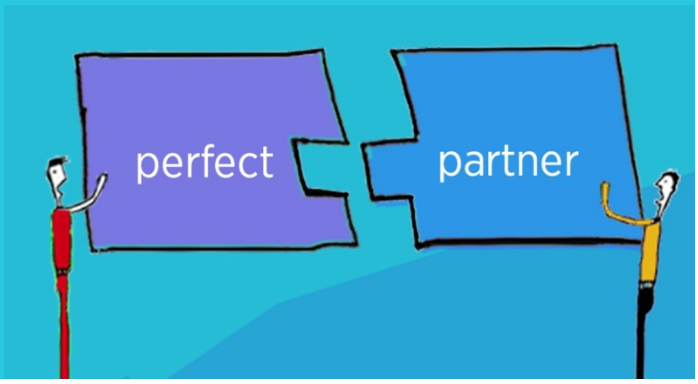
piran PARTNERS

Digital Identity:

The Commercial Opportunity



Miles Cheetham, Director

December 2013

Table of Contents

Table of Figures

1 Overview

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.

- Digital Identity 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.

So Digital Identity is 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 report explores the issues around Digital Identity and the opportunities open to organisations that are ready to develop their own part in this vital value chain.

2 Introduction

2.1 Background to the Report

This report provides an introduction to Digital Identity as a commercial opportunity. There has been a great deal of interest in creating a more trusted environment for online and mobile transactions, and this trust is acknowledged as essential for the future growth and prosperity of the digital economy.

However, while technical solutions to provide this trusted environment already exist, the long-term sustainable commercialisation of Digital Identity has remained tantalisingly out-of-reach.

This report seeks to introduce Digital Identity to a wider audience, providing an overview of the current activity in this area, the regulatory environment, the basic structure of the Identity Ecosystem and the way in which it operates. It advances a hypothesis about the nature of the propositions required and the likely value chain in a commercially sustainable business model.

How businesses can best address this market opportunity is the main subject of this report, which concludes with a series of recommendations for those seeking to develop their revenues in this area.

2.2 Report Content

In the following sections, this report explores eight key areas:

- An explanation of Digital Identity
- Digital Identity and trust frameworks
- European and US Initiatives
- The regulatory, legal and standards environment
- The importance of Digital Identity to mobile network operators
- Customer needs, use cases and propositions
- Monetising Digital Identity - value chain and business model
- Recommendations

2.3 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 could be a mobile network operator. 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

3 What is a Digital Identity?

3.1 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.

3.2 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.

3.2.1 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

4 Digital Identity in a Trust Framework

4.1 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.

4.2 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.

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

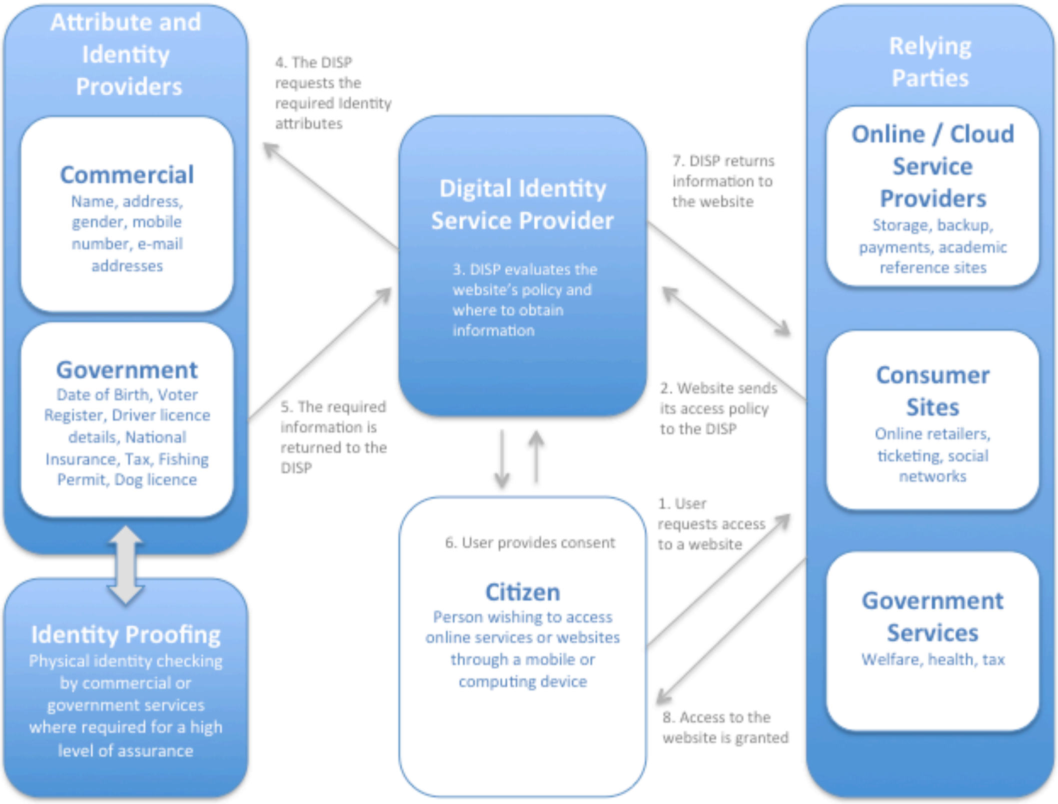
4.2.5 Relying Party (RP)

