# eIB: eIDAS enabled i-banking

# White Paper

## Interim Report

This document is issued within the frame and for the purpose of the eIDAS enabled i-Banking project. This project has received funding from the European Union's Innovation and Networks Executive Agency (INEA), under Grant Agreement No INEA/CEF/ICT/A2018/1633440. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

# The eIB (eIDAS enabled i-banking, INEA action number 2018-EU-IA-0044)

The eIB project aims at leveraging the potential of combining eIDAS based identification and e-signature technologies (especially remote e-signatures) to fully automate and secure the process of online registering with a cross border bank.

To achieve this, the project will develop a business process model for automating the process of opening a new customer and bank account cross – border (OBA c-b) by a user coming from another EU Member State.

This business process model will combine the use of eIDAS eID for customer identification and e-signature (based on eSignature DSI DSS) for signing of necessary documents.

Moreover, the project aims at creating a new generation of cross-border e-banking services.

Specifically, the project will create an eIDAS enabled value chain where a Bank and Retail Service Providers (operating in different locations across Europe) collaborate in real-time to unambiguously identify users with high level of assurance, via their eIDAS identifiers, exchange assets and information and ultimately offer banking products and automated e-services

Between the other activities, eIB will setup an eID and e-Signature Monitoring Group (IMG).

**Scope of this White Paper** is to activate the discussion on the several identity models that are available for the European Financial Industry to have a safe and efficient customer identification for remote digital transactions and activities.

The eIB project aims to discuss and deploy an innovative model for customer identification that:

- could be used between the several National economic communities within the EU without impacts on the already existing initiatives,
- and at the same time usable at National level where no other initiatives have been activated to facilitate the collaboration between banks and Institutions on the digital ID domain.

The eIB project has been funded by the EC, action number 2018-EU-IA-0044

# Executive Summary

60% of world GDP will be digitalised[1] by 2022.

Moreover, digital payments are growing at an estimated 12.7% on an annual base and are forecast to reach 726 billion transactions annually by end of 2020[2].

These figures make self-evident that modern life increasingly takes place online, with a wide array of services and platforms.

However, unlike in the real world, there is not a trusted mean that reveals the true nature of these digital inhabitants that can be used smartly and safely for financial activities.

Several surveys are showing that digital identity is rapidly becoming an essential ingredient of successful customer onboarding at financial institutions. Customers are increasingly frustrated with proliferation of paper-based documents needed to digitally activate a new financial service. When onboarded, then the customers complain with the different passwords' management, the data privacy and are concerned about data breaches.

From 2014, the eIDAS-based eID authentication would provide banks with a high level of assurance about the identity of the newly on-boarded customers and their main ID attributes. But eIDAS is not adequate to ensure a smooth onboarding process (e.g. to open cross border a bank account) because the information handled are not enough to conclude a customer journey that can be perceivable as smart.

In fact, the minimum data set of eIDAS is composed of key identification attributes: Family Name, First Name, Unique identifier and Date of birth.

This dataset may be completed by financial-specific attributes that are used by banks for Know Your Customer requirements.

What the eIB is doing in this field is to complete the eIDAS data with an enrichment of information not owned in Public Authorities files but coming from KYC databases, like the ones managed by the banks, to onboard (and access) to financial services.

This model is called "Federated-ID" that will be discussed in this White Paper in term of architectures and technologies (like the DLT one or the Public Key Infrastructure) that can be used successfully by the banks and other players. The project will focus on customer attributes, linked to the digital identity.

---

1 International Data Corporation (IDC), IDC FutureScape: Worldwide IT Industry 2019 Predictions "Prediction 1: Digitized economy. By 2022, 60%+ of global GDP will be digitized, with growth in every industry driven by digitally enhanced offerings, operations, and relationships and almost $7 trillion in IT-related spending in 2019–2022."

2 Capgemini & BNP Paribas (2018), World Payments Report 2018, accessed online at: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf.

De facto, the regulatory obligations, the operative and security needs to which the banks and financial institutions are subject in terms of identity verification have placed them in a strategic position.

The challenge is now how to capitalize this opportunity for the European banks in creating benefits for the European citizen and companies.

Banks, Payment providers and other economic players can do a lot if they will have a clear understanding of what they are allowed to do. Jeopardized national solutions on eIDs and KYC could create an obstacle to the introduction of a European wide banks' offer as requested by the Payment Account Directive.

