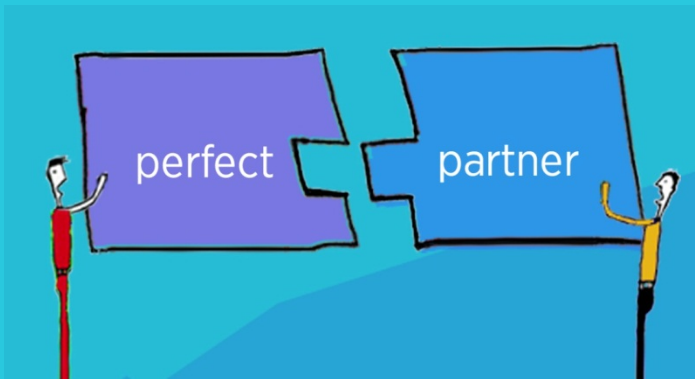
piran PARTNERS

Digital Identity:

An Introduction



Miles Cheetham, Director

December 2013

Table of Contents

1 Introduction

The rapid growth of the digital economy in the developed world since the mid 1990s has placed online and mobile services at the heart of business and government strategic thinking and planning. As the industry matures, there are increasing requirements to provide the infrastructure and enablers that will ensure the continued success of the sector, addressing consumer, business and public sector concerns.

One of the key enablers of the future digital economy will be trust – provided by a highly secure Digital Identity service: this will be critical to underpin the growth of the digital economy as a whole and is rightly being given a great deal of attention by national governments and regulators worldwide.

Concerns over security and trust must therefore be comprehensively addressed if the potential value inherent in the digital economy is to be realised.

Digital Identity is therefore synonymous with fundamental trust. This trust will allow private and public entities to know with whom they are dealing, and vice-versa will allow the individual to know that they are dealing with a trusted party. As consumer and business confidence increases, so consumers will transact more often and more freely. Increasing amounts of consumer-controlled identity information with increasing value to the economy will be consumed, enabled by stronger authentication, increased privacy and higher security in a safer online environment.

This white paper provides an introduction to Digital Identity and how such services operate.

1.1 Report Glossary

As the subject is evolving rapidly the terminology in the industry has not yet standardised, but the underlying roles and processes remain the same. The following terms are used within this report.

Term	Explanation
Attribute Broker	Attribute Brokerage can exist in both the Attribute Provider entity and the Digital Identity Service Provider. The entity verifies the attribute request and provides attributes subject to user consent: what can be shared, who can have access, and for how long.
Attribute Provider	Provides information that collectively creates the Digital Identity of the individual, such as address, telephone number, e-mail, national insurance number or student enrolment number.
Authentication Provider	Provides an authentication step using (e.g.) a one-time-password for explicit authentication, or can provide various forms of implicit authentication such as IP address, device, location or social verification.
Claims Provider	An alternative name for an Attribute or Identity Provider.

Credentials	Sometimes passwords or other means of authentication are referred to as credentials, but generally credentials are certificates and associated key material issued in public key cryptography.
Digital Certificates	Issued by organisations such as mobile network operators, Banks, Public Sector to provide the authenticity and integrity and non-repudiation in online transactions.
Digital Identity Service Provider	The consumer-facing entity providing the Digital Identity service. This entity may also provide a range of services ranging from registration, varying levels of authentication or potentially acting as an attribute broker.
Digital Signature	A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.
Federated Identity	The means of linking a person's Digital Identity and attributes, stored across multiple distinct identity management systems. This allows the Digital Identity to be used by different Relying Parties and Digital Identity Service Providers seamlessly.
Identity Proofer	Checks the identity of individuals – either from public records or in person - in order to provide a high level of assurance that they are who they claim to be. This might be a lawyer, notary or Post Office checking a passport and utility bills. Can also be called a Registration Authority.
Level of Assurance	There are generally accepted to be four Levels of Assurance (LoA), ranging from basic self-assertion through to the requirement to use a hardware token. The LoA reflects the level of certainty that the person is who they claim to be, and the level of security attached to that Digital Identity.
Personal Data Store	A personal data store (PDS), vault or data locker is a service to let individuals store, manage and deploy their key personal data in a highly secure and structured way. It also enables individuals to acquire and reuse proofs of claims or of relationships and qualifications (such as bank account, verified address, driving licence or passport).
Relying Party	The organisation, service provider or online retailer that requires proof of identity and/or information about the individual in order to grant access to an online service or resource. This organisation has therefore chosen to outsource identity management and may accept Digital Identities from more than one Digital Identity Service Provider.
Trust Framework	Large scale networks with multiple organisations that use a common and mutually agreed set of operational, process, technical, legal and enforcement standards to provide confidence when securely exchanging information relating to the management of Digital Identities.

