Understanding Digital Identity
CONTENTS

The role of Digital Identity in the connected economy

The business perspective

The world of Digital Identity

Use cases

Developments in Digital Identity

Future trends
The role of Digital Identity in the connected economy

Within developed and emerging economies, individuals use the Internet as the main communication engine between themselves, as well as between themselves and other organizations or governments. Even though countries who are still developing have less broadband and Internet reach, mobile has already become the top environment for several key actions, with payments as a leading service.

This enables digital identity to be a strategic opportunity for the public and private sector across the globe.

Individuals and organizations moved tax paying, financial management, purchasing and formal or informal communication online. The online identity market has begun to grow through single initiatives led by large private organizations, while governments followed on R&D and regulations.

The current fragmentation has generated issues for citizens and consumers, as they struggled to manage multiple digital identities. Soft identities, easily to create and self-validated by the owner have grown, and organizations like Facebook, Twitter and Google have allowed digital users to create and access a vast array of online services that do not need to secure the real identity of a person. Currently more than 30 organizations are acting as social identity providers.

Source: www.hashdoc.com user: gigya
Online services have shown great potential to streamline and improve social security infrastructures and deliver effective and inclusive services. As governments and financial institutions became involved in providing stronger digital identities, which would allow users to perform more secure transactions, the challenge of policies, service delivery and security grew.

The benefits are easy to identify and range from fueling economic growth through improved services and ease of access, to extending government initiatives reach, improving citizen protection in the digital world and reducing public service costs.

For enterprises, digital identity in the connected economy means better customer service, deeper consumer insights and understanding, personalized service and product delivery or targeted marketing.

At the basis of digital identity, privacy and security stand in the way of mass adoption. Identity Assurance is key when it comes to distributing and using online identities, and policies, regulations and procedures need to be laid out. Soft identities and strong identities are now two different concepts, which require better positioning and regulation of service providers for each segment.
The business perspective

Digital identity is experiencing a high growth curve, being driven by consumer and enterprise requirements for secure access to digital services and products. Liberty Global and Boston Consulting Group have analyzed the depth in which the sector affects the economy and the results show that identity is not only a consumer or financial trend but also a business opportunity for existing enterprises in all sectors.

Direct monetization of Digital Identity services would account for a third of the volume with an impact of €330 billion annually to the bottom line of European organizations. The rest is part of secondary/indirect market that will generate an estimated €670 billion through its core strengths: Automation, Personalization, Delivery and Autonomy.

According to the study, the public sector and health care industry are expected to take 40% of the total market.

**Automation**
Using digital identity, users can easily mandate organizations for using the data in delivering more automated services, based on usage patterns and historical data. With potential benefits in public transport or financial transactions, automation is a key strength of streamlining business and governmental processes.

**Personalization**
High tech production lines deliver customized products, and organizations worldwide rely more on customized services for attracting and retaining customers. Using automation and data companies become more relevant to the individual customer. Having an identity that matches and records these interactions is key.

**Delivery**
Online activity generates unique footprints and traces of what users engage with. When combined with research and development in fields such as healthcare, retail or finance, these footprints generate patterns that allow organizations to improve service delivery.

**Autonomy**
Self-service is becoming key in improving citizen and customer services. Relying on digital identity organizations can allow customers to access core offerings anytime, anywhere without limitations to an operating schedule or location.

The main challenge: trust. The benefit on an individual using fewer identity providers to access most online services is the reduced effort in identity management. Becoming reliant on a single, strong and secure identity source reduces associated risks of identity theft and fraud but it also increases the potential loss an individual experiences if such cases occur.
The world of Digital Identity

Identity is a combination of self-declarations and third party assertions about an entity. The digital identity is a collection of records and attributes stored electronically that uniquely describe and identify a person or organization in the digital space.

Individuals today are used to having multiple digital identities. Currently, identity providers span across several services:

- National ID card or Passport
- Banking credentials
- Health card
- E-Commerce identities
- Social network accounts
- Email account (private and corporate)

Digital identities can be self-declared, the individual creates it and uses it as he sees fit, or validated by third parties, making an identity more secure and extending its level of trust in electronic transactions. A trusted identity is provided by a commonly recognized, trusted third party that generates, manages and validates identities through a set of security practices involving both online and offline processes.