Collaboration is a pillar of every reasonable design for digital identity services. There is no single government, technology company, financial institution, or even industry sector that can effectively deliver a digital identity service by itself.

# Executive Takeaway

The ongoing eIB project has shown a set of issues in the existing market situation:

a. As is, eIDAS is not adequate to ensure a smooth onboarding process (e.g. to open cross border a bank account) because the information handled are not enough to conclude a customer journey that can be perceivable as smart.

b. The missing dataset could be completed by financial-specific attributes that are used by banks for Know Your Customer requirements but telecommunication standards for these attributes are missing and there is a need to adopt a classification on KYC information.

c. The Banking practises for digital onboarding at European level are very differentiated, and very often still rely on paper-based IDs.

d. There are already national examples of integration between eIDAS eIDs, with KYC information that are only applicable at national level: European wide projects or initiatives are still missing.

What is needed to successfully integrate KYC and eIDAS trust service in a European wide approach?

1. A **relation framework** between the players involved in the KYC data exchange to define at least "what is required", level of trustworthiness requested, eligibility criteria for exchanging data. This could be achieved in 2 different ways:

   i. Standardization and Regulatory guidance and/or

   ii. The creation of an eID/KYC scheme, that has been defined Identity Governance Service, that will drive the discussion and will work to create a "unified customer journey"

2. **KYC data communication infrastructures and rules** to exchange data. This result could be achieved via different solutions:

   i. Use of eIDAS DSI: after authentication where, upon instructions of the client, the new service provider reaches out the KYC Attribute Authority (the owner of the KYC profile of the customer) to receive the needed information with the support of the eIDAS framework.

   ii. API Integration: when doing authentication, the customer is asked to approve the transfer of additional data which follows the authorisation response to the party initiating the authentication.

   iii. Integration into DLT: A third alternative is to use the distributed ledger technology solution to create a sort of identity wallet, composed by Attributes, directly managed by the customer.

# Summary

# Introduction

25 years ago, the customer had to visit the bank to perform any transactions.

In a global situation where 76% of individuals[3] have a smartphone available, technology is lowering the barriers to entry for more and more financial services.

Now the technology evolved banking services and we no longer need to visit the bank, as a large majority of transactions are carried out from a computer at home and now even from our mobile phones. Today, banks rely on their digital platform to sell their banking products and to increase their market share.

As part of their digital transformation, banks are striving to deliver customer friendly onboarding experiences.

Now more than ever, attracting prospect customers has become a crucial challenge, as they demand a smooth and customer-friendly onboarding experience, enabling them to establish a business relationship with financial services providers within a matter of minutes. In fact, according to a recent report[4], it seems that the line is drawn at fourteen minutes and twenty seconds. After that time more than half of the potential customers abandon the onboarding process, blaming the amount of personal details they have to fill in and the large process duration.

Meanwhile, Regulators are taking an increasingly active role in the EU in ruling the digital world.

To conclude a contract with a potential customer a European bank must respect, among others, the GDPR (General Data Protection Regulation), the PSD2 (second Payment Services Directive), the eIDAS (electronic Identification Authentication and trust Services), the PAD (Payment Account Directive) and the 5AML (fifth Anti Money Laundering directive) that are demanding deep Know Your Customer (KYC) process, robust protection, privacy and control for users.

However, despite these efforts, it is still impossible today to use eIDAS to do digital onboarding for bank services within several European Countries and cross-border in any EU bank.

But also, eIDAS is not adequate to ensure a smooth onboarding process because the information handled is not enough to conclude a smart customer journey.

The minimum data set of eIDAS is composed of key identification attributes: Family

---

[3] Median of results about smartphone availability for customers in advanced economies (pew research, 2019) https://pewresearch-org-preprod.go-vip.co/internet/2019/06/13/mobile-technology-and-home-broadband-2019/

[4] Signicat 2019 Battle-on-Board 3 report, summary available at: https://www.signicat.com/resources/financial-institutions-have-only-14-minutes-20-seconds

Name, First Name, Unique identifier, and Date of birth[5]. Place of birth, Current Address, Gender, and Name at birth are optional attributes, which may be provided by a Member State if available, and if this is acceptable by national law. This dataset may be completed by sector-specific attributes. Yet the latter is limited to attributes supporting the identification of customers and can in no case concern attributes aimed at evaluating the eligibility of the customer for a potential service or performing KYC checks to detect fraud and risks (e.g. credit score).