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.

4.3 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.

5 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.

5.1 European Union

5.1.1 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.

5.1.2 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

5.1.3 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/.

5.1.4 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

5.2 United States

5.2.1 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.

5.2.2 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.

6 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.

7 Importance of Digital Identity

7.1 Economic Benefit

Digital Identity Service Provision (for example by Mobile Network Operators and Banks) will play a key role in the digital economy, becoming pivotal as more and more people choose to access online services or make purchases via their smartphone. Mobile services, being highly personalised and context-aware, are increasingly assuming a central role in business and government strategy, where until relatively recently they had been considered an adjunct to online and more traditional ways to interact. Identity is at the heart of this mobile centric approach for a number of reasons which, if correctly addressed, will enhance the prospects for the digital mobile economy.

One of the main reasons that consumers cite for not buying online is a general level of concern over payment security, privacy and trust. As previously stated if this is addressed, then a more productive, innovative and competitive economy will develop that provides greater value to the consumer than ever before.

Consumers will therefore gain social and economic benefit, with significant economies, from a broader range of goods and services once the inherent lack of trust online has been overcome. Both business and state must respect the rule of law and be accountable and answerable. The macro-economic benefits can therefore be summarised as:

- Supporting the growth of online services. Digital Identity is an ideal access tool for all kinds of mobile and online services, enabling personalised or tailored service delivery, both in the public sector and commercially, such as access to government services, or personalisation of offers on retail websites.
- Improved security. A Digital Identity can deliver better accountability in transactions as it creates a bond of trust between the individual and the online service or resource.
- Economies of scale. A Digital Identity approach can reduce the cost of integration between systems (for example online services for students and resources on a university intranet). This will in turn reduce barriers to entry and will stimulate the introduction of new online services.
- Increasing administrative efficiency, reducing cost. Costly manual work or human intervention in a process can be much reduced or eradicated.

Collectively, these benefits will underpin and enable a healthy digital economy.

7.2 New Commercial Opportunities

With mobile devices increasingly the preferred consumer choice for internet access, it naturally follows that Digital Identity can be a key driver of growth for MNOs and Financial Services businesses operating mobile applications, providing a platform for trusted transactions where security is higher, administration is easier and overall costs are lower.

Importantly, this puts the Digital Identity Service Provider at the heart of the value chain. With trust so critical, the DISP can play a key role in:

- Ensuring that online service providers and retailers can be sure about the identity of the individual wanting to access the service;

- Providing certainty to the consumer that they are accessing a reputable site and that it can be trusted;
- Managing the preferences and permissions of the consumer, thereby placing them in control of their personal data and building strong trust.

7.2.1 MNO and Banking Assets Applied to Digital Identity Service Provision

MNOs are well placed to undertake a Digital Identity Service Provision role. They possess:

- Well established processes for identity checking and proofing through both their online credit-checking procedures and their retail estate (for physically checking e.g. passports, driving licences);
- A large marketplace of consumers that is attractive to Relying Parties – essential for critical mass;
- Extensive CRM capabilities and a great deal of customer insight, including the ability to identify location and behavioural characteristics (with consumer consent);
- Payment capabilities as a way to monetise commercial opportunities.

The technical capabilities required are core to their business. For MNOs in particular the SIM can be used as a secure element when key storage or encryption is required.

