Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

11-Jun-2009

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2008)10/FINAL
Unclassified

Working Party on Information Security and Privacy

THE ROLE OF DIGITAL IDENTITY MANAGEMENT IN THE INTERNET ECONOMY:

A PRIMER FOR POLICY MAKERS

JT03266499

English - Or. English

FOREWORD

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.

TABLE OF CONTENTS

THE ROLE OF DIGITAL IDENTITY MANAGEMENT IN THE INTERNET ECONOMY: A PRIMER FOR POLICYMAKERS

> "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 trustworthy 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 appropriate 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 tele-medicine 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 Annex 1. 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 interoperability.

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. Annex 1 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.

ANNEX 1

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 Annex 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 diagram 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.

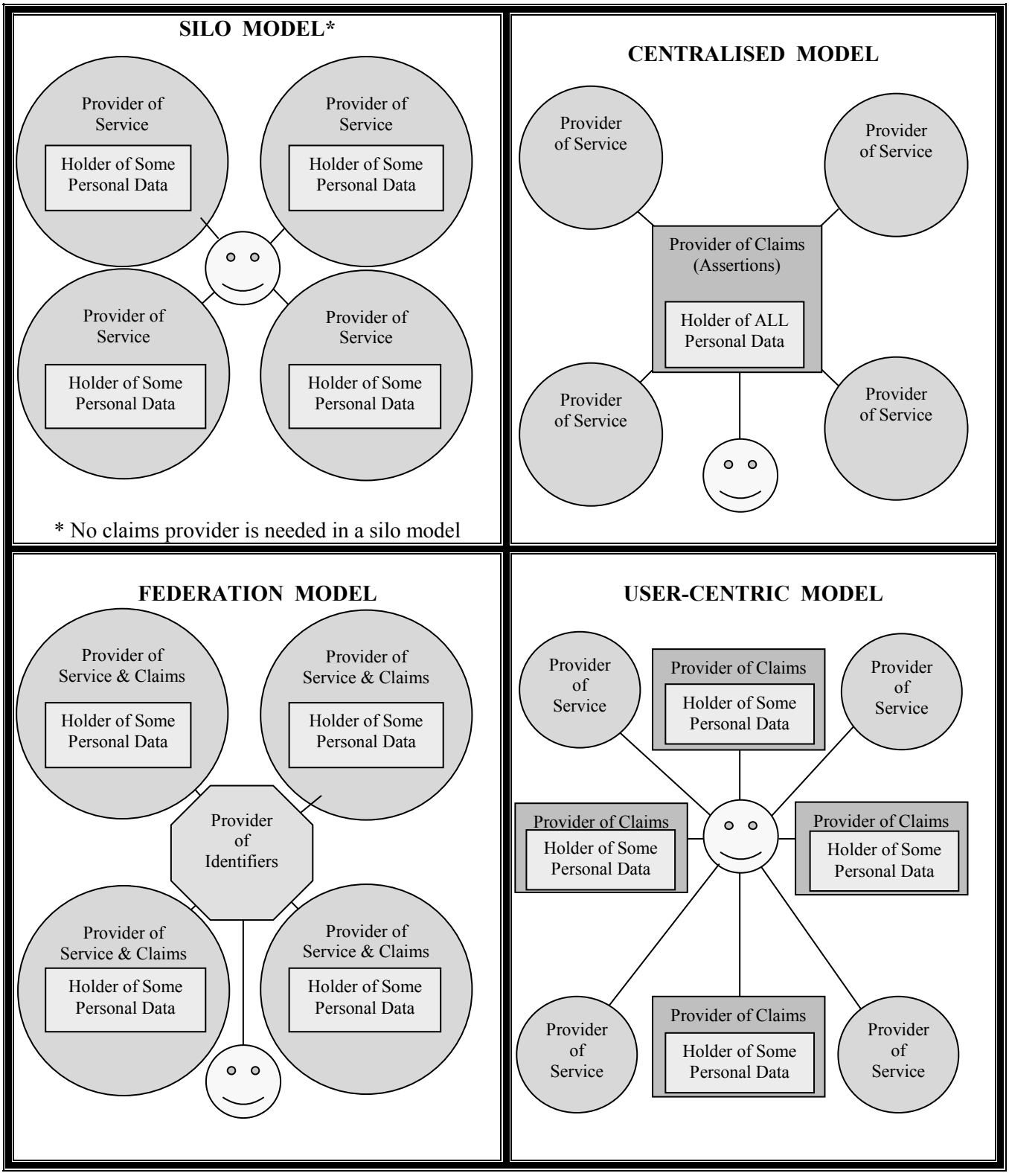
To close the gap when a user and relying party distrust each other, an identity provider can also serve as a trusted third-party broker. A user will typically only trust a broker if s/he can control it; relying parties will not trust a broker if the claims asserted are actually self-vouched by the user. 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 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.
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.

Diagram 1: Individuals (Data Subjects☺) *and* Providers of Services, Claims, and Identifiers: Who Holds the Personal Data *and* What are the Links between These Parties?



ANNEX 2

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.