On the other hand, KYC data managed by the banks (and other third parties) would benefit from the trust conveyed by a "legal stamp" like the one provided by eIDAS. There is a real case for the banking and financial sector to explore the use of eIDAS-based trust services[6] and/or eID for strong authentication and identity proofing of customers.

In the context of AML legislation, the direct use of an eIDAS-based authentication process can be envisaged considering that the KYC process is a one-off procedure at the time of onboarding.

While additional attributes may be requested by banks to complete national requirements or shared via sector specific attributes, eIDAS-based eID authentication would provide banks with a high level of assurance with regard to the identity of the newly on-boarded customers and their main ID attributes.

Banks could also rely on derived identities that have been verified by an eIDAS-based eID.

The choice between the two solutions will depend on the usability and uptake of the eIDAS-based eID solution used in a specific country.

The European market has already given some answers in creating solutions that are combining the trust of eIDAS together with a wider set of information typical of KYC process.

In Belgium, a cooperation between the public initiative "eCard" and the bank driven initiative "itsme" are having an increasing role in the customer perception: the public Administration provides the enrolment and the authentication services while the "itsme" platform offers the option to use a mobile identification mean to authenticate oneself on public or private applications.

At present, over 50% of all itsme-enabled transactions are in the banking sector.

The model behind the ecard/itsme Belgian solution is normally defined as "Federated

---

5 European Commission - eIDAS SAML attribute profile available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjQnYDNioboAhXD_qQKHS6ABdIQFjAAegQIAhAB&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F82773108%2Feidas_saml_attribute_profile_v1.0_2.pdf%3Fversion%3D1%26modificationDate%3D1497252920317%26api%3Dv2&usg=AOvVaw2vK-XWTM8EI43Xmq4teWnk

6 Trust services refers to a broad range of services for authentication and signatures for protecting electronic transactions. Trust services can include the following activities:

- Issuing certificates for signing, sealing, and website identification, such as certificate authorities providing public key infrastructure (PKI) services
- Issuing digitally signed time stamps
- Long-term preservation of signed data: for example, ensuring the long-term validity of signatures on archived documents
- Electronic registered delivery services, where evidence of delivery from an identified source is required
- Signature and seal validation

Identity with Trusted third-party attestation" (FTTP), that has several positive scores related to enhanced customer experience and compliance with existing EU legislation.

Another model that is gaining relevance into the market is the "Federated identity with Self declaration", mainly used via Facebook or Google, that is not usable in a European Financial context because it lacks AML compliance and reliability.

The third model that has been considered is the Self Sovereign Identity model (SSI). A global card scheme is proposing an application of this model adopted by the North Macedonian Identity Service system.

This last generation of digital identity returns the control of PPI to users by issuing them digital credentials that can be self-custodied and shared only with trusted parties. This model also provides infrastructure for such credentials to be issued, stored, and verified at scale and regardless of whether two parties are meeting in person or interacting online.

Two technical innovations make this possible—the process innovation of verifiable credentials and the technological innovation of distributed ledger technology (DLT).

This model could represent an enhancement for the ID platform, but at this stage it is not clear if yet it will be deemed acceptable by the EU and National Authorities, and who will make/govern the public DLT required for the sharing of data.

In this sense, it must be considered the recent European Commission document "EIDAS supported self-sovereign identity"[7] where it is represented a potential way forward in how to integrate the eIDAS Framework together with the SSI architecture.

Under the SSI approach, the trust on the actual identities of the parties is built out of the system, as the specifications does not foreseen mechanisms for binding the digital identifiers to real-world entities.

The eIDAS Regulation can play a key role, since it does not require a previous relationship between the involved parties for verifying their identities in the digital world; they can rely on the verification done by the entities entitled for that: trust service providers and identity providers of the electronic identification schemes.

Having said that, the eIB project is studying an overall approach based on both "Federated Identity with Trusted Third party attestation" and "Self-Sovereign Identity" architectures to allow the European cross border onboarding of digital services, and at the same time flexible enough to be usable in the countries where a cooperation between public and private actors still needs to be established to allow a smooth usage of eIDAS ID by customers.

