CROSSVERIFY

Identity: The New Digital Challenge

CrossVerify: The Solution

Richard Naimer | DIT Network Ltd | August 2018[1]

[1]The contents of this article is based to a large extent on the BBVA 18-01 work paper titled "Digital Identity: Current State of Affairs" written by Ana I. Segovia / Alvaro Martin Enriques.

Contents

1. Introduction

In an era when shopping, banking and even socializing are shifting online, the global economy and society are evolving very fast towards a world where interactions are mostly digital, and we can already foresee what a fully digital economy might look like. The revolution lies in the possibility for individuals to establish communications with remote computer systems which can take into account who they are in order to deliver information and services in a personalized way, in a global world that transcends national borders.

Traditionally, our identity systems have been based on physical interactions and documents. The capacity to prove that you are who you say you are is a fundamental component of economic, financial and social development and essential in accessing essential services, such as healthcare, education, finance and even justice.

The gap in time and location between buyers and sellers is the new norm. The main driver for the future efficiency and growth of online businesses is the existence of reliable and strong digital identities which allow new players and incumbents (both public and private) to operate in an efficient and secure way.

Private companies, governments and regulators are actively searching for comprehensive, cost effective and secure solutions that enable clients and citizens to identify themselves. Current systems for managing identity and data security are clearly deficient due to the fact that they are still largely based on physicality. In the financial services field, for example, most banks still require clients to appear in person, at a branch, with a physical ID card or a birth certificate to open a bank account.

Furthermore, the development of new technologies , such as the 'Internet Of Things', will lead to a massive expansion of devices - from refrigerators to shipping containers - coming online. If all of these elements start to communicate with each other, standards will be needed to establish and verify their identities.

For financial institutions, the identity issue has long played a significant role (mostly in terms of regulatory compliance and extensive back office costs). But new empowerment through identity is so powerful a disruptive force, that it threatens the viability of the traditional banking model. In this time of change it is necessary for banks to create strong and trustworthy digital identity schemes that are secure and cost efficient. Indeed, new identity paradigms are required to increase inclusion in the world's financial systems, both to expand the marketplace and to overcome social inequality which results from an inability to secure identity. The World Bank estimates that over 1.1 billion people worldwide are unable to provide sufficient identification to enable their inclusion in financial and social systems.

2. Digital Identity: Essentially Human

At its core, identity, is any set of characteristics that define a person and can be used to uniquely identify that person. Consequently, digital identity would be the digital version of a person's physical identity; in essence, the digital representation of the individual and the identity of a person must rely on the 'human factor.' Indeed, current regulation paradigms also support this idea. For instance, in Europe, the recently approved eIDAs Regulation, which provides a framework for electronic identification schemes in Europe, denies the existence of a full identity for legal entities, proclaiming instead that only natural persons are allowed to have electronic signatures. Under eIDAS, the "signatory" will always be a natural person. Hence, certificates for eSignatures may now not be issued to corporations or other legal entities. Though entity signatures are still extant, they must be based upon the characteristics of the entity's human signatories or beneficial owners.

New dimension of identity in the digital world: Unbundling identity

The way of moving an individual entity into the digital world has involved the creation of a digital representation of ourselves. But that does not necessarily mean that this representation of ourselves is always by means of our full identity. The use of new technologies has facilitated the unbundling of identity, whereby we can share selected attributes of our identity online. The new scenario allows us to combine different attributes or data in the use of identity in different contexts. And every combination of the data necessary for any given purpose is different. As such, a person can demonstrate different aspects of his personality – or even none of them – into different web-presences.

The increased data-intensity generated by individuals during the second half of the twentieth century can, supposedly, be collected and the accumulated data about an individual may in itself be sufficient to uniquely define ones identity . The digital persona could be a model of an individual's public personality based on data and maintained by transactions, which could serve as a proxy for the individual – together with an accumulation of his online presence, IP addresses, cookies, social media accounts and other inputs. In this context, a digital identity is the set of attributes that links one's entity with his online interactions. But is this sufficient?

Digital identity, veracity and level of assurance

Veracity is essential to identity. Can there even be identity without veracity?

Even if all aspects of our identity are accurate, do we always give the full picture? In some interactions, the user might not wish to reveal everything. Sometimes, people will omit nconvenient facts. At other times, they will concoct and represent outright falsehoods.

