The development of digital identity in the Financial Service Industry: From an element that enables digital transactions to a new strategic asset for business

Received (in revised form): 24th May, 2021

Michele Guido Mario Lavizzari
Chief International Development Officer, InfoCert, Italy

Michele Guido Mario Lavizzari, Chief International Development Officer, InfoCert, is Senior Executive Manager with considerable experience within the ICT industry. He is in charge of InfoCert's business expansion across EU and LATAM markets. In addition to his technical and commercial background, he has strong financial and managerial skills, developed on the job in an international multicultural environment over the years and by attending multiple training courses, most of which were held at the Ashridge Management College of Berkhamsted.

InfoCert, Via Carlo Bo, 11 20143 Milan, Italy
Mob: +39 345 3467429; E-mail: michele.lavizzari@infocert.it

Marco Di Luzio
Chief Marketing Officer, Tinexta Cyber, Italy

Marco Di Luzio is Chief Marketing Officer for Tinexta Cyber. He oversees the marketing unit in Tinexta Cyber, Tinexta S.p.A. BU, operating in the cybersecurity market. His mission is to position Tinexta Cyber as the leading company in the field of cybersecurity solutions for large enterprise markets and define the value proposition for vertical segments. Marco is in charge of developing the coordination for all marketing activities at the group level, managing communications and event and media planning for the domestic and international markets. He is responsible for the products evolution road map and new business development.

Tinexta Cyber, Piazza Sallustio, 9 00187 Rome, Italy
Mob: +39 3356373490; E-mail: marco.diluzio@tinextacyber.it

Claudio Tommasino
Digital Communication Specialist, InfoCert, Italy

Claudio Tommasino is Digital Communication Specialist at InfoCert. In his role he supports InfoCert's marketing and communication department with the aim of positioning the InfoCert brand as a European leader in digital trust services. He is in charge of the management of the company's social channels and digital communication activities, including content creation and digital ADV.

InfoCert, Via Marco e Marcelliano, 45 00147, Italy
Mob: +39 3407240043; E-mail: claudio.tommasino@infocert.it

Abstract This paper aims to illustrate how digital identity has become an important element of business transformation in the financial sector and how digital identity is evolving from an asset to support business in a new revenue stream. In an increasingly digitised world, the trusted digital identity assumes the important role of enabling the legal

validity of any type of digital transaction. This centrality has attracted huge investments by companies to make the onboarding of online customers and the release of digital credentials to their customer base increasingly effective and frictionless, while preserving compliance and user experience. We illustrate the main models adopted in the current context in which a progressive transfer is taking place from identification processes helped by specialised staff to completely unattended processes. Finally, we show how the digital identity evolution is moving to a new paradigm that will revolutionise the approach to digital identity management. Thanks to the development of Blockchain technologies, digital identity is evolving even further. In the self-sovereign identity (SSI) vision, digital identities will no longer be merely an element to support commercial transactions but a new strategic asset to leverage in order to generate new business. This new paradigm will offer a new business opportunity to banks that will allow them to capitalise their information assets securely in full compliance with the privacy protection regulations, General Data Protection Regulation (GDPR). In the new SSI paradigm, digital identity management of the customer base represents the asset around which financial institutions must leverage to create new value, develop new business models and generate new revenue streams.

KEYWORDS: Digital identity, digital trust services, self-sovereign identity, digital onboarding

INTRODUCTION

COVID-19 is catapulting the entire economy several years ahead in its evolution towards digital transformation. From banking to supply chain management, industries everywhere are accelerating the digitisation of their processes.

This trend promises to advance further, thanks to the proactive actions of governments. Consider, for example, the European case and the Next Generation EU. The EU recovery plan has budgeted €10.6bn[1] to foster the growth of the single market, innovation and digital. In a framework where we are observing the exponential growth of digital transactions, it is necessary to respond with increasingly innovative solutions to ensure their security and validity. One of the most important elements to leverage in this context is digital identity and digital identity management. Trustworthy digital identity solutions make it possible to streamline onboarding procedures and improve the security and efficiencies of digital transactions.