A detailed analysis will be in the project' result, but it can be anticipated that the eIB proposal is adding to the existing FTTP model the Multi-Source Identity feature, allowing multiple credentials from multiple providers (connected via an Identity Governance Service) to be shared, flexibly and conveniently, in a situation where trusted attestations are needed for the participants in a workflow to make progress.

A valuable collaboration is planned to come from the Berlin Group, which is contributing with their experience on financial APIs and their knowledge on standardized formats to exchange data.

---

7 https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

# Chapter one The digital identity situation

## 1. Everything started here

"On the Internet, nobody knows you're a dog."

In 1993, *The New Yorker* published an iconic cartoon about the Internet: in it, one dog says to another, "On the Internet, nobody knows you're a dog." In 1993 many people saw the ability to remain anonymous as a *feature* of the Internet, not a liability.

We are now in 2020, 27 years later, then why is digital identity (still) a problem? Three reasons:

1. The technological advances and widespread digital diffusion that have occurred over the past 25 years have exasperated the need of trust on the internet players.
2. There are standardized formats for digital credentials, but not yet a winning model.
3. There are standardized methods to verify the source and integrity of digital credentials, but silos are still prevailing over a digital (European) market of the related (financial) applications.

The internet was originally designed to enable machines to talk to other machines. It was not designed to enable the secure identification of the persons using those machines. In the absence of a ubiquitous digital identity framework, the identification processes used for different services on the internet have evolved independently. The identity ecosystem has become fragmented and complex, with too many stop-gap solutions creating and propagating vulnerabilities and friction.

The rapid pace of digital transformation has left many industries scrambling to find secure, convenient ways of establishing identity for digital services.

Sectors as diverse as healthcare, banking, the sharing economy, gambling and air travel all suffer from a common problem – it is difficult to remotely identify a customer, with confidence, as is required online. Many identity checking processes still rely on physical documents, more traditional proofs of age or entitlement, or digital workarounds in the absence of access to the trusted attribute data necessary to build effective digital identity solutions.

For authorities, maintaining digital databases of their citizens' basic information for the issuance of identity documents, as well as allowing third parties in the public and private sectors to interact with these databases, has become a needed (but costly and risky) process. So far, centralizing public databases, allowing control to **Trusted Third Parties (TTPs)** to manage the verification between transacting parties, and making

digital identity interoperable by connecting the public and private sectors through a common data exchange platform have been seen as some of the efficient solutions for identity management.

## Regulatory Drivers: list of the European Regulations in short

EIDAS, PSD2 and GDPR show that EU regulators recognize this situation. Data protection law, payments regulation and new initiatives make the Banks' identity ecosystem an evolving space:

- Data Protection regulations are set to significantly change how personal data is used
- Open Banking is revolutionising how personal financial data can be shared with the customer's consent
- Payment regulation will set more stringent rules for establishing identity for electronic transactions
- New Anti-Money Laundering legislation will require stronger checks on customers, and significantly increase the fines for firms that fall foul of the rules

## List of EU regulation and Date of Implementation

| Regulation | Date of Implementation |
|---|---|
| Electronic Identification and Trust Services (eIDAS) | 2016 |
| EU Payment Account Directive (PAD) | 2016 |
| EU 4th Money Laundering Directive (4MLD) | 2017 |
| Second Payment Services Directive (PSD2) | 2018 |
| Open Banking | 2018 |
| General Data Protection Regulations (GDPR) | 2018 |
| PSD2 Strong Customer Authentication (SCA) | 2019 |
| EU 5th Money Laundering Directive (5MLD) | 2020 |

### eIDAS

eIDAS provides a shared set of standards, which enable digital identities and signatures to be relied upon across national boundaries to specific, predetermined levels of authentication. However, eIDAS is focused mainly on allowing access to public services and development for business use are still ongoing.

### PAD

By requiring banks to extend their usual services to resident customers applying from elsewhere in the EU, PAD exposed the international and digital limitations of banks' current onboarding processes. It highlighted the growing need for banks to remotely identify individuals and organisations securely and with confidence, wherever they may be located.

### 4MLD

The 4MLD introduced higher levels of security and customer due diligence required of a wider range of organisations, introduced the recognition of electronic signatures, and raised the fines that can be applied to firms. These factors are even more pushing organisations to explore new identity processes, in order to keep abreast of their 4MLD obligations in a more efficient way.