Social media interactions are replete with fake identities, causing users to doubt the veracity of

the identity of their interlocutor. But even those profiles on Facebook or Google that do not seem to be real are rarely removed. Indeed, nicknames and pseudonyms are considered breaches of the terms of service, yet they are ubiquitous throughout the major social media platforms, without consequence.

In order to have online interaction with integrity, validation of identity must be performed to verify the attributes that define that identity. As the level of assurance becomes more extensive, an even higher degree of verification is required, enabling confident high level interactions, such as in the trade sphere. In today's market, opening a bank account or filing income taxes requires real identity proof, but to friend someone on Facebook does not. This is one reason identity providers with a high level of assurance, such as governmental authorities or financial institutions, will be the leaders in the future ID market.

Identity and personal data

The set of attributes that configures identity always involves the processing of personal data. Our physical, psychological or behavioural attributes -- when registered, stored or collected -- represent the type of information that data protection and privacy regulation cover. Nevertheless, we must not confuse personal data with identity attributes.

While all the identity attributes are personal data, personal data is not always an identity attribute. For instance, one's physical address is a piece of personal data, but, as several persons can have the same physical address, this isolated datum is not an attribute of identity. Only when physical address is combined with other data points can it be considered an identity attribute. As exponential technologies grow, the amount of personal information companies own about online users is growing exponentially too.

According to IBM, 90% of all of the data in the world has been created in the last two years. Every object the individual uses, every time he transacts and everywhere he goes generates digital evidence. As more and more users depend on this overabundance of data and even extrapolation based on their own behaviour, not availing oneself of these data is rapidly becoming impossible. Indeed, users are often not even aware of the extent to which the collection and use of their data is already taking place and shaping their options.

The surge in collection and use of data causes users to lose control of their digital identity. Only when the user knows exactly when, where and to what extent such information is being collected will he be able to control his digital identity and take measures to protect it. Today, the gathering, packaging and selling of people's online data is already a huge business and the source of intense debate and controversy.

According to the Boston Consulting Group, in the European economy the applications built on the

use of digital identity can drive significant value growth for public and private institutions: At a 22% annual growth rate, the annual economic benefit is in the position of reaching €330 billion by 2020. **The sharing of personal data in a private, controlled, secure and convenient way is critical for the future of digital identity, with respect to which the user must be the owner of his personal information.**

Current Identity management approaches

The OECD defines Identity Management "as the set of rules, procedures and technical components that implement an organization's policy related to the establishment, use and exchange of digital identity information."

Traditional approaches to digital identity management have been focused mostly on the creation of static digital identities, based on cryptographic tools like digital signatures and digital certificates. Some of the problems with these technologies stem from a lack of a good integration with Internet-based services. For PC-based online access, users sometimes also need to have ad-hoc readers to use their smart card. As a result, eIDs are not always integrated into third party services as broadly as was originally intended. These are also less suitable for the increased migration to mobile services as opposed to PC services. There are also concerns about its adequacy over a long period as these technologies need to be periodically verified to remain trustworthy. This model has been adopted in the implementation of almost all national eIDs and in traditional KYC processes.

The second approach to digital identity management is dynamic verification based on an iterative process. This form of digital identity uses multiple sources (including, for instance, the user's mobile phone, his social media activity, geolocation, etc.). To support this system's assurance level, continuous assessment and monitoring is critical. These identities are usually self-asserted, because it is the individual who communicates his attributes, and therefore the level of assurance is low. Nevertheless, the user experience is more satisfactory, due to reduced difficulty during the on-boarding process. However, the system is less efficient for the service provider, as these identities are self-asserted. This is the verification approach of Facebook Connect.

In the financial services field, however, it is unlikely that this approach would succeed to meet the strict KYC and anti-money laundering (AML) requirements. Current trends are heading towards a mixture of these approaches: using both static and dynamic factors.

