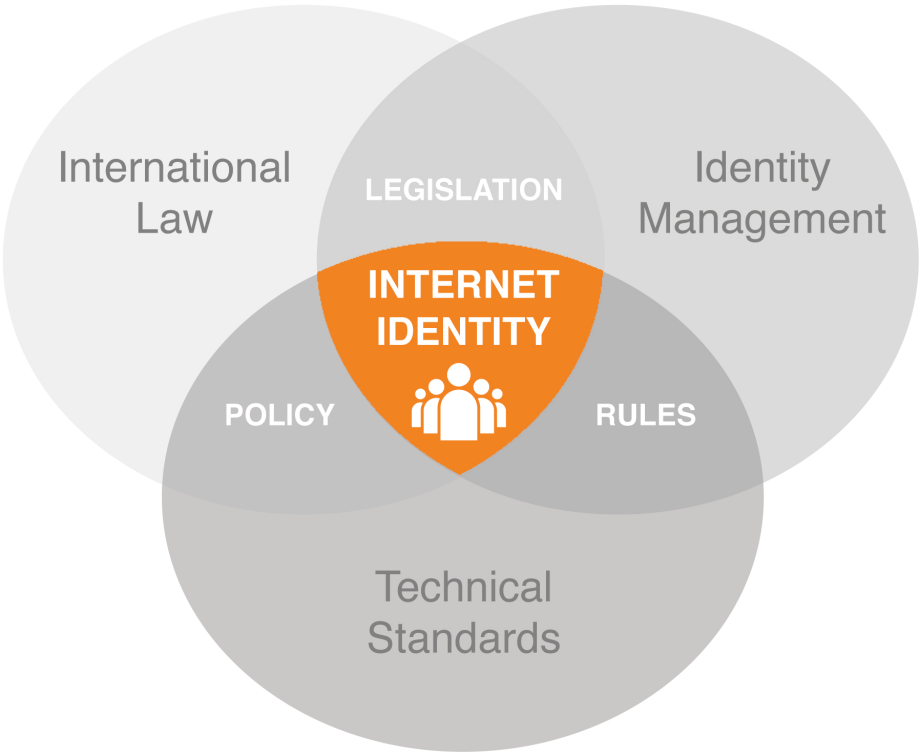
REPORT:

IDENTITY LAW AND POLICY WORKSHOP



Supported by:

digidentity IMN verizon

REPORT: IDENTITY LAW AND POLICY WORKSHOP

Introduction

The Open Identity Exchange organised and facilitated a legal and policy workshop on March 24, 2016 in Amsterdam, with the objective of advancing the discussion of the key issues surrounding the adoption of identity management legislation and in particular eIDAS[1]. The workshop was co-sponsored by Verizon,[2] Platform Identity Management Nederland (PIMN),[3] and Digidentity BV,[4] and was hosted by Verizon.

This workshop is the second in a series. The first workshop was co-sponsored by OIX, the World Bank, and the American Bar Association Identity Management Legal Task Force, and was hosted by the World Bank in Washington DC. The goal of that meeting was to discuss the direction that planned or proposed projects to develop new identity management legislation should take, the issues it should address and the desired approaches. Attendees were lawyers, business leaders, policy experts, and technologists representing a broad spectrum of public sector and private sector leaders in identity.

The Amsterdam workshop participants were reminded of the three tiers of legal rules presented and discussed at the Washington event. These three levels represent the legal environment in which each identity system (i.e., eID scheme) operates.

