gov.pt*

57. *E.g.* the Instituto Superior Téchnico *https://id.ist.utl.pt*

58. See *https://www.eid-stork.eu/*

59. Tax Procedure Act. Official Gazette of the Republic of Slovenia, No 117/06 in 24/08-ZDDKIS.

60. Additional information stored in chip include : filiation details, face picture, image of the handwritten signature, digital fingerprint, advanced certificates for authentication and for signature, certificate of the issuing authority and PIN code for each certificate.

61. Ley 59/2003

62. Ley 11/2007. See also the Royal Decree RD 1671/2009.

63. For a list of private sector services, see *www.dnielectronico.es/servicios_disponibles/serv_disp_priv.html*.

64. See IDABC country report.

65. This approach would change if it was decided to create a central European validation authority in charge of cross-border validaiton services or if other EU member states would establish a national validation authority to which it would be

necessary to make request and referral cross-border validation. Regarding the Trusted List of Certification Service Providers, see *http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm.*

66. Åke Grönlund, 2010.

67. See IDABC Sweden Country Profile, 2009.

68. "This is BankID". See also: "BankID in Sweden", Porvoo Meeting, 10 March 2008.

69. Law 2000 :832

70. Retrieve personal information using the Identity Number, the Identity Number using personal information, identity information based on information of the place of registration, copy of civil status records using various criteria.

71. The Identity Information Sharing System, 12 February 2009.

72. Official Gazette of 23 January 2004, entry into force on 23 July 2004.

73 . Information provided by the Turkish Delegation.

74. Prime Minister Circular 2007/16, 04 July 2007.

75. Prime Minister Circular No 2006/33, 21 October 2006.

76. *www.tk.gov.tr/eng/pdf/Communique_on_Electronic_Signature.pdf.*

77. Additional identity management efforts in areas such as screening, federal employee credentialing, healthcare, etc., are also underway but are beyond the scope of this survey's focus.

78. Such as the "Identity Management Task Force Report 2008" by the National Science and Technology Council (NSTC) and the National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Identity Management Strategy.

79. *http://csrc.nist.gov/drivers/documents/FISMA-final.pdf*

80. *http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf*

81. In November 2010, the United States Senate Judiciary Committee approved S.139 (Data Breach Notification Act) which would require entities engaged in interstate commerce to notify victims whose personal information is compromised in a breach — unless disclosure would harm national security or in some way hinder a law-enforcement investigation. Breached entities would have to notify the Secret Service if more than 10 000 individuals are affected by the breach, or if the breached database contains information on more than one million people, is a Federal Government database or is involved national security. This bill will now face a vote in the full Senate. S.1490 (Personal Data Privacy and Security Act), contains similar provisions and has been sent to the Judiciary Committee.

HR.2221 (Data Accountability and Trust Act), which has passed the House of Representatives, also contains breach notification provisions.

82. *www.internetac.org*.

83. OpenID (*www.openid.net/*)

84. IMI – Identity Metasystem Interoperability (*www.oasis-open.org/committees/imi/)*

85. OAuth (*https://datatracker.ietf.org/wg/oauth/charter/)*

86. UMA – User-Managed Access (*http://kantarainitiative.org/confluence/display/uma/Home*)

87. OASIS – Organization for the Advancement of Structured Information Standards (*www.oasis-open.org/*)

88. IETF – Internet Engineering Task Force (*www.ietf.org/*)

89. OpenID Foundation (*http://openid.net/foundation*)

90. Kantara Initiative (*http://kantarainitiative.org/*)

91. X.509/PKI - ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005

92. SAML – Security Assertion Markup Language (*www.oasis-open.org/committees/security/)*

93. XACML – eXtensible Access Control Markup Language (*www.oasis-open.org/committees/xacml/*)

94. InCommon Federation (*www.incommon.org/*)

95. eduroam – Education Roaming (*www.eduroam.org/*)

96. Janet(UK) – UK Education and Research Network (*www.ja.net/*)

97. STORK – Secure Identity Across Borders Linked (*www.eid-stork.eu/*)

98. DNSSEC – DNS Security Extensions (*www.dnssec.net/*)

99. DKIM – RFC 4871 DomainKeys Identified Mail (DKIM) Signatures (*http://datatracker.ietf.org/doc/rfc5672/*)

100. TLS – Transport Layer Security (*http://datatracker.ietf.org/wg/tls/charter/*)

101. OIX – Open Identity Exchange (*http://openidentityexchange.org/*)

102. Seventh Framework Programme (*http://cordis.europa.eu/fp7/home_en.html*)

103. PrimeLife (*www.primelife.eu/*)

104. SWIFT (*www.ist-swift.org/)*

105. PMRM – Privacy Management Reference Model (in process of formation at OASIS)

106. P3WG – Privacy and Public Policy Work Group (*http://kantarainitiative.org/confluence/display/p3wg/Home*)

107. E.*g.* public/private sector, e-government, e-commerce, sector-based strategy, etc.

108. See *www.oecd.org/dataoecd/32/45/38921342.pdf*.

109. In addition to the Primer, section 5.4 second bullet, please refer to OECD Guidance for Electronic Authentication, Part A, principle 5 (page 23 of *www.oecd.org/dataoecd/32/45/38921342.pdf*).

Annex 2

The role of digital identity management in the Internet economy: A primer for policy makers

This primer aims to provide policy makers a broad-brush understanding of the various dimensions of digital identity management (IdM). Consistent with the Seoul Ministerial Declaration, it also aims to support efforts to address public policy issues for securely managing and protecting digital identities, with a view to strengthening confidence in the online activities crucial to the growth of the Internet Economy.

*The primer is a product of the Working Party on Information Security and Privacy. It is part of a broader work programme on IdM that began with a workshop held in Trondheim, Norway in May 2007 (*www.oecd.org/sti/security-privacy/idm*). It was prepared by a volunteer group of experts led by Katarina de Brisis of Norway, with additional assistance from Nick Mansfield, consultant to the Secretariat, and Mary Rundle, who provided assistance in her capacity as a Research Associate with the Oxford Internet Institute through a project funded by the Lynde and Harry Bradley Foundation.*

This report was declassified by the Committee for Information, Computer and Communications Policy on 5 June 2009. It is published under the responsibility of the Secretary-General of the OECD and is available online at www.oecd.org/sti/security-privacy.

"WE DECLARE that, to contribute to the development of the Internet Economy, we will . . . strengthen confidence and security, through policies that . . . ensure the protection of digital identities"

OECD Ministerial Declaration (Seoul, June 2008)[1]

1. Introduction

National and global economic, governmental and social activities rely more and more on the Internet.[2] Digital identity management ("IdM") is a critical component of those activities. Today, organisations in both the public and private sectors differ significantly in their approaches to IdM, devising their own means for establishing, verifying, storing and using digital identities over their networks and the Internet. The lack of common policies and approaches creates privacy, security and productivity issues in our increasingly interconnected economies, and hampers the ability of organisations to provide users with convenient services.

This Primer is intended to give policy makers a broad-brush understanding of the various dimensions of IdM. It introduces, in non-technical terms, the basic concepts and issues raised by IdM and points to additional sources where policy makers may gain a deeper understanding of the topic. Consistent with the Seoul Ministerial Declaration, it aims to support efforts to address the public policy issues for securely managing and protecting digital identities with a view to strengthening confidence in online activities crucial to the growth of the Internet economy.

There is a wide spectrum of uses for which IdM is needed and contexts to which IdM schemes can be tailored. For example, IdM can be used within and across applications, systems and borders. This complexity is one of the main challenges to be addressed. Whether an IdM system is limited or expansive, another major challenge for its effective implementation is the creation of trustworthy environments, through good security and privacy policies and practices, user-friendly interfaces, and attention to user education and awareness.

For the purposes of this Primer, "***IdM***" is the set of rules, procedures and technical components that implement an organisation's policy related to the establishment, use and exchange of digital identity information for the purpose of accessing services or resources. Effective IdM policies safeguard digital identity information throughout its life cycle – from enrolment to revocation – while maximising the potential benefits of its use, including across domains to deliver joined-up services over the Internet.

The scope of the Primer is limited to the management of the digital identities of individuals, or natural persons. While issues related to the management of online identities for entities or objects are growing in importance,[3] they are beyond the scope of this document. On the other hand, the range of activities covered is intended to be wide, touching on the use of IdM for government, commercial, and social applications.

OECD consideration of IdM builds on prior work in a number of areas.[4] One is e-authentication, an essential component in the verification and management of identities online.[5] Other key building blocks are OECD work on privacy and information security.[6] The 1980 *Privacy Guidelines* continue to serve as an international benchmark, providing guidance on the handling of personal information in the private and public sectors, and the OECD's *Information and Network Security Guidelines* (2002) call for governments, businesses and individuals to factor security into the design and use of all information systems and networks and provide guidance on how to do so. Finally, consideration of IdM benefits from recent OECD work on the impact of identity theft on individuals.[7]

1.1 The importance and benefits of IdM

Online transactions – and many other types of online interactions – have become mainstream activities in OECD countries. By 2007, 95% of medium and large-size businesses in OECD countries were using the Internet, with some 25% of individuals buying goods and services on line, and 30% using Internet banking services. E-government is also on the rise, with, on average, 30% of citizens in OECD countries using the Internet to interact with public authorities.[8] Trustworthy IdM can only support continued online growth if it is more deeply and efficiently integrated into Internet activities.