7.2.2 Proven Services as Entry Point for Value Creation

MNOs in Finland, Turkey and Estonia in particular have already demonstrated success with services such as Mobile Digital Signature. These services are high value-added services that are used, for example, to access government or banking services. By their very nature they include both a high level of security through strong authentication and stringent identity checking.

There is potential to extend beyond these services to include simpler login services (equivalent to Facebook Connect) and add an authentication, identity checking/proofing and attribute provision layer.

There is significant scope for value creation. For example, the Assure UK initiative has identified use-case pilots that include the reduction of fraud in ticketing solutions, and enabling tax relief on charitable donations made through digital payment mechanisms. A strong business case exists for both.

7.2.3 New Services Enabled by Value in Personal Data

Any Digital Identity Service Provider will need to make a truly compelling offer to the consumer if they are to overcome their natural inertia and opt in to a Digital Identity service. The consumer must see value – whether in terms of convenience or real money – if they are to embrace Digital Identity services. Feeling good about a donation to charity with associated tax relief may be one form of value, but consumers will want to share in the monetary value of their personal data as well. In other words, they will want to use their market power to obtain benefit.

Digital Identity services are therefore envisaged that deliver value through monetary rewards, while being convenient to use and providing the consumer with increased privacy and higher levels of security. These would be powerful tools to deliver revenue growth and protect against disintermediation.

For example, the consumer could choose to manage marketing preferences and associated permissions through a login service. They need not think of it as managing their identity – simply a better way to get easy access to the services or online retailers that they want to use. This same service could provide them with the ability to opt in to contextual or personalised offers that would have value to them.

Such services would not only provide significant value to the individual, they also open the door to very precise, context aware, personalised marketing: in effect, a whole new sales channel. It is this fundamental change which will allow the sustainable development of commercially based Digital Identity services which will support mobile commerce and will be highly valued, both by consumers and businesses.

8 Digital Identity Customer Proposition

8.1 Customer Use Cases and Needs

The starting point for designing a successful proposition is to clearly understand customer needs. For any business considering Digital Identity as a service offer it is essential to understand this both for the consumer and the Relying Party. Once these are understood, the proposition can be developed, and the value determined. So how is a Digital Identity service going to be used? What do consumers want to do?

8.1.1 Use Cases for Digital Identity

A wide range of use cases exist: the list below is indicative.

- Allow brands that I like to have access to my personal data in order to market to me (Attributes).
- Let a charity have permission to have my name and address in order to claim tax relief on my donation (Attributes).
- Allow my children to enter a children-only chat-room knowing that a strict age-restriction policy is in place (Authentication and Attributes).
- Request a student identity card that enables me to obtain discounts on products and services (Attributes).
- Prove that I am the person entitled to access chargeable services from third party providers (Authentication and Attributes).
- Login to my university network and student web portals (Authentication and Attributes).
- Login to commercial cloud services offered by providers such as Microsoft (Authentication and Attributes).
- Digitally sign a credit agreement or direct debit (Authentication and Identity Service).
- Respond to a customer survey anonymously (Identity Service).
- Prove my identity when making a formal offer to purchase property (Identity Service).
- Digitally sign a Tax declaration (Authentication and Identity Service).
- Register a business with the authorities (Identity Service).
- Prove who I am when presenting an entry ticket (Identity Service).
- Undertake a *Know Your Customer* check for financial services (Identity Service).

Services enabled by Digital Identity are now beginning to gain traction and have been deployed by a few forward-looking MNOs.

Figure 5 **Existing Mobile Network Operator Initiatives**

MNO	Service	Use Case
Dialog	Single Sign-On	Simple, convenient access to multiple online service providers, replacing multiple usernames and passwords
KDDI		
Orange	SIM-Based Authentication	Access to secure websites including paid-for subscriptions, SaaS, online banking and corporate intranet
Telenor		
TeliaSonera	Mobile Digital Signature	Provision of a legally binding proof and document authenticity for Banking, Legal Services, Government and Healthcare
Turkcell		

Source: Piran Partners

Clearly, this is only a small sample of the potentially huge range of applications for Digital Identity. Long term acceptance and success for Digital Identity must therefore take user needs into consideration above all else. Like any successful consumer service, it is critical to understand what users need, the problems that they want to solve or the opportunities they want to take advantage of.