Presently, identity systems tend to establish a single identity for each individual based on some or all of the following elements:

- What the individual knows (password, PIN, security code)
- What the individual has (identity card, bank card)

- What the individual looks like or how he behaves (biometrics spanning physical/behavioural features)
- Where the individual is located (mobile number, geo-location, IP address, social network site)

As a result of the poor user experience associated with the use of passwords, some companies, such as financial institutions, have been migrating to new digital identification systems that meet both the objectives of ensuring secure identity and improving user experience. Behavioural biometrics technology, for instance, is able to learn patterns in user behaviour in order to build an identification model. The software analyses the way users interact with the different devices (phone, PC, tablets), how they hold the mouse, how they make keystrokes, how quickly they move, the pressure with which they hold the phone, etc. Over time, these biometrics are interpolated through algorithms and are able to define a unique pattern for each user in order to determine his or her identity in a certain way. One element that differentiates this technology from static biometrics in verifying identity is that the data are collected passively and the collection does not interrupt user activity, a key element of user experience.

3. Identity Providers

The key issue to operating with our digital identity is the validity that others give to the veracity of the attributes of our digital identity. A digital identity needs a verifying and attesting provider, but, as of yet, there are no globally-accepted identity providers. ISO standards for identity management state that a digital identity authority is the entity in whose domain a particular digital identity is valid. The identity authority and identity provider sometimes rely on the same entity. Several attempts have been made to create a universal identity provider (including projects like OpenID, which seeks to offer a universal digital identity accessible across all platforms), but, to date, all have experienced problems in implementation.

Which are the main digital identity providers?

Public Sector: Traditionally, in the physical world, governments have been the main providers of identity verification. Official documents, such as passports or ID cards, managed by public authorities have constituted a legally validated way to prove that these credentials correspond uniquely to a single individual. The passport has for eons stood as proof that a person has fulfilled identity requirements for purpose of traveling and entering other countries.

National eIDs are usually issued in order to provide access to government services. The notion of a public ID card issued and valid for the analogical and digital spaces has already started for millions of people. In some countries, citizens and public and private organizations are starting to experience the benefits.

The European Union is also trying to provide a framework to enable mutual recognition of identity systems for EU Member States. The aim of a global digital identity is to reach even higher levels of efficiency in the virtual world: to have a valid digital ID that allows citizens to participate in several domains.

At a global level, by early 2017, 82% of all countries issuing national ID cards had rolled out eID programs, according to the World Bank. Most developing countries have some form of digital ID scheme tied to specific functions and serving a subset of the population, but only a few have a multipurpose scheme that covers the entire population. Eighteen percent of developing countries have a scheme that is used for identification purposes only; 55% have digital IDs that are used for specific functions and services like voting, cash transfers, and healthcare. Only 3% have foundational ID schemes that can be used to access a collection of online and offline services. Twenty-four percent of developing countries have no digital ID system whatsoever. Only a small fraction of those that do have digital ID programs incorporate a biometric element as part of the digital ID that is used to access the service on an ongoing basis.

Private sector: Private sector firms need to verify the attributes of the customer in order to facilitate commerce and transactions. The private identity provider transforms individuals into users of their systems by creation of credentials (e.g. an online banking user). Often they require the client to present physical documents that prove his identity in order to incorporate the data into the new identity.

Federated identity: While some identity providers manage isolated and centralized identity systems, the rapid emergence of services that require identity validation, necessitate identity provider systems that can administer identities and credentials for multiple service providers. These are the so-called 'federated identity' systems. According to Gartner, federated identity management enables identity information to be developed and shared among several entities and across trust domains. Tools and standards permit identity attributes to be transferred from one trusted identifying and authenticating entity to another for authentication, authorization and other purposes. This provides "single sign-on" convenience and efficiencies to identified individuals, identity providers and relying parties.

A classic example of federated identity is the use of government issued IDs for various private services. Public and private sector firms have a mutual interest in developing digital identity systems that allow the identification and authentication of users for different functions and services. Moreover, both public and private incumbents may rely on each other to build and manage identity schemes as complete as possible. Collaboration models can be different depending on the type of the project and the scope of private sector involvement. At times, private providers may act proactively to use public IDs. In other instances, public authorities ask the service provider to rely on their own ID.

Occasionally, collaboration is set by a service agreement, in which a private firm plays a particular role in one or more steps of the digital identity process. In other cases, the private sector is primarily in charge of the design, construction and management of a project, usually for an agreed-upon concession period. In federated identity systems, a third party or identity intermediary usually manages the identification process. The identity data are transferred between different systems, and service providers and users can operate with the same credentials in different transactions with different service providers. In this scheme, service providers could be e-commerce, banks or e-government web applications and identity providers could be government entities or private providers. In some European countries -- Estonia, Finland, Norway, Switzerland and the United Kingdom, for example -- the private sector, particularly the mobile industry, has played a key role in building national digital identity systems and authentication programs.