Source: Piran Partners

2 What is a Digital Identity?

2.1 Real Individuals Online

Digital Identity, at its simplest, is an online proxy for a real individual. It can be thought of as a set of information or claims made about an individual that may have been made either by the person, or other entities such as companies or government organisations that hold information about that individual. This information is considered as a set of attributes for that individual, which can be used to identify them. These attributes can include the obvious, such as name, address, date of birth, driving licence number and so on, and less obvious such as the length of time they have been active on social networking sites. This information can be used to create a picture of that person, with varying degrees of certainty – a level of assurance (LoA) that that person is who they say they are.

This set of individual attributes can then be used to create a Digital Identity, allowing the holder to gain access to services or resources either in the real world or online. There are numerous definitions, but The European Commission summarises that a Digital Identity is:

> *A means for people to prove electronically that they are who they say they are and thus gain access to services. The identity allows an entity (citizen, business or administration) to be distinguished from any other.*

Digital Identity is not new. There are already millions of Digital Identities in use every day, and without stopping to think about it many people own one or more from Microsoft (Hotmail, Outlook, Windows Live), Google, Yahoo!, Twitter, Amazon or Facebook. Many consumers are already using advanced Google services, and both the Android and Apple iOS operating systems support their respective identity propositions. Furthermore, everyone expects a secure login process for their online banking, and will at some point have been required to prove their identity at their bank branch by showing proofs, such as a passport and utility bill. Banks themselves are well placed to offer Digital Identity services and are a likely participant in the future Digital Identity ecosystem.

However, current Digital Identities are often limited in how they can be used both to the owner and to potential Relying Parties, since they are mainly self-asserted, and therefore a relatively low level of assurance can be attributed. These become more useful (with a higher level of assurance) if validated attributes about the person using the Digital Identity can be provided, such as an address that has been confirmed as correct. The Digital Identity can be more strongly linked to the real person if these attributes can be verified, so the Digital Identity begins to have more value to the citizen, Relying Parties and the entire Identity ecosystem. Digital Identity can therefore become a realistic and user-friendly alternative to a username and passwords.

2.2 Levels of Assurance

Digital Identity has different strengths, which are appropriate in different situations. These are called Levels of Assurance, or LoA. For example, it may be fine to use a self-asserted Digital Identity – effectively just a user name and password – to access a website or social networking site. However this would be inappropriate for government services such as tax collection systems or welfare provision.

The definition varies from country to country, however the principles are broadly the same. The UK Government, for example, has defined four levels for access to public online services in a series of Good Practice Guides. These four levels each have increasing confidence and decreasing risk due to the stringency of the identity checking, coupled with more rigorous security checking.

2.2.1 Determining the LoA required

In determining the LoA required, there are some key questions:

- What is the online service intended to do and what security challenges will it bring?
- Who will be involved in delivery and consumption of the service and what expectations and concerns do they have?
- What risks will be posed as a result of putting this service online?
- What security profile should the service seek to achieve?

For example, UK government departments determine the LoA (from zero to three) they require for digital services as follows:

- LoA 0 is used when the service provider does not need to know who is accessing the service (for example, when users access a support FAQ service, no sensitive information is delivered or solicited).
- LoA 1 is used when the service provider needs to know that it is the same user returning to the service but does not need to know who that user is.
- LoA 2 is used when it is necessary to know who the user is and that he/she is a real person.
- LoA 3 is used when it is necessary to know who the user is and that he/she is a real person - to a sufficient level of confidence to be offered in support of criminal proceedings.

The LoA levels are further described in Figure 1 below.

