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

06-Nov-2015

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

DSTI/ICCP/REG(2015)12
Unclassified

Working Party on Security and Privacy in the Digital Economy

DEVELOPMENTS IN DIGITAL IDENTITY

SPDE Roundtables

1-2 December 2015

L. Bernat: e-mail: laurent.bernat@oecd.org

JT03385892

English - Or. English

NOTE BY THE SECRETARIAT

OECD work on digital identity management, developed following the 2008 Seoul Ministerial Declaration on the Future of the Internet Economy[1], resulted in guidance for policy makers[2]. Recognising the significant technical, policy and economic evolutions in the identity space since 2011, the OECD Working Party on Security and Privacy in the Digital Economy (SPDE) organised two roundtables: the first one at its December 2014 meeting to take stock of current trends, in particular the evolution of the use of digital credentials in online commercial and social interactions, and the second in June 2015, focusing on progress made in several countries and regions with respect to public policies for digital identity. This document includes a high-level summary of key points mentioned during the discussions as well as possible ideas for future work in this area. It also includes the summary of the two roundtables.

The roundtables have been organised with the generous support of Industry Canada.

1. OECD (2008), "The Seoul Declaration for the Future of the Internet Economy", www.oecd.org/sti/40839436.pdf

2. OECD (2011), "Digital identity management. Enabling innovation and trust in the Internet economy", www.oecd.org/sti/ieconomy/49338380.pdf

DEVELOPMENTS IN DIGITAL IDENTITY
SPDE ROUNDTABLES

Over the last year, the Working Party on Security and Privacy in the Digital Economy (SPDE) has held two Roundtables on digital identity that included various speakers from governments, business and the technical community. A summary of each Roundtable describes the presentations and the discussions that followed (see Annex). During these discussions, a number of themes or key messages emerged. These themes are summarised below, followed by several proposals for potential areas where the OECD could make an additional contribution in the area of digital identity management.

Key themes

Digital identity management has the potential to foster economic benefits but only if some degree of coherence/co-ordination is brought to the currently fragmented landscape.

There is a growing need for digital identities to be interoperable across a broad range of infrastructures and online services.

In most cases, validation of identity information is restricted to a particular online activity; it cannot be shared beyond the particular service or platform. While online social network providers are offering third party authentication solutions, they introduce policy considerations that should be explored.

The current siloed approach, where individuals are required to create and manage digital identity for each online service or offering, is not sustainable. It is increasing the risk of data breaches and identity theft as individuals respond by creating weak passwords and reusing them.

The potential for digital identity to provide economic benefits and foster innovation is lost when individuals avoid new online services due to password fatigue.

Digital Identity does not stop at national borders

In addition to the growing demand for digital identity to interoperate across products and organisations, there is a need for digital identity to be recognised and accepted beyond geographical borders.

Governments that have previously focused on "national" digital identity approaches are now considering how to transition to more global approaches such as cross-border applications of their national digital identity approaches. They are also exploring use of derivatives of "government-based" identity approaches in the global online marketplace with the private sector.

Innovation and the evolving uses of technology will raise challenges in offering digital identity services that are privacy respecting, sufficiently safe and convenient

Connected devices or the Internet of Things (IoT) and the linking of devices to individuals will dramatically increase the scale and complexity of digital identity management and its ability to contribute to privacy protection.

Security, privacy and trust considerations are central to achieving the maximum potential of IoT development.

Advances in biometric technology, which have the potential to replace "face to face" validation requirements, is one example where digital identity can contribute to innovation and growth. Its use in the mobile environment is another.

The new data-driven economy has brought with it a fundamental change in the nature of digital identity.

In a modern hyper-connected world, an individual can be identified by means of attributes, metadata, and data linkage.A detailed profile of an individual can be used to predict future behaviours in ways that are simply not possible with the traditional methods of identity based on credentials. While this may offer consumer convenience and benefits to business in terms of innovative new services, this change in the nature of digital identity introduces policy concerns if not implemented in a sufficiently secure and privacy-respecting manner.

There are significant benefits of moving away from digital identity controlled by organizations to a user-centric model of digital identity

A user-centric model has the potential to offer individuals increased access and control over their digital identities and personal information.

Increased usability, through measures to increase consistency of approach for the sign-on experience, together with predictable processes, would increase consumer trust and confidence online.

There is a need to empower individuals in the digital identity environment and develop approaches that put them in control.

Innovation in the private sector is important to digital identity

There is increasing interest from the private sector and the role this sector could play in advancing the digital identity ecosystem.

There is an opportunity for government and the private sector to establish partnerships or other collaborative approaches for digital identity to be inclusive of both public and private sector entities, and benefit the economy and society more broadly.

Innovation in digital identity, such as creating a market in secure identity, requires government and the private sector to collaborate.

Potential Areas for Digital Identity Work

Further to the two Roundtables on digital identity, the Working Party could make ongoing/additional contributions to the area of digital identity that would offer policy guidance to member countries, help introduce a degree of co-ordination/coherence into the marketplace and contribute to global interoperability. In considering potential forward work of the SPDE in this area, the Working Party is invited to consider elements that could be referenced at the Ministerial as well as those that could be undertaken by the Working Party in its future programme of work.

In the past, the Working Party has made strong contributions[3], such as the 2007 OECD Recommendation and Guidance on Electronic Authentication[4], and the 2011 Guidance for Policy Makers on Digital Identity Management[5]. These guidance documents, and the work they represent, serve as a bridge to future OECD work on identity management; they are built on the overarching concept that digital identity management is at the core of the digital economy. The 2011 Digital Identity guidance document summarized this view indicating that:

> *"what is at stake from a public policy point of view is the development of effective and efficient digital identity management strategies to fully realize the economic and social potential of the Internet by migrating economic and social interactions online and unleashing innovations to create trust-based digital services"*[6]

With this as the starting point, several paths could ensure continued work by SPDE to further explore the economic and social benefits of digital identity management and how effective digital identity management can contribute to innovation and growth, enhance privacy and security in the digital economy and foster the adoption of new technologies. Six potential areas of future work are described below as a starting point for the discussion.

1. Raising Awareness of Digital Identity

This activity would focus on raising awareness of the importance of effective digital identity management and emphasize its key role in the digital economy and its contribution to Internet privacy and security. The 2016 Ministerial on the Digital Economy, and its resulting Declaration, offers an opportunity to raise global awareness and set the stage for continued work in this area. The SPDE draft issues paper, which relates to Panel 3.2, Public/Private Sector Co-operation in Managing Digital Security and Privacy Risk for Economic and Social Prosperity, already highlights the importance of trusted digital identities as a possible area of future work and a potential element in the draft Ministerial Declaration. Working Party confirmation of these elements as part of SPDE's contribution to the Ministerial Declaration would help ensure that future work in this area is recognized.