One example of this federated identity in financial services is BankID32 , a solution developed in Sweden by a number of large banks that can be used by both the public and private sectors. The BankID network includes Danske Bank, ICA Banken, Ikano Bank, Länsförsäkringar Bank, Nordea, SEB, Skandiabanken, Sparbanken Syd, Svenska Handelsbanken, Swedbank and Ålandsbanken. Seven and a half million people use BankID on a regular basis for a wide variety of private and public services. In Sweden, 80% of the adult population has a digital identity and through the use of BankID32, an individual can easily open a bank account, and the financial institution can be assured that the customer's identity has been verified according to anti-money laundering (AML) standards.

Estonia has one of the world's most highly-developed national ID card programs. Estonians can arrange municipal or state services online in minutes. Since 2002, about 1.2 million credit-card sized personal identification documents have been issued that allow citizens to be identified and sign documents. The system is based on two main principles: a national register (called the Population Database), which provides a single unique identifier for all citizens and residents; and identity cards that provide legally binding identity assurance and enable electronic signing.

ID-cards are mandatory for Estonian citizens and they are valid both for digital and physical identification. The digital functionality of the ID-card is based on an electronic chip and the two PIN codes supplied with the card. By using a smart card reader and a computer connected to the internet, citizens can use the two core functionalities provided by the ID card, both of which are essential to the development of e-government. They are personal authentication (related to PIN 1) and digital signature (related to PIN 2). In order to ensure safe communication between public databases and institutions that use different management systems and technologies, Estonia has developed the X-Road, a secure internet–based data exchange layer that enables different information systems to communicate and exchange data with one another.

In the X-Road environment, encrypted data are directly transferred through secure servers from one information system to another. Data does not pass through the X-Road command center and cannot be viewed there. The command center only has statistical information about data transfer.

4. Identity Drivers

Trends that are driving the need for digital identity systems

With customer interactions expanding to physical, online, social and mobile channels, firms are driven to develop new capabilities that will enable continuous, safe and robust identity recognition over time, and across different countries and industries. The main drivers that we identify behind the investment in and development of digital identity systems comprise new user behavior and rising customer expectations. Customers expect seamless, 24/7 omni-channel service delivery and they are ready to change quickly to services that offer the best customer experience. But in contrast, and especially as result of the recent massive data breached such as those experienced by Equifax, Yahoo, Uber and a long list of others, users are highly cautious about sharing personal data.

Users neither understand why organizations require all the information they seek, nor what is done with that information once it is gathered. For transactional purposes, mobile is becoming the dominant channel for Internet usage, so companies have been forced to offer identity validation via apps, as clients frequently do not wish to go to the physical store or even use PCs. In financial services, banks have been using multilayered authentication for years via username and password schemes.

Due to PINs and security codes being so easily forgotten, up to 30 percent of all support requests to call centers are password reset requests. Consumers are not happy with cumbersome and difficult to recall passwords. They certainly prefer to reuse a single digital identity instead of constantly changing their credentials. This is why companies are investing resources to find new convenient ways for customers to access their services, particularly using behavioral biometrics as a replacement for passwords on mobile devices. Need for Trust Digital identity is a way for an individual or a business to prove who they are online with a certain level of trust. The more reliable a digital identity, the more complex online transactions the user will be able to effect.

Proper Identity management in the analogue world helps to address risks derived from human interactions and increases trust between the parties. This is crucial for economic and social development. If we translate proper identity management to the online world, a lack of a connection between a physical person and a digital identity will create additional uncertainties that do not exist offline. Safe digital identity management is essential to the security of the entity that validates access to its informational resources. Confidence is fundamental for the security of the individual who accesses these resources, particularly when he is an owner (e.g. money in a bank, a medical record). The impact of the lack of trust on an internet businesses is very high. As a result of a lack of confidence, many consumers may hesitate to make online transactions. It is reported that, after a security breach, up to 12% of loyal customers stop shopping at a compromised retailer, and 36% keep shopping at the retailer, but not as frequently.