Figure 1 **Levels of Assurance**

Level of Assurance	LoA 0	LoA 1	LoA 2	LoA 3
End User	**Not required**	**Asserted**	**Tested**	**Verified**
Personal Registration	The real identity of the individual is not relevant to the service. Users may save preferences and other material but no personal information is solicited.	User asserts an identity. This identity (need not imply a real identity) is not tested. Personal information solicited is not shared externally.	User asserts a real identity with information that allows it to be tested independently of the immediate presence of the subject.	User claims a real identity that is subject to rigorous independent testing to verify the individual's identity and presence.

End User	Not required	Asserted	Tested	Accountable
Corporate Registration	The legal identity of the organisation is not relevant to the service. Users may save preferences but no commercially sensitive information is solicited.	User asserts an identity. This identity is not tested. Commercially sensitive information solicited is not shared externally. The user is assumed to be entitled to act on behalf of the organisation.	User claims a corporate identity and provides information that allows it to be tested, sufficient to confirm the legal identity of the business, the user's real identity and the user's claim to represent the organisation.	Physical identity proofing required. Hardware token essential. System must use strong cryptographic authentication for every party and for all sensitive inter-party data transfers using public key or symmetric key.

Source: UK Government Good Practice Guide

The higher the LoA required, the stronger the form of authentication imposed, as detailed in Figure 2. This ranges from username and password through to One Time Passwords, software and ultimately hardware tokens. LoA 3 could, for example, be achieved using a hardware token with strong cryptographic authentication. This could be delivered using a Mobile Digital Signature with associated Identity Proofing by an Mobile Network Operator. The higher the LoA required by the Relying Party, the more complex and therefore the higher the cost associated with achieving this.

Figure 2 **Authentication Requirement for Levels of Assurance**

Level of Assurance	LoA 0	LoA 1	LoA 2	LoA 3
	Not required	**Minimal**	**Robust**	**Accountable**
Requirement	Self Asserted. No identity Proofing. No additional authentication actions are required to access the service. Implicit Authority by virtue of the access path may be inferred.	Basic identity. Use of a password/PIN. The user is required to hold an authentication credential that is recognised by the service. A secret may be directly quoted during authentication.	Multi-factor authentication using physical or software token and memorised secret. User must possess a robust credential that is recognised by the service.	Must use hardware token and use strong cryptographic authentication using public key or symmetric key technology. User must possess an authentication credential.

Source: UK Government Good Practice Guide

3 Digital Identity in a Trust Framework

3.1 Rules Within a Trust Framework

The ecosystem for Digital Identity is referred to as a Trust Framework. These are large-scale networks with multiple organisations that use a common and mutually agreed set of operational, process, technical, legal and enforcement standards so that they can be confident about securely exchanging information relating to the management of Digital Identities.

Before explaining the processes and players in the Digital Identity ecosystem it is important to understand the rules that apply. Widely respected for his insight and influence, Kim Cameron, formerly the Chief Architect of Identity and Access at Microsoft, defined Seven Laws of Identity. These laws have set the foundation for the development of strong digital identities that can be reliably employed for user authentication and authorisation in a federated trust framework.

Figure 3 **Seven Laws of Identity**

The Seven Laws Of Identity: Kim Cameron

1. *User Control and Consent - Digital identity systems must only reveal information identifying a user with the user's consent.*
2. *Limited Disclosure for Limited Use - The solution which discloses the least identifying information and best limits its use is the most stable, long-term solution.*
3. *The Law of Fewest Parties - Digital identity systems must limit disclosure of identifying information to parties having a necessary and justifiable place in a given identity relationship.*
4. *Directed Identity - A universal identity metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.*
5. *Pluralism of Operators and Technologies - A universal identity metasystem must channel and enable the interworking of multiple identity technologies run by multiple identity providers.*
6. *Human Integration - A unifying identity metasystem must define the human user as a component integrated through protected and unambiguous human-machine communications.*
7. *Consistent Experience Across Contexts - A unifying identity metasystem must provide a simple consistent experience while enabling separation of contexts through multiple operators and technologies.*

Source: http://www.identityblog.com

The important theme is therefore consent and privacy protection. User-centric identity systems must allow the user to see how their personal data is being shared between the different endpoints. This allows the user to intervene and stop unwanted sharing of information. Any Relying Party must obtain consent before asking for any information, so meeting with data protection and privacy law.