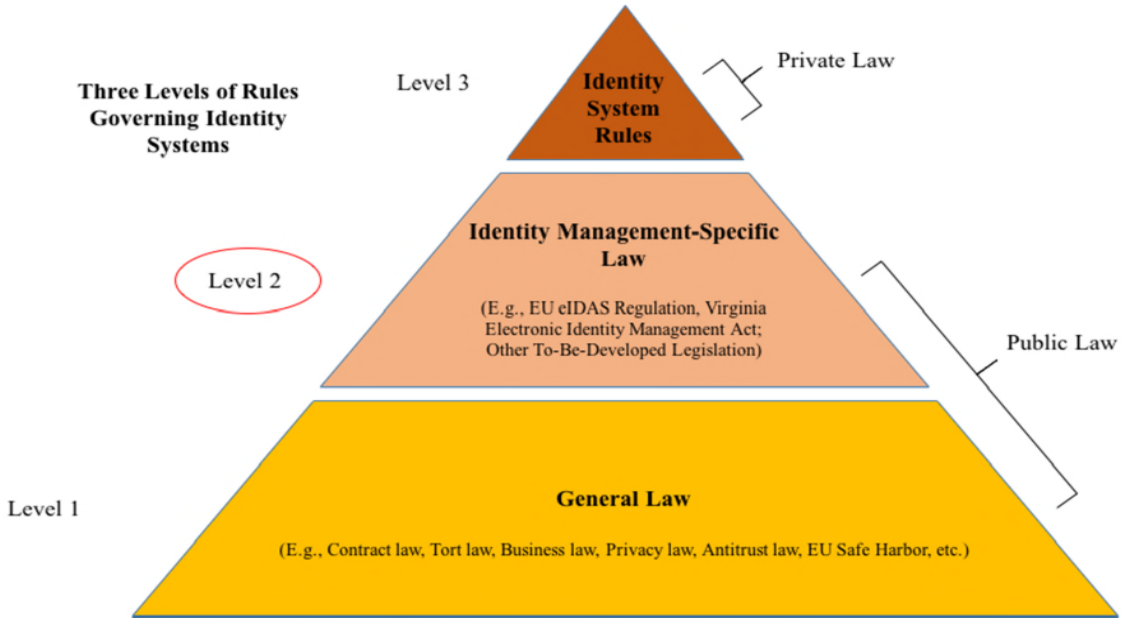


Figure 1: Three Levels of Legal Rules Governing Identity Systems

[1] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
[2] www.verizon.com
[3] www.pimn.nl
[4] www.digidentity.eu

Individuals involved in the drafting of existing Level 2 legislation in the EU -- specifically, the EU eIDAS Regulation -- participated in the event and provided invaluable insight into the goals and approaches of this legislative initiative.

The goal of this Amsterdam workshop was to build on the outcomes of the Washington event by bringing together technology, policy, and legal leaders to talk about identity in the context of European regulations, explore potential International integration and agreements as well as the secondary effort of the GOV.UK Verify programme, to accelerate market identity services. OIX will continue these threads throughout this year at the Cloud Identity Summit (CIS) in the summer and London later this year. Now is the time to explore these issues - secure digital identity is now and in our hands: https://www.youtube.com/watch?v=cYwxDlP1vBM

Key themes reiterated throughout the event were the role and importance of identity attributes, the need for more trust tools, and the importance of global registries as a transparent mechanism for forging that trust.

This Report summarises at a high-level the robust, thought-provoking and productive discussion in which both the panelists and participants engaged.

Law and Policy Panel: International Regulatory and Legislative Interoperability

Theme: Mapping Law and Policy to Technical Interoperability

The first panel discussion focused on how different governments in the EU had interpreted and implemented the eIDAS legislation, and examined whether the Digital Single Market[5] between the 28 member states would really appear.

The following questions were posed:

- Is a standard look and feel needed for identity management?
- Is IT and Identity Management now a bigger burden than before?
- Could e-residency be extended to Europe wide, avoiding the need for 28 separate country e-residencies?
- eIDAS provides the gateway, governments can accept an e-Identity but how do they use it?

Governments have implemented and interpreted the eIDAS Regulation in different ways but have seemingly reached the same conclusions. All agreed that the Regulation addresses only identification and authentication, not authorisation. The purpose of eIDAS was 'interoperability', which gives governments the freedom to innovate and operate.

The work carried out in Estonia was referenced, with recommendations to leverage the work already carried out in Estonia and to build a common understanding across the member states of the language used -- i.e. what do 'Substantial' and 'High' mean when applied to Levels of Assurance.