For those who continue to shop physically at the compromised vendor, 79% are more likely to pay in cash instead of using credit cards. The same studies state that shoppers who use cash statistically spend less money after these events. Indeed, 26% say they will knowingly spend less than before. As a consequence, companies are forced to design and operate identity systems that are both robust enough to protect data from being stolen by third parties for fraud purposes, and simple enough so as not to affect user experience[1].

Increased concerns on privacy

In every project related to the implementation and management of an identification system, issues about privacy and personal data protection quickly become a focal point. The privacy principle involves the idea that the data subject must decide how, where and by whom that information is used. Use of personal information comprises initial collection and all subsequent uses. Accurate data protection and respect for consumers' privacy are fundamental for transactional purposes. If consumers do not feel that their data are protected, they will not transact online. A recent global survey shows that, in countries with a significant history of online fraud, 69% of consumers expressed that they are 'much more concerned' about their online security than they were just a year ago. This affected their online behavior, with 51% less likely to do financial transactions online, and 47% making fewer online purchases.

Cost Efficiencies

Digital identity systems are cheaper to run than physical ones. For organizations that need to verify customers' identities with a high level of assurance, it is much cheaper to use a digital identity already validated by a trusted third party than to have to constantly gather and check the customers' IDs or driver's licenses. Deloitte has studied large retail banks and concluded that, by streamlining processes and adding technology to eliminate paper, operating expenses can be reduced by as much as 25% (a reduction of between 60% and 70% of records management associated costs). For governments, an analysis by the Boston Consulting Group shows that the efficiencies of digital identity systems could yield global taxpayer savings of up to $50 billion per year by 2020.

The rise of exponential technology

The current available solutions for balancing the need for veracity, security and seamless user experience are insufficient. Fortunately, new technologies are emerging, improving the ability, speed and efficiency of the identity management systems, allowing companies to eliminate unnecessary processes and paperwork, extensive human resource efficiencies and improving the customer experience. Some of the most relevant are:

- Biometrics improve the ability to validate, with a high level of certainty, a client's identity, allowing for automated onboarding and remote access to services. There is a range of biometric solutions

[1] https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_9/Accenture-Future-Identity-Banking.pdf

available at increasingly affordable prices. This technology enables automated recognition of users based on their physical (facial, fingerprints, voice, veins, iris) and/or behavioral characteristics (keystroke and signature recognition). Valued at US$5 billion in 2010, the global biometrics market is growing at a CAGR of 18.5%, and was predicted to reach US$17 billion by the end of 2017. According to Deloitte there will are one billion smartphones with fingerprint readers in use as of the end of 2017. By 2018, iris and face recognition started to rival fingerprints.

- Distributed ledger technology, or blockchain, could be used to centralize identity attributes storage and sharing among different firms. This system could allow the sharing of some sensitive individual data (the ones the user chooses) across several entities without compromising private information. Blockchain technologies can provide a solution to many digital identity concerns, as they can be uniquely authenticated in an immutable and safe ledger. Blockchain authentication is based on identity verification, using digital signatures based on public key cryptography. With this technology, the only verification performed is whether or not the transaction was signed by the correct private key. We can rely that the person who has access to that private key is the owner. The owner's identity is not relevant. "An innovative development in the world of customer on-boarding in financial institutions is the use of blockchain technology to build Know Your Customer (KYC) utilities. A KYC utility provides a centralized location where client identification and verification can be performed once per person, rather than several times by different organizations for the same customer[2]."

The combination of both – elements of biometrics and blockchain – is the way to create the ideal Digital Identity utility, serving the needs of the customers and service providers in a highly secure and cost-efficient fashion.

5. CrossVerify – designed and built to meet the Digital Identity Challenge

The DIT Network, Ltd. has created CrossVerify, a blockchain based identity bank which can securely store digital ID's, together with verified KYC and biometric data, as well as perform ongoing AML checks. CrossVerify provides veracity, simplicity, accessibility, security and user experience – satisfying everything required for effective digital identification solutions in a way suited for our enhanced digital era. Plus, these metrics are achieved without the necessity of any codes, pin numbers and is platform agnostic.