Article 13 of 4AMLD clearly requests that due diligence be performed for "*identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source*". The directive also requires the identification of the beneficial owner', the obtaining of information on the purpose and intended nature of the business relationship, and scrutiny of the transactions undertaken within the framework of this relationship.

Requirements under 4AMLD have evolved since 5AMLD to integrate key evolutions in the banking and financial sectors (like eIDAS) linked to remote identity verification based on videoconferencing systems. The Directive has also introduced higher levels of assurance required regarding the attributes collected about customers, as well as the fines applied in case of non—compliance.

### PSD2

On top of introducing changes to payment and data sharing regulation, PSD2 crucially introduces several requirements concerning increased identity and authentication checks, via the Technical Standards on Strong Customer Authentication (see below).

The EU Directive no. 2015/2366 on payment services in the internal market (PSD2) requires under article 97 that payment service providers (PSP) apply strong customer authentication. With the exception of low value or repetitive transactions, authentications must be based on two-factor authentication solutions (or more) when the payer "accesses his payment account online, initiates an electronic payment transaction, or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse".

### GDPR

GDPR is designed to enable individuals to exert control over their personal data, how it is used or shared, and with whom, and sets out higher fines for any transgressions.

### 5MLD

As well as strengthening the core provisions introduced by the previous 4MLD, the 5MLD amends the rules to allow organisations to accept digital identities under simplified Customer Due Diligence rules, provided they are derived from eIDAS-notified national identity schemes, or from national schemes recognised by the national regulator.

The 5AMLD strengthens anti money laundering provision. Recital 22 also makes an explicit reference to the use of eIDAS-based eID to perform accurate identification and verification of natural and legal persons. Article 13 of the 4AMLD is amended to specify that eIDAS-based eIDs are recognized as a valid solution to identify customers and obtain ID information about them. Additionally, annex III is modified to recognize eIDAS-based eID as a way to secure non face to face business relationships or transactions.

Consequently, the reuse of eIDAS-based eIDs by banks and financial institutions is encouraged to perform the strong identity proofing and authentication required under SAMLD. The Directive does not prescribe which level of assurance of the eID Schemes is required. The current status quo among the members of the KYC expert group established in Spring 2018 by the European Commission, is that eID schemes qualifying for level substantial and high could be reused. The minimal LoA required would depend on the assessed risk of the customer.

### SCA

An element of PSD2, the Strong Customer Authentication Technical Standards has introduced measures concerning increased identity and authentication checks required for online payments, requiring payment providers to find new identity authentication processes.

To conclude, although eIDAS based eIDs are recommended both in AML and PSD2 legislations to perform strong customer identification, there is no obligation to reuse this solution.

The EU Payment Account Directive is not referring directly to the eIDAS Regulation but is putting pressure on banks and financial institutions to support the on-boarding of

customers located in another Member State, which is one of the use cases supported by eIDAS.

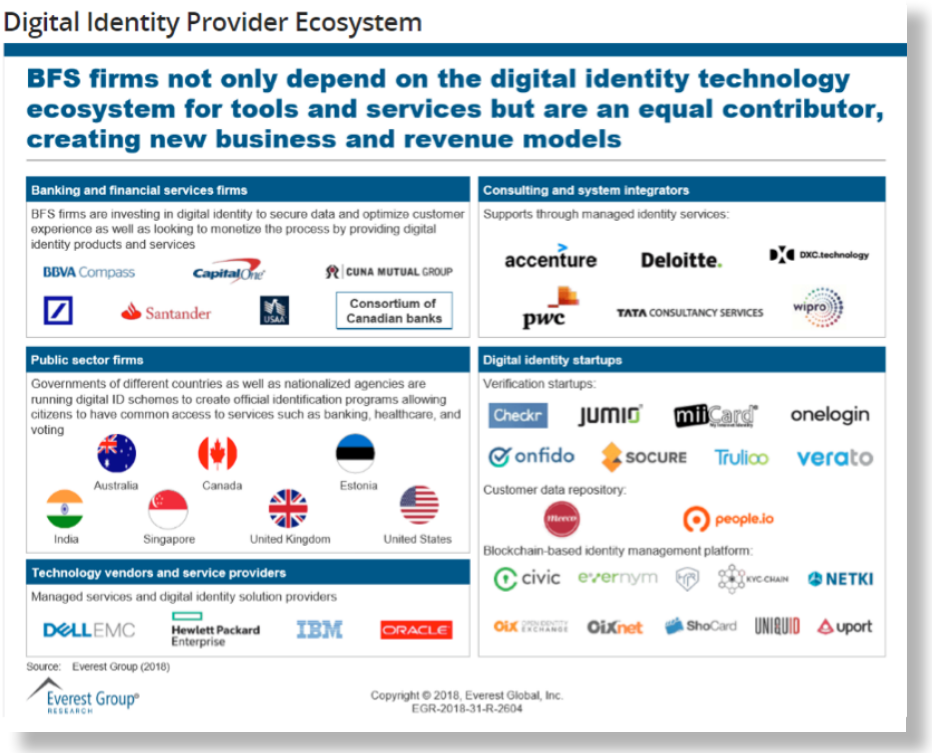
The General Data Protection Regulation (GDPR) and Second Payment Service Directive (PSD2) both include aspects that impact digital identity. GDPR means that the consequences for an organisation of a data breach due to poor implementation of digital identity are now severe. PSD2 now requires payment transactions to use Strong Customer Authentication unless specific exemptions apply.