3.2 Roles within a Trust Framework

The roles in the ecosystem can be described in terms of the task that they perform, but it should be noted that there can be some ambiguity as, for example, a Relying Party can also be an Attribute Provider; both supplying Attributes into the marketplace for consumption by third parties and using a Digital Identity service to allow access to its own website.

These players operate as a federation where they trust the data that is passed between them – hence the term Trust Framework.

3.2.1 Digital Identity Service Provider (DISP)

The Digital Identity Service Provider has a number of roles. From the customer's perspective, it may be the initial registration authority accepting the consumer's request for service, it can manage the login/authentication process and provide the control point for the consumer over consent to access the user's data and the preferences that the consumer may record. In simple terms the consumer would see this as the login manager. It can also assume roles such as an Attribute Broker, although this role can exist separately, buying and reselling Attributes in a free market.

It therefore acts as a central point in the ecosystem, receiving requests from Relying Parties and obtaining the Identity and Attribute information that they want. For example, a Charity wants to know the name, address and postcode of a donor in order that they can claim tax relief on the donation. The DISP in turn makes a request to the appropriate Attribute and Identity Providers for this information and presents the required information back to the Relying Party. Requests made by Relying Parties can therefore be distributed to different Identity and Attribute Providers as appropriate and then aggregated by the DISP before being returned to the Relying Party. The DISP therefore has the role of presenting the right Identities, Attributes and credentials to each of these endpoints in a secure and privacy preserving way, and to collect the information required from Attribute and Identity providers.

3.2.2 Attribute Provider (AtP)

An attribute is simply an address, age, gender, national insurance number, driving licence class or other piece of information about an individual. This may be served by a range of organisations including banks, mobile network operators, employers, vehicle and driver licencing authority or even other Relying Parties who have information about someone, such as date of birth. AtPs are very similar in nature to IdPs. The distinction is organisational and not technology: an AtP will manage and provide extra attributes about the person, while the IdP issues the core identity claims.

3.2.3 Identity Provider (IdP)

The IdP is a specialist entity responsible for validating the online identity of the entity, or the core identity claim. This will typically involve standard online checks. These organisations may also provide Identity Proofing services.

3.2.4 Identity Proofing

Where a higher level of assurance is required the Relying Party might require a face-to-face check, through an Identity Proofer, such as showing a passport, utility bill or driving licence.

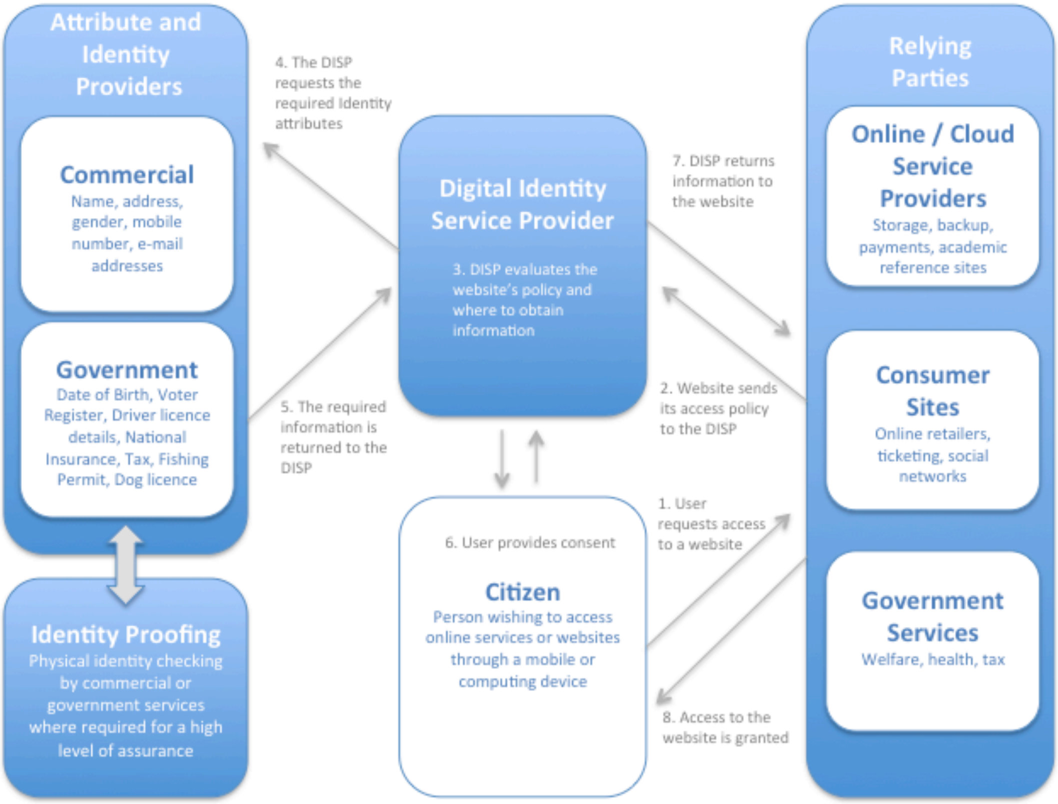
3.2.5 Relying Party (RP)