2. Furthering the Implementation of the Privacy Guidelines and Security Risk Recommendation

This suggested work item would look to further the implementation of these two OECD guidance documents by considering how digital identity can contribute to enhanced privacy and security in the digital economy. Potentially taking the form of a specific case study, this work would examine the 2013 OECD *Privacy Guidelines*[7], and the new OECD *Recommendation on digital security risk management for economic and social prosperity*[8] relative to digital identity management in order to identify gaps and

3 . See www.oecd.org/internet/idm.

4 . OECD (2007), OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication. Available at www.oecd.org/sti/ieconomy/38921342.pdf.

5 . OECD (2011), "Digital Identity Management: Enabling Innovation and Trust in the Internet Economy", available at www.oecd.org/sti/ieconomy/49338380.pdf.

6 . OECD, 2011, p.9.

7 . http://oe.cd/privacy

8 . http://oe.cd/dsrm

opportunities. Other related OECD policy instruments (such as the OECD Guidance on Electronic Authentication[9]) could help identify further areas where policy guidance is needed.

3. The Business Case for Digital Identity

This potential work item would further develop the business case for digital identity, specifically considering the opportunity costs of not developing an effective digital identity ecosystem. For example, work to define the business case could consider the opportunity costs associated with the status quo; the absence of a trust framework or working ecosystem for digital identity. Building on existing work on the economics of digital identity such as the study commissioned by Canada[10], further study of the opportunity costs would help define the economic benefits of having a safer, more secure and privacy-respecting ecosystem for managing digital identities.

4. Environmental Scan of Multi-jurisdictional Approaches to Digital Identity

This proposed work item would undertake an environmental scan of multi-jurisdictional approaches to digital identity including existing and planned initiatives for interoperable digital identity management by member countries (e.g EU eIDAS[11]). It would also include other work related to digital identity by international organisation. A report summarising multi-jurisdictional approaches to digital identity would provide an excellent foundation for forward work items on digital identity with the objective of furthering interoperability of digital identity approaches. Also, an environment scan would complement and build upon the 2011 OECD comparative analysis of national strategies and policies for digital identity management in OECD countries[12] which summarised national approaches to digital identity management.

5. Principles for Trust Frameworks

This potential work item would include the development of a set of high-level principles for trust frameworks. Such principles could form the foundation for a global interoperable ecosystem for digital identity and could form the basis for an OECD Recommendation or guidance document. This work would realise a recommendation from the OECD Guidance for policy makers that called for governments to work together to enable cross-border digital identity management"[13] and would help encourage or create the necessary conditions for effective use of digital identities beyond national borders.

6. Exploring the Role of Public-Private Co-operation in Digital Identity Management

Work in this area would be based on the emerging role for the private sector in digital identities and recognition that the private sector plays an important role in this area. An examination of the policy considerations surrounding an increased role for the private sector, as well as the potential for public/private partnerships would provide guidance on how working collaboratively with the private sector could advance interoperability. This work item would build on the 2011 comparative analysis of national strategies and policies for digital identity management in OECD countries[14] which encouraged

9 . OECD, 2007.

10 . Cf first roundtable.

11 . Cf. second roundtable.

12 . OECD, 2011, p.19.

13 . OECD, 2011, p.16.

14 . OECD, 2011, Annex 1, p.19.

governments to foster "interoperability of e-government digital identity with non-governmental identity solutions".

ANNEX
FIRST ROUNDTABLE ON THE DEVELOPMENTS IN DIGITAL IDENTITY
37th SPDE meeting – 9 December 2014

Agenda

The management of digital identity has many facets – technical, legal, economic, social and cultural – and is complex to understand and address as a whole. It raises the issue of how to translate in the digital world the mechanisms through which individuals trust each other as a prerequisite to interacting. OECD work on digital identity management has developed in furtherance of the Seoul Ministerial Declaration on the Future of the Internet Economy (2008). It stands at the crossroads of OECD activities in the area of digital security risk management and privacy protection.[15]

Since the SPDE completed work on guidance for policy makers in 2011, there has been technical and economic evolution in the identity space. As OECD work on data-driven innovation shows, it is increasingly clear that significant economic and social benefits can be derived from the use of information that is highly personal, but does not conform to the narrow, traditional view of "identity" as a credential. At the same time there is growing interest in finding ways to move beyond the siloed username/password approach to online authentication.

This Roundtable aims to take stock of current trends in the evolution of the use of digital credentials in online commercial and social interactions.[16] It can consider how the concept of authentication is morphing into one of identity assurance. It can also reflect on the current challenges, which continue to include privacy and security, but likewise interoperability, user control and convenience, costs and efficiencies. What are the roles of transparency (data and policies), accountability (appropriate enforcement), and manageability (tools for service providers and users for personal data management) in enabling digital identity to usher new economic and social benefits to online interactions?

Moderator: *Robin Wilton*, Internet Society

Introductory Remarks

- *Salim Hasham*, PricewaterhouseCoopers (for Industry Canada)
- *Joni Brennan*, Kantara Initiative
- *William Heath*, Mydex CIC

Roundtable Discussion. Speakers and SPDE delegates will be invited to discuss the issues raised, possibly to include:

- What evolution can be seen in the identity and authentication ecosystem for commercial and social interactions online? Who are the key players today and how is the roles government evolving?
- What is the business case for improving the current approaches to digital identity?

15. OECD work in this area is available here: www.oecd.org/internet/idm.

16. The role of identity in the provision of government services could be considered as a future discussion topic.

- How are the interests of the individual/consumer (e.g. privacy, security, convenience) being addressed?

Summary of the Roundtable

Robin Wilton (Internet Technical Advisory Committee - ITAC, Internet Society) introduced the speakers in the roundtable. He then turned to **Salim Hasham** who took the floor by audio conference to introduce the research carried out on behalf of Industry Canada to better understand the contribution digital identities can make to the digital economy. The work was developed by PwC in collaboration with the Digital Identity and Authentication Council of Canada (DIACC). Mr. Hasham provided an overview of the study which used surveys and interviews with leaders as well as a literature review to examine digital identity trends in five key sectors: financial services, high tech, telecom, retail and public sector bodies.