[5] http://ec.europa.eu/priorities/digital-single-market_en

From a legal perspective eIDAS has six components, the one discussed in detail was eligibility. Similar to the OIXnet registry, the European Commission manages a 'list' of eligible identity systems (referred to as "electronic identification schemes"). To be added to the list, a member state can self-certify to the European Commission that its eID scheme meets the applicable requirements to be listed (a process referred to as "notification"). This listing helps to create a level playing field, allowing the consumer and stakeholders to benefit from the competitive nature of the marketplace. The EU Commission's list of notified eID Schemes Trust lists have been considered, there is no legal requirement to use them but they are being considered.

One of the objectives of the eIDAS initiative, to change the behaviour of developers, decisions makers and stakeholders to instil optimism concerning the Identity Management part of the eIDAS Regulation, and will have practical consequences on how identity applications will be developed.

Next Steps:
The long-term goal is to build the single market by 2020 - to take away borders so that a citizen can do everything (online) throughout the EU that they can do in their own country. The eIDAS Regulation was needed so that the platform could be created to facilitate cross-border recognition of that person's identify. Next steps are to combine how to use this platform with applications and then it will be up to the sectors (health sector, etc.) to start to build these applications. The recent EU Cross borders Farmers pilot in The Netherlands and Belgium was cited; following its success it is being extended to Germany and The Netherlands.

Summary:
eIDAS was something that had to be done. It provided the initial building block and legislation to allow the re-use of eIDs in cross border transactions; however it addresses identification and authentication only. A simple example: I am an Estonian citizen, Estonia is on the EU Commission's Scheme list – thus my Estonian e-ID will be recognised by public sector agencies in the UK - but that's it! The next step, needed now, is to build services so the citizens can benefit from the cross-border recognition of their eID. eIDAS provides the legal framework but the end goal is services that citizens find useful; services they both trust and use. The next steps may be the result of the work being carried out in STORK and e-SENS. There are possibilities foreseen with International agreements and integration with other international schemes, however the timing is too early for this step. eIDAS is restricted to Public sector currently.

Schemes Panel: Policy Interoperability

Theme; Schemes/Trust Frameworks: Business, Legal and Policy Interoperability

A trust framework sets forth the rules and conditions for issuing an exchanging Identity information in a secure, reliable, trustworthy, and interoperable manner. eIDAS defines these rules and conditions to the extent necessary to facilitate cross-border recognition, but additional issues relating to the issuance of identity credentials are addressed in separate

trust frameworks on a national level.

- How do these national trust frameworks interoperate with the eIDAS framework?
- Do we need to exchange identity attributes, and do we need a trust framework for such attributes.
- Can the eIDAS framework be used for private sector service providers that also want to do cross border eID exchange?
- Business Model: Cross border identifications need to be free of costs. What does that mean for the national identification providers?

Attributes:

Identity Attributes are very important in eID schemes. How can you trust who I am? A definition of the two major classes of identity attributes was given:

1. Core Attributes that are about 'me' and who I am: Name, date of birth, etc.
2. Assigned Attributes that are about my rights, privileges, or authorisations: these allow me to do something or prove eligibility to access a service - these are about me but they are not my identity (e.g. they specify my employer, where I studied, the fact that I am a doctor, etc.)

Core Attributes about 'me' are covered in eIDAS as the minimum data set. This is the minimum amount of data needed to prove that I am 'me'. These attributes may allow a UK citizen to 'sign in' for example to a Dutch government service, but it doesn't mean that such person can do anything as it does not prove eligibility to use a particular service.

For services to work, assigned attribute services are needed - attribute providers that can consume a core identity and provide more information about that individual. Laws and standards are needed to say 'this is what an identity looks like' and 'how I can trust it'. Many believe this is an important element of the discussion and further development of this topic would be beneficial.

Sectors need to agree to cross border standards of trust in identity. In some sectors there are already initiatives such as the eHealth network - an additional layer on top of eIDAS for the health sector that deals with the assigned attribute problem.

Participants noted that Identity providers are naturally collecting assigned attributes - some contribute matching data sets, which, with the individual's permission or self-assertion, could be utilised and turned into a verified assigned attribute. Reference OIX White Paper: The Industry Working Group on Attribute Exchange.

More assigned attributes are needed to get richer attribute exchange beyond the core attributes of eIDAS. There is more work to be done to address assigned attributes.