The Relying Party is the organisation that wants to collect the information that is needed in order to allow access to a service or allow a transaction to proceed. In a commercial sense this could be a car rental company wanting to know date of birth and driving licence details, or in government it could be the Department of Work and Pensions to allow a claimant to obtain welfare support.

3.3 Using a Digital Identity

The process for an individual to use their Digital Identity is straightforward from their perspective, but there may be complex information flows within the Trust Framework behind the scenes. The illustrative diagram in Figure 4 illustrates the way in which the system works.

Figure 4 **Accessing a Website using a Digital Identity (Illustrative)**


Attribute and Identity Providers
Commercial
Name, address, gender, mobile number, e-mail addresses
Government
Date of Birth, Voter Register, Driver licence details, National Insurance, Tax, Fishing Permit, Dog licence
Identity Proofing
Physical identity checking by commercial or government services where required for a high level of assurance
4. The DISP requests the required Identity attributes
5. The required information is returned to the DISP
Digital Identity Service Provider
3. DISP evaluates the website's policy and where to obtain information
6. User provides consent
Citizen
Person wishing to access online services or websites through a mobile or computing device
7. DISP returns information to the website
2. Website sends its access policy to the DISP
1. User requests access to a website
8. Access to the website is granted
Relying Parties
Online / Cloud Service Providers
Storage, backup, payments, academic reference sites
Consumer Sites
Online retailers, ticketing, social networks
Government Services
Welfare, health, tax

Source: Piran Partners

The process follows a number of steps:

- The user wishes to access a website. He/she will click on an icon marked with a familiar trust mark or text that indicates that the site accepts their Digital Identity.
- The website issues a request to the Digital Identity Service Provider (DISP) for the information that it requires. This may be very basic, such as username and password, or more complex, asking for other attributes such as confirmation that the user is over 18, or has a valid driver's licence. Banking and Government sites will typically require the highest level of assurance.
- The DISP evaluates the website's policy and where the required information can be obtained.
- The appropriate Attribute and Identity Providers are asked to provide the required information.
- The Attributes and Identity information required are returned to the DISP, which then applies back to the user for their consent to share it with the website that they wish to access.

- The user grants their consent.
- The DISP processes the request back to the website.
- Upon receiving the correct Attributes and Identity information the website grants access to the user.

This is, however, a simplified process in order to illustrate the important interactions in the system. In practice, the DISP will offer different services as it seeks to differentiate and innovate, and whether it offers simple registration and login/authentication service, or whether it extends this to cover services such as digital signatures and higher levels of assurance.

4 EU & US Digital Identity Initiatives

A major current trend is the establishment of private and state initiatives to create large-scale Trust Frameworks. The key initiatives in the European Union and United States are described below.

4.1 European Union

4.1.1 STORK (Secure Identity Linked Across Borders)

The original STORK pilots, now completed, aimed to establish a European electronic Identity (eID) Interoperability Platform to allow citizens to use services across borders, just by presenting their national eID. The aim was that citizens and legal entities should be able to start a company, interact with the tax authority, obtain university papers and similar activities, without a physical presence; all they need is to enter their personal data using their national eID, and the STORK platform will obtain the required guarantee (authentication) from the appropriate government.

It was designed from the outset as a user-centric approach with a privacy guarantee. The STORK platform identifies a user who is in a session with a service provider, sending the required data to this service. Whilst the service provider may request various data items, the user always controls the data to be sent. The explicit consent of the owner of the data, the user, is always required before his data can be sent to the service provider.