Digital identity can be considered as one of the enabling characteristics shared by mature digital economy markets, together with user centricity, multi-channel delivery of service, security and privacy, as well as effective partnerships. The current concept of digital identity results from the evolution of the need to "know who you are", as a means for authentication, towards the need to "know who you are in the context of the information about you, aggregated in the digital ecosystem". Regarding security and privacy, surveys are showing that the growing frequency of security incidents and mounting privacy concerns are eroding user trust and making individuals more cautious around their digital data. This suggests that organisations should support an approach to digital identity based on selective disclosure of identity information relying on user choice, consent and control.

The study shows that, over the last ten years, organisations have been approaching digital identity value creation through three main stages. In the *digitisation* phase, digital identity is used in basic digital product experience to improve processes and cost effectiveness within existing business processes. In the *internal enhancement* phase, digital identity drives value added services by better understanding customers and individuals, and leveraging data to create a more personalised experience. For example, in the telecommunications sector, there is interest in embedding digital identity within the mobile device to create rich context about an individual in order to bundle services. And finally in the *external enhancement* phase digital identity extends this understanding of customers to the broader digital ecosystem to create new business opportunities. For example, the retail sector tends to focus on enabling shopping across channels based on user preferences tied to their identity (omni-channels) although the extension towards external enhancement is limited by the absence of consolidated identity across retailers.

Digital identity is at the core of achieving private and public sector benefits but its value takes different shapes in different sectors. For example, most of the sectors studied rely on digital identity to improve process automation. However, the telecom sector focuses on digital identity to enable monetisation of consumer insights and the creation of new business opportunities, the high tech sector views digital identity as a driver for continuous innovation, job creation and reduced brain drain, the retail sector approaches it as a means for targeted advertising and data driven product development, and, finally, the public sector uses it to enable online fraud reduction and enhanced trust in government services.

The use of digital identity to foster economic benefits faces a number of challenges. The digital identity landscape is fragmented: user names and passwords are siloed per service/ecosystem, limiting the interoperability and exchange of information across ecosystems. Each silo collects different levels of information about people with different levels of assurance. Each ecosystem is driven by one entity which can validate the identity information of a person it knows. The information cannot be validated beyond that silo and that entity.

The digital ecosystem of the future would be based on convergence, whereby a person's identity information can be shared across a broad range of infrastructures and services. It promises the full participation of the individual within this multitude of services. Although organisations generally seek to retain digital identity information and build intellectual property around it, some organisations are starting to trade identity information about individuals for purposes of monetisation and to create some form of exchange that allows high assurance credentials and attributes to be validated.

From a user adoption perspective, seven key elements can be identified as key success factors: *i)* user-centricity, *ii)* long term goals and strategy, *iii)* increased awareness of existing services, *iv)* development and adoption of industry standards, *v)* privacy and in particular the empowerment of users to control data disclosure, *vi)* increased security to support increased account consolidation, and *vi)* trust building among ecosystem actors. In this context, Canada's evolving identity ecosystem addresses some of these key criteria for example through defragmentation via credential brokering or brokered authentication, and an identity exchange ecosystem in relation to validation of proof of residence.

Finally, the study identified six main findings for a path forward: *i)* clear standards for exchange of information and priority on validation rather than transfer, *ii)* adoption and use by government and private sector, *iii)* compliance, *iv)* adoption driven by use cases, *v)* periodic consultation with users and relying parties as well as user education, and *vi)* consultation with industry leaders on use cases.

Joni Brennan briefly introduced the Kantara initiative as a non-profit organisation founded in 2009 and gathering public and private member organisations to develop innovations and programmes for trustworthy online experiences. She provided a broad overview of varying approaches, rules, tools and concepts that have emerged over the last couple years in the area of digital identity.

Early digital identity was based upon the idea of keeping the perimeter safe and, over time, the number of credentials has grown exponentially with the number of systems, devices and interconnections used by individuals. Today, digital identity is not only about "who am I?" but also about "how does my identity or its attributes interact with systems?" Therefore, there is a need to reconsider digital identity around foundational concepts such as federated identity (identity exchanges), considering that a digital identity does not only consist of a specific credential or set of credentials but also the personal data that is generated as part of user interaction with varying services and devices. Personas and profiles can be generally grouped into three contexts: work, home and mobile.

From an international perspective, several trends are emerging. A number of governments are encouraging global solutions for digital identity management and many stakeholders are currently working on issues such as the scalability of such global approaches, and how to foster benefits of global markets in a way that respects the sovereignty of nations, cultures, and contexts. Many groups, including the OECD, are participating in technology and Internet governance. Some challenges are related to privacy with, for example, the implementation modalities of the European Union "right to be forgotten". It is interesting to note that some surveys are showing that a majority of individuals in the United States would be favourable to a protection such as the right to be forgotten. While there seems to be a trade-off of privacy for convenience and access, individuals and consumers are expressing strong desire for privacy, thus raising the question of how to balance these aspects.

A number of national and regional approaches echo those of Canada mentioned in the previous presentation. For example, the European Electronic identification and trust services legislation (eIDAS) is calling for an identity hub for exchange from every nation. New Zealand has a service called "RealMe" that performs similar functions. It is likely that there will be an increasing number of these hubs that are trusted and verified in some way at national level. The United States is implementing its National Strategy

for Trusted Identities in Cyberspace (NSTIC) which is more private sector focused, and the United Kingdom is developing its Identity Assurance Programme (IDAP).

One challenge is the verification of identity services actors as well as hubs and services. A layer of verification is needed to support users and stakeholders' confidence in ecosystems. This can be called a "trust framework", whereby stakeholders set their boundaries for what is trusted in their context in order to enable a scalable interoperability scheme. It can take place in national identity programmes as well as private sector initiatives enabling economic growth and access to e-commerce. It includes rules and policies for sets of stakeholders, as well as tools for different technology profiles.

An important idea on which Kantara and others are working is that of identity registry, a registry of trusted and verified identity services which can be called on in a machine and human readable way by different stakeholders who connect to these services. Another key trend is the recognition that the user and password scheme is ineffective. There is agreement among technology players on the need to "kill the password", with several stakeholders offering and sometimes mandating strong authentication, such as multi-factor or biometric authentication.

Some key principles with respect to personal data can be underlined for systems and tools developers: *i) transparency*: how is user data collected and managed, *ii) accountability*: how will a data holder be held responsible if something goes wrong with the data, *iii) manageability*: giving the user a way to interact with his/her data to manage or verify it, *iv) consent and notice*: being able to tag that a consent actually happened. However, for consent and notice to be effective, more tools are needed to empower and educate individuals. The "digital footprint reference framework" and set of tutorials developed by the Internet society is a step in that direction. Finally, individuals agree to hundreds of terms of references and end user agreements without having a means to track what they have agreed to and universally control the sharing of information between their services. Providing users with such tools, including regarding data that is owned for example by a government authority, would certainly be useful.