PSD2 and the arrival of Open Banking is forcing banks to radically revisit their approach to payment authentication, and the identification technologies underlying it. For banks willing to think beyond compliance this gives them a great opportunity to work together to fix the usability and convenience problem also. If banks get this right, then their way of handling identity can become the de facto standard for securing the internet.

Of course, there are other parties interested in solving the problem, not least the digital tech giants, such as Google and Facebook. However, a 2018 survey (before privacy scandals) found that in Germany, over 60% of consumers would prefer banks to provide their digital identity, compared to the 5% who would prefer a social media platform[8].

Identity on the internet is not trustable. The regulators want it fixed, from a security and privacy perspective at least, but the usability and convenience should be addressed by the private sector.

**A legally recognized digital identity is the enabler for a full digital customer journey, that will require much more information to be perceived as smart by the customer.**




[8] See https://www.paymentsjournal.com/id-eal-banks-and-trusted-digital-identity/

# 2. The digital identity challenges

Digital service delivery is expanding rapidly but is often inhibited by a lack of trusted digital identity. Society is riddled with examples of everyday activities where people are prevented from enjoying the benefits of seamless delivery due to a lack of suitable digital identity infrastructure, from renting a flat to applying for a job or opening a bank account.

In Italy 38% of the customers left the onboarding process for a financial service, stressed by the excessive number of paper-based information required.

Solving digital identity has the potential to bring huge economic value to both individuals and businesses. It offers the opportunity to remove inefficient and time-consuming manual processes and achieve a reduction in fraud, enabling high value digital services that are difficult to deliver today.

Whether the realisable value of digital identity is estimated from 0.1% to 2.5% of GDP[9], here is great value to society in solving this problem, and therefore great opportunity for the organisations willing to solve it.

With the focus of PSD2 being on the banking community, banks are in a unique position to take advantage of the infrastructure they are building for compliance. This infrastructure provides them with an opportunity to reinforce their consumer relevance and open new streams of revenue. Banks are not the only industry operator that could solve this problem but they:

1. have high levels of consumer trust
2. are used to establishing long term relations with customers
3. are already investing in digital identity and Strong Customer Authentication
4. are used to cooperate, e.g. to achieve interoperability payments, to create critical mass

[9] OIX "ECONOMICS OF IDENTITY the size and potential of the UK market for identity assurance"

# 3. The evolution of digital identity models

The first and still most common form of digital identity is the siloed shared-secret model that anyone who has ever used a username and password is familiar with. Service providers use a combination of online and offline processes to onboard users, then authenticate their identity for future interactions via secrets such as passwords, mothers' maiden names, and confirmation emails. In this model, user information is fragmented across a pool of service providers. This method is inconvenient for users, who must remember an ever-growing list of usernames and passwords and makes it easier for hackers to commit identity theft. For service providers, this solution is neither secure nor efficient. User passwords are often compromised (in part because users repeat passwords across services) or forgotten, leading to costly security breaches and password reset customer service calls.

In the centralized model[10], multiple SPs authenticate their users against a central IdP (Figure 1). In this way the problems faced by the siloed model are resolved. But since the central Identity Provider is a single point of failure, the centralized model presents reliability issues. Its most valuable characteristic is that it enables Single Sign-On (SSO), allowing the user to access several SPs based on a single identification instance.