Digital identity is crucial to ensuring that all types of digital transactions are legally valid. Being certain of the identity of the counterparty, be it a person, subject or legal party, lies at the heart of all legal dealings, both in the real world and in the world of computers. In order to legally validate a digital transaction, the *digital identity* has to be *trusted*; that is, it should be checked by obtaining *proof of identity* using *qualified trust service providers,* specialised companies that are certified in accordance with European regulation eIDAS 910/2014. Thanks to the digital trust services, the digital identity becomes *non-repudiable and enforceable against third parties* with full legal validity. Anyone who wishes to disown their own identity certified by such companies is now subject to a reversal of the burden of proof, that is the obligation to produce the proof in the appropriate legal settings.

DIGITAL IDENTITY CENTRICITY

Nowadays, the digital identity market is very fragmented: there many players who recognise a business opportunity in digital identity management and many countries

that are working on their own identity schemas. This fragmentation generates interoperability issues. For this reason, start-ups are founded to operate as brokers of verified credentials, to allow 'communication' between all types of identity.

Furthermore, at the European level, projects are being started to make the digital identity schemas of the various governments interoperable. One of them is *First Italian Cross Border eIDAS Services* Project (FICES).[2] The FICES project is based on strategic partnerships between banks, payment service providers, certification authorities, insurance companies and other relevant stakeholders, with the aim of creating an identity *cross-border* interoperability for EU citizens.

These projects demonstrate that we will move towards consolidation and convergence on established technology and process standards, simplifying the emerging market around digital identity. Moreover, a consolidation of the market could also be an evolution for the users that will have the biggest and strongest providers, ensuring a frictionless experience in the use of their eID credential cross-border and a durable management of their e-identity credential.

Digital identity centricity in digital transactions has long attracted huge investments, resulting in a more rapid development of new approaches in the wake of increasingly sophisticated, high-performance technologies.

This need is becoming increasingly relevant since other core activities in the banking business have recently been losing value. It is enough to consider that many new players (PISP — payment initiation service providers) are starting to manage payments thanks to the new regulations (PSD2) or that new parties are starting to manage banking transactions by introducing new peer-to-peer transfer models.

Similarly, back office work is being outsourced in order to reduce costs and raise efficiency of the processes. Therefore, what is the core asset left to banks? They know their customers, and this differentiates them from FinTech, allowing them to create value and new ad hoc service profiles. In addition to progress in biometric recognition, liveness detection and document checking algorithms, there are identity corroboration technologies that increase the rate of reliability of the digital onboarding by up to almost 100 per cent, along with strict application of the related processes.

The forms that allow interfacing with external databases (domestic data registers, public security forces, IP blacklists, etc.) fall within the aforementioned *identity corroboration* family, along with those that make use of artificial intelligence to make an online behavioural rating that can report 'anomalous' behaviour.

The challenge was and continues to be making the user experience as frictionless as possible, without forfeiting the need to ensure the necessary level of trust established by the digitalisation of the process, all in full compliance with prevailing laws.

It is precisely the need to sacrifice something at the user experience level, along with the results of the analysis of the risk associated with the digitalisation process that encouraged some countries (usually northern European countries and English- and French-speaking countries) to place the trust requirement lower than the need for more simplified business processes. Recently introduced technology will allow these countries to maximise the legal protection without sacrificing the user experience in order to resolve the issue.

There is a progressive transfer from identification processes helped by specialised staff to completely unattended processes in the current environment, where a party's identity is verified by an algorithm on the basis of records gathered in the robotised interaction with the party themselves, sharply reducing time and costs.

Technological progress, however, has not necessarily been mirrored by regulatory progress. The scenario is currently very

diverse since, apart from the applicable international regulations (eIDAS 910/2014, Anti-Money Laundering 129/2019, GDPR 190/2018), each country has adopted these laws within the domestic legislative framework and sectors with interpretations that either authorise or forbid the use of certain digital trust technologies.