STORK 2.0 is now underway. This will further contribute to the realisation of a single European electronic identification and authentication area, by building on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities and the facility to mandate.

Further information can be found at www.eid-stork.eu.

4.1.2 TDL (Trust in Digital Life)

Building on the experience of STORK, European Union strategy aims to develop and maintain a strong and globally competitive position using widely accepted innovative solutions that facilitate growth in the European digital economy. Trust lies at the heart of this approach. TDL, therefore, brings together European public and private stakeholders in order to address the trust issue, and enable European industry to innovate successfully, taking particular account of European culture, economic necessity, and real human behaviour.

TDL has the role of encouraging industry to develop innovative information and communication technologies and supports the industry and government in achieving a take-up rate of trustworthy ICT by:

- Raising awareness through the monitoring of the impact of incidents.
- Raising awareness through the definition and testing of interoperable frameworks for e-authentication services in public and private domains.
- Defining end-to-end technology platforms for user controlled data life cycle management.
- Defining end-to-end technology platforms for mobile service integrity.

Further information can be found at www.trustindigitallife.eu

4.1.3 Identity Assurance Programme (IDAP)

The UK Government has launched IDAP in order to enable secure citizen access to online government services. The government has endorsed the federated identity assurance model as essential for the *digital by default* initiative and stated the importance of this digital policy, not just for public services but for the wider economy. Its objectives are to give wider access to government services and bring more services and citizen/government interactions online while saving money and improving efficiency. IDAP is a co-opetition model so Identity Providers must co-operate in order to set scheme rules while competing to win customers.

Ultimately, the aim is to create an open market for Identity Service Provision. Five organisations including Verizon, The Post Office and Experian have been awarded licences through the Cabinet Office Identity Assurance Framework, giving them the opportunity to operate in this market. It is not a given, however, and individual government departments issue call-off contracts to Identity Providers under the framework. The initial pilot is set to be with the tax authority, HMRC.

Further information available at http://digital.cabinetoffice.gov.uk/category/id-assurance/.

4.1.4 Assure UK

Assure UK is a commercial trust framework initiative, which aims to increase UK consumer and business confidence in online transactions and commerce. It is a cross-industry initiative established by the GSMA, OIX and UK Government IDAP, and is intended to provide a contractual, organisational and technical framework that allows consumers to control and share their personal data with service providers and online retailers.

Its key objective is to give UK business a core framework within which trusted identities and attributes can add value by:

- Increasing the commercial value of the transaction
- Reducing fraud risk
- Simplifying the user experience
- Enabling innovative new services

4.2 United States

4.2.1 NSTIC (National Strategy for Trust Identities in Cyberspace)

NSTIC is a White House initiative, working collaboratively with the private sector, advocacy groups, public sector agencies, and other organisations to improve the privacy, security, and convenience of sensitive online transactions. The Strategy calls for the development of interoperable technology standards and policies — an Identity Ecosystem — where individuals, organisations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. The goals of the Strategy are to protect individuals, businesses, and public agencies from the high costs of cyber crime such as identity theft and fraud, while simultaneously helping to ensure that the internet continues to support innovation and a thriving marketplace of products and ideas.

NSTIC has four Guiding Principles:

1. Identity solutions will be privacy-enhancing and voluntary
2. Identity solutions will be secure and resilient

3. Identity solutions will be interoperable
4. Identity solutions will be cost-effective and easy to use

The NSTIC vision is for an online environment where Digital Identity significantly improves on the current username/passwords approach used to login online. Significantly, a key aim is for a vibrant marketplace – an Identity Ecosystem - that allows people to choose among multiple Digital Identity providers. It envisages both private and public organisations that would issue trusted credentials that could be used widely to prove identity. Establishment of such an Identity Ecosystem would allow individuals to validate their identities securely during sensitive transactions (like banking or viewing health records) and let them stay anonymous when they're not (like blogging or surfing the web). The Identity Ecosystem would protect the privacy of individuals by reducing the need for individuals to share personally identifiable information in order to identify themselves at multiple websites and by establishing consistent policies about how organisations use and manage personally identifiable information in the Identity Ecosystem.

Further information at www.nist.gov/nstic.