How it works

CrossVerify is a technological solution and system which together form the ultimate solution of Digital ID storage, KYC, AML and verification:

[2] PWC. The future of onboarding. Retrieved from https://www.pwc.com/gx/en/financial-services/pdf/pwc-the-future-ofonboarding.pdf

Step 1. Network. The Network access points are made up of Trusted Parties which, by regulatory authority or by accepted market integrity, can be trusted to verify the authenticity of the data introduced to the Network. Such as: Government agencies, Banks and Notaries Public. The accreditation of the Trusted Party is determined by the ultimate application provider until ultimately dictated by the regulator. The User physically presents himself to a network Trusted Party for the verification of ID and upload process.

Step 2. Digital ID data. The data which compose the digital identity can vary, but at a minimum, will include the following: Government picture ID; Current Utility bill; Upload of biometric data, in the presence of the Trusted Party via the Cross Verify software system only; Tax ID number. Additional KYC documents and data can be added if required, including additional ID's, certification, accredited investor status. Eventually, this can included medical history and other documentation of value.

Step 3. Digital ID Upload. Digital Identities are uploaded to the Cross Verify Corda-based blockchain, in a procedure to be strictly followed by all Network members. Such procedures include, but are not limited to verification of authenticity and validity of government issued ID, verification of authenticity and validity of current utility bill, and oversight of the biometric data capture and upload in the presence of the Trusted Party ensuring that the biometrics uploaded are in fact those of the person holding the government issued ID.

Step 4. AML check of the Digital ID. The verified uploaded identity is checked against all currently available Anti-Money Laundering (AML) lists, including: Counter Financing of Terrorism (CFT), Anti-Fraud and Financial Crimes (AFF), Office of Foreign Assets Control (OFAC), Bank Secrecy Act (BSA), USA PATRIOT Act and the FACT Act, World-Check. Such checks are conducted automatically on a periodical basis to ensure that identities previously entered into the Network but subsequently blacklisted are weeded out of the Network.

Step 5. Access to the uploaded Digital ID. Access to digital ID is only possible with the use of a 'hash'. A Hash can only be generated by the owner of the biometric, by applying his biometric, identical to the biometric uploaded when creating the digital ID. Once admitted to the Network, the digital identity can be used for various applications – for example: Accessing a bank account, obtaining and accessing a digital wallet, accessing trading and other applications and accessing a private network.

The user can also allow, at his discretion, access to his KYC information, in whole or in part for the purpose of enabling a financial institution to open an account on his behalf. As the KYC information is Trusted Party ensured and AML verified, such account openings can be done immediately without the bank having to conduct its own separate duplicate KYC. Similarly, the User could allow other providers access to different identity attributes. For example, if the User only permits confirmation that he is a verified and compliant User, in most cases this would suffice to confirm the authenticity of a social media account, or authenticity of User credentials to online vendors to avoid or limit fraud and charge backs.

Digital ID Management Over Blockchain

Management of the Digital ID via blockchain presents many advantages over currently available digital ID mediums:

- Maintaining the Digital ID on a blockchain renders it unhackable – the entire network would need to be hacked in order to alter/delete data, making it far safer than current data base modalities;
- A User's identity is not known to anyone other than the Trusted Party, unless specifically allowed by the User;
- Access to data is available only to the holder of the hash – and the hash is obtainable only from the biometric identity owner;
- A full audit trail is available, back to the verifying Trusted Party;
- Application providers can tag an identity as flawed and immediately halt exposure to all other network participants;
- An additional benefit of tokenization of the Digital ID process is the limiting of spamming and phishing schemes, as the User credentials and contact details remain at all time secured, unless the User specifically allows otherwise. This in turn will enhance the User experience and trust in the CrossVerify methodology.

Incorporation of the User biometrics as part of the Digital ID

Incorporation of the User biometrics as part of the Digital ID presents two strategic advantages over current forms of Digital IDs. First it eliminates dependency on pin codes, dongles and access keys which hinder user experience. Second, the use of biometric keys for each system access or interaction guarantees that the use of the ultimate application is affected by the specific identical User for which the KYC and AML clearance has been obtained, as opposed to current banking systems whereby the bank does extensive KYC on the owner, who may grant the access pin codes to be used by an unknown unverified third party. In fact, it could be said that any AML/KYC methodology which does not incorporate biometric validation of the User prior to any interaction, is inherently flawed and easily susceptible to manipulation.