With respect to the future, several trends can be highlighted: *i)* modularisation, i.e. breaking trust and assurance down into useable modules, *ii)* finding intersections between the concepts of digital identity and the Internet of Things; *iii)* understanding how identities interplay with relationships and services, what the connections are, how they work and what their design principles are; *iv)* "block chain", the cryptographic function of Bitcoin, and its potential applications to privacy protection; and *v)* the possible emergence of a new market related to verified and trusted attributes management and exchange (beyond identity and credentials exchange).

William Heath introduced the user-centric model provided by Mydex. He stressed that personal control over personal data is good for all actors, as well as for trust and security and the emergence of a new economy. Nevertheless, the online world faces many problems. Individuals do not really understand the terms and conditions they agree upon, and this limits their trust and stifles innovation. Organisations would like to roll out innovative trusted services to help individuals better manage and finance their health, but they face a high regulatory cost: privacy legislation is difficult to conform to, particularly for services that require data to cross different organisational boundaries. Individuals suffer loss of convenience and control. Research suggests that individuals are depressed and in denial with regards to what happens to their personal data. In the United Kingdom, there is a cross party consensus that personal control over personal data is a policy statement, but no one knows how to implement that.

Switching from an organisation-centric to a user-centric model requires that individuals be provided with true control, avoiding the focus on monetisation of personal data, and "consumer"-related terminology. The data should be aggregated around the individual, but there is a missing piece of infrastructure to do so that should be provided through a variety of protected, supervised, audited and

interoperable solutions. The community company Mydex CIC is one of them. It provides an online personal data store to individuals to which only these individuals have the key and that is connectable with end-to-end encryption to any contracted organisation. It can be a business, phone company, bank, organisation exercising data portability, or a government service. It includes an identity which carries a free sign-on credential. The service is wrapped in a legal and technical trust framework, as per the Kantara definition introduced by Joni Brennan, to enable audit (by the Open Identity Exchange in the case of Mydex).

Mydex CIC is one of the five contractors to the GOV.UK Verify initiative by the UK government which aims to provide additional identity assurance to the new generation of online public services. The difference from other approaches is that with Mydex, the individual acquires verified attributes, stores them under her own control (i.e. even Mydex cannot have access to them), and can redeploy them as she wants. The individual acts as data controller. The government has accepted the principle that an individual can contract for public services based on credentials they have acquired and encrypted themselves, and that are released in a controlled manner to the services they are willing to use. The situation is then much clearer to the individual, dispelling the mystery of why he or she is or is not trusted by an online public service.

Trust is built incrementally: individuals don't have full biometric or DNA credentials online when starting using this service. They accumulate proof that is checked when they apply to new services. Individuals can open a Mydex account for free, starting with an email from any connected trusted organisation, and they progressively add proof of identity when using their Mydex account for additional services. When using a service, there is no leakage of the fact that the individual is using any of the other services. To exchange data in a structured way, that data can include proof of the relationship one has with the phone company, the local authority, the housing association and it comes as a by-product of that connection. Those verified attributes can show that one has a degree, a driving license, the right to live in a country, etc. This is what will support identity services and drive convenient trusted digital services, which in turn reinforces the system in a virtuous circle. Individuals can connect to organisations they want to use and personalise services in a privacy friendly way.

Mydex is an illustration of a person-centric ecosystem. Individuals need to control their own data, for reasons of security, privacy and cost saving, and for building a platform for new economic developments. When that happens, identity and trust become a healthy and inexpensive by-product of that process. A multi-billion market in identity *per se* is unlikely to emerge. Rather, identity is a by-product of how we live online, which will underpin a multi-billion market of new industries based on permissioned and volunteered personal information.

Robin Wilton opened the floor to questions and remarks from SPDE delegates.

A question was asked to panellists about the difference between transactional identity and personal identity and trends in this respect.

Joni Brennan responded that the concept of identity and how it is made up is evolving towards the idea of personas and collections of verifiable sets of attributes. There may be certain interactions in which a certain set of attributes about someone are appropriate and not in another. Part of the challenge which is not yet solved is to find a way to scale this set of attributes and use it in contextually appropriate ways, i.e. appropriately to both the end user and market growth.

William Heath stressed that people need to "get stuff done" and, to do so, they need to prove the claims they make, anonymously or pseudonymously. However, there is a missing and transformational

element which is the ability for individuals to control their own data, and to acquire and share it in a highly controlled way. A diverse ecosystem that makes that possible is needed.

Salim Hasham noted that concepts of authentication and authorisation are still true and that the transactional process can be privacy enhancing. For example, there are privacy-by-design use cases where the individual's consent is injected in the middle of a transaction where two organisations are interacting to validate or exchange attributes. For example, the individual would receive a message on his/her mobile asking for consent, and making the transaction more user-centric.

One delegation underlined efforts made at EU level with respect to digital identity, including the interoperability framework project (STORK) and the recently adopted EU-wide digital identity legislation. He highlighted the interrelated issues between interoperability and security and the fact that each country is likely to favour its own digital identity approach. The solution might be the development of appropriate interoperability gateways or mechanisms to translate one identity from a framework to another. In addition, as trust and identity will become increasingly important, such systems will become critical and will need to be appropriately protected, audited, with relevant incident reporting, etc. Suspicion of failures of these systems would undermine the whole trust chain.

A delegate asked panellists to underline relationships between their approaches and the identity of devices in the context of the Internet of Things (IoT).

Joni Brenner stressed that Kantara is addressing this question at multiple levels. One level is the interaction of personal privacy with the IoT, considering that there is a person behind every device. For example, a tractor has a driver, and there may be privacy laws applicable with respect to what the tractor movements reveal regarding the person behind it. Another level is standardisation for things, such as device identifiers. There are varying ways of identifying devices from the phone to the tractor to the silo, fitness band, etc. Several standard associations are working in that space (e.g. IEEE). The identity management layer needs to evolve beyond the concept of the person identity. Issues to be addressed include the relationship from the human to the device, whether a device can be used as an identifier for a person, and standardisation in this area. Standardisation is key at the IoT-device level and on how the device will interact with humans. The Kantara Initiative would like the current convergence of hardware with software taking place at the standards level as well. Trust frameworks and identity management will need to move to modular contexts, so that pieces of trust can be put together in ways that will scale appropriately depending on context (e.g. home, work, mobile). Frameworks should consider the device level, and standardisation needs to happen in IoT itself to maximise the benefits of personal and society use.