IdM could be an enabler for e-government, e-commerce, and social interactions. The potential benefits of a well thought-out approach to IdM are many, including:

- ***Better use of resources.*** IdM could help in optimising processes that are duplicated across organisations and in reducing the complexity of integrating business applications, thus enabling organisations to sharpen their focus on the provision and quality of core services.
- ***Overcoming barriers to growth and fostering innovation.*** By helping organisations secure and control the sharing of identity information with partners and customers, IdM could spur collaboration, competition and increased user choice.

- ***Facilitating global services.*** For individuals and organisations with activities in multiple jurisdictions, IdM could improve online accessibility to private and public services across borders and simplify administrative formalities.
- ***Improving user convenience.*** When used across organisations, effective IdM could reduce the inconveniences and inefficiencies caused by the need to keep track of multiple accounts, passwords and authentication requirements. Likewise, more consistent user-interfaces for registration and log-in processes can improve usability, and consequently increase the use of online services.
- ***Enhancing security and privacy.*** Security and privacy are both increased by minimising the flows of data during transactions, only requesting, transferring, and storing what is required. Effective IdM can minimise the transactional data required for users of multiple systems and thereby decrease security and privacy risks.

1.2 The need for governments to be proactive

The report that accompanies the Seoul Ministerial Declaration on the Future of the Internet Economy highlights the relationship between trust-worthy user identities and sustainable growth of the Internet economy. It also emphasises the importance of addressing public policy issues raised by IdM, many of which are linked to trust.[9]

Trust is a cornerstone of electronic government, electronic commerce, and social interactions on line. With improved trust amongst participants, electronic delivery of government and business services can accelerate and higher levels of confidence can be achieved. This confidence can in turn encourage innovation in the online marketplace and create new ways of doing business. It can also encourage social interactions and the exchange of ideas between organisations and individuals, confident in the identities of those with whom they are dealing.

Without trust, individuals may develop a sense of vulnerability and insecurity regarding their online activities. In the absence of sound IdM policies and practices, there is a risk of identity information being released into the digital environment, facilitating the tracking of individuals' movements on the Internet or creating opportunities for identity theft. Some of this risk can be addressed through appropriate governance rules and procedures. Accordingly, governments may need to help ensure an appro-priate policy environment for the protection of individuals and their digital identities.

As a key factor in increasing trust in online activities, IdM is also a key factor in fostering the growth of the Internet economy. Given the current state of the global economy, the need to maximise the potential of the Internet economy assumes added significance.

2. Core concepts and processes

This section explains some of the key concepts and outlines some of the basic IdM processes. The range of conceptions of identity is very broad. The examination of the following concepts is for the purposes of this Primer only and recognises that they may be used differently in other contexts.

2.1 Identity, attributes, and credentials

The core issues at stake revolve around the term **"*identity*"**, a real world concept with digital manifestations. Off line, an identity is established from an extensive set of "***attributes***" (*e.g.*, name, height, birth date, employer, home address, passport number) associated with an individual. These attributes may be permanent or temporary, inherited, acquired, or assigned. In the digital world, on line, an individual identity can be established by combining both real world and digital attributes such as passwords or biometrics.

Selected attributes are used to establish an identity – off line or on line – and can be said to uniquely characterise an individual within a system or organisation although they may differ in character and number depending on the context. This context-specific notion of identity is sometimes referred to as "partial" identity.

To engage in online interactions that require some measure of electronic assurance that a person is who they claim to be, a person can be required to present a "***credential***": data that is used to authenticate the claimed digital identity or attributes of a person.[10] Examples of digital credentials include: an electronic signature, a password, a verified bank card number, a digital certificate, or a biometric template.

2.2 Enrolment and the issuance of credentials

While the technical aspects of IdM are complex, the basic processes can be described simply. They begin with enrolment, the process by which organisations verify an individual's identity claims before issuing digital credentials. These credentials can subsequently be used by the individual for authentication in the organisations' computer applications. Enrolment may require, depending on the applications and their policies, no personal information, little personal information or detailed personal information

(*e.g.* from name, address, date of birth to credit reference to social security number). For certain applications, the enrolment process may require other types of personal data, including the capture of one or more types of biometric data.

The verification requirements for enrolment can be fulfilled entirely on line or include an offline component, for example, mailing a verification code to the individual's residence. More stringent enrolment processes may require the presentation in person of physical credentials issued to the person by other entities. These may include government-issued credentials (*e.g.* passports, identity cards and drivers licenses) and/or credentials issued by private sector entities (*e.g.* employee badges, mobile wireless SIM cards, and credit cards). Government institutions such as motor vehicle departments and post offices sometimes accomplish identity verification through this type of "in-person" proofing." In addition, in-person proofing is common among banks, schools, and employers in their enrolment processes.

The enrolment process is completed with the issuance by the organisation of a digital credential. Credentials may be modified or suspended for various reasons, for example, to extend or restrict their duration or reflect a change in relevant attributes.

2.3 Authentication, authorisation process, and revocation

When an individual seeks access to an organisation's systems, he or she "***authenticates***" him or herself by providing the credential issued during the enrolment process. The authentication process provides a level of assurance as to whether the other party is who they claim to be. The level of assurance and associated authentication credentials required depends on the level of risk inherent in the transaction or interaction.

"***Authorisation***" refers to the process of assigning permissions and privileges to access a set of the organisation's resources or services. Different permissions can be associated with different digital identities. "***Revocation***" is the process of rescinding a credential which might occur, for example, when the individual leaves the organisation.

2.4 Biometrics

Biometrics are measurable biological and behavioural characteristics and can be used for strong online authentication. A number of types of biometrics can be digitised and used for automated recognition. Subject to technical, legal and other considerations, biometrics that might be suitable for IdM use include fingerprinting, facial recognition, voice recognition, finger and palm veins.

Biometrics can help reduce identity data duplication and ensure that an individual appears only once in any IdM database. Since biometrics do not depend on the possession of a physical object or the memorisation of a password, they may offer a potentially attractive option to strongly authenticate the identity of persons who have been enrolled in IdM systems designed to use them.

Some types of biometrics may be vulnerable to being copied (*e.g.* fingerprints) or otherwise subject to errors having consequences for individuals. These risks may be reduced by advances in technology. For maximum authentication strength, biometrics may be used in conjunction with other credentials, including additional types of biometrics ("multiple biometrics").

Because of their sensitivity, more frequent use of biometric data for online authentication would require careful balancing of the rights of individuals, interests of organisations and responsibilities of law enforcement agencies. For individuals, a higher degree of control could result from limiting the use of biometrics to those that remain under the local control of the individual (*e.g.* securely stored in an encrypted format on a device over which the person maintains control).

3. Examples of IDM usage

This section provides a few examples of current and anticipated uses of IdM in online applications.

3.1 Governmental uses of IdM

IdM can help governments provide citizens, including those who are home-bound, remotely-located or otherwise difficult to reach, with online access to their services. The importance of IdM grows as services increase in range and level of sophistication, particularly as more governments offer "joined-up" or integrated services within or between government organisations. Increasingly, risk management becomes crucial to the delivery of online government services as organisations strive to improve usability while addressing privacy and security.

Healthcare

IdM-enabled electronic health records can assist patient care by providing timely access to patients' medical and treatment history and connecting records held in multiple locations. Developments such as telemedicine can help provide medical care in remote areas but depend on accurately and securely linking patients and their medical information. The

range of organisations with a legitimate need to access relevant health information is broad, and may include medical practitioners, hospitals, laboratories, pharmacies, government and private health and insurance companies, employers, schools, and researchers. The sensitivity of health-related information highlights the importance of data minimisation and more broadly the need for security and privacy in this area.

Education

IdM also opens up opportunities in the area of education. The distributed nature of education and research means that resources are commonly scattered across different institutions around the world. Distance education and collaborative e-learning may require the establishment of authenticated relationships between students, institutions, and sometimes parents and guardians. IdM can help to address the problem of managing identities throughout a person's educational life-cycle, as well as multiple interactions with both educational systems and educational officers, within and across establishments.

Government employee identification

Efforts are underway in many countries to develop common standards for secure and reliable forms of identification for government employees. The benefits of these efforts could be interoperable identity cards which could permit access to government facilities and IT resources beyond the agency that issued the cards, through IdM systems that offer enhanced security, efficiency, reduced identity fraud, and the protection of personal privacy.

Identity cards and travel documents

Governments increasingly deliver national identity cards and passports containing embedded electronic data, often including biometrics, that have the potential to be used for public and private sector digital interactions. For example, a number of countries have or are considering implementing voluntary or mandatory national e-ID card programmes that enable cardholders to authenticate themselves to e-government services and digitally sign documents online using digital credentials stored on the cards. Some governments may also offer businesses and private organisations identity verification services (from age verification to proof of the absence of a criminal record). Electronic identity cards and e-passports can ease verification and authentication processing, but also require careful balancing of the benefits against factors such as security, privacy, costs, and customer experience.

3.2 Commercial uses of IdM

IdM can assist organisations in providing online access to existing services and in offering additional services. It can help businesses to build online customer relationships, to improve and customise the goods and services they offer and to target those services more effectively. Much of the potential of IdM for commercial applications lies in the possibilities to expand IdM beyond a single organisation or application and to do so while maintaining or improving the levels of convenience, security and privacy.

Travel industry

Some of the more innovative examples of IdM have emerged from the travel industry. For example, service providers can use information contained in flight reservations to offer hotel or rental car bookings by third parties. This reduces password administration for travel agencies and travellers. With alliances and protocols in place, airlines can also offer travellers single sign-on access to multiple providers and common use of passenger profile information, such as seat preferences.