Business Model:

The differing business models representing the current situation in two different member states, The Netherlands and the UK, were presented. In the UK, the government is funding the service and paying IDPs for identities used. This service is free to the citizen. In The Netherlands, the government is not putting money into the service. IDP costs are not fully

covered and may be passed on to the citizen. Cross-border opportunities will allow citizens to seek to secure an identity in the cheapest place. A Dutch citizen may get a (free) identity to use when dealing with the Dutch Government.

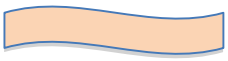
The solution may be permissible re-use of identities so that the IDP's can get money from the private sector - the private sector becomes very important in this type of scheme. If permission is given in the UK as it has in The Netherlands, both government and private sector will benefit.

OIX has undertaken projects to examine the permissible re-use of e-Identities issued by GOV.UK. Such projects include consultation work with the private sector to determine what a fully functioning identity market might look like, and to identify the characteristics and the commercial benefits of such a market. Information regarding the progress of this work is available on the OIX UK website. A white paper detailing the results of a recent private sector survey to consider aspects such as standards, certification process, branding, privacy and other issue will be posted in May 2016.

New Trust Frameworks

With the explosion of the Internet of Things, a global view is being taken by a considerable number of involved organisations that are working collaboratively to create the standards needed for this market. The Trust In Digital Life Association[6] have carried out a number of interoperability pilots testing eIDAS and GSMA's Mobile Connect, looking at bridging across different industries and how to use an identity for everything. The idea was proposed that the Identity 'ecosystem' should look to do the same; i.e., that the ecosystem needed is global with both governments and private sector.

Summary:
More assigned attributes are needed to get richer attribute exchange beyond eIDAS. There is more work to be done to gain trustworthy attributes. There are still a many challenges: the private sector has specific requirements and they do not know what information they need and how it might be facilitated.



Standards Panel: Open Identity Standards and Technical Interoperability

Theme: Technical Interoperability and Open Identity Technical Standards

The purpose of this panel was to explore the role of standards in this ecosystem of supply chains that we are trying to develop between public and private sectors and between different industry sectors, and speak to standards experts about how these standards have evolved and their direction. Standards were described as the 'plumbing' of the industry, but are only as good as their adoption. Each open standard enables new things to happen.

OpenID Connect is a simple protocol, which has been applied to different use cases, and it is now being proposed as the next generation enterprise federated identity protocol. It makes

[6] http://www.trustindigitallife.eu/

other things possible; it has become a 'transport layer'. The evolution of OpenID Connect for consumer identity, signing into social networks in a unified way, looks poised to become the unified protocol across enterprise and consumer identity with adoption by Google and Microsoft's adoption of OpenID Connect. The next phase will see systems built on top of OpenID Connect. The GSMA's[7] Mobile Connect is a one example of that. The OpenID Foundation's Mobile Operator Discovery, Registration and Authentication (MODRNA) Work Group is building a profile of OpenID Connect - telecoms operators can use the profiles to have their subscribers sign in to web or mobile apps using their existing telco account. This provides a number of business advantages; there is an existing relationship with the telco, there is a payment relationship, and possibly an assured identity. Add in the SIM in the mobile phone, and it can be used to authenticate, leveraging two or single factor authentication. More information can be found at http://openid.net/wg/mobile/

The notion of the OpenID Foundation Work Group IGov is to create a profile, built on OpenID Connect that is applicable to multiple international governments. The core standard would make interoperability simpler, allowing for the creation of easily accessible services by consumers. This would offer governments the ability to leverage the commercial infrastructure, as referenced in the discussions, expanding the opportunity for adoption. Governments want to meet citizens where they currently hold Internet accounts such as Google mail etc. This becomes relevant to not only the technical developers but to the legal and policy makers as well. They can build on existing infrastructure to provide better value for citizens, governments and enterprise.

Privacy is a key issue of our time. How do we "build on what has been built" and turn the control to the user enabling them to manage access to their data? Privacy was considered as a business driver. That is, by giving users privacy controls, a more trusting and therefore meaningful relationship is built. User Manager Access (UMA), an extension of OAuth, takes it roots from OpenID Connect; it is a new standard built on top of other standards that has not yet been fully adopted.