Responding to another question on the measurement of attacks that are enabled by personal data leakage, **William Heath** noted that there are two approaches to managing crime online: *i)* assume that 100% of people are suspects and total surveillance is needed, with the result that crypto should be prevented wherever possible and data should be shared extensively to identify the bad actors or *ii)* make it easy for people to prove they are trustworthy, since it is the case for most of them, in order to focus on less than 1% of the population.

A delegate questioned the assumption that digital identity management would help privacy protection and observed, on the basis of Mr. Heath's presentation, that privacy protection technologies would help digital identity management so that people would use the system because they trust it.

Another delegate noted that while there is potential economic value in interoperability identification technology, it depends on security and privacy assurances given to individuals. Ease of use has to be

coupled with ease of context limitation and ease of anonymous interaction where the identity is not necessary to the interactions. A mix of policy and technology is required to help give those assurances.

Robin Wilton thanked the Chair and the Secretariat for organising this roundtable, as well as the speakers for their participation. His concluding remarks focused on two main points. First, he noted that the data-driven economy has brought up a fundamental change in the nature of digital identity. The traditional idea of identity is that it is based on a trusted credential, like a passport or a driving license, and therefore a digital identity is based on a trusted digital credential. But in the modern hyper-connected world, one is far more likely to be identified by means of attributes, metadata, and data linkage. In this context, a detailed profile of individuals is far more likely to be built, and to predict one's future behaviour in ways that are simply not possible based on the old-fashioned idea of credential-based identity. Second, as the reality of digital identity changes, so do the conditions under which anonymity and pseudonimity are possible. SPDE's work in relation to digital identity is therefore directly related to its work on privacy, security and the data-driven economy. For example, when we discuss the potential benefits of big data relating to clinical and health care datasets, there is often an assumption that the data must be anonymised. If we subsequently find that the anonymisation of these datasets can be reversed, then it may call into question the benefits of having released them. Changes like these in the way digital identity is understood and used have far reaching effects and SPDE should consider them very carefully in the course of its future programme of work.

SECOND ROUNDTABLE ON THE DEVELOPMENTS IN DIGITAL IDENTITY
38th SPDE meeting – 24 June 2015

The first roundtable focused primarily on the evolution of the use of digital credentials in online commercial and social interactions and reflected on the challenges from a private sector perspective. It was the first opportunity for SPDE delegations to discuss digital identity since the publication of OECD guidance on *Digital identity management: Enabling innovation and trust in the Internet economy* in 2011.[17] This guidance, addressed to government policy makers and focused on digital identity of natural persons, was developed on the basis of a survey of public policies for digital identity in 18 countries. At the time of the survey (2010), the majority of countries were at an early stage of development and/or implementation of their digital identity policies. Such policies were generally aimed at furthering e-government, fostering innovation in public and private e-services, and strengthening security and privacy. In most countries, the existing offline identity approach was the natural starting place. As a result, relatively different approaches were adopted across countries, depending on the pre-existence and nature of offline credentials and registration policies (e.g. offline national identity card, population register, and/or identification number).

The second Roundtable provided delegations with an overview of progress made in several countries/regions with respect to public policies for digital identity, addressing in particular how they: *i)* Foster economic growth and innovation; *ii)* Support security and privacy risk management; and *iii)* Address technical aspects (e.g. Internet of Things).

With the review of the *OECD Privacy Guidelines* in 2013 and the expected adoption of the new *Recommendation on digital security risk management for economic and social prosperity* by Council in September/October 2015, concluding the revision of the 2002 Security Guidelines, it was timely for the Working Party to consider how digital identity can contribute to innovation and growth, enhance privacy and security in the digital economy, and foster the adoption of new technologies.

This second Roundtable informed the Working Party's contributions to the 2016 OECD Ministerial on the Digital Economy, noting the importance of effective digital identity approaches for economic and social prosperity.

Moderator: *Robin Walker*, UK Government Digital Service

Presentations

Speakers will be invited to provide a brief update on progress made with respect to digital identity policies, with a focus on the main lessons learned, for example with respect to opportunities and challenges to develop and implement their policies.

- *Robin Walker*, UK Government Digital Service – A federated approach to identity assurance and GOV.UK Verify
- *Neil Clowes*, European Commission (DG Connect) – Overview of EU Digital Identity policy

[17] www.oecd.org/internet/idm

- *Prof. Tai Myung Chung*, Sungkyunkwan University (SKKU), Korea – Presentation of Digital Identity Management in Korea
- *Joni Brennan*, Executive Director, Kantara Initiative – Internet Technical Advisory Committee (ITAC) - Internet of Things by 5 Ps: A user-centric approach
- *Jane Hamilton*, Industry Canada, SPDE Chair – Private/Public Sector Initiatives to Develop a Canadian Framework for Digital ID and Authentication

Robin Walker (UK Government Digital Service) outlined the roundtable's agenda of five presentations followed by a short Q and A session.

As the first speaker, Mr Walker, introduced his topic on the UK federated approach to identity assurances. This approach uses GOV.UK Verify (GovUK), a system which allows people to prove who they are when accessing government services online. The approach focuses on two key issues: *i)* GovUK users need a convenient and safe way to access online digital services, and *ii)* Government services need to be assured that people are who they claim to be. This approach represents a shift away from the previous proposed approach relying on an identity card.

There is no centralised national database in the UK and British citizens are not comfortable with this idea or with the use of unique individual identifiers. The system used by GOV.UK is based on private sector identity service providers. An individual sets up an account with an identity service provider (for example, Experian, UK Post office, Horizon, or Digi-identity) and goes through a proofing process. In this process the individual must provide personal information such as passport details and utilities information. The identity service provider then assures the relevant Government agency of that individual's identity by disclosing that individual's name, address, birth date and gender through the "Hub". From this point on, all interaction between the individual and the Government agency takes place on that side of the Hub. The identity service provider does not know what service the individual is seeking, and the Government agency which identity service provider the individual engaged. The main security concern is ensuring individuals sign up using their true identity. To manage this, all identity service providers and their identity verification systems are assessed against established levels of assurance. The assessments are outcomes based and assess the quality of the credentials each identity service provider uses to assert an individual's identity, and that provider's assessed level of trust.

The identity service providers themselves must decide how to meet these assurance levels. Current identity verification processes complete online identification verification using passport, drivers licence and credit personal information. The security infrastructure of this system involves the use of encrypted messages sent using a PKI-based system.

