Please cite this paper as:

OECD (2011-11-23), “Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers”, *OECD Digital Economy Papers*, No. 186, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5kg1zqsm3pns-en

OECD Digital Economy Papers No. 186

Digital Identity Management for Natural Persons

ENABLING INNOVATION AND TRUST IN THE INTERNET ECONOMY - GUIDANCE FOR GOVERNMENT POLICY MAKERS

OECD

Unclassified DSTI/ICCP/REG(2011)8/FINAL

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

23-Nov-2011

English - Or. English

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

Working Party on Information Security and Privacy

DIGITAL IDENTITY MANAGEMENT FOR NATURAL PERSONS: ENABLING INNOVATION AND TRUST IN THE INTERNET ECONOMY

Guidance for government policy makers

JT03311996

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

DSTI/ICCP/REG(2011)8/FINAL
Unclassified

English - Or. English

FOREWORD

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.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

DIGITAL IDENTITY MANAGEMENT FOR NATURAL PERSONS: ENABLING INNOVATION AND TRUST IN THE INTERNET ECONOMY

GUIDANCE FOR GOVERNMENT POLICY MAKERS

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.

[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.

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]:

i) 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;

ii) Appropriate permissions and privileges to access the organisation's resources must be assigned to the individual, a process often called *authorisation*;

iii) 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;

iv) 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;

v) 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

[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.

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.

[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.

- 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 favorable 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.

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

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.

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.*