What is the path forward then?

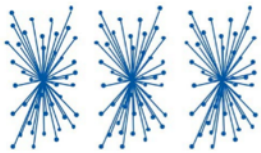
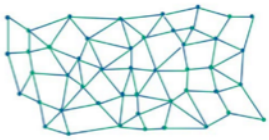
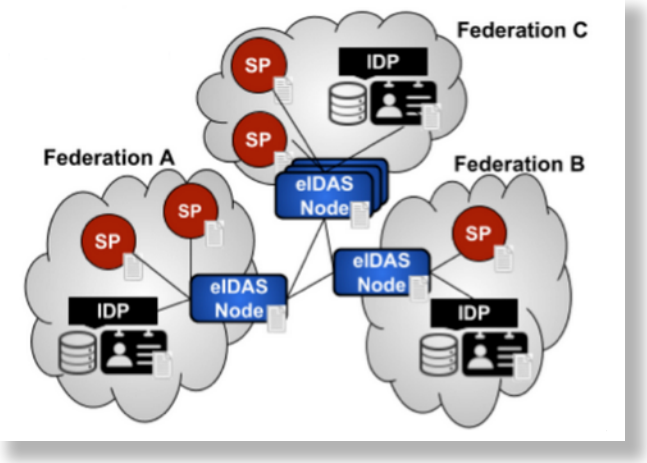
| IDENTITY MODELS | Centralized | Federated | Decentralized |
|---|---|---|---|
| |  |  |  |
| TECHNOLOGY | • ID/Password<br>• Multifactor Authentication<br>• Single Sign On | • OAuth<br>• OpenID<br>• SAML | • DLT<br>• Cryptography |
| CHARACTERISTICS | • Identity fragmented across many enterprises<br>• Enterprises control user data<br>• Centralized data is a honeypot for cyber attacks | • Less fragmentation of login credentials<br>• User information fragmented across many enterprises<br>• Enterprises control user data<br>• Centralized data is a honeypot for cyber attacks | • Identity can be portable across enterprises<br>• User information in user's wallet or a secure cloud<br>• Decentralized data limits data exposure on cyber attacks<br>• Users control their data |

Figure 1

[10] Citi "Digital Identity: Moving To A Decentralized Future"

## Federated identity

From an end user perspective, "Federated Identity" is the means of using only a single set of credentials for e.g. (username, password) to login to various applications, websites, services etc. Technically, "Identity Federation" is the mechanism which enables various applications forming a federation to rely on a separate entity, belonging to a different federation, to authenticate the users (instead of them themselves performing the authentication). The entity that performs the authentication is called Identity Provider (IDP) and the entities that rely on the IDP for user authentication are called Relying Party Parts (RP). In a federated identity architecture like the one underlying the eIDAS network, a Relying Party in one domain (federation) can grant authorized access to a resource it manages based on the exchange of identity, attribute, authentication and authorization assertions with an Identity Provider in another domain (see image below).




The most popular providers of federated identity services are social media sites, and their primary offering related to identity is portability (technically known as Single-Sign On). People can have the same username and password combination across multiple services, and online services do not need to build their own identity management infrastructure.

## Self-attestation

Google and Facebook are examples of self-attested schemes of federated identity. Any claim to a identity is made based solely upon the information provided to the IDP (Google or Facebook) by the individual, with no verification of that information. Indeed, many relying parties may well ignore most – if not all – of the personal data which may be received from the IDP. Users, meanwhile, are free (within the terms & conditions of the scheme) to create many different identities, whether 'real', anonymous, or pseudonymous.

In this category, the RP is trusting that the individual has authenticated to the IDP, and not necessarily anything more than that.