Extensive CrossVerify Use Case Possibilities

CrossVerify is a highly efficient and cost-efficient solution for Digital ID verification and access control. Aside from the obvious use cases for national ID systems, the following are diverse use cases in which CrossVerify can be particularly efficient, some of which are in the process of implementation:

Compliant Digital Currency. CrossVerify has been coupled together with an equivalent of Bitcoin,

to create the AML Bitcoin (ABTC). The inclusion of the CrossVerify system in the infrastructure of the ABTC has created the world's only digital currency compliant with AML and KYC requirements of the world's banking systems. Consequently, ABTC is the only digital current that can be used and accepted by regulated authorities.

Humanitarian Aid. It is a sad fact that only a fraction of the humanitarian aid actually reaches the intended recipients. If the eligible recipients were certified biometrically via CrossVerify the percentage of aid reaching those truly in need would be increased exponentially. For example, if each person in a disaster-stricken area eligible to receive a bowl of rice 3 times a day were entered onto CrossVerify, contractors and support agencies could then be paid the allocated fee based upon the number of times the eligible person biometrically confirms receipt of the bowl of rice.

Pension Payout. It is estimated that over one billion dollars are wasted each year through error or fraud in pensions, including massive payments incorrectly paid to deceased persons. Using CrossVerify and requiring every recipient to confirm his biometric once a month would eliminate virtually the entire amount currently wasted.

Medical Insurance and Medical Records. US veterans are eligible to free healthcare services anywhere within the US. If a veteran residing in LA takes a trip to Hawaii and needs emergency medical care, the system is almost guaranteed to deny or delay treatment because of an inability to access his medical records or to confirm his identity. If the veteran had a CrossVerify Digital ID and his medical records were uploaded as part of his personal documentation, treatment would be immediately forthcoming.

6. The role of banks in digital identity

The OECD has predicted a growth in the demand for digital identity management solutions and envisaged a substantial increase in consumer demand for privacy and protection from identity fraud. The financial sector possesses an enormous amount of personal data due to the nature of its core business. This wealth of data will mean a world of possibilities. So far, the sector is just scratching the surface of what can be achieved with digital identity. Given the highly competitive environment and constant need for both security and cost efficiency, and especially considering the erosion of services traditionally provided by banks, the banking industry is perfectly suited to lead the trend market.

- Banks have a long experience in validating identities. Initially in the physical world, and now in the digital one, as holders of digital accounts, banks have had to create secure processes to verify customer identity. Now they will be able to seamlessly migrate their knowledge to other industries, especially in terms of on-boarding individuals, assets, and institutions onto digital systems. They are well positioned to act as identity intermediaries.

- Financial institutions are typically highly trusted by consumers. As the key issue in digital identity management is trust, the higher the level of assurance providers have, the higher is the level of the transactions they are allowed to perform. Other than official government offices, private sector banks are viewed as most reliable.
- Banks, existing in the highly regulated financial sector, are used to dealing with compliance standards and can offer other industries their expertise in identity-based networks. Regulation increasingly requires banks to perform due diligence on their customers in an effort to identify money laundering. Complying with these regulations requires major investment of financial and human resources for banks.
- Regulation favors the entrance of banks into the digital identity management business. In Europe, the Second Payment Services Directive (PSD2) requires banks to provide access to account data to third parties that may be potential competitors. It also creates a chance for banks to leverage their relations with their clients by offering Strong Customer Authentication (SCA) to third-party providers above and beyond what is required by regulation. By doing so, banks would accomplish two things: create a market for value-added services on top of the basic services required by PSD2 and strengthen the relations with the end-customer using the strong eID from the bank to access other services. This could also be used as part of an attractive value proposition to corporate customers of the bank.

7. The bank as a digital identity provider. Use Cases

Banks and public institutions worldwide are starting to develop new and secure ways for individuals to prove their identity. As demonstrated, there is a clear advantage to all parties – user/institution/private sector/governments - in the creation of a system whereby Users identify themselves once via a trusted party rather than having to share sensitive data with numerous third parties. Examples of such efforts include:

- In the UK, GOV.UK was launched by the Government Digital Service in May 2016. GOV.UK Verify is a building block in the transformation of UK public services that was created to use government services online. The tool (via API or web) allows users to select and register with an identity provider, and then use their 'assured' identity to access digital services. Users are allowed to choose between multiple identity providers that then perform several background checks to verify that the person is who they say they are. These checks, depending on the level of assurance the service requires, could include counter-fraud checks and activity history. An individual accessing a government service, such as a Self Assessment tax return, will need to verify their identity from a panel of certified companies. Barclays, is certified by GOV.UK to verify identities. When the user chooses Barclays, he is transferred to the Barclays Identity Service where his identity can be verified. Once the identity check is complete, the user will be returned to the government service. The user does not have to be a Barclays' client to register for an identity profile, but if he is, he can use information from its online banking service to accelerate the process.