Another dimension considered by the group was the set of standards instantiated in 'cards' and the 'things' that are part of the identity Internet ecosystem. Standardisation needs to be tested. Frameworks need to be developed to test that both rules and products are 'safe' to use. In some ways its counterintuitive to think about standards, if everyone is doing the same thing in the same way, how does that help security?

- Standards drive increased usage
- Standards drive the potential for more user control and managed access
- Standards drive uniformity

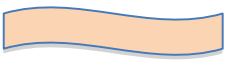
All of these drivers have security implications - the 'bad guys' thrive in confusion and standards help with security in this way.

Standards appear in both regulated and unregulated industries. Some of these unregulated industries (e.g., social media and search) are able to move in a more agile manner than the global marketplace. The regulators have not yet caught up with the innovators. This model is changing. With the evolution of Safe Harbour to the Privacy Shield and new thinking around privacy, standards will be under pressure and increased momentum around building profiles

[7] GSMA is a member of the OpenID Foundation

for existing standards to enable greater security and privacy. The participants concluded that everything is being disrupted including auditing and third party certification. The Internet needs to scale. We need Internet scale trust mechanisms to replace high overhead and challenging tasks like auditing. New tools that can be trusted need to be found. In OpenID Connect a new experiment began 2 years ago, a self-certification experiment that has the following characteristics: a legally binding self-attestation of technical conformance. This new trust tool allows anyone at any time, at no cost to look at the results.

Summary:
OpenID is a simple protocol that is used on user devices such as cell phones to log on to email applications. On top of OpenID, profiles can be added - including a government profile. Implementation of Open Standards can be registered on registries such as OIXnet - it is open and transparent. The OpenID Foundation's Self-Certification Program together with the OIXnet Registry can help to provide a quality assurance and quality control mechanism as well as some level of trust because they can be easily and continually checked by competitors, solution providers, systems integrators and a world wide network of independent developers.



Case Study Panel: Current & Future Projects

Theme: How do we align Identity Law and Policy to Projects?

Through OIX pilot projects, OIX members test real world use cases. Projects are defined as small scale, low risk assessments, analysis or tests of interoperable components that address some of the key challenges of creating convenient, secure and privacy-enhancing digital transactions. All projects result in White Papers.

In this portion of the meeting current and potential projects, specifically looking at global and cross-border issues, were presented and discussed. Through such OIX projects participants in both the public and private sectors can collaborate, protected by the OIX "IPR wrapper,"e.g. the requirement for all project participants to sign the IPR agreement this allowing low-risk exploration of global identity issues to take place.

Proposed: Travel Industry and Identity
Identity in the traveller life cycle today does not have a federated approach. Each step of the process requires separate identification. Handling of the traveller's private data, and the associated costs and liability, are currently met by each organisation at each point of the process, resulting in a rather inefficient model. The travel industry's hope for the future is identity federation across the whole process from initial web searches, through pre and post trip so that it can be secure, federated and personalised. With a federated travel industry, one secure, federated login (with privacy by design) can allow the traveler to be in control; can provide benefits for both the providers/retailers (lower costs and risks), and benefits for the traveler (less form filling, clear understanding of where personal data is held). The proposal is for a trusted framework for the travel industry, linking who you are physically with your digital identity could enable a streamlined unified security process.

Current: Digital identity across borders: doing financial transactions in another EU country
This discovery project looked at the use of a digital identity across borders by exploring the hypothesis: individuals coming to the UK will be inclined and able to open a UK bank account online, prior to arriving into the country, using their national digital identity. The proposition from Barclays is to open a bank account in ten easy steps. Collaborating organisations included banks, governments and regulators: Barclays, BankID, BBA, difi, Cabinet Office and the FCA. This project was paper based with user testing. Around 50% of accounts opened in the UK are by people new to the country and they do not have a digital footprint; the process can be both difficult and lengthy. This project looked at the re-use of eIDAS within the private sector and the development of digital identities such as GOV.UK Verify in the UK. This pilot project looked at a complete online process. This project has been completed with a white paper.