Digital Identity definition

Source: http://www.libertyglobal.com/
Personal data is currently stored across several Internet services. The main challenge today is the management of shared data and the fragile security surrounding it – how data is distributed and managed by several soft and strong identity providers and stored on personal and workplace devices.

Social engineering is a primary component of most exploits. It consists of tactics aimed at convincing people to divulge sensitive information. Though not tightly coupled to the digital identity security, social engineering is a key component used in over 66% of hacking attempts, and a strong enabler of successful breaches. In order for social engineering to be effective, existing information is needed about the target, which is why scattered soft identities represent an easy-to-breach layer for more advanced hacking activities.

A Digital Identity holds three main components:

- **Identification / Registration**: the process that allows an entity to obtain a digital identity;
- **Authentication**: the verification process of the identity’s attributes;
- **Authorization**: the process that allows an entity to use the digital identity in electronic transactions.

Identities are characterized by assurance levels, which provide the level of trust a digital identity has with third parties. Identity Assurance is the process of using a set of verified attributes or data protected by a set of secure credentials. The main components of Identity Assurance are Identification and Authentication.

### Identification

Identification practices can be broken down in four major components.

**Self-asserted**: An entity makes a self-assertion of its own identity and no verification is performed by a third party. Online email accounts are self-asserted identities, as there is no verification performed to validate the true identity of an individual, allowing the account to be used with no restrictions or identified with other services.

**Third party**: a third party performs the verification process. A good example in this area is validating the attributes of a new requested identity (phone, address) by a telecom company.
**Direct:** the verification process of the existing identity is performed directly by the identity management provider, most common being a background check.

**Detailed direct** provides the highest level of assurance, having the new entity prove identity in person and through detailed information that includes government ID’s as well as verifications that third parties validate current identity.

### Authentication

Factor authentication is a security process, which allows an entity to validate itself by using a set of credential categories. There are three types of factors that can be used in authentication:

- **Something an individual** refers to a key, token or device that uniquely identifies the owner.
- **Something an individual knows** refers to PIN codes and passwords and is a set of data that only the owner of the identity could hold.
- **Something an individual is** usually refers to biometrics.

**One-factor authentication** is usually based on what the user knows and the most common type of one-factor authentication is the username / password combination.

**Two-factor authentication** adds something a user has or is, which generates a more secure authentication sequence. A signed digital certificate, a fingerprint, or a passcode device are examples of real world applications.

**Three-factor authentication** combines all three factors in the authentication process. The entry code can be generated by a device only the user has, and that generates the code only in the presence of a biometric such as voice, fingerprint or a retina scan.

---

Source: entrust.com
Trusted digital identities are self-asserted

Bank credentials are one of the most known and trusted digital identities today. Even though a bank identity is limited, allowing access only to financial accounts, it has the potential to grow and serve more use cases and industries.

As with most digital identities, the individual is required to provide evidence of their physical identity together with historical information that validates the identity. This can be a financial history from another bank, utility bills, telecom invoices, etc.

A simplified analysis of the identity creation process shows that historically even a trusted identity is self-assertion:

- Creating a digital identity requires a physical ID. The consideration is that the government has already verified that you are who you say you are by issuing an identity card, passport or driver license.
- The government identity is obtained by providing a birth certificate, which is the only physical document an individual has when creating the first trusted identity.
- At birth the government issues the birth certificate; it is a self-assertion of the parents to the identity of the new individual and a validation from a legal representative that is in this case the hospital or doctor that the individual does exist.
Use cases

While government services are just a part of the digital identity ecosystem, the transformation in recent years from offline to online services has been one of the key drivers in developing the policies and regulations required for the technology to take off. Security of public records and citizen records is the main concern as tax or healthcare services move towards releasing more information online.

Digital Identity has been identified as a potential game changer in all major sectors. Each of them will face different challenges in implementing and drawing value from online identities and services in the following years.

Finance shows great potential in both generating identity services as well as generating return from the technology, while Healthcare services could be positively impacted both in terms of deliverability of service and associated costs. Retail, telecommunications and media, e-commerce and entertainment are other areas where a digital identity approach could yield high benefits.