4.2.2 OIX (Open Identity Exchange)

OIX is a non-profit trade organisation focused on internet identity solutions. OIX is a *team of rivals*, with a membership of industry players representing a cross-section of private and public sectors such as the internet (e.g. Google, PayPal), data aggregation (e.g. Equifax, Experian), telecommunications (e.g. AT&T, Verizon) and government (UK Cabinet Office). The OIX's goal is to enable the expansion of online services and adoption of new online products through the development and registration of trust frameworks and sharing of domain expertise, joint research and pilot projects to test real world use cases. OIX is building OIXnet, an authoritative registry for online identity trust to enable global interoperability among identity federations.

For more information, visit www.openidentityexchange.org.

5 Regulatory, Legal and Standards

The regulatory framework is still developing as the market itself evolves. However, the key principle is that as the online economy develops, trust and reputation will become important assets. National policy makers are therefore concerned that they maintain a consistent approach both with respect to the borderless nature of the internet and the legal and regulatory frameworks already in existence.

In the EU in particular, a consistent approach between national regulators is essential in order to ensure cross-border harmonisation and cross-platform interoperability, encouraging competitiveness and a common user experience. This is a significant challenge and the framework is under development, aided by the learning from initiatives such as Trust in Digital Life (TDL), which seeks to commercialise cross-border, cross-platform and cross-community Digital Identity services.

It is therefore necessary to refer to the existing regulatory framework. At this point much of this is determined by online authentication and user identification, being process-driven and considering the way in which data is processed in order to enable online transactions. This is, by its very nature, a rapidly developing and complex area that includes:

- Electronic identification, signature and trust services
- Data protection and security
- Technical standards
- Mobile banking, payments and commerce

The EU is developing a framework for trust services such as online authentication and digital signatures including a specific obligation to legally formalise digital signatures. Furthermore, EU member states are expected to mutually recognise and accept those electronic identification services that have been notified as recognised schemes.

Data protection and privacy laws are currently under scrutiny, but may differ widely between EU member states as across the world. This is a serious issue – the legal certainty and trust, essential for markets to operate, restrains cross-border flows of information and therefore hinders the development of cross-border Digital Identity services. For mobile network operators this manifests, at times, as a distinctly uneven playing field, as telecoms regulation governs the use of mobile traffic and location data used in value added services, whereas un-licenced internet-based service providers with over-the-top services may not be bound by the same rules. Clearly, this is an area where legal clarification is required and it will be necessary to implement a consistent approach – not straightforward when technology has the tendency to run faster than the lawmakers.

Technical standards for Digital Identity are similarly complex, and may be rooted in approaches that were originally developed to support national legislation. Consequently, there are many standards, managed not only by national standards bodies, but also by international agencies such as ITU (International Telecommunications Union), ISO (International Organisation for Standardisation and ETSI (European Telecommunications Standards Institute). There is a great deal of work to be done in this area and, of all the regulatory frameworks, this has the highest level of uncertainty associated with it.

Mobile payments, banking and commerce are all subject to sectoral regulations, which differ across the world. The EU has been very active in this area, and sees these services as priorities to enable strong development of the digital economy in Europe. As these are new types of business opportunities there are not so many underlying national legacy regulations rooted in the past, although, of course the banking sector is well regulated.

6 About Piran Partners

Piran Partners provides clear, practical and straightforward advice to clients in the converging mobile, media, retail and financial sectors.

We enable businesses to capitalise on the revenue streams that can be achieved by placing mobile technology and mobility at the heart of your business strategy.

We approach consultancy engagements from a wholly commercial perspective, implementing solutions that solve problems, create deeper customer relationships and drive results through commercial value.

The Piran Partners' team consists of world leaders in the field, and works with an impressive client list of Mobile and Virtual Network Operators, Vendors, Banks, Retailers and Media Companies.

For more information on our services, please visit **www.piranpartners.com**, call **+44 (0) 207 349 5127** or email **info@piranpartners.com**

Piran Partners, Warnford Court, 29 Throgmorton Street, London, EC2N 2AT, UK

Every effort has been made to ensure that the information in this document is true and correct at the time of going to press. However the contents in general are subject to change and improvement. Piran Consulting Ltd. cannot accept liability for any loss or damage whatsoever arising or resulting from the use of or reliance on information or particulars in this document. Registered in England, number 8594227.