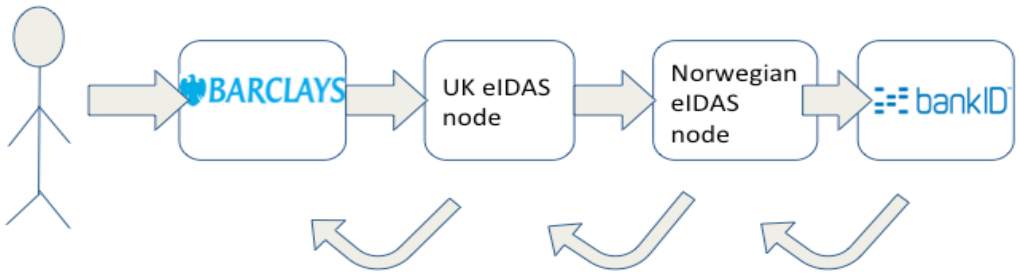


Diagram: User journey workflow

A reference was made to the STORK eBanking project

Current: Creating a Digital Identity in Jersey - States of Jersey
This Crown Dependency of the UK has been looking at how they can provide their citizens with a safe and secure digital identity, with a future vision of how those eID's can be interoperable under eIDAS. Jersey has a small demographic, around one hundred thousand citizens, and has the same constitutional monarchy as the UK. It is a self-governing parliamentary democracy with its own financial, legal and administrative systems, with the power of self-determination. The starting point to this OIX discovery project was to look at the existing GOV.UK Verify scheme to see what could be reused to create digital Identities in States of Jersey. Key questions included how will these elements [of GOV.UK Verify work and how can they be made interoperable between the UK and Jersey and also between Jersey and other European member states. Working with OIX for this project has allowed for open conversations with other OIX members, which includes most of the GOV.UK Identity Providers and UK Cabinet Office GDS and transparency of both the journey and decisions made following the outcome of this project for this government.

Current: Shared Signals
This OIX alpha project is looking at the hypothesis: what if we could share in a privacy preserving manner, a small signal that would indicate the email account you are depending on is no longer trusted at this point. This proposition could have a significant effect on a huge range of password base fraud. This project builds on the previous two OIX projects Shared Signals How to Protect the Identity Ecosystem and Shared Signals IDP to IDP. This project

involved two of the UK Identity providers, and is looking at two use cases, Registration Velocity and Account Takeover. The base infrastructure was deployed, simple API's written and test signals exchanged. These test signals, a multi task mechanism, are carefully designed so that no additional information about the customer is released. End to end signals that deal with these two use cases using data limited signals have been complete between the two identity providers taking part in the project. The white paper is due shortly. The discussions at the meeting concerning the next steps indicate that if Identities are soon to be shared amongst member states, we need protection against Account Take Over (ATO), Identity Fraud. As an ecosystem and group of identity professionals we have the opportunity now to consider how we deal with problems in our ecosystem in an interpretive fashion that preserves privacy.

Diagram: Identity Eco-System

Current: ReCred: From Real-World Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

This research project has a goal to promote the user's personal mobile device to the role of a unified authentication and authorisation proxy towards the digital world. This project is funded by Horizon 2020 and is led by University of Piraeus, Greece. It involves 4 pilot projects:

Pilot 1: Device-centric campus WiFI and web access control
Pilot 2: Student Authentication and offers
Pilot 3: Attribute-based age verification online gateway
Pilot 4: Financial services - micro-loan origination

Through these four pilots, using well known protocols such as OpenID Connect and Mobile Connect amongst others, this research project looks to test problems such as password overload, lack of real-world binding, identity fragmentation and lack of support for attribute

based access control.

Conclusions

We have global, Interoperable eco-systems that are referencing each other. Telecommunications, airlines, mobile, and the credit card system all employ trust frameworks of business, technical, legal rules developed over thirty years to provide the user experience we have today. eIDAS is maturing quickly to provide a platform for trusted identity transactions. However, it is maturing in a time when we also have other global ecosystems, such as the social networks and other social players. Assigned attributes are becoming increasingly important. Identity could be visualised as the bag with a name on it and the assigned attributes are inside the bag. If you shake the bag you can hear money clinking together. In some cases there is monetising of these attributes. We see these as different islands of identity - public, private and this new grey area of private public partnerships that we are trying to work through today. Registries are a common term with different definitions. We are beginning to reconcile the vocabulary between these different islands of identity, these different eco systems and that's where we need to start if we want to talk about business, legal and technical interoperability.