Communications services

In the area of communications, a shift is occurring from number-based connections to person-based connections, with a different type of IdM framework required to manage these communications. From a communications provider's viewpoint it is necessary to develop service architectures that enable users to be provided with services over different platforms (Internet and mobile platforms, for example) and to provide a basis for users to access their chosen applications over multiple platforms in ways that are customised to their own preferences.

Electronic payments

Perhaps the most successful use of IdM in the commercial sector today is in the area of electronic payments for e-commerce transactions. Payment cards offered by financial services organisations and other online payment systems facilitate the exchange of funds. Through proprietary networks, a number of parties work together to make this possible (*e.g.* merchants, card networks, third party processors), exchanging information relating to consumers' payment card accounts.

3.3 Social uses of IdM

IdM used for online social purposes differs from other uses because of the widespread use of pseudonyms. Individuals can use multiple pseudonyms to participate in different activities such as checking news feeds, publishing blog posts, managing social networks and swapping photographs or music online. IdM can help provide individuals with more choices about how they participate in different communities, and the degree to which they want aspects of their different identities to be linked. Of course, the fact that two services allow for shared authentication does not necessarily mean that they will or should be allowed to exchange other kinds of user data.

Social networks

A number of social networking sites are currently exploring options for sharing authentication information and in some cases user data, such as "friend" lists and profile information. This could make it easier for individuals to bring aspects of their social networking profiles to their activities at affiliated sites and in turn to have information about those activities exported back to their social networks. Ensuring the individual's privacy preferences are exchanged between organisations along with the personal data is important, along with sufficient transparency and accountability to facilitate effective user control.

4. Technical and organisational aspects

Operating beneath the organisational objectives and policy choices are the technical IdM layers: the architectural (or functional or conceptual) layer and technical (or implementation or operational) layer. Current discussions about IdM in commercial environments often refer to a wide spectrum of different architectural and technical models, from a centralised IdM within a single domain (silo model) to multiple IdM systems distributed across multiple domains. These discussions can become confused when architecture and technology are mixed.

Directory systems usually provide the means by which identities are managed. In the paper-based world, directories connect people and organisations. In the early development of information technology, the use of directories was expanded to include the managing of digital credentials for users to log on to an online system. These uses form part of the evolution towards what we consider today to be IdM systems.

The earliest directories were known as technical control systems and provided centralised administration over a single domain network. The technical term "domain" has evolved from simply describing a single

network with a centralised technical controller into a much broader term to describe a bounded environment − whether legal, geographic or technical − within which there are commonalities such as the same rules, policies, and technical consistency. Early individual domains became described as "silos" because of the independent (and often unique) way in which they operated. The desire to join-up silo-based systems inspired the move to develop cross-domain IdM systems. A number of technical models are described in Appendix I. These can be viewed from both the service provider and user points of view. Typically, efficiency, trust and cost drive the choice of architecture, while the choice of technology is often driven by its ability to fulfil the functional requirements of the architecture, such as inter-operability.

The need to balance efficiency and trust across silo services is such that no single architecture is likely to fit all situations. However, where the goal is to join-up as many services as possible across multiple networks with a single user identity management interface, then the number and diversity of architectures that can be adopted will naturally be limited. Similarly this, in turn, will limit the choice of technologies that can be used to implement the architecture.

From the user perspective, the identity management system interface must be trustworthy, and an important factor for user trust is related to the privacy governance model. Appendix I includes trusted service provider-centric as well as trusted user-centric models. Usually a risk assessment will be undertaken to identify how to establish mutual trust between service providers and users. This may include trusted third parties acting between users and service providers.

Technical models help channel the flows of data in ways that serve users and organisations. But they essentially help operate and enforce the organisation's IdM policy, in compliance with law and regulation. Innovation, interoperability, and standardisation also play a role in the development of IdM.

4.1 Innovation

Innovative technology developments ultimately have to be tied back to actual uses in order to bring a return on investment. Recent experience in IdM has shown that, although ideas may have sufficient merit to be developed into products, the investments are unlikely to pay off unless embraced by a critical mass of participants in the Internet economy. The promise of the technologies depends not just on their development, but also on actual uptake in the context of different value transactions. For

commercial IdM systems, one challenge is that consumers do not seem to be willing to pay for IdM services.

The deployment of IdM with a view to enabling the use of identity information across systems, organisations, and borders, is waiting to reach a tipping point, where the dynamics change and compound growth takes over. This would cause the use and value of IdM systems to increase exponentially as more and more people use them, in turn making it likely that other users are equipped and familiar with the technologies.

Monitoring the impact of government-issued electronic identities in countries that are moving in that direction may provide useful insights. Government activities that may help spur the development of IdM could include for example, serving as an identity provider or mandating certain sub-sectors of the economy (*e.g.* healthcare, education) to use certain technologies in providing services. Clarification of accountability, liability and privacy issues may also be an enabler for innovation.

Another key factor influencing innovation is interoperability. Although some innovators may seek to corner their market in a proprietary manner, others may see greater possible benefits in adopting open standards if there is potential to reach all individuals rather than just a subset. For effective IdM, a key challenge is to create a shared infrastructure that facilitates interoperability between different IdM systems, their components, information and interconnection flows, and data exchanges. Specifically, common standards should enable components to support major protocols, claim types and token types, and to communicate their policies in a shared language. Meanwhile, the user experiences should be consistent throughout, independent of the underlying architectures and technologies.

Ultimately, the real benefits to innovation that could be brought by interoperability come from the services that interoperable IdM supports rather than from novel approaches to IdM itself.

4.2 The role of standards

Standards – thought of in the broadest sense of a common way or approach to doing things– reflect a consolidation of the requirements of suppliers, users, relying parties and law makers for co-ordinated implementation of IdM. When standards development is market-driven and consensus-based, they are most likely to be adopted. They can serve both to reduce complexity and enable interoperability.

International IdM standards

Formal standards produced by international organisations can have a stabilising function globally. Currently, a number of international organisations produce formal standards and guidelines relating to IdM, including the International Organisation for Standardisation (ISO), the International Telecommunications Union (ITU), and International Civil Aviation Organisation (ICAO).

ISO is a network of the national standards institutes of 157 countries which bridges the public and private sectors. The primary ISO voluntary standard focused on IdM is the Framework for Identity Management. However, various other standards are also relevant. [11]

Within the United Nations family, the ITU is the agency primarily responsible for co-ordinating international telecommunication. It has a number of groups working on telecommunication-related aspects of IdM in its Telecommunications Sector. Study Group 17, which is responsible for network security standards, has produced two recommendations, one on requirements for global identity management trust and interoperability and another on user control of digital identity.

ITU Study Group 13, which deals with Next Generation Networks, approved a recommendation on an NGN identity management framework in January 2009 with a number of others pending. A number of joint co–ordination mechanisms have been formed to co–ordinate the IdM work within the ITU and between the ITU and other organisations. In addition, the ITU Development Sector, which promotes capacity-building in the developing world, is preparing a best practices report on cybersecurity, which includes a basic discussion of IdM.

The ICAO, also within the United Nations family, has adopted standard specifications for machine readable travel documents to facilitate international travel. In particular, ICAO work to address biometrics in passports may be of interest in relation to enrolment and authentication in IdM systems. [12]

Other IdM standards bodies

There are a number of influential private-sector standards bodies in the area of IdM. These groups can comprise representatives from ICT companies, banking and credit card industries, consumer organisations, and government. They come together to devise IdM systems and projects that work across different networks, service platforms, and services. For example, Liberty Alliance is a global alliance of over 150 diverse organisations representing government, software and hardware companies, finance system integrators,

consumer services and end-user companies. Similarly, the Organization for the Advancement of Structured Information Standards (OASIS) consortium is the leading producer of standards for Web services (enabling machine-to-machine interactions), among other standards.

5. Public policy considerations

One of the main public policy goals for governments is working with all stakeholders to create favourable conditions for the development of IdM to benefit users. Given the broad spectrum of IdM applications – which can combine different identity attributes, apply different standards and technical processes, and provide different levels of assurance – the challenge for policymakers is to make available sufficient high-level guidance on user empowerment, security, the protection of privacy, and interoperability as they apply to IdM.

5.1 Interoperability issues

Public policy issues related to interoperability can arise at different levels: policy, legal, business process and technical:

- *Policy implemented at organisational level:* The challenge for organisations will be for each of them to articulate a clear set of IdM policies containing a common set of elements at high level to enable comparison of those policies across organisations, highlight areas of compatibility and facilitate policy interoperability.
- *Legal level*: Compatibility of regulatory compliance obligations across organisations will facilitate legal interoperability. From an international policy perspective, a key challenge is to minimise regulatory complexity and turn regulatory obligations into an enabler rather than a barrier to interoperability across borders. Issues may also need to be addressed regarding the role of contractual obligations.
- *Business process level:* Issues also arise at the business process level, where progress towards the adoption by organisations of common methods for IdM systems to communicate with each other may need to be considered.
- *Technical level*: Some measure of standardisation is necessary to achieve interoperability. The challenge is to encourage the development and use of all types of standards, in the broadest senses, (*e.g.* formal, informal, and private sector as appropriate) without stifling competition or undermining innovation.

5.2 Empowering users

Education and awareness have long been recognised as key elements for empowering users and fostering trust. To most users, IdM can be a confusing, technical, and rapidly changing topic. Several considerations and challenges can be identified:

- Incorporating privacy and security controls and training into the design and operation of IdM systems, which might alleviate some of the challenges and concerns for users.
- Consumers and citizens are currently faced with numerous digital identification systems and techniques. Greater transparency in the enrolment processes and the transfer processes for identity data are key issues to enabling them to make informed choices. Similarly addressing the education and awareness challenges can help consumers and citizens manage their digital identities appropriately.
- The proliferation of IdM systems could dilute accountability and transparency for how they are managed and operated, and in particular who bears what responsibility in the case of an incident. A major element of building user trust is the level of accountability and transparency that can be attributed across individual components of complex interconnected IdM systems. Accountability and transparency across multiple services in diverse legal and technical regimes is an important issue in empowering users.