8.1.2 Consumer Needs

For the consumer, the immediate need may simply be managing a multiplicity of user names, passwords and personal information. For most, this has reached a point where it's simply out of control, and recognised as a problem, but one to which there are only limited solutions.

However, if needs are explored in depth, it becomes clear that there is potentially value functionally, emotionally and financially. How consumer needs are met can deliver not just a solution to everyday problems, but also return some of the huge value inherent in the data back to the customer.

There are four clear needs sets.

8.1.2.1 Control and Privacy

I want to be able to:

- Prevent unauthorised use and place tight control over the use of my personal information;
- Have confidence that I can represent myself as any persona (work = professional, social = fun) while being the same underlying person;
- Have a choice of organisations that manage my identity;
- Manage my preferences concerning the type and quantity of marketing communication that I receive;
- Only reveal things about myself that I really need to.

8.1.2.2 Convenience

I want to be able to:

- Use the service easily, whoever my identity is managed by;
- Use my Digital Identity with any provider, in any community, and in any country;
- Have easier management of the login process, particularly managing multiple usernames and passwords.

8.1.2.3 Trust

I want to be able to:

- Be confident that my privacy will not be compromised, for example by companies retaining or sharing my personal data without my permission;
- Improve my online security;
- Limit the possibilities for fraud, identity theft and phishing.

8.1.2.4 Value

I want to be able to:

- Share in the value of my personal data;
- Use my personal profile to get offers that are more relevant to my interests and circumstances;
- Exercise my buying power to my benefit.

On this last need set, value, Digital Identity presents a huge commercial opportunity. If consumers can control their information on the internet, and manage their preferences, why not turn that to their advantage? Knowing who consumers are, and what they want, is commercial gold. With consumer consent this information could be used by consumers to get exactly the offers they want from the brands they like, just when they want them.

The critical point with this is that it's not about business making offers they think consumers might like, but reversing the relationship so that the consumers can exercise their power to get what they want. It's no longer about mass-market, it's about niche-markets of one or a few consumers whose needs can be efficiently met through deep insight and a one-to-one relationship. This can deliver emotional benefit alongside financial benefit.

This is the key to a compelling consumer proposition. Not only can Digital Identity solve a lot of life's annoying little problems such as remembering a plethora of passwords for different sites that we access from different devices, it can put the consumer firmly in control of the relationship that they have with the brands and services that they like. However, the user experience is key to this. Experience with mobile advertising reminds us that because of the highly personal nature of the mobile it may be easy to intrude, so any marketing must be intelligent, relevant, personal and contextual. What might the consumer say?

> *I want to get the best offers, tailored to my needs, when and where I want them. I've got great loyalty to the brands that I like, and they say a lot about me. Give me the things I want, and save me money, and I'll reward those brands with my loyalty.*
>
> *I don't want to be bombarded with things I'm not interested in, so keep them away…don't intrude and don't assume. I'll say how brands talk to me, on my terms.*

> *I know my data is valuable – and doubly so when you can talk to me direct. So give me a share in that value. I want the best discounts and rewards for my loyalty, and for letting you know who I am.*

The key to successful commercialisation is therefore meeting immediate functional needs, but delivering value to the consumer in the form of convenience, trust and financial benefit.

8.1.3 Relying Party Needs

A successful Digital Identity service must meet the requirements of the consumer described above, as well as the following high-level requirements from the Relying Party. These business needs are split into four groups - better customer relationships, business efficiency, security and simple administration.

8.1.3.1 Better Customer Relationships

My business wants to be able to:

- Easily adopt a much more secure and reliable method of identifying customers;
- Have an identity solution that fits easily with the existing proposition and customer touchpoints;
- Have an identity solution that is easy to integrate with existing infrastructure and processes;
- Know my customers much better;
- Engage in strategic activity such as the ability to identify individuals with particular characteristics;
- Derive better insight from my customer data;
- Have access to a larger overall potential market;
- Reduce barriers to the website;
- Obtain required or desired information on the user for commercial or administrative purposes;
- Obtain permission to use customer data and know the rules that the user has set;
- Obtain customer preferences on marketing activity.

8.1.3.2 Business Efficiency

My business wants to be able to:

- Reduce the cost of system integration, security and anti-fraud measures required;
- Reduce the cost to acquire and securely transact with my consumers;
- Improve my ability to manage my online or mobile business securely.