* * *

Throughout 2016, Open Identity Exchange will return to these pivotal issues in a series of International Identity, Law and Policy Workshops. Each workshop will examine these issues through the different lenses of a range of experts and stakeholders in the United States and Europe for a global discussion. Each workshop's output will in turn inform discussions at the next. We will report findings at the Cloud Identity Summit in New Orleans in June and at our third annual "Economics of Identity" Conference in London in September.

This White Paper and those to follow reflect OIX's goal to complement the work of public and private sector organisations seeking to address international legislation, policy, regulation and law. OIX members hope to contribute to better laws and regulations so as a result, users, customers and citizens might be better served online, and their privacy and security better protected.

Registered Event Participants

Company	Name
ABN Amro	Waheeda Rahman
AET Europe	Carlos Serratos
Agentschap Telecom	Denise Kramer
Agentschap Telecom	Melle Schol
Agentschap Telecom	Robert Adrian
Amadeus	Hervé Prezet
Barclays	Bryn Robinson-Morgan
Betaalvereniging	Allard Keuter
BNP Paribas	Gaelle Berrier
BNP Paribas	Stephane Mouy
Call Credit	Andrew Mulligan
Callcredit	Charlotte Elmer
Capital One	Kajal Bansal
Capital One	Kshitij Zulkanthiwar
Capital One	Ollie French
Capital One	Thomas Bosley
Centralny Ośrodek Informatyki	Rafal Drewnowski
Complaints & Disputes Commission.	Marten Voulon
Confyrm	Andrew Nash
Consultant	Jon Webb
Dep. of Economic Affairs	Hans van der Burght
Dep. of Economic Affairs	Huub Jansen
Digidentity	Dick Dekkers
Digidentity	Marcel Wendt
EAB	Max Snijder
ECP	Jelle Attema
EEMA	Jon Shamah
Equens	Inge de Ruijter
Estonia	Thijs de Neeve
EU Commission	Neil Clowes
Evidos	Kick Willemse
Experian	Jim Lound
Fedict	Frank Leyman
Forgerock	Chris Adriaensen
Forgerock	Nick Taylor
GBG	Amy Garner
GDS	Adam Cooper
Gemalto	Alexander Korthals Altes
Government eSENS	Freek van Krevel
ID Checker	Michael Hagen
ING	Andrei Ilchenko
ING	Loes Bomans
ING	Mark Kramer
ING Bank NV	Matthew Nunnink

Innovalor	Bob Hulsebosch
InnoValor	Maarten Wegdam
Innovate Identity	Emma Lindley
iSignthis	Marc Bongers
KeyControls	Erik Verheul
KPN	Haydar Cimen
LexisNexis	Dave Webber
Logius	Michiel Dollenkamp
Mazars auditors	Jan Matto
Morpho	Freek van Gijn
Morpho	Jouri de Vos
Mydex	Jack Mitchell
OIXUK	Don Thibeau
OIXUK	Sue Dawes
Paidstrategies	John Devlin
PIMN	Jaap Kuipers
Ping Identity	Hans Zandbelt
PKI Partners	Poppe Wijnsma
RDW	Gert Maneschijn
ReCRED project	Christos Xenakis
Reece Conrad	Reece Conrad
Shell International	Friso Abcouwer
Shell International	Jaap Oostindier
Shell/Capgemini	Paul Hendriks
SIA	Jerome Boudineau
SIDN	Esther Makaay
States of Jersey	Stephen Hart
Stierman Advies BV	Job Stierman
Time Lex	Jos Dumortier
UL	Remco Schaar
Unibet	Krzysztof Rusajczyk
Verizon	Bharadwaj Pulugundia
Verizon	Chris Zijderveld
Verizon	Eric Krol
Verizon	Essam Mahmood
Verizon	Harm-Jan Arendhorst
Verizon	Johan Beekhuizen
Verizon	Oziem Bilgili
Verizon	Rob Kroneman
Verizon	Ron Jacobs
Vix Verify	Arjen Kooi
YOTI	Paco Garcia