5.3 Ensuring security

The security of IdM systems and communications requires the development and implementation of consistent policies to ensure the availability, confidentiality and integrity of identity data stored and exchanged by participants across private and public systems and networks. Reliable and robust IdM systems will be central and critical to the delivery of electronic government and private sector services online. The following are some challenges inherent in ensuring effective security:

- To have confidence in online services, users will expect identity information to be available when and where required. They will also expect that it is accurate and can only be accessed in storage and transfer by those who have legitimate authority and purpose.
- Other challenges relate to the need to minimise the impact of the disruption or corruption of an IdM system on any other services that may be dependent upon it. Consistent security policies that can be applied across all components of the services will need to be

developed and implemented. Joined-up services may raise particular challenges in this respect.

- The architecture, design and technology choices of all IdM components will be an important element to take into account in the assessment of the security risks to− and privacy impact on − the delivery of online services, and in determining appropriate levels of security.
- In the case of sensitive personal data, security concerns will be especially important. Auditing controls may be useful, including automated enforcement of user roles and rules. Developing processes and procedures to address the possibility of a data breach will also require attention.
- Another important consideration will be to ensure that the security of IdM systems is rigorously maintained in all public and private components. Audit controls can help to ensure that the security measures in place are operating as intended. Likewise, regular appraisals can help ensure that the security of the IdM system is appropriate and fit for the purpose.

5.4 Ensuring privacy

Much of the identity data in an IdM system will be personal information. If designed with inadequate privacy and data security controls, the use of identity information could lead to adverse consequences for consumers, including the risk of identity theft. When deployed effectively, however, IdM can play a privacy protective role, particularly in the context of social interactions. Important privacy considerations relate to data collection, data usage and storage, data minimisation, anonymity, pseudonymity, and the extent to which individuals have control over how their personal data is used. A number of these issues are identified below, not all of which are unique to IdM, but each of which is particularly implicated by the deployment of IdM.

- The potentially unlimited lifespan of digitised identity information and the declining costs of storage and processing raise issues regarding long-term assurances of safe storage and appropriate usage, and highlight the value of eliminating identity-related personal information when it is no longer needed.
- There is a risk that the greater availability of credentials from high-level assurance systems could increase their use in systems with lower-level assurance needs. This could increase the risk to personal data.

- Identity systems that facilitate anonymity and pseudonymity may offer promise. Their deployment would raise issues regarding who has the right to decide which data should be veiled and the circumstances under which it might be unveiled. This is of particular importance to the exercise of free expression, free association, and the security of the person. Linking identities that do not share the same degree of anonymity, or that contain different sets of attributes may allow others to overcome pseudonyms and discover the user's identity.
- Differences may arise as to which practices of identity and other data collection, use, and retention can be left to market forces and those that should be the subject of government intervention.

6. Conclusion

Achieving the Seoul Ministerial mandate to strengthen confidence and security through policies that ensure the protection of digital identities will require a global perspective across the broad areas of policy, law and technology. Key to developing policies for IDM is balancing privacy and security with the need for usability and interoperability while at the same time recognising that such policies will touch economic and societal interests of governments, businesses, and individuals.

Integral to these challenges is the role of government and its involvement in providing both assurances for online interactions and protection for individuals. As the Internet economy grows in importance, OECD governments recognise that there is a need to foster collaboration with private sector and civil society groups on the development of a policy framework for the protection and management of digital identities. Such a framework should provide an opportunity to strengthen trust, confidence and security in the online marketplace and e-government. It should provide assurances of identity online while preserving privacy, thereby contributing to the sustainable development of the Internet economy.

Notes

1 OECD, "The Seoul Declaration for the Future of the Internet Economy" (2008), available at: *www.oecd.org/futureinternet*.

2 The use of the term "Internet" is intended to be broad, and reflect the convergence of digital networks, devices, applications and services.

3 The OECD has done significant work on the privacy and security issues associated with RFID tags. See, OECD, "Radio-Frequency Identification (RFID): a Focus on Information Security and Privacy" (2008), available at: *www.olis.oecd.org/olis/2007doc.nsf/linkto/dsti-iccp-reg(2007)9-final*. It is now undertaking work on sensor-based networks.

4 OECD consideration of IdM began with a workshop held in Trondheim, Norway in May 2007. See, *www.oecd.org/document/41/0,3343,en_2649_34255_38327849_1_1_1_1,00.html*.

5 OECD Recommendation on Electronic Authentication (2007). This Recommendation builds on an e-authentication report providing policy and practical guidance. Both are available at: *www.oecd.org/dataoecd/32/45/38921342.pdf*.

6 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), available at: *www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html*; OECD, *Information and Network Security Guidelines* (2002), available at: *www.oecd.org/sti/cultureofsecurity*

7 OECD, "Online Identity Theft: Measuring the Threat to Consumers" (2008), available at: *www.oecd.org/document/59/0,3343,en_2649_34267_40830139_1_1_1_1,00.html*.

8 OECD, "The Future of the Internet: A Statistical Profile" (2008), available at: *www.oecd.org/dataoecd/44/56/40827598.pdf*.

9 OECD "Shaping Policies for the Future of the Internet Economy" (2008), at page. 26, available at: *www.oecd.org/futureinternet*.

10 OECD Guidance for Electronic Authentication (2007), at page. 12, available at: *www.oecd.org/dataoecd/32/45/38921342.pdf*.

11 The ISO IdM standard is ISO/IEC 24760. Other ISO standards that may be relevant include: Information Security Management (ISO/IEC 27001 and 27002); A Privacy Framework (ISO/IEC 29100); A Privacy Reference Architecture (ISO IEC 29101); Authentication Context for Biometrics (ISO/IEC 24761); Biometric Template Protection (ISO/IEC 24745).

12 See, *www2.icao.int/en/mrtd/Pages/default.aspx*.

Appendix I

Technical models

Historically, computerised identity systems kept identity-related information in separate "silos" that did not allow it to flow between different organisations and accounts. Over time, technical models have emerged to provide innovative ways for identity data to flow across silos. Continuous evolution has brought about hybrids and will likely give rise to new models.

The first part of this appendix presents a brief overview of the models as though they are completely distinct so as to highlight their different features. It is followed by a table describing the models' characteristics and a figure of each model showing the links between the parties to indicate who may hold personal data.

1. Siloed identity systems

A "siloed" identity system is one that is designed and operated in an independent manner, with no formal connections with other identity systems. Informal connections inherently exist in siloed systems (for example, the use of common attributes such as a name or date of birth) yet their influences are often overlooked. The main benefit of siloed identity systems is that corruption has a more limited reach, since user attributes in one system cannot be easily linked to different identifiers of the same users in other domains. As a result, a security problem in one domain (such as identity theft) is less likely to spill over into others.

However, siloed identity systems do not afford the convenience of linked-up systems. As soon as a person has multiple accounts on many different systems, the user experience becomes complicated and difficult to manage with a proliferation of account names, passwords, and profile data. From the point of view of an organisation providing multiple services to an individual, siloed systems are inefficient since identity data has to be maintained in multiple accounts within the organisation. The organisation is in some sense wasting resources and duplicating efforts in maintaining separate profiles with (mostly) the same information.

Nonetheless, there can also be value in controlling – not sharing – the use of identity data. There may be strong reasons for keeping profile data, even aspects of it, isolated from other data and particularly isolating profile data from other organisations or uses.

2. Centralised identity systems

One attempt to address the inconvenience of having identity information separated in silos is the centralisation approach. With this model, a person's data is housed independently of the application silos in a repository such as a directory, with data then made available to service providers from that one central source. Directories have evolved over the years to meet the increasing needs to share and reuse identity information and are the most common model for storing and managing digital identities.

3. Federated identity systems

With the "federated" model, service providers do not aggregate their account information, but rather establish a central "identity provider" that keeps track of which user identifiers correspond to the same user. In other words, federation links up previously unlinked identifiers. Begun in part as a reaction to the policy issues (privacy and security) created by centralised identity management, federation was designed to keep different account data distributed among service providers, with centrally linked up identifiers facilitating data flow among those service providers in the group who agree to trust each other.

A user can access services by authenticating to the central identity provider (which can also be a service provider), which in turn informs other service providers in the federation about his authentication status. The value for the person is that a single authentication event at their primary account can be used with multiple service providers. The arrangement is also valuable for the organisations that are members of the federation, because most of them do not need to create and maintain an account for the user in order to offer him services. By relying on a person's primary account to authenticate him, other members of the federation avoid the burden of password management. The identity provider can also facilitate any data sharing that is to take place between any two accounts of a user, since it knows which identifiers correspond to the same user. The provider in effect becomes a trusted third party.

Federation can be more convenient for users and efficient for the organisations managing their accounts, but it also gives rise to new challenges. For example, it may not be easy to enable information sharing between organisations that do not have a pre-established relationship but from whom an individual would like co–ordinated service delivery. More recently, contractual and policy models have emerged to supplement the technology in order to help mediate relationships between unknown parties. In addition, automated trust negotiation that relies partly on reputation

engines may help unknown organisations to form relationships for service delivery.