Assurance complements innovation. As the identify service providers, the private sector is responsible for innovating and developing new products for online identification. For example, a Dutch organisation, DigID[18], consistently provides new ideas and views on innovation. One idea included developing a user friendly smart phone identity application which allows individuals to take a photo of their passport, a photo of themselves, and an additional movement photo to prove they are a living human to set up an account. This application meets satisfactory assurance levels.

Mr Walker emphasised that innovation includes collaboration between Government agencies and the private sector. Innovation is creating a market in secure identity. Banks, the sharing economy, airlines, insurance companies and e-commerce are all interested in online identity. For example, UK Government

18. https://www.digid.nl/en/

Digital Service and the UK Branch of Open Identity Exchange share research and run projects together, to explore new ways to identify people, the cross border potential, and how identity can be used into the future.

Online identity does not stop at national borders. The international environment is likely to progress based on national recognition of another nation's identity standards. For example, France and Germany recognising an identity process used in the UK would eventually create an internationally accepted standard. Efforts under way include European regulations, the identity authentication standards developed by the International Organization for Standardization (ISO) and work by the UN Commission on International Trade Law towards a legal framework. In the coming years, it will be interesting to identify the correct forums in which to discuss issues such as how to recognise identity processes internationally, or whether the private sector will develop the identity market itself.

Neil Clowes (European Union Commission DG Connect) delivered an update on the EU Regulation on electronic identification and trust services known as eIDAS[19]. The eIDAS approach is based on trust and security. It aims to make life easier for citizens and reduce the friction between customers and institutions when verifying identities. The objective is to facilitate efficient online transactions moving away from traditional over the counter services. The regulation focuses on mutual recognition of means of identification. For example, a country accepts the digital identity verification issued in another country on the basis that the verification is subject to an accompanying liability scheme. The regulation covers the following topics: electronic identity and trust services such as electronic signature, time stamps and electronic seals, trust mark (a company certification confirming to consumers that it has met certain criteria and is a real company) and electronic delivery. As an aside, Mr Clowes mentioned that an electronic signature has the same legal value as a handwritten signature in European courts and potentially world-wide.

One of the key principles of eIDAS is cross border application. The Commission does not have the power to tell EU member States how to manage their identity infrastructure. However it provides guidance on cross border identity and information sharing. It is mandatory, for countries using a certain identity scheme to verify individuals' identities, to recognise another country's verification of that individual, if it uses a "notified" scheme with the same level of security assurance. To be notified, a scheme must meet requisite levels of trust and security, and liability in technical protection profiles as set out in the Implementing Act. This notification process informs the Commission whether a scheme has a high, substantial or low risk online identification means.

In three years, the recognition of electronic identities will become mandatory. However, the Regulation was adopted in September 2014 and some Implementing Acts will come into effect in September 2015. Following September 2015, member States may voluntarily adopt the Regulation and Implementing Act. Additional requirements such as peer review are likely to be developed over six months. Under this requirement, member States will review the schemes of other member States to assess whether they meet the obligations.

The private sector is a big player in the identity space. Although it is not mandatory for the private sector to adopt the rules set out in the Regulation, the Commission encourages it. The Commission recognises that identity verification is a regulatory and business need in the banking, finance and aviation sectors. eIDAS can assist with anti-money laundering processes, Know Your Customer (KYC), etc. In response to an appetite for this service in the private sector, the Commission wishes to work with representatives in each sector to drive the use of eIDAS forward.

19. http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond

Professor Tai Myung Chung (School of Information and Communications, Sungkyunkwan University (SKKU), Korea and Vice-Chair of the SPDE) introduced the use of the i-PIN Digital Identity Management system in Korea. This system has been successfully used for over 10 years. Mr Chung provided background information to understand the importance of identity management and security in Korea, as well as the uses and characteristics of i-PIN, and the issues related to the use of i-PIN.

After the Blue House Raid in 1968[20], the Korean Government began assigning citizens with an individual Residency Registration Number (RRN). Subsequently, all Korean information systems adopted RRNs as unique individual identifiers. Consequently, RRNs are now widely used online for convenience and efficiency. This wide use was believed to be a good idea until RRNs began to become vulnerable to cyber-attacks. A 13 digit RRN may include the birth date, gender and place of birth. An individual's RRN remains the same until the person dies.

RRNs continue to be widely used in Korean cyber society although it is known as a common hacking target. Examples of such incidents include a shopping mall hacked and 10 million RRNs leaked in 2008, a subsequent hack which resulted in the leak of 35 million RRNs in 2011, and 8.7 million RRNs hacked in 2012. There is significant growing concern over the recurrent secondary damage of these hacks as RRNs are used to create new entities and steal individual's identities.

The i-PIN system was introduced in Korea to manage the security problems associated with RRNs. The Internet Personal Identification Number is an alternative to an RRN. The public sector i-PIN guidelines were established in July 2005, and a private sector i-PIN trial was launched in October 2006 by the Minister of Information and Communications. In August 2008, Ministry of Public Administration and Security (MOPAS) studied the public sector use of i-PIN and found vulnerabilities in the system. Its name was later changed to i-PIN 2.0 in 2009. This year changes were made to i-PIN identity verification processes to address ongoing security challenges.

There are two types of i-PINs: a public and private sector i-PIN. Private sector i-PINs use cell phone numbers and face to face verification to authenticate an individual's identity. Private i-PINs are used for online shopping, games and e-commerce. Service providers pay a verification fee and it is an expensive burden. The identity verification method is the same for public sector i-PINs which is used by public institutions for eGovernment. eGovernment relies heavily on i-PINs and verification is free of charge. The Korea Internet & Security Agency (KISA) supports the interoperability of i-PINs through i-PIN linkage systems. The i-PIN process starts with the user sending an authentication request to a web site. Then the web site refers the request to the "trusted party" for identity authentication. The trusted service provider then speaks directly to the user, and checks the i-PIN and the password.

The i-PIN insurance procedures are managed by three trusted parties in the private sector, and one in the public sector. There are four methods for an individual to authenticate his/her identity: with an operated certificate, credit card details, a cell phone or face to face verification. After verification, the individual is issued with a unique and random i-PIN. I-PINs are completely different identifiers to RRNs. The i-PIN can be changed or updated at any time if an individual is concerned about its security. I-PINs contain no personal information. The sub provider can also check how often an individual uses their i-PIN.