Some of the main benefits identified in using Digital Identity throughout these sectors are:

- Consumer insights
- Targeted Marketing
- Product enhancements
- Connected / intelligent devices
- Enhanced automation
- Personalization

Financial Services

Within the industry, digital identity brings a variety of opportunities. Banks especially have already established themselves as digital identity providers for their customer
base. With a careful risk analysis and enhancements, these systems can move further and become identity providers for a larger array of services, from citizen to ecommerce identity management.

Automation and self-service have a considerable impact within financial services. Leveraging the new mobile-enabled individual and the existing web infrastructure could save time and reduce cost as transactions move away from office into customer devices.

**Healthcare**

Healthcare systems today generate and store large numbers of personal information. High levels of security and good procedures for storing and sharing this data with the permission of the owner are required throughout the industry in order to further develop the technological infrastructure.

*Digital Identity is an opportunity to ease access to patient data that will drive improvements in patient care and related services.*

Access to health data by all parties, from patient to hospitals and pharmacies, will become more transactional, and just like with electronic payments, the patient will be able to validate with whom and when the information is shared. This development will allow diagnoses, medicine prescriptions or patient medical histories to be accessed easily through any array of devices.

**Public services**

The public sector holds large numbers of standardized “transactions”, most of which require an identity component. Citizen services have diversified throughout the years and providing an online component can only be achieved through a digital identity. The services impacted are tax reporting, personal information
management, policy compliance, license requests and applications for physical identity documents, address registration, fees and fine payments.

Considering the rise of population, streamlining the interaction between government and citizen becomes critical in managing costs and providing a high level of service. Citizen self-service is one of the main drivers of development for digital identity within the EU over the coming period.

Retail

Retailers have implemented several programs in which digital identity plays a key role. As the industry focuses mainly on consumer insights analysis, loyalty programs and targeted marketing, the digital identity used is many times a self-asserted version. Some large traditional retailers combine their offline and online services with basic financial services (e.g. credit cards) in order to gather additional insights.

<table>
<thead>
<tr>
<th>Ecommerce</th>
<th>Online networks</th>
<th>Entertainment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reviews, Consumer insights, recommendations</td>
<td>Service improvement, monetize consumer insights, soft identity provider</td>
<td>Personalized products/services: monetize consumer insights</td>
</tr>
</tbody>
</table>
Developments in digital identity

Within the European Union there are two sets of developments regarding digital identity at a citizen level. Belgium, Germany, Italy, Netherlands, Estonia, Malta or Spain adopted a government centric model. eID’s are issued and managed by central authorities which are also responsible for integrating public and private services into the identity scheme.

Norway and Sweden introduced a bank issued identity, known as BankID. The banking sector is in this case responsible for managing the identity infrastructure and provides scalability of service.

Estonia

Estonia has been at the forefront of digital identity for citizen services. The Estonian electronic service systems allows citizens to use one single identification for an array of services such as:

- Travel identification
- National health insurance card
- Access to bank accounts
- Public transport
- Digital signatures
- Electronic voting
- Access to medical records and taxes
- Electronic prescriptions

Belgium

The Belgium eID card has the form of a traditional identity card that also holds a chip component. Within the chip signature keys and certificates are stored for online and offline transactions and, depending on the scenario, the card requires a PIN code to be used for authentication.
BankID

More than 5 million people are using BankID for private and public services access. The initiative belongs to a number of large banks and has reached a network of 10 banking institutions that act as issuers for the digital identity.

The program allows citizens to access online services offered by government, banks and educational institutions.

MyBank

MyBank is releasing an identity service that allows individuals to identify themselves through their bank identity. The main purpose MyBank envisions is to allow consumers to verify their identity and personal details to third party organizations without sharing other real data. A few use cases envisioned are:

- Tax declaration
- Age restricted products
- Car rentals
- Residence verification
- Address for shipping
- Agreement signature

United Kingdom - GOV.UK Verify

In the United Kingdom, the development of a digital identity framework took a different form. The government is using a group of service providers to develop identity solutions. GOV.UK Verify created a unified portal for accessing public services and has delegated the identity validation and authentication processes to the supplier of choice for each individual.

There are 5 identity providers in the program: Digidentity, Experian, Mydex, the Post Office and Verizon, operating:

- Vote registration
- Patent renewal
- Student financing
- Benefits
- Civil claims
- Visas
- Claim management
- PAYE and Tax accounts
Future trends

Blockchain Identity

Blockchain technology enables a new identity paradigm. The blockchain identity service allows users to replace online accounts with a block value / identity registered in the chain. Passwords and access tokens are then replaced by a digital signature that holds a private key associated to your new digital name.