Ideally, federated environments would have developed rules to control downstream transfers of information to other actors. This can make federation somewhat unwieldy for users who want their accounts to be portable and who find themselves at the mercy of the organisations that control their primary account. If those organisations choose not to establish a federation relationship with users' preferred service providers, users may be unable to use their federated accounts to access those service providers. Another challenge relates to the problem of determining liability for these complex business relationships and protecting against theft and errors. The main vulnerabilities stem from the fact that the identity provider knows which identifiers correspond to a given user. This knowledge places the identity provider in a position where it could impersonate the user or enable others to do so.

Single sign-on

Single sign-on technology (SSO) reduces the number of times a user must remember and use a password. In a typical deployment, single sign-on does not usually reduce the number of logon events; instead, it uses client-side technology to automate logons and hide them from the user, while still protecting the security of user passwords and account information. Single sign–on can be used in both federated and user-centric systems.

4. "User-centric" identity systems

User-centric identity systems are one approach to give users greater control over their personal information. Users are allowed to choose identity providers independently of service providers and do not need to provide personal information to service providers in order to receive services. Identity providers act as trusted third parties to store user account and profile information and authenticate users, and service providers accept assertions or claims about users from identity providers. However, with the user-centric model, identity providers are not part of a federation and so are said to operate in the interest of the users rather than in the interest of the service providers. These service providers are called "relying parties." In this model, users choose what information to disclose when dealing with service providers in particular transactions – although service providers may still require certain information for the transaction to take place. Individuals may use several identity providers as well, so that their information is not all stored in one place.

To close the gap when a user and relying party distrust each other, an identity provider can also serve as a trusted third-party broker. A user will typically only trust a broker if s/he can control it; relying parties will not trust a broker if the claims asserted are actually self-vouched by the user. To respond to this dilemma, approaches are being developed with appropriate steps used to prove identity so that all relying parties are assured that the information is correct before engaging with the user, while leaving the individual in control. Cryptography and other technologies can play a part in this process.

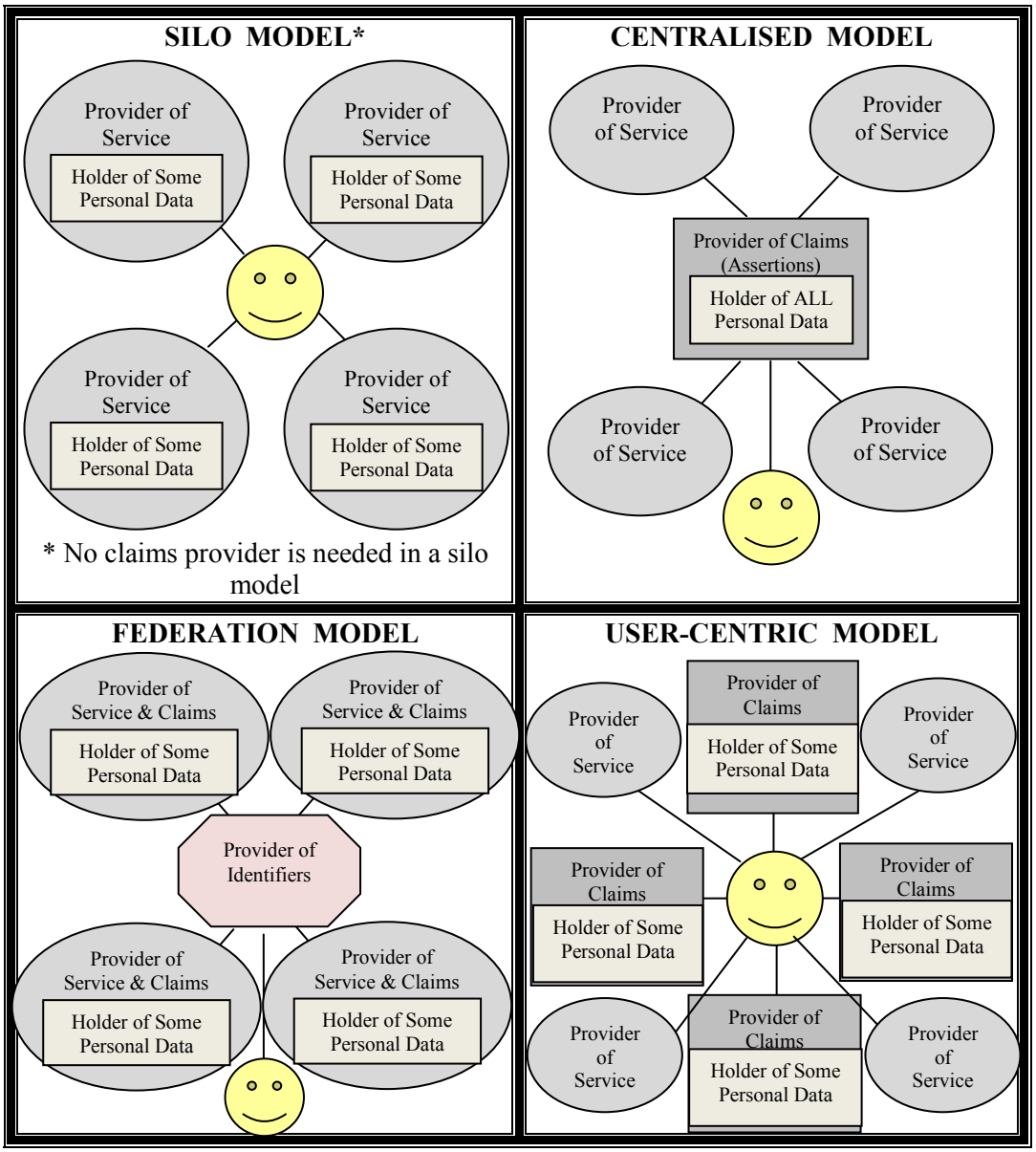
Table A2.1. Features of Technology Models for IdM systems

	Siloed	Centralised	Federated	User-Centric
Method of Authentication	The user authenticates to each account when he wishes to use it.	The user authenticates to one main account.	The user authenticates to an identity provider, with this one authentication serving for the federation.	The user authenticates to identity providers, and service providers have to rely on that authentication.
Location of Identity Information	Identity information is stored in separate service provider accounts.	Identity information is stored in the one main account, a super account.	Service providers in the federation keep separate accounts in different locations. They may have agreements for sharing information.	Identity information is stored by identity providers chosen by the user. The user can help prevent the build-up of profiles that others hold about him.
Method of linking accounts/ learning if they belong to the same person	There is no linking between accounts and no information flow between them.	Linking between accounts is not applicable. (A user's full profile resides in that single place.)	The identity provider can indicate what identifiers for accounts with federation members correspond to the same person.	Uses of cryptography can prevent linkages between a user's different digital identities, leaving the user in control.

Table A2.1. Features of Technology Models for IdM systems (cont'd)

	Siloed	Centralised	Federated	User-Centric
Trust Characteristics (who is dependent on whom, for what)	The user is reliant on the service provider to protect their information, even if limited. The absence of information sharing has privacy advantages.	The user is reliant on the service provider to maintain the privacy and security of all of his or her data.	Users have rights from contracts, but they may be unfamiliar with options. The federation has leverage as it is in possession of the user's information.	Users can keep accounts separate and still allow information to flow, but bear greater responsibility.
Convenience	Siloed accounts are inconvenient for users and service providers due to multiple authentications, redundant entry of information, and lack of data flow.	This arrangement is easy for the user since he or she only has to deal with one credential to call up the account and since he or she has to authenticate just once.	Other members of the federation avoid the burden of credential management. Organisations that provide services to a user can coordinate service delivery.	Users may be ill-equipped to manage their own data (also a vulnerability) and may need training and awareness-raising.
Vulnerabilities	Siloed systems offer the advantage of having limited data on hand, thus creating less of an incentive for attack. They also have a better defined and stronger security boundary to keep attackers out and limit exposure from failures.	The central party controls the person's entire profile; other entities have little to check that profile against, and an insider could impersonate the person or alter data. Currently there is no way to safeguard data after it has been shared.	Users have little input into the business-partner agreements. Some service providers will set up federation systems to exploit users. Currently there is no way to safeguard data after it has been shared.	Concentration in the market for identity providers could leave them with much power. Currently there is no way to safeguard data after it has been shared.

Figure 1. Individuals (data subjects ☺) *and* providers of services, claims, and identifiers: Who holds the personal data *and* What are the links between these parties?



Appendix II

Additional IDM Resources

International organisations

ENISA, "Privacy Features of European eID Card Specifications" (2009), available at: *www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_features_eID.pdf*.

ENISA, "Security Issues of Authentication Using Mobile Devices" (2008), available at: *www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf*.

FIDIS, Identity in a Networked World" (2006), available at: *www.fidis.net/resources/networked-world/*

ITU-T Focus Group on Identity Management "Report on Requirements for Global Interoperable Identity Management" (2007) available at: *ftp3.itu.ch/fgidm/Deliverables/0296-att-1.doc. Additional information is available here: www.itu.int/ITU-T/studygroups/com17/fgidm/index.html*.

ITU-T Study Group 13, "Framework architecture for interoperable identity management systems" (2009).

PRIME, "Prime White Paper" (2008) available at: *https://www.prime-project.eu/prime_products/whitepaper/index_html*.

PrimeLife, "First Report on Standardisation and Interoperability" (2008), available at: *www.primelife.eu/images/stories/deliverables/d3.3.1_d3.4.1-public.pdf*.

Governments

Australia, "National Identity Security Strategy" and "Documents Verification Service", *www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity#q1*.

Australia, "National e-Authentication Framework", *www.finance.gov.au/e-government/security-and-authentication/docs/NeAF-framework.pdf*.

Industry Canada, "Protecting and Managing Digital Identities Online: Understanding and Addressing the Public Policy Issues of Online Identity Assurances" (February 2009).