There are, therefore, countries where any unattended digital identification process is not permitted in order to issue digital identities with the maximum level of trust (certified electronic certificates), others where it is possible only after verification and taking on the end responsibility using specialised staff, and yet others where it is allowed provided that it is part of pre-established processes and with the use of specific technology.

It started with systems that could certify the identity of a party each time the party had to engage in a digital transaction, using a centralised identity model, and then developed into identity brokering systems, that is the reuse of one's own digital identity.

This is this case, for example, with certain players who developed technology that could import ID assertion from one of the banks, where the interested party is a customer, in order to allow the customer to carry out a legally valid digital transaction with a third party without having to be digitally identified again by the third party.

The important assumption in this approach is the absolute trustworthiness of the entity exporting the ID assertion, and, therefore, the entity could only be a bank. In Germany, for instance, there are many institutions that were able, in that sense, to create a new source of profit by agreeing pre-established fees associated with each export of the ID assertion with the service providers.

To date, at the government level, an increasing number of countries are engaged in the distribution of new electronic ID cards or unique digital credentials; for example, Germany, where the project has just been completed, or Italy, where 25 per cent of the population already has the new electronic ID card and with this number expecting to rise to 100 per cent within 24 months, or where the SPID — the Unique Digital Identity System — allows the public to access government portals with unique credentials that will also soon enable access to the services of private operators. Spain is also replacing the current documents with the new electronic DNI as the old IDs expire, and in France the deadline for the new system is mid-2021. The investment prospects relating to digital identity at the government level were made even clearer by the declarations of the president of the European Commission, Ursula von der Leyen, who, during the most recent 'State of the Union 2020' meeting relating to strategic development projects for the EU, announced interest in a new project for a unique digital identity for all European citizens: 'Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality.'

The assumption is that we are experiencing a progressive dematerialisation of the ID cards currently being used and still in physical form, even though they have evolved and have become digital. The digital ID card as an item validating one's identity will therefore turn into our identity itself, consisting of a set of verified credentials in a digital wallet that can be used by any portable digital device.

The market understood the opportunities for innovation and creation of the value enabled by the digital identity and is creating systems with increasing added value around this concept. This is why digital identity is already developing towards an *enriched identity* concept now.

These solutions that are emerging onto the market add further business information (scoring, risk ratios, exposure to the

banking system or any outstanding criminal proceedings, educational qualifications, professional track record, employer, etc.) to the simple *digital identity*, with the necessary information for the identity proofing of the party attached (name, surname, date of birth, tax code and trusted contact information).

The value of the enriched identity is to enable new business processes.

FROM DIGITAL IDENTITY TO SELF-SOVEREIGN IDENTITY (SSI)

Thanks to the development of Blockchain technologies, the development of digital identity is progressing towards a paradigm shift in digital identity management. In this new vision, digital identities will no longer be merely elements that support commercial transactions but a new strategic asset that can be leveraged in order to generate new business.

This is why the union between customer identity — business information — and trust service is an opportunity to take advantage of since they are three enabling factors that can cast banks in a new role and ensure that the information on millions of customers held by the banks begin to produce value (Table 1).

This new approach to the customer base, however, involves overcoming many of the methods that the bank now uses to manage the information on their customer bases. The principles at the base of the self-sovereign identity paradigm are set out on the right. As can be noted, banks will have to radically rethink their methods for managing information on their customer base for most of the principles.

This approach must also be said to go in the direction defined by the GDPR (European General Data Protection Regulation 2016/679).

In the coming years, thanks to the spread of Blockchain technology to manage and check the 'digital credentials' and the new SSI paradigm, it will be easier to manage,

Table 1: Self-sovereign identity paradigm

- **Existence:** Users must have an independent existence.
- **Control**: Users must control their identities.
- **Access:** Users must have access to their own data.
- **Transparency:** Systems and algorithms must be transparent.
- **Persistence:** Identities must be long-lived.
- **Portability:** Information about identity must be transportable.
- **Interoperability:** Identities should be as widely usable as possible.
- **Consent:** Users must agree to the use of their identity.
- **Minimisation:** Disclosure of claims must be minimised.
- **Protection:** The rights of users must be protected.