- Canada offers another example of banks entering the eID business. In 2012 the Canadian government launched a digital identity project called SecureKey. In a similar model to the UK, leading financial institutions (National Bank, Scotia Bank, Tangerine) manage the identification process for government services by means of a network called Secure Key Concierge. The system is storing the credentials of seven million Canadian consumers and adds 250,000 new consumers each month. They are now considering using blockchain technology to manage digital identities.
- In the United States, BBVA Compass partnered with Dwolla, a payments provider, to develop an authentication process (FiSync) where customers use their same BBVA username and password to sign on at Dwolla without providing sensitive information. USAA is also using the firm's identity-as-a-service product, ID.me, to verify identity by remotely checking government issued identity documents. By using ID.me's Identity Gateway service users can link their official identity to a digital login which is accepted across different webs (such as the State of Maine or the Department of Veterans Affairs), without the need to create a new login or to prove identity at each site directly.
- In Germany, Deutsche Bank is promoting an alliance with several firms in order to create a global digital identity in Germany. They are attempting to create a single sign-on digital identity valid across different banking and other services platforms. The project is scheduled to be launched as early as 2018.

8. Challenges

The most obvious concerns when addressing Digital ID systems are those of security, integrity and standardization of the entered information entered, retrieval mechanisms and securing the User control and selectiveness of the accessible data. As detailed above, the CrossVerify system, with its foundation on a blockchain platform and its reliance on biometric verification, has been designed and built to satisfy these concerns. Nevertheless, there are larger issues which would need to be addressed in order to enable the swift adoption and implementation of such central Digital ID systems:

Regulatory uncertainty. Current regulation in the financial services industry places a high burden upon the institutions in order to meet their KYC and AML standards. That burden effectively bars most financial institutions from relying on KYC and AML performed by another institution. In order to reap the cost efficiently benefits of the Digital ID system and enable financial institutions to significantly downsize their KYC and AML departments, standardization would need to be introduced whereby one institution could rely on KYC and AML performed by another. Once that is achieved, resources can be shifted from compliance at opening of accounts to the vital monitoring of suspicious activities by operating accounts.

Liability. Even the best designed systems have vulnerabilities that create liabilities. These potential liabilities can be mitigated through transparency, risk allocation and insurance. Other liabilities will have solultions that could include legal or contractual liability and obligation.

9. Conclusion

The economy and society are moving very fast towards a world where interactions are mostly digital. At a global level, identification is a fundamental enabler of economic and political development. Identity has become a key issue for the global economy. The OECD has predicted significant growth in the demand for digital identity management solutions and envisaged a dramatic increase in consumer demand for privacy and protection from identity fraud. In the new digital environment, it is essential to be able to rely on efficient access, storage and sharing of critical data in a secured and private way.

The evolution of a digital economy requires simple, efficient and secure identity systems which can be used in different domains and platforms that require different levels of assurance. Individuals and companies need identity solutions which are valid across services, markets, standards and technologies. New technologies such blockchain and biometrics have engendered the creation of CrossVerify which uniquely delivers identity solutions that meet both the objectives of ensuring secure identity and improving user experience.

Financial institutions, under current regulations, see themselves as relying on parties in a federated system rather than as identity providers using the information already gathered by other firms. It would be much simpler and cheaper for them to interact and on-board Users if they could get fast access to a token or digital certificate that verifies the User's identity.

CrossVerify has succeeded in achieving the required the design and creation of the building blocks of such an integrated Digital ID solution. What is required is to begin the implementation of such solutions and cooperation between governments, financial institutions, Users and market participants to implement the system and reap its benefits.

Given their background in the identity figment and their high regard within the marketplace, it is expected that banks and financial institutions will lead the way towards the implementation of unified Digital ID systems.

DIT Network

23 Austin Friars, London, EC2N 2QP, UK

hello@dit.network | www.dit.network