Information and Privacy Commissioner of Ontario, "The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation" (2009), available at: *www.ipc.on.ca/images/Resources/F-PIA_2.pdf*.

Privacy Commissioner of Canada, "Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues" (2007), available at: *www.privcom.gc.ca/information/pub/id_paper_e.pdf*.

U.S. National Science and Technology Council, "Identity Management Task Force Report 2008", available at: *www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf*.

Other resources and initiatives

Biometrics Institute Privacy Code: *www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8*.

Higgins Open Source Identity Framework: *www.eclipse.org/higgins*/.

Identity Commons: *idcommons.net*/.

Information Card Foundation: *informationcard.net/*.

Jericho Forum: *www.opengroup.org/jericho*/

Liberty Alliance, "Liberty Identity Assurance Framework" (2008, v1.1) available at: *www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf*.

Mary Rundle and Paul Trevithick, "Interoperability in the New Digital Identity Infrastructure," (2007), available at: *papers.ssrn.com/sol3/papers.cfm?abstract_id=962701*.

Mary Rundle, *et. al*, "At a Crossroads: 'Personhood' and Digital Identity in the Information Society"(2008), available at: *www.oecd.org/dataoecd/31/6/40204773.doc*.

OASIS Identity Metasystem Interoperability (IMI) TC: *www.oasis-open.org/committees/tc_home.php?wg_abbrev=imi*.

OpenID: *openid.net*/.

Pamela Dingle (OSIS), "Analysis of a User-Centric Interoperability Event" (2008), available at: *www.nulli.com/documents/I3_Analysis.pdf*.

Robin McKenzie and Malcolm Crompton, "Use Case for Identity Management in E-government" available at: *www.iispartners.com/IEEE_artilcle_Apr2008.pdf*.

3G Americas, "Identity Management: Overview of Standards and Technologies for Fixed and Mobile Internet" (2009), available at: *new.3gamericas.org/documents/3GAmericas_Unified_Identity_Management_Jan2009.pdf*.

Annex 3

Report of the OECD workshop on digital identity management

The OECD held a Workshop on Digital Identity Management (IDM) on 8-9 May 2007 in Trondheim, Norway, that was co-hosted by Norway's Ministry of Government Administration and Reform and Ministry of Education and Research. The event was organised by the OECD Working Party on Information Security and Privacy (WPISP) and attracted some 70 participants, gathered from government, industry, academia and civil society organisations across the OECD.

The objective of the two-day workshop was to bring together experts to explore the main policy issues surrounding digital identity management, and in particular to establish a common understanding of the challenges raised by IDM with respect to information security and privacy. Discussions on the first day concentrated on illustrative examples of IDM frameworks, solutions and applications. Day 2 focused on the users of IDM systems, both in terms of their needs and the challenges they face. The concluding session brought together some of the main themes raised during the workshop, with a view to arriving at some useful steps that could be taken at the international level, including by the OECD.

This document presents summaries of the four sessions, the last of which includes the Chair's main points from the workshop. It has been prepared by the OECD Secretariat. Presentations delivered at the workshop and other workshop materials are available online via the OECD website at: www.oecd.org/sti/security-privacy/idm.

Welcome and keynote speeches

On behalf of the Norwegian Ministry of Government Administration and Reform, **Hugo Parr** welcomed participants to Trondheim, noting its reputation as the IT capital of Norway. Describing the most recent eNorway Plan, he explained that public ICT systems in Norway will have a common backbone, based on common standards, and certain common components across all sectors which will include eID. Turning to his aspirations for the workshop, Mr. Parr expressed his hope that participants could identify good, simple, trustworthy interoperable systems as well as helping to bridge the gap between the policy makers and the experts.

Welcoming participants on behalf of the Norwegian Ministry of Education and Research, **Jan Peter Stromsheim**, conveyed the regrets of Mr. Hans Christian Holte, who was unable to participate in the event as had been planned. In his remarks, Mr. Stromsheim highlighted the increasingly crucial role of ICT for education, describing the Federated Identity Management program that has been developed for the Norwegian education system. Already operational within institutions of higher education, the identity management system is expected to be available by 2010 for all schools – a considerable challenge given the large number of schools and students involved, as well as the variations in ICT skill levels.

The Workshop Chair, **Katarina de Brisis**, offered participants words of welcome as well. Beginning with an introduction to the work of the WPISP (which she serves as a vice-chair) Ms. De Brisis also linked WPISP work on IDM to an OECD Ministerial meeting on the Future of the Internet Economy to be held in Seoul in June 2008. In terms of key IDM issues, she expressed her hope the workshop would help participants get a better grasp of the relationships between identity and digital identity, as well as the challenges of achieving interoperability in this space. In this respect she highlighted the importance of understanding the architectures and frameworks currently under development.

Daniel Greenwood, from the MIT Media lab, delivered the first of two keynote addresses. He provided a broad context on IDM systems and architectures, beginning with the identification of three models for IDM systems. The first model is characterised by centralised ownership and decision making, the second is a federated model, and the third is oriented around individual ownership and decision making. Further distinctions can be drawn in terms of the trust models around which IDM systems are based. Some are authority-based (*e.g.* national identity card), others power-based (*e.g.* in the employment context), and still others agreement-based (*e.g.* federated systems).

The presentation also noted that distinctions can be drawn between organisation models for IMD systems and their technical architectures.

Mr. Greenwood observed that digital identity is a key component of the transformation to an information society/economy, noting that existing processes for handling digital identity are not sufficient. ID theft, for example, has social impacts – sense of violation, loss of self-confidence – the economic consequences of which are difficult to measure. Key short-term needs for improved IDM can be seen in areas like social networking, aggregate intelligence, group decision making, and reputation engines. Noting that special protections are needed for protecting the core element of identity, Mr. Greenwood called for the creation of an international identity bill of rights (inspired by the OECD *Privacy Guidelines*) as well as a global infrastructure for the interoperability and integrity of identity and authentications in all sectors. There is, he explained, a unique need for international co-operation in this area.

The second keynote address was delivered by **Andreas Pfitzmann**, who focused his presentation on the concept of digital identity itself. Digital identity primarily is a set of attributes, some of which change over time and some of which may be certified by third parties. Given the increasing collection and use of digital data, a digital identity is only growing – never shrinking.

One of the key concepts introduced by Mr. Pfitzmann is that of the partial identity (pID). Achieving security and privacy, he explained, requires users to subset their digital identity into pIDs, each of which might have its own name, identifier, and means of authentication. Using pIDs requires at least one personal computer administrating personal data and executing cryptographic protocols that is controlled by the user; digital pseudonyms for secure authentication, and anonymous credentials to transfer certified attributes from one pID to another pID of the same digital identity.

Mr. Pfizmann offered a variety of ways to classify identity attributes, including whether they are authenticated by third parties; easy to change; varying over time; given vs. chosen; and pure attributes vs. attributes containing side information. Attributes that are not easy to change, that do not vary over time, are given, or contain side information require greater protection than others and may be considered "core ID". For online use, Mr. Pfizmann recommended that users manage their own IDs, presenting pIDs via digital pseudonyms. He also noted the importance of having the right tools and communications partners. He concluded his keynote explaining at the present we have an identity management patchwork. Just as security is only as good as the weakest link of the chain, privacy is at most as good as the most privacy-invasive "layer" you are using. What is needed therefore is an identity management framework to address both security and privacy.

The discussion that followed the keynotes was oriented around the degree to which individuals should be thought of as "owning" their identity, as an antidote to the view of many organisations who consider that they "own" the personal data they have accumulated on their customers. It was suggested that ownership is not a particularly useful concept in this context, and that a discussion oriented around the notion of "control" is more likely to be constructive.

Session 1: Frameworks, solutions and R&D projects

The aim of this session was to provide an overview of interoperable identity frameworks, models and solutions, whether federated or "user-centric," already developed or still being researched. **Dirk Van Rooy** of the European Commission served as the moderator, noting his interest is taking from the session discussion some good ideas for future research projects.

Speaking on behalf of the Liberty Alliance Framework, **Robin Wilton** of Sun Microsystems, explained that five years ago Liberty was formed to address the challenges of federated identity, not just from the supplier perspective but also from the one of the adopters. The work being done by Liberty includes not only the development of technical specifications but the preparation of advice and guidance along with an ecosystem of products and services. In terms of the challenges, Mr. Wilton highlighted privacy and liability issues, noting the need to ensure that an individual's privacy preferences are "stuck" to data as it moves between organisations.

The second speaker in this session, **Chris Brunio** of Microsoft, began by observing that identity is the missing layer in the Internet, leaving us in identity silos. He described the "laws of identity" as a way to structure our understanding of identity, and the role of the "laws" in an identity metasystem that includes devices, technology, applications, governments, organisations, businesses and individuals. In order to return control to individuals, Mr. Brunio explained, Cardspace allows users to select an identity (a graphical representation) and transfer only the identity that is desired/requested.

The next speaker, **Thomas Gross** of IBM, provided an overview of the Privacy and Identity Management Project for Europe (PRIME). The vision of this joint industry-academia initiative is to enable users to act and interact in a safe and secure way while retaining control of their private sphere. Mr. Gross highlighted a number of design principles for PRIME: design must start from maximum privacy, with privacy rules being explicit, enforced, trustworthy and usable. He noted that identity management with strong privacy protection is emerging significantly and that open standards are vital

for enabling collaboration. He advocated the promotion of pseudonyms, partial identities, and controlled attribute release, concluding that when in doubt, the user should be empowered to make the decision.