Source: 'The Path to Self-Sovereign Identity', Christopher Allen, 2016

control and use the verifiable credentials linked to the identity of an individual.

It will be easier for *users* to manage their credentials, which will be unique and usable in all their digital transactions, including those with other parties, without having to manage an extensive number of credentials and without having to undergo continuous identification processes. Users will have full and exclusive control of their credentials in their wallets, managing the access and use requests of their credentials from the various service providers (banks, insurance, government, etc.). These credentials will also follow the *users* through their lives, regardless of the relationship with *specific service providers*.

It will be easier for *service providers* to recognise a new customer using previously existing, certified credentials, without having to carry out long, costly recognition processes, thereby facilitating the acquisition of new customers.

A digital identity management founded on the SSI paradigm offers new opportunities to all companies or governments that need to identify their customer base/citizens.

The SSI can be applied in simpler contexts such as affiliation to loyalty programmes, where needs for verifiable

credentials are lower and limited to only a few details, to public contexts or legally binding digital transactions, where governments or other organisations can have quick access to all verified credentials about the citizen/customer. Consider in healthcare the ability to quickly access all citizen clinical information uploaded to the Blockchain by different healthcare structures. All the information is in the full control of the customer/citizen, in compliance with GDPR, who can consent in his wallet to share his verifiable credentials with third parties in a very simple way without having to provide the same information each time.

This approach will open the route to new possible forms of sharing personal data, when it will finally be possible for everyone to have complete control over their digital identities on an independent basis from individual entities or governmental organisations. With SSI in the future, each person will have a set of certified information resulting from certain identifications occurring within the scope of secure digital transactions.

It is easy to understand how the extreme requirement for confidentiality and security of this type of information requires technology that can ensure this; this is why the new systems have employed Blockchain technology, which constituted the enabling layer over which certain multi-stakeholder foundations were created with the aim of implementing scalable technological solutions that fully comply with the fundamental principles of SSI to guarantee privacy by design and guarantee the governance of the global ecosystem.

Blockchain technology makes SSI a reality, enabling a decentralised self-service registry for public keys. Since every transaction in a Blockchain has a digital signature that requires a private key, it is an obvious choice to use the Blockchain itself for the storage of the associated public key or any other cryptographic key over which the key owner needs to prove ownership.

By moving to cryptographically verifiable digital credentials, we can finally start proving our identity, attributes or relationships without intermediaries.

The operational activities of the foundations operating in the area of SSI are generally carried out by three committees:

- Legal Circle — a committee of legal experts, professionals and enthusiasts of the subject who define the network rules and processes, ensuring compliance with the various laws of the sector
- Business Circle — made up of representatives of business operators and institutions that outline and provide advice on the network business model and on the pricing policies of the credentials
- Technical Circle — made up of experts in the identity and Blockchain world, with the job of defining the applicable technological framework of the network, selecting the software and vendors, defining the technical aspects relating to the relative agreements and the operating budget.

The Foundations deal with

- defining the rules of creation of the verifiable identity credentials and the other context-specific credentials when considered necessary by the members and ensuring compliance
- defining the payment rules for use of the verifiable credentials and ensuring compliance
- promoting the network of the community of stakeholders with respect to the market for the implementation of use cases and new business models based on the SSI vision
- designing a data-monetisation model to benefit the wallet users
- guaranteeing the adequacy of the technological choices on which the good performance of the network is based and the necessary interoperability.

Qualified Trusted Service Providers (QTSPs) are increasingly finding a place in these foundations, that is companies that add a further element of security through the placement of digital signatures on the credentials. Some of these QTSPs are already proposing service architectures and creating ecosystems with the involvement of their top enterprise customers.

