Unclassified **DSTI/ICCP/REG(2007)17**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **09-Jul-2007**

English - Or. English

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

Working Party on Information Security and Privacy

REPORT OF THE OECD WORKSHOP ON DIGITAL IDENTITY MANAGEMENT

8-9 May 2007, Trondheim, Norway

Contact: Anne Carblanc, tel : +33 1 45 24 93 34, E-mail : anne.carblanc@oecd.org

JT03230102

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

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/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 infrastructures. 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 telecommunications 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.