Tony Rutowski, Verisign, addressed his remarks on the topic of bridging the IDM gaps, through a discussion of a recently formed group at the ITU-T. The ITU work is motivated in part by a growing realisation by critical infrastructure protection communities of the vulnerabilities of today's ubiquitous nomadic use of public IP-Enabled network infra-structures. Mr. Rutowski identified as a key challenge that global discovery capabilities are rapidly diminishing. Given the variety of perspectives through which IDM is approached – user centric vs. network operator vs. application service provider – there is a need for a common global Identity Management framework. The objectives of the project are the development of a trusted ability to manage ICT credentials, assigned identifiers, attribute information and reputation/patterns. It will also aim to accommodate a variety of autonomous and evolving platforms. Mr. Rutowski closed his presentation noting the need to identify and close IdM "regulatory gaps" both at the national and international levels.

Moving the discussion to research and development, **Jim Dray** highlighted the vision of his work at the US National Institute of Standards and Technology: identities that work seamlessly everywhere, that allow user control over private information, and that relying parties can trust. He noted that smart card interoperability still faces challenges, both in term of platforms (tokens, interfaces) and credentials (data formats, name space management). The latter challenge – semantic interoperability – is the tougher of the two. Mr. Dray identified a number of key research topics, including the need for common models and approaches to ontology, namespaces, and interoperability. He also noted the need for research into more basic questions like why do we want globally interoperable eID? Even more basic questions regarding what is an identity and what aspects of it do we need/want to manage still need work.

Denis Royer, Goethe University Frankfurt, described a European research programme, the Future of Identity in the Information Society (FIDIS). He highlighted the interdisciplinary character of IDM, which includes socio-cultural, technology, governmental, and economic elements. FIDIS is seeking to determine how the different identities, roles, and systems can be integrated. This requires answering questions like, which processes and workflows are actually affected? How is privacy and data protection handled? How to deal with compliance? Who is actually responsible? This approach makes clear that Identity Management is not a purely technology driven topic, but also has a scientific, social, legislative, and economic dimension.

During the discussion at the conclusion of the session, workshop participants provided a number of responses to the Chair's request for an identification of the key topics for further research. Reiterating themes of the speaker presentations these responses included a catalogue of models and use cases that individuals can understand, research on how to ensure the discoverability of identity, addressing the semantic challenges through the development of common language and vocabulary.

Session 2: Government and business case studies

Jane Hamilton, of Industry Canada, moderated the second session, which focused on government and business case studies. She encouraged the speakers to touch on a number of issues in their presentations, including the degree to which the case study fits with the "silo", walled garden or more interoperable models as well as the type of architecture and trust model on which it relied.

The first of several speakers providing IDM examples from the public sector was **Ingrid Melve**, UNINETT Norway. She described FEIDE, a federated IDM system for connecting all users in the Norwegian education sector. She noted that the benefits of the FEIDE system include a single username/password for users across services. This provides user convenience and creates savings for the service providers in terms of password resets. She described the trust fabric, which is based on contractual arrangements, as well as the technologies, and business drivers. Highlighting the challenges, Ms. Melve observed that finding trusted means of authentication remained a challenge, along with enforcing the information policy flows.

Moving the discussion from the education sector to public sector employees, **Curt Barker**, US NIST, described the US government programme called PIV (Personal Identity Verification) for employees and contractors. The NIST has been working to develop standards and guidelines for the PIV. Mr. Baker noted that a number of impediments have been encountered, including a tight schedule, large and mutually non-interoperable installed base, business models predicated on proprietary discriminators, privacy interests, biometric interoperability issues, and varied use cases. Among the lessons learned to date, a key point is the value of minimising the amount of information on the card.

Highlighting the role of government as a provider of identities, **Sara Marshall** described the work of the UK Home Office Identity and Passport Service, including the policy framework for maximising the benefits of a new national identity scheme. She highlighted a context that includes economic migration, money laundering, terrorism, and aging populations. She highlighted the need for careful balancing, for example, between

security and costs and customer experiences or between effective public services and safeguarding privacy, or finally, simply balancing the benefits to the state vs. the benefits to the individual.

Speaking on behalf of the Korean Information Security Agency (KISA) **Chanjoo Chung** described the genesis of the i-PIN in Korea, which was developed in part to respond to problems with theft of the Korean Resident Registration Numbers. The i-PIN is provided and managed by a trusted third party. The benefits of the i-PIN include the fact that it can be reissued at any time, contains no personal information (only issuer information), employs strong identity verification methods, and cannot be used to trace other website registration information. Currently some 25 000 Koreans have an i-PIN, with the goal that all Koreans will have at least one soon. The next version of the i-PIN, expected in 2008, is planned to be interoperable with an e-wallet.

Re-orienting the discussion from IDM in the public sector to private sector examples, **Stephen Whitlock**, Boeing, highlighted the challenges of adapting a silo-based IDM system to an increasingly global enterprise needing to manage identities of non-employees, devices and applications. In some jurisdictions companies cannot ask for citizenship, but at the same time some export decisions cannot be made without citizenship information. He noted the increasing need for identity assurance levels between enterprises, as well as challenge related to the blurring of identification, authentication, and authorisation in products, protocols and ceremonies.

Continuing the focus on business case studies, **Michael Barrett** of PayPal described the challenges of federating three highly decentralised business units that had grown rapidly, emphasising the security issues. Good anti-fraud procedures can help reduce financial losses, but do not necessarily prevent a loss of user trust. Mr. Barrent noted that PayPal is the top-phished brand on the Internet. The security measures implemented by PayPal include authenticated e-mail, safe browsers, and a new PayPal Security Key programme, which though still in beta has already issued 40 000 RSA tokens to allow more secure access to PayPal accounts.

Jean-Pierre Tual, Gemalto, presented a case study from the tele-communications industry. He described IMD for telcos as a "nightmare", particularly for mobile operators. One response has been the creation of the Fidelity project, a consortium of leading European telcos, industry and research organisations that are implementing circles of trust according to Liberty Alliance specifications. The goal is to enable an exchange of identity and authentication of citizens between service and identity providers, while leaving the identity data under the user's control. Among the challenges he identified is presenting the whole process (user consent, interface, registration,

etc.) in an understandable way to the user, as well as attribute brokerage, authentication delegation, security, and neutrality.

In concluding Day 1, the Workshop Chair, Katarina de Brisis, highlighted some key themes, including the need for terminology to make discussion easier. She also noted the need for a narrative to help individuals and stakeholders better understand the benefits and requirements of IDM. Likewise, a better understanding of the trust issues could be of assistance. On the whole, a key emerging theme is the role of governments in this area.

Session 3: Technical, legal and societal challenges and responses

This session focused on technical, legal and societal dimensions of IDM, with a view to identifying critical success factors for developing coherent and trustworthy systems. It was moderated by **Jan-Martin Lowendahl** of the Gartner Group who highlighted his hope that some simple guidance would emerge from the discussions.

Three speakers addressed the topic of interoperability, the first of whom was **Andre Vasconcelos**, of the Portuguese Knowledge Society Agency. He described the interoperability framework for the new Portuguese citizen's card, which will replace five other national cards. The card is a physical document that allows the visual identification of a citizen and it is also a digital document that allows the citizen to identify himself/herself and to electronically sign documents. In addition to addressing interoperability challenges related to data formats, authorisation processes, and general incompatibility between different public administration databases, it is planned that the card should be interoperable with other European systems. Plans are already made with Belgian authorities in this respect.

Gillian Ormiston, Motorola, began her presentation by noting some of the basic challenges related to interoperability and identity: dates are rendered in formats that appear the same, but reverse the places for day and month; the same names can result in transliteration problems depending on the language in which it is being rendered; the same person can have multiple residences and even citizenships. Ms. Ormiston emphasised that cross-border interoperability requires standards, but also an understanding of how to interpret the standards. A European standards testing and accreditation body would be useful in this context. Other interoperability issues identified by Ms. Ormiston include data storage and equipment issues, and variations in data protection legislation.

Paul Trevithick described Higgins, an open source identity agenda and interoperability framework. It takes a privacy enhancing user-centric approach. Maximum decentralisation is good for privacy and security,

which can be accomplished by using the user to link things back together. Users have many partial identities, each in its own context or silo. All these separate contexts can be linked via a metaphor called an i-card, with each partial identity having a separate i-card. The i-cards in turn are managed by an identity agent (*e.g.* Microsoft Cardspace) which can run on a computer or a mobile device in the Internet cloud. Once the user is authenticated to the agent, there is no further need for passwords. The agent projects and protects identity attributes for authentication and personalisation. Attributes can be blinded using PRIME/Idemix technology. As an interoperability framework Higgins also provides a common data model that enables linking across heterogeneous contexts.

Moving the discussion from interoperability to security, **Ben Laurie**, Google, presented his ideas on selective disclosure, a technique for minimising the privacy risks associated with the use of digital signature in connection with an IDM system. More precisely, Mr. Laurie's objective was to be privacy protective by ensuring that data a user shares with one website is not linkable to data shared with any other site with which the user interacts. For an IDM system to be both useful and privacy protective it must permit assertions that are verifiable, minimal, and unlinkable. The challenges arise when traditional digital signatures are used to authenticate a user or make a verifiable assertion that permits replying parties and assertion issuers to collude to link the assertions and therefore the identifiers. The solution proposed by Mr. Laurie, involves the use of a cryptography technology that permits zero-knowledge and selective disclosure proofs. These can allow a user to prove an assertion and link that proof to an identity, but to do so in a way that does not provide the relying party access to material that could be later linked to other assertions. Of course, some assertions will contain inherently identifying information, like a physical address, which will usually be linkable. But selective disclosure can prevent users from being exposed to the risk that less obvious kinds of information be linked.