The verifiable credentials ecosystem[3] is based on the following main concepts see Figure 1

- **Verifiable credentials** can represent all information that a physical credential represents. The addition of technologies, such as electronic signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.
- **Holder**: A role an entity might perform by possessing one or more verifiable credentials. Holders include citizens, students, employees and customers.
- **Issuer**: A role an entity performs by asserting claims about one or more subjects, creating a verifiable credential from these claims and transmitting the verifiable credential to a holder.

  Example issuers include corporations, non-profit organisations, trade associations, governments and individuals.
- **Verifier**: A role an entity performs by receiving one or more verifiable credentials from the holder for processing. Example verifiers include employers, security personnel and websites.
- **Verifiable data registry**: A role a system might perform by mediating the creation and verification of identifiers, keys and other relevant data, such as verifiable credential schemas, revocation registries and issuer public keys which might be required to use verifiable credentials.

  Example verifiable data registries include trusted databases, decentralised databases, government ID databases and distributed ledgers. Often more than one type of verifiable data registry is utilised in an ecosystem.

Token: Unit to count the number of requested transactions from a verifier to access verifiable credentials enrolled by the issuer. This is to enable monetisation of identity proofs.

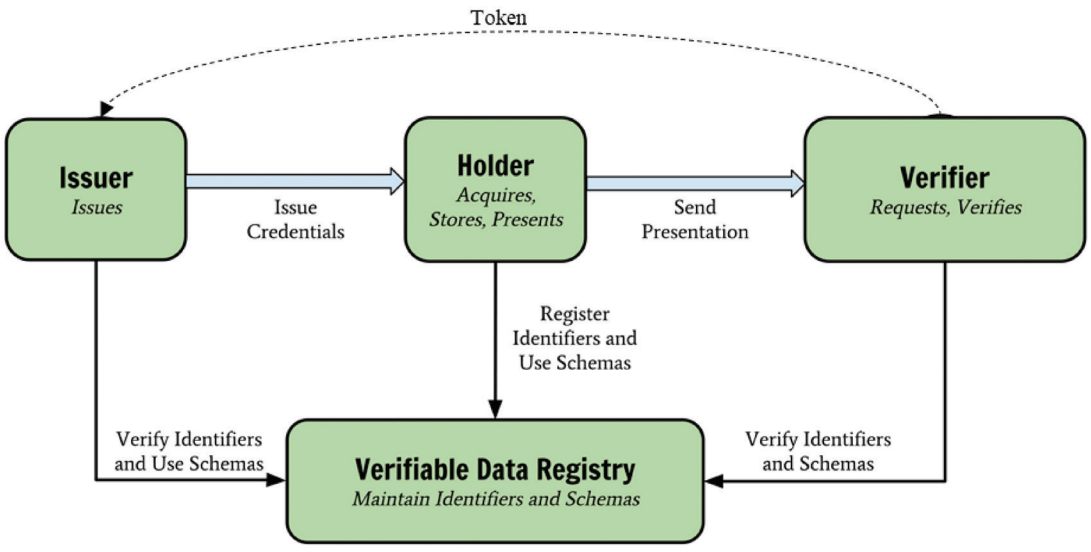

Figure 1: W3C Verifiable Credentials

Each *issuer*, that is any entity that has certified information on the identity of a party, can share it with other parties who form part of the ecosystem.

We can consider the banks that, in their capacity as *issuers*, can share, in exchange for a fee, the KYC credentials of their customers to third parties (*verifiers*) who need that information to enter into a business transaction.

This chart of interactions in the SSI will encourage new business models where the customer base starts producing new revenue streams.

The advantages are clear, even from the perspective of the *verifiers*, who can access the information previously certified from another entity without having to implement any further identification mechanisms. For example, consider the onboarding of a new customer that could occur with a simple request for access to information that is already available and certain.

The entire set of certified information will go to populate the wallet of each individual party and his or her unique digital identity that he or she can manage on a fully independent basis, also enabling reward mechanisms each time a sharing transaction is completed with a member of the ecosystem. It will be up to the *holder* to decide — on a transaction-by-transaction basis — what credentials to share with the third-party entity (*verifier*) in order to complete the transaction successfully.