8.1.3.3 Security

My business wants to be able to:

- Trust the digital identity, with strong authentication and authorisation;
- Ensure the security and integrity of online services or resources;
- Meet the security and stringency requirements at login for access to the site.

8.1.3.4 Simple Administration

My business wants to be able to:

- Be able to create user roles and assign permissions;

- Have a solution that is easy to access and use;
- Have reporting, audit and usage tracking tools.

Many of these needs are being met already through existing solutions. The big differentiators will therefore be in the way that the Relying Party is able to improve its relationship with customers and its internal efficiencies.

In order for the Relying Party to adopt an outsourced Identity Management service there must be a compelling commercial reason – for example access to a larger market, increased revenue, easier and lower cost of integration, lower fraud and so on. Therefore, the business case must focus on cost/benefit, as below.

- The business should achieve a reduction in the cost to acquire and securely transact with its consumers.
- It should also increase revenue derived from improved sales promotion activity and cross selling based on personalised, context aware offers. This incremental revenue is achievable because of a deeper analytics capability providing better customer insight. This insight is important as a source of competitive advantage, as it allows consumer behaviour to become more predictable.
- Benefit will also arise from more effective strategic activity, such as the ability to identify individuals with particular characteristics (for example, in Higher Education) in order to establish a long-term relationship with a high customer lifetime value.

8.2 Proposition

The proposition must address the needs described above, positioned based on the benefits derived from the service features. Illustrative proposition features, based on point of view, are described below.

8.2.1 Consumer Proposition Features

For consumers the service must be:

- Easy to use, saving time and trouble;
- Improve their online security and privacy;
- Enable them to share in the value of their personal data.

Core service features, together with the benefits that the consumer would expect in a compelling proposition, are illustrated in Figure 6.

Figure 6 **Consumer Proposition Features**

Service Feature	Advantage	Benefit
Simple login	Reduce multiple usernames, passwords and PINs	Faster, easier, frictionless access to websites. No more trouble caused by lost passwords
Consent/permission management	Control over who uses personal data, how and when they use it, how long for	Trust in the way that my personal information is used by businesses and government bodies
Privacy settings	Control over the way shared data is presented	Confidence that consumers can represent themselves

	including options such as anonymous, pseudonymous or actual	as any persona (work = professional, social = fun) while being the same underlying person
Security options	Ability to meet the requirements of the website or to set additional levels of personal security	Confidence that the user is in a secure environment, or that others cannot access lower security sites: therefore more inclined to use or make transactions
Marketing preferences	Choose the brands and companies that have permission to market to you, and restrict unsolicited/unwanted marketing	Save money through personalised, relevant offers and discounts from the brands I like, helping me save money on things I want

Source: Piran Partners

8.2.2 Relying Party Proposition Features

For the Relying Party the service must:

- Reduce the overall cost to serve a customer;
- Reduce the level of risk and fraudulent activity;
- Provide a better customer experience;
- Provide access to a larger overall potential market;
- Increase customer insight;
- Increase the ability to sell into the customer base effectively;
- Enable a better relationship with the customer and therefore greater loyalty/entanglement;
- Enable new services.

A proposed set of core service features to a Relying Party are described in Figure 7 below in order to illustrate the benefits that would be expected.

Figure 7 **Relying Party Proposition Features**

Service Feature	Advantage	Benefit
Cost effective outsourced Identity Management	Focus on the core service offering with less distraction over security, data protection and integrity	Lower overall cost to serve, reduce internal costs, investment and risks, higher confidence in the quality of the data
Ease of set up	Relatively short timescale and cost implication	Fit with existing business process & infrastructure makes it easy to adopt successfully (sales, CRM)
Frictionless login	Reduced barrier to website or service visitor traffic	Increased usage, better user experience
Tailored Level of Assurance for access control	Meets the security and stringency requirements at login and for access to information within a site	Higher confidence in integrity of user ID, higher security, control over access to areas/ resources within website
Attribute request	Obtain required/desired info on user for admin/ commercial purposes	Richer data set that can facilitate better service, & knowledge of customer
Customer permission management	Obtain permission to use customer data and know the rules that the user has set	Lower risk of inadvertently mis-using customer data, clarity over the user's wishes
Customer preference management	Obtain customer preferences on marketing activity	Better understanding of the customer, improved relationship, more effective dialogue where permitted
Reporting tools	Understand performance of the solution	Ease of audit, tracking, confidence in solution

Source: Piran Partners

9 Making Money from Digital Identity

There is a clear theme that runs through every initiative described in this report - that of the fundamental trust that is required in order to develop a thriving, vibrant digital economy. Trust therefore must be at the heart of the commercial model.