The second speaker on security, **Bob Blakley** of the Burton Group, highlighted what he considers to be the absurdity of "owning" your own identity. A lot of identity information is owned by others. And a person cannot sell her identity, or access services without disclosing it. Even if my records are de-identified, data mining can reconstruct them. The problems relate to asymmetry and risks posed by aggregation of data. What needs to be abandoned is the notion of privacy as secrecy. A person can retain his/her dignity even if people know something about him/her. The key, Mr. Blakey concluded, is to ensure that people who receive personal information treat it with respect and are held accountable.

Frank Leyman, FEDICT, discussed security architectures and trust modeling. He highlighted increasing risks for users, including the theft of data, misuse of data for other purposes, and easier linkages between databases, but also the potential benefits, like more efficient use of available data, electronic handling of formalities, and the simplification of procedures. Mr. Leyman described a paper-based single sign-on identity that is being introduced in Belgium to be accompanied by a mandatory smartcard electronic identity card. A strong focus will be placed on ensuring the sources are authentic. Potential public sector uses include the signing of digital documents, on-line tax declaration, on-line consulting of a personal file in the National Register, and a variety of local authorities' applications (*e.g.* change of address, request for attestations, library access cards, etc.) Other possible uses include e-commerce, student cards, and e-banking.

Richard Mapleston, Shell, discussed the importance of risk management and auditing. His presentation highlighted the increasing demands for transparent audit trails from electronic documents and the need to securely bind content and identity. The challenges are particularly acute when a company wants to work outside with third parties. The default solution for the moment is e-mail, but this is not robust enough and digital signatures could be the future. Mr. Mapelston pointed out that the real challenges to adoption are organisational not technical. He concluded that government leadership and direction appears to make the difference, particularly in the context of government procurement.

Discussion focused on identifying the most critical challenges. Proposals were varied, ranging from the need for an exceptions-handling process, to the difficulty of getting all key stakeholders in the same room; from the need for success stories based on decentralised architectures to the need to focus more on outcomes for individuals and less of technology architectures.

Toby Stevens of the Enterprise Privacy Group proposed a reorientation of the debate from identity management to identity assurance. Highlighting the challenges related to enrolment, he explained that the benefits of large-scale approaches to IDM flow to the organisations who will be able to limit their liabilities, rather than to consumers who will simply end up revealing more personal data. We don't often need to know who someone is, just whether or not they are authorised to do something. Mr. Stevens proposed that governments should establish a uniqueness register, established via biometrics and other attributes, and then vouch for the uniqueness of an individual in the register. What is needed is uniqueness management, not identity management.

Reporting on a recent Federal Trade Commission workshop, **Naomi Lefkovitz** focused her remarks on the challenges of creating consumer trust and acceptance. Held on April 23-24, the workshop explored use of authentication and IDM processes as a means of reducing identity theft. The key message from the workshop is that without consumer trust and acceptance any IDM system would fail. Ms. Lefkovitz identified consumer beliefs about benevolence, integrity, and mental models as key factors in influencing trust. Building trust required a confluence of: an alignment of drivers (*e.g.* convenience, access to services); effective design and usability, consumer education, and a legal framework that protects privacy, appropriately allocates risk and provides failure management.

Fred Carter, from the Ontario Information and Privacy Commissioners Office, continued the discussion of privacy issues, echoing the notion that weak public confidence and trust is the primary obstacle to user acceptance. Mr. Carter described work done in his office to condense the fair information practices into three principles: data minimisation, user participation and control, and information security. He noted that IDM should be considered in the context of other privacy enhancing technologies, which have experienced considerable difficulties in becoming operational over the past ten years. He commended the application of the privacy embedded seven "laws of identity" in the deployment of IDM systems and also noted the privacy benefits possible with biometric encryption.

Irma von der Ploeg, Zuyd University, began with some opening remarks about attributes and identifiers before describing her assessment methodology which focuses on three key elements: identifiers, system architecture, and systems in use. She identified a number of emerging IDM challenges: avoiding security and privacy risks (skimming, phishing, hackable databases etc.); limiting identity to where it is strictly required; maximising PETs, pseudonymity, anonymity. She noted that universal identifiers (*e.g.* biometrics) exacerbate security and privacy risks, that there is a need to design digital identities for a specific context/domain, and that different definitions and forms of 'security' lead to contradictory priorities in IDM system design. She further noted that managing digital identity should not remain a prerogative of the system owners but allow for end user control and that technical issues should be considered as normative/political issues. Ms. Von der Ploeg concluded that further transparency and public debate is needed, along with informed citizens/customers.

Mary Rundle, Harvard Law School, began by highlighting the potential benefits of IDM in terms of convenience and security, reduced fraud and phishing, the hassles of lost passwords and even helping to usher in a new Internet boom. To bring these benefits, however, Ms. Rundle identified as a key challenge the need to bridge data protection principles and identity

management technologies. To be effective potential solutions should: observe international data protection standards; be clear and easy for people; hook into the IDM infrastructure; allow audits of how data is treated; and afford a mechanism for redress. One way to implement the clear and easy aspects of a solution would be to develop Creative Commons-like icons that are readable by humans, lawyers, and machines. Ms. Rundle concluded by proposing that the OECD or another international body consider offering redress services in the data protection context.

Session 4: Conclusions and next steps

The final session wrapped up the two-day discussion and provided an overview of the key policy concerns. Participants included the two keynote speakers and the moderators, joined by **Malcolm Crompton** of Information Integrity Solutions and **Thomas Gross** of IBM.

Ms. de Brisis offered preliminary thoughts as workshop chair to facilitate the panel discussion. There was widespread agreement that the workshop had been interesting, had brought together a wide range of interests, and had offered a "concentrated reality check" that revealed: *i*) the confusion still surrounding IDM; *ii*) the need for further analysis and research; *iii*) the need for common understanding, and; *iv*) the need to identify policy actions. Confusion included questions still unanswered such as: why are we talking about digital identity management? what are we talking about? who are the stakeholders? what are the key success factors for the stakeholders? She reminded participants of the role that OECD could play here, namely to foster trade and development in the information economy while ensuring respect of essential requirements in market democracies (*e.g.* trans-border data flows, security and privacy).

The discussion was then conducted round the table, indicating a general support for the Chair's remarks. **Mr. Crompton** emphasised the need to approach IDM with a user focus and to examine the real issues faced by individuals. Those include control (as in "who is in control"; "how is control shared") and risk (what risks faced by the individuals are improved or made worse or newly introduced by any ID management scheme and how might they be re-allocated, mitigated or otherwise handled in order to make sure that the IDM proposition is attractive and fair from their perspective) as well as convenience. He noted that the user requirement for identity management for e-enabled services between citizens and business and government is different from a security law or enforcement requirement and that separation of these objectives, and possibly separate delivery vehicles, is likely to be essential for full citizen acceptance of IDM initiatives.

More generally, the discussion revolved around the recognition of the broad scope and multifaceted nature of identity management. IDM is at the intersection point between various contexts from national ID schemes to e-commerce and user-centric systems. There are multiple challenges as well as conflicting objectives and tensions between the needs of various stakeholders. The roles of some stakeholders are multiple, subtle and complex. Governments for example have up to three roles: as a protector of the greater good, provider of digital identities and as a provider of services. IDM can be approached from a technical, legal, or social point of view but all need to be taken into account in a holistic manner. IDM is an important issue for countries, not only for companies, and OECD is well placed to assist.

Various suggestions for next steps were made, such as: developing a thesaurus mapping the terms used in relation to IDM in different contexts to facilitate a common understanding of the issues to be addressed (noting that several already exist such as the effort of the ITU); further examining models and catalogues of architectures, trust and discovery, and business cases behind the use of IDM; analysing use cases to better understand the life cycle of IDM and how to build in end-to-end security and privacy. The need for sharing good practice among governments and with other stakeholders as well as the need for guidance on the ideal IDM ecology elements, including "agreed universal rights" for digital identity and identifiers, were highlighted.

Ms. de Brisis noted that basic questions remain about the public policy issues surrounding IDM and the varied ways in which they are viewed by governments. Other key questions concern the IDM marketplace and the roles of various actors. Various business models for IDM would need to be examined to determine what efforts can be made towards securing interoperability of IDM-schemes. Finally, more work is needed to identify the costs/benefits of IDM as wells as interests of government, business and individual users in IDM systems. Nevertheless, a number of areas of agreement were found and next steps for OECD might *inter alia* focus on:

- *Digital identity* to determine what constitutes identity (core elements providing unique identification independent of context) and how identity maps into the digital world, to clarify who needs to be "in control" of an identity and what being in control actually means. It would be useful to identify ID attributes that need not be commonly used (*i.e.* should only be used in "silos"), as well as the extent to which core identity is compatible with partial identities and pseudonyms.

- *Identity management systems* to clearly articulate the benefits of IDM for the different stakeholders and in various contexts, to remedy the lack of a compelling narrative for IDM across domains or borders. Work also remains to be done to identify security and privacy requirements for the different stakeholders, what are the similarities and differences between IDM approaches – user-centric, service provider-centric, and network-centric (*e.g*. Liberty Alliance, InfoCard, OpenID). Finally guidance could be developed on design and implementation of IDM across domains, in respect to:
  - Usability / user friendliness
  - Security
  - Privacy protection – user control
  - Cost-effectiveness
  - The role of businesses and the role of governments.

Ms. de Brisis closed the workshop by thanking speakers and participants for their active contributions during the workshop and also the Norwegian government for hosting the event.