Though the concept is in its early stages, there are initiatives building up blockchain identity protocols and services. The majority of use cases are open source, but as technology begins to mature and tackle the issues and challenges surrounding it, commercially viable solutions could be launched.

Namecoin

Namecoin is a decentralized open source information registration and transfer system based on the Bitcoin cryptocurrency. Namecoin's ledger provides a blockchain system for secure name registration and usage. The company also envisions its names to be used in scenarios as file signatures, electronic voting or escrow services.

https://namecoin.info/

OpenName

The OpenName protocol is used as a distributed identity service leveraging the bitcoin ledger. As a decentralized identity & naming system residing on Bitcoin blockchain, the main use case to date is providing a simple and secure way for individuals to register with Bitcoin blockchain, and ease the transactions process.

https://opename.org

BlockchainID

Known as the World Citizenship, the blockchain is to create a simple framework and process that allows individuals to create their own digital identity. Known as a Private Passport Service, World Citizenship is used for proof-of-existence using the decentralized model and tools from blockchain technology.

http://bit.ly/1Nxl7t1
Identity of Things (IoT Identity)

Identity concepts are undergoing high challenges even before establishing themselves in the personal identity and business identity space. With the growth of wearables and IoT technology, devices are becoming "connected" and “aware” by nature. There is a rise of smart devices that know without even asking who we are, where we are and what we do. The challenge in IoT and wearables world, is how to make sure devices know each other’s identity so they can assess if information can be transferred and under what circumstances.

IoT introduced the need for identity into the physical objects space. We already have cars phones, clothes, jewelry or TV’s that are aware of their environment and our presence. Holding as much information about us as they can collect and process, there is a need to ensure these devices know and identify themselves, and understand how information should be stored, shared and accessed.

Identity of Things (IDoT) is a new research and development trend that is tackling the management of identities, of existing and future devices in an attempt to secure personal and business identities.

Technically, Identity of Things is assigning unique identifiers (UID) to attributes and data on devices. The process is fairly similar to a Digital Identity for a person. The set of attributes associated with a unique identifier creates the final identity, which is then used to exchange data over networks.

ForgeRock is a good example in the area of assigning digital identities to devices. The identity platform built by the company is directed towards matching a user’s device to a user. This enables the IoT component to assess how to use real-time data and decide contextually how to personalize or protect information.

Why it is important? As IoT develops, these devices will become more entrenched in the daily life of consumers and businesses alike. An individual has one identity, but the devices used will have different purposes. Each device needs to act as part of the owner’s identity: bracelet for payments, necklace for medical information, fridge for food ordering alone, door for access to home, etc. The ability to identify themselves against other devices, will be the market enablement for the rise of IoT.
Maxcode

Deliver your next finance or ehealth application.

Maxcode is an IT service company building tailor made applications for the European market. We focus on financial and healthcare industries. Maxcode is located in The Netherlands with offices in Romania, and the Republic of Moldova. We are a modern company and a reliable partner for our customers and employees.

Koninginnegracht 19
2514 AB Den Haag / The Hague
The Netherlands

info@maxcode.net

Disclaimer

The materials in this document may contain inaccuracies or typographical errors. Maxcode does not warrant the accuracy, reliability or completeness of the materials, advices, opinions, statements or any other information displayed or distributed in this document. All information in this document is provided “as is” and “as available”, and shall not be binding nor shall it be construed as constituting any obligation, representation or warranty on the part of Maxcode. You acknowledge that any reliance on any information in this document shall be at your sole risk. Maxcode mentions others, their products and ideas as a convenience to you. Those others, products and ideas are not under the control of Maxcode. Accordingly, Maxcode makes no representation or warranty in relation to others, their products, or ideas, other than simply listing them as relevant for your consideration. By listing them, Maxcode is not endorsing or recommending them to you.
Sources

Cover image credit: Matt Brown under c.c. 2.0 (modified).


https://www.forgerock.com/


http://blog.blockchain.com/2015/02/05/blockchain-api-profile-onename/


https://www.gov.uk/service-manual/identity-assurance


https://www.mybank.eu/mybank/documentation/