Any analysis of the commercial opportunity for Digital Identity as a commercial service requires a clear understanding of the value chain, the players involved, what they contribute, and what they might expect to earn. To understand why the consumer or Relying Party might be prepared to pay for a Digital Identity service, whether directly or indirectly, it is essential to maximise the benefits underpinning the value proposition. This will derive entirely from understanding and meeting their needs.

In the eyes of consumers, however, they are so used to online services being provided (apparently) for free that a chargeable model may prove to be a barrier to mass-market adoption. The implication is therefore that in many cases (but not all) the commercial or government body using the service - the Relying Party - must be prepared to pay, because it derives value from the service.

- These needs suggest three main ways that a Digital Identity service can be successfully commercialised: however a number of ways exist in which the charging model can work.

9.1 Charging Models

9.1.1 Relying Party Pays

The Relying Party can pay for the service through a managed service fee, made up of a number of elements. This could be offered as a range of options and will include:

- Login/authentication management, in which the Digital Identity will be accepted or rejected according to pre-set requirements. The process may include chargeable services such as implicit authentication, where location or device attributes are checked, social verification is undertaken or explicit authentication is required such as a one-time-password.
- Level of Assurance. If the level is low, the inherent value is low, but if a high level is required this will attract a premium. The charge will therefore increase the greater the level of stringency and security required.
- Attributes will vary in value according to their richness and importance. For example, a simple attribute such as being aged over 18 would be worth less than a specific date of birth. They will therefore be priced accordingly.
- Analytics services could be purchased in order to gain deeper insight into the consumer data. Typically as an outsource service this is priced on a range of options ranging from a one-off hard report through to real-time analysis of transactions or consumer behaviour.
- Marketing capabilities such as mCommerce could be purchased as a value-added option.

9.1.2 Relying Party Pays on a Transactional Basis

Opting into a Digital identity service can open up a very significant new market for Relying Parties wishing to sell – effectively the service is a route to market. Using an online or mobile commerce platform consumers could have access to personalised offers based on the permissions they have granted and preferences they have stated. The greater the number of consumers using the service, the more attractive this becomes to Relying Parties. The transaction-based model where the service is monetised using a revenue-share model on every purchase is therefore attractive to online retailers and service providers. The Relying Party only pays when a transaction has taken place, so it is certain to be affordable.