I-PIN is stable, it is user convenient and it is service provider convenient. Unlike the Government run RRN system, the i-PIN allows individuals to manage their i-PINs. Since 2006, 21 million private sector i-PINs were issued to individuals and 5 million public i-PINs. Unfortunately, for convenience and resistance to learning a new identification number, people continue to use their RRN. Alternative identification

20. i.e., the unsuccessful attempt by North Korean commandos to assassinate the President of Korea, Park Chung-hee, at his residence at the Blue House, on 21 January 1968.

measures, based on i-PIN, are currently being developed. In one case, for example, a service provider can link the i-PIN and the cell phone number to authenticate an individual's identity. Another measure is operative certificates which are used by organisations which need stronger security measures. Each organisation or company can develop its own authentication methods using this certificate.

Use of i-PIN system as a verification system remains low compared to other identification methods. Out of habit, individuals continue to use RRNs. The i-PIN system is subject to cyber-attacks. On one occasion, hackers attacked the i-PIN issuing system and stole 755 000 public sector i-PINs. Subsequently, all of these numbers had to be changed. PKI systems have also been used in regards to i-PINs. Korean laws were recently changed to enforce i-PIN security compliance, for example, the annual amendment of password change, etc. An alternative method involves the use of a secondary password. If a service provider suspects an authentication request to be suspicious, they can request a second password.

Mr Chung summarised by stating there is a recognised need to enhance the personal identification methods used by the i-PIN system. Developers are seeking to diversify the system and integrate more advanced authentication methods. The four important values taken into consideration when reviewing alternative methods include: interoperability, security enhancement, reliability and technological extension. Mr Chung concluded that in the longer term, the aim is to be able to use i-PINs internationally.

Joni Brennan (Executive Director of the Kantara Initiative, member of the Internet Technical Advisory Committee to the OECD (ITAC)) stepped in to present her topic: "The Internet of Things by 5 Ps: a user-centric approach". Ms Brennan thanked the group and referred to previous collaborative work amongst the group on trust marks and the accreditation of national identity verification systems. This presentation took a slightly different approach to the others and covered high level concepts associated to the IoT by ITAC. Ms Brennan acknowledged the massive adoption of IoT devices. ITAC aims to connect identity management (IDM) professionals with the engineers developing the IoT devices – the idea being to connect the learnings of the IDM systems with the engineers' expertise. Ms Brennan introduced five high-level concepts that can be used to manage IDM: Potential, Patterns, Privacy, Purpose and People.

1. Potential: Potential refers to the wide range of predictions made regarding the potential for economic growth based on IoT development. For example, over USD 7.3 trillion of investments are anticipated by 2017. These predictions inspired a frenzy of visionary collaborative projects to further develop IoT. Security, privacy and trust considerations are central to achieving the maximum potential of IoT development.

2. Patterns: Patterns refers to the ability of IoT devices to reveal a number of patterns which can be leveraged for beneficial uses, public good and prosperity, such as health care data, and efficiencies such as in relation to smart cities. Patterns can also be maliciously used to take advantage of the data and create new vectors of attack. Patterns created by IoT in particular IDM and personal data related patterns are a key consideration.

3. Privacy: Ms Brennan depicted privacy using a recent example from the USA. After replacing his old TV with a smart TV, a consumer discovered in the TV policy that microphones may record him at home, and that any adjustment to the volume or channels may be logged and sent to an external third party. A discovery which had a chilling effect as he was terrified to use his new smart TV. IoT development must consider: the types of users' data that will or could be collected, how this collection is communicated to the user and how the user is active in this exchange. Otherwise, unlike the traditional devices that were free of privacy concerns, users will not trust smart products.

4. Purpose: Purpose refers to the why and how data is collected. Users need to be made aware that their personal data may be used for a purpose other than the purpose for which it was originally collected. Further, users need to be provided with tools to manage the collection and sharing of their own personal data, whether these tools are built into devices or separate from them. Ms Brennan stressed that multiple identities can be managed in IoT relationships, such as a tractor, its driver and cows. When considered in relationship to each other, each "object" raises a number of identity considerations. The purpose of what data is collected in what context will be a key consideration of IDM within IoT.

5. People: People are at the centre of the IoT commercial movement. People need tools to engage with IoT, to move from a model where data collection is something that happens to users to a model where users are able to take an active role in their interactions with different devices and identities. This way, users will be more informed to manage their own personal data. People are not things. For example, a refrigerator is thing. People believe they have signed up for a number of functionalities when using a refrigerator: preserving food, potentially smart cameras to manage stock and create smart shopping lists. However, users may be unaware of the extent of the functionalities of their smart devices and the personal information being collected. For example, "refrigerator use" information, such as the brand of groceries and patterns of food consumption in a household, may be recorded. This information may have broader reaching implications that is not yet understood. Limitations on the collection of personal data will influence the introduction of implanted devices such as a pacemaker. It may be undesirable to allow individuals to engage with personal data management in this instance. However, for example , there may be many smart lightbulbs an individual wishes to manage at one time.

Ms Brennan underlined additional concepts such as Static Identity (SI) (e.g. a car) and Transient Identity (TI) (e.g. a rental car). Data may be collected from a rental car revealing various different patterns about its drivers, such as where it goes. Overall, the IoT industry and community must work together to develop the meanings of SI and PI in IoT, and their impact on persons. A number of actions are being taken to address IoT challenges. One is the use of an open standard called User Managed Access. This standard allows users to control access to their personal data, including setting the parameters for how their data may be collected, managed and shared. It was implemented as a portal and can manage several devices and relationships at once. This standard focusses on the user and does not force him/her to work between different systems to manage their personal data. The user can more easily manage consents and revocations to access their personal data, which is currently extremely difficult to do.

Jane Hamilton (Industry Canada, SPDE Chair), speaking as representative of Canada provided a brief update on digital identity developments in Canada. Canada aims to move away from a "silo" approach to digital identity management, where instead of engaging with each sector separately, all sectors will be involved. The government is developing a Pan-Canadian approach which aims to develop an identity exchange mechanism or hub, in the model of the UK example. The federal and province governments are working on this together. The Digital ID and Authentication Council (DIACC), working in a public/private sector partnership, will produce a roadmap for digital identity development in Canada. Industry Canada is participating in this project as an advisor and contributed to a recently released white paper discussing Canadian digital identity future[21].