SELF-SOVEREIGN IDENTITY USE CASE

Today it is the company or government that is responsible for collecting the information whenever an identification is required with the user responsible for proving his verified credentials. Think of every time we have to complete administrative procedures in which we have to prove our identity through the display of multiple documents. Every time we perform this action there is a lack of a shared system of verified credentials. The creation of a shared, secure, durable and business-enhancing system like SSI addresses all administrative processes where certified information is required for legally binding digital transactions.

In order to better understand the aforementioned dynamics, consider the following example of a use case: A person is interested in taking out a loan with a consumer credit entity.

This person connects to the website of the entity, enters the section providing the service, opens his or her wallet on the portable device, scans the QR code of the service on the website, agrees to share certain credentials that he or she has in his or her wallet, accepts the general contract terms of the electronic signature provider and the service in question and then signs the contract. This can all be done in just a few minutes.

Shared credentials (eg mail and telephone number) could come from a previous issuer who performs the verification of these credentials.

When the party (*holder*) agrees to share his or her credentials, the system will ask the *issuer* for confirmation of their validity and will authorise the subsequent steps of the transaction only if the credentials are valid. The *issuer* will then be given a fee using a token system each time it validates a credential. If the *holder* does not have all the credentials necessary to complete the transaction available in his or her wallet, or the authentication level of some of them does not correspond to what the company providing the loan (v*erifier*) requires, the *holder* will ask to issue the credentials to the *owner,* who has them.

Thereby, the owner's credentials will be enriched with further verifiable credentials, increasing the 'level of assurance' of the owner (ie LoA 0, LoA 1, LoA 3, ...).

At the issue of each credential to the verifier, the verifier itself will acknowledge a credit with respect to the *issuer* that is added to that generated by the validity

verification of the same credential. Normally, a credential corresponds to an attribute of the identity of a party (e-mail address, physical address, mobile phone number, etc.), but in accordance with the requirements, an *issuer* may also issue credentials that comprise a combination of attributes.

It is clear that this new paradigm is about to offer new business opportunities to banks that will allow them to capitalise on their company records in a safe way in full compliance with privacy protection laws. For GDPR purposes, the identity of a data subject resides solely in the wallet of the data subject and is shared, only to the extent necessary, on a transaction basis subject to the explicit acceptance of the data subject him/herself. This is also different from the present situation where service providers are forced to 'accumulate' data and information on customers, exposing them to high risks of data *breaches* and possible serious legal consequences; using the SSI approach, the information will return to the full control of the owner, reducing the exposure of the data to potential privacy breaches.

The creation of increasingly broad ecosystems will simplify the implementation of and subscription by customers to new services that can generate new revenue streams on an increasing basis.

The bank may act as an *issuer* or *verifier* in accordance with the type of transaction that it will be involved in, and in both cases may obtain significant benefits in financial terms; for example it may act as an *issuer* when the party asks for the issue of its credentials and as a *verifier* when it is interested in acquiring a party as a new customer; in this case, the validity of the necessary credentials will be confirmed by the respective *issuer* who has issued them, which could also be another bank. This is all in a framework in which it is up to the interested party only, as the *holder*, to decide whether to share his or her credentials or not.

In accordance with the foregoing, digital identity is undergoing a strong process of development because of the profound innovation that these types of solutions are already introducing into the financial sector, which will only increase in the future.

References

1. European Commission. (n.d.) 'Recovery plan for Europe', available at: https://ec.europa.eu/info/strategy/recovery-plan-europe_en (accessed 5th July, 2021).
2. FICES. (n.d.) Available at: https://www.fices.eu/ (accessed 05th July, 2021).
3. W3C. (n.d.) 'Verifiable credentials data model 1.0', available at: https://www.w3.org/TR/vc-data-model/ (accessed 05th July, 2021).