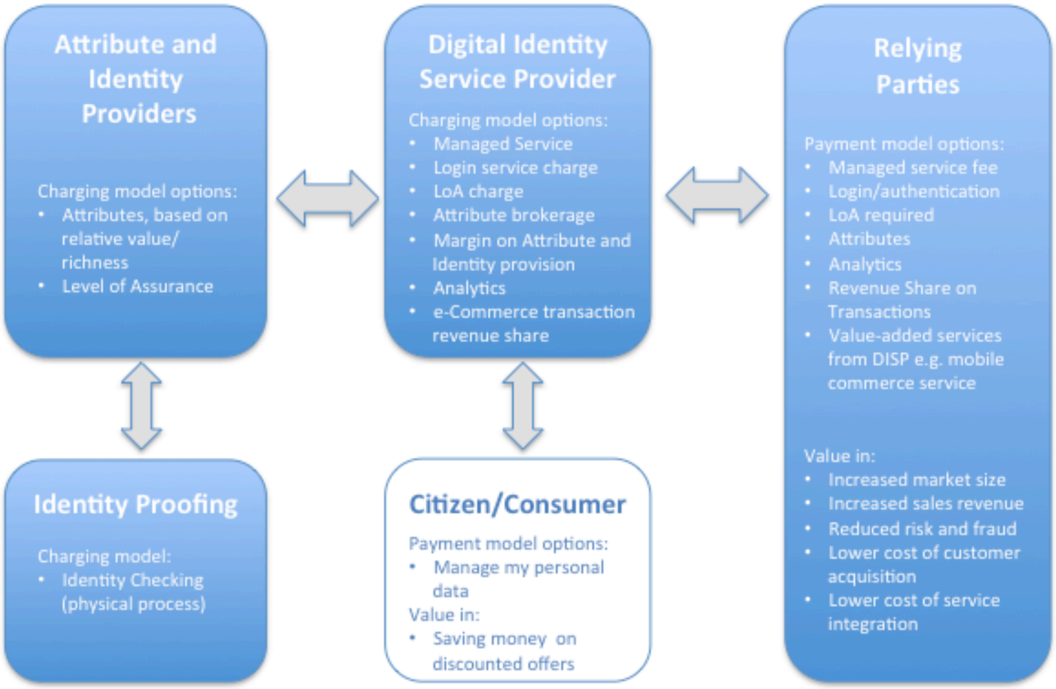
9.1.3 Consumer Pays

The consumer may, in certain circumstances, be prepared to pay for the service. As described, MNOs have seen that there is a paid-for market in services such as Mobile Signature, albeit only to relatively better-off consumers. There would have to be a strong perceived benefit to achieve mass-market take-up. This may be through access to personalised offers which would otherwise be unobtainable, as exists in the form of student identity cards today. For example, a student will pay today for an identity card that entitles the holder to discounted offers such as travel, software and even pizza because the "student" attribute has value to both those Relying Parties that want a long term relationship for future software or travel sales (a strategic approach) or those that simply want to sell more pizza on a Monday night (a tactical approach). Therefore, a relatively small outlay by the consumer can amount to considerable savings over a period.

9.2 Value Chain

Figure 8 below captures the basic value chain and the types of charging mechanism that could be applied. This is a simplified model: in practice the Relying Party may not require all the services proposed by the Digital Identity Service Provider and will use only some of these. The proposition for the DISP would therefore be modular in order to provide the market flexibility that would be needed.

Figure 8 **Illustrative Value Chain**


Attribute and Identity Providers
Charging model options:
• Attributes, based on relative value/ richness
• Level of Assurance
Digital Identity Service Provider
Charging model options:
• Managed Service
• Login service charge
• LoA charge
• Attribute brokerage
• Margin on Attribute and Identity provision
• Analytics
• e-Commerce transaction revenue share
Relying Parties
Payment model options:
• Managed service fee
• Login/authentication
• LoA required
• Attributes
• Analytics
• Revenue Share on Transactions
• Value-added services from DISP e.g. mobile commerce service
Value in:
• Increased market size
• Increased sales revenue
• Reduced risk and fraud
• Lower cost of customer acquisition
• Lower cost of service integration
Identity Proofing
Charging model:
• Identity Checking (physical process)
Citizen/Consumer
Payment model options:
• Manage my personal data
Value in:
• Saving money on discounted offers

Source: Piran Partners

The complicating factor is that there is ambiguity in the roles as noted earlier. A Relying Party could also provide Attributes – so both selling and consuming data – some of which is charged for, and some of which is paid for. These Attributes could be sold to more than one DISP or Attribute Broker in a free market, so the model illustrated is greatly simplified in order to explain the basic principles at work.

10 Recommendations

There is a clear strategic benefit to businesses such as Banks or MNOs if they are able to deliver a Digital Identity service that enables them to position themselves at a sustainable point in the value chain. Adding value through Digital Identity could allow them to:

- Maintain and strengthen their customer relationships and;
- Position themselves as trusted providers of their customers' online security and privacy.

The challenge is in developing valued, easy to adopt Digital Identity services. Initially this might be through free consumer services such as a login manager that enables consumers to take advantage of personalised marketing offers or simplified claiming of tax relief on charitable donations. Once these achieve critical market mass, Relying Parties will find the service benefits and access to the large consumer marketplace of mobile consumers attractive.

A portfolio of services could include:

- Replacement of the username and password for websites with a login solution;
- Secure login with implicit (device, location) and explicit (one-time password) authentication;
- Mobile Signature services, including fully identity-proofed services;
- Marketing preferences and permissions for online or mobile commerce (attribute brokerage).

Such services could be combined to provide a compelling Digital Identity proposition that provides sufficient consumer value that habitual usage develops in their existing customer base, before extending the service to third-party Relying Parties.

The key is trust: if the Digital Identity service is trusted then this can be extended for use within the wider world. A convenient service and a large base of users will be necessary before Relying Parties adopt it, but once critical mass is achieved they will be keen to access a large and well-understood marketplace.

11 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**

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.