This paper defines the requirements for a digital ecosystem with robustness, security, scalability, privacy protection, inclusiveness and openness. Such a system would also include transparent governance, facilitate the minimum transferral of personal data, and be convenient. Feedback on this paper will drive

21. "Building Canada's Digital Identity Future" (DIACC, May 2015). See www.diacc.ca/wp-content/uploads/2015/05/DIACC-Building-Canadas-Digital-Future-May5-2015.pdf.

the plan forward. Such forward work includes developing a trust framework, looking at what regulatory adjustments might need to be made, as well as education and awareness. The paper takes a proof of concept approach, elaborating on a concept, and testing how it works in practice.

Robin Walker summarised the roundtable meeting, citing the three presentations on different national approaches and insight on the EU Commission's perspective regarding cross border aspects, and general thoughts regarding the IoT. A number of trends were noted, such as the increasing role of the private sector, given digital identity management was previously the domain of the State and now extends to the commercial world. Mr Walker felt the roundtable raised several questions, such as was identity being used appropriately? Did identity need to be backed by the government?

Robin Walker opened the floor to questions and remarks from the SPDE delegates.

The delegate from the Civil Society Information Society Advisory Council (CSISAC) noted that digital identity management had been a key privacy topic for many years and that this concept now needs to be understood from the user's perspective. There are many instances were an individual can be authenticated without his/her identity being known. However, once it is it necessary to identify that individual, the personal data and all of its legal consequences follow it as well. A key question is: "how do we enable online commerce without our whole personal lives following us"?

Further, while is wonderful to empower users, we should not underestimate the difficulty for empowered user to manage default settings. Currently, all the settings are set towards disclose. A user can change them and discover later that they have been switched back to disclose. With respect to the Samsung TV example, the Electronic Privacy Information Center (EPIC) brought a complaint to the FTC when it became clear that the audio recorder was always turned on. That TV recorder picks up channel changes, volume changes and personal conversations conducted within a radius of it. Recently, Mattel released a new Barbie doll that included a feature to record and listen to the interactions of children, and process that information. Companies provide users with the opportunity to opt out of recording functions on devices but it is usually presented in complicated and inaccessible terms to users. The key take away for digital identity management is the default settings. Hopefully privacy risk can be minimised by building as many safeguards as possible into the front end of technologies/devices to make it easy for users to manage.

Joni Brennan stressed that there is not one single solution for these digital identity issues, it will take a combination of solutions. Such solutions include Privacy Enhancing Technologies (PETs), privacy by design and by default. All of these solutions are moving forward and hopefully can scale where users will have the opportunity to share a lot or a little. Consent, which was not discussed during the roundtable, is another serious challenge for users.

The delegate from Finland noted that the Finnish government recently released new digital identity legislation. The model is based on public-private partnership and there is legislation on information security and data protection.

Another delegate emphasised that the difference between identification and authentication is as important as the concept of authorisation. At this point, with these three concepts in mind, it is important to think about the severability of identity. There are elements of an identity that are necessary for an authentication but these same elements may not be necessary for an authorisation.

The delegation from the Business and Industry Advisory Committee to the OECD (BIAC) noted that the EU digital signature directive included the concept of a self-proofing signature or non-repudiation in authorisation. These concepts are better addressed in the EU than in the United States. Notarily participation enables the recording of entries onto a register to make something public by registration, and

allows the register to become an element of active authorisation. A question was asked whether these concepts would make it into the EU Regulation.

He also made a comment related to the Industrial IoT, where information collected is mostly not personally identifiable information. IoT is an input into another system, and that system may add personally identifiable information to the equation. For example, there is a problem with an engine. The system sends a message to headquarters requesting the problem be fixed. That request is sent to HR, allocated to an individual, Joe Smith, to repair. At this point, personally identifiable information is introduced. The personal identifiable information was not made available by IoT but as a result of the interaction between IoT and another system. This example relates to purpose specification. The purpose specification of the system together with the data should be considered rather than only the purpose specification of a sensor. A sensor is a mechanism to collect data but the purpose of the collection is a data control issue. The use of data is determined by the purpose, not the sensor that collected it. The scope of the collection may be programmed into the sensor, and that can be analysed. The collection of that data is already covered by data protection law. Whether there is transparency in collection, and the individual understanding what is collected is a different issue. IoT devices will be working in larger systems, and the larger system may dictate the choke points of compliance. At a supermarket, a loyalty card may associate your purchases with you, however a credit card associate you with your purchases due to legal constrictions. There are legal frameworks in place and those frameworks do not disappear when new technology is created.

One delegate stressed that the tests included in the Canadian DIAAC study provide a private sector perspective on privacy by showing how banks could associate their cards to individuals using established levels of assurance.

The delegate from Estonia underlined that recently gathered information indicated Estonian citizens wanted a digital identity system to be delivered by the government. The Estonian Government's approach is founded on cohesiveness and transparency. It is a system trusted by citizens and businesses. The delegate reported that to date, 350 million instances of authentication are using Estonian national ID cards. The Government is trying to understand how the system is being used, and how to move forward. Research has shown there is a demand outside of Estonia for a government backed system that could work across borders. Further, businesses wish to use the government run digital identity management system to interact with other businesses, not necessarily the government. Earlier this year, Estonia launched its e-residency card for non-residents. From the beginning, it has been in great demand with thousands of people signing up. Feedback from card holders indicates that the card facilitates business transactions, and that often a government backed proof of identity is necessary to work or do business outside of Estonia. In fact, the card is often a starting point for new businesses. The Estonian delegate suggested government run digital identity management remain on the Working Party's agenda.

Robin Walker stated that is also important to ask what is government backed identity appropriate to be used for? Mr Walker identified stressed Finland had extensively considered this issue when developing its new privacy legislation.

Neil Clowes pointed out the new data protection directive about to be adopted which will clarify some issues. In response to digital certificates being addressed in the eIDAS Regulation, there is a clear distinction between qualified and not qualified signatures. Certain trust service providers need to meet a stricter set of criteria before they are issued with a certificate, and they are non-refutable. There are various levels of supervision depending on whether they are qualified or non-qualified. It is a fairly strict regulatory regime for the qualified trust service providers. For the others, it is a light touch approach: unless they come to notice for some reason, they are not under direct supervision. The Regulation needs to be considered in cross border terms which make authorisation/ authentication mandate a different

”animal”. The Commission constructed a minimum data set to avoid the proliferation of identity information across borders. There are unique identifiers which help this system.

Professor Tai Myung Chung stated the vocabulary surrounding identification, authentication is all different but they are very closely related in use. Also, technically, standards are being developed for the IoT. Policies must follow the technical changes and ensure that new standards are made to adopt privacy protective procedures.

Finally, **Robin Walker** thanked the OECD and SPDE delegates.