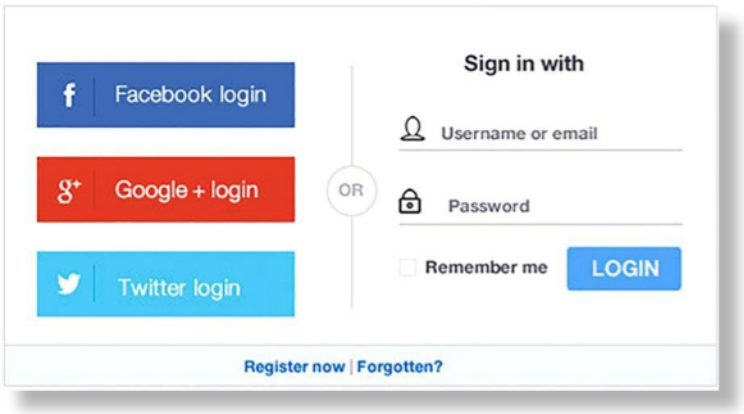



Figure 2

This approach has some major drawbacks. It is useless for high-touch services such as banking that have more stringent onboarding requirements (e.g. AML). It also creates massive pools of user data that can be monetized by social media sites at best and serve as honeypots for hackers at worst.

Some of the more shocking online developments in recent years (Table 1), including the Cambridge Analytica scandal and the Equifax data breach, can be traced back to the limitations of the centralized and federated approaches to digital identity. The economic and personal cost of such scandals and breaches have opened the door to more enhanced solutions.

| Year | Company | Impact |
|---|---|---|
| 2018 | Blank Media | **7.6 million** compromised accounts |
| 2018 | Quora | **100 million** compromised accounts |
| 2018 | Facebook | **50 million** compromised accounts |
| 2018 | Cathay Pacific | **9.4 million** compromised accounts, including **860 thousand** passport numbers |
| 2018 | Marriot | **500 million** compromised accounts |
| 2017 | Equifax | **143 million** accounts exposed, including **209k** credit card numbers |
| 2016 | Uber | **57 million** compromised accounts |
| 2016 | MySpace | **360 million** compromised accounts |
| 2016 | Linkedin | **117 million** emails and passwords leaked |
| 2015 | Anthem Inc | **80 million** company records were hacked, including social security numbers |
| 2014 | ebay | **145 million** compromised accounts |
| 2013 | Target | **110 million** compromised accounts |
| 2013 | Yahoo | All **3 billion** accounts compromised |

Table 1: Known major data breaches throughout history

## Trusted Third Party attestation

The coexistence of Public Authorities that are issuing identities that are valid for real life and the digital world is a large improvement of the Self Attestation model previously described.

The Federated ID with Trusted Third-Party (FTTP) attestation creates a single means of enrolment, identification, authentication and digital signature that can be used across any number of different participating service providers. One ID provider could serve an entire market, utilizing a single technology platform. This enables better safety, security and user- experience, including support for 2 Factor Authentication (FA), eID, mobile apps and much more besides.

Providers that embrace such schemes are typically spared the costs and implementation burden that are associated with operating a proprietary ID programme, whilst also ensuring comprehensive and ongoing regulatory compliance.

The FTTP model:

- represents a model in line with the AML requirements
- this Spikes & Hubs model allows to plan a network enlargement based on common rules (e.g. eIDAS). This is crucial in a geopolitical situation like Europe, where national ownership of Identity data must coexist with European Regulations and initiatives
- in the physical world, we all still use the physical credentials in our wallet to prove our identity, so we still have a TTP (typically an EU Public Institution) handling our data.

## Self-Sovereign Identity

The latest generation of digital identity uses a blend of the old and the new. As in the pre-digital era, it returns control to users by issuing them digital credentials that can be self-custodied and shared only with trusted parties. Unlike in the past, it provides infrastructure for such credentials to be issued, stored, and verified at scale and regardless of whether two parties are meeting in person or interacting online. Two innovations make this possible—the process innovation of verifiable credentials and the technological innovation of distributed ledger technology (DLT). The decentralized nature of the infrastructure moves digital identity from an application to an ecosystem (Figure 3).

The underlying principle behind self-sovereign identity is that the individual is in control of their own identity data. In practice, however, it will be necessary to place trust in a wallet service, such as a cloud-based wallet and/or a smartphone application.

Rather than an external central repository (or repositories) of various pieces of personal data each of which may ‘vanish’ when an account is closed, or access is otherwise terminated, the individual now holds their own data in the same way as

they do with their physical identification documents (driving licence, passport, etc.). Ending a relationship with one provider does not necessarily invalidate any claims that were issued. For instance, if an individual's driving licence is revoked, a claim made about their age by the driving licence authority could still be valid, since their date of birth does not change just because they no longer hold a driving licence; however, any claim that they are authorised to drive will cease to be valid. Therefore, whilst the individual retains control of claims, the IDP may still expire or revoke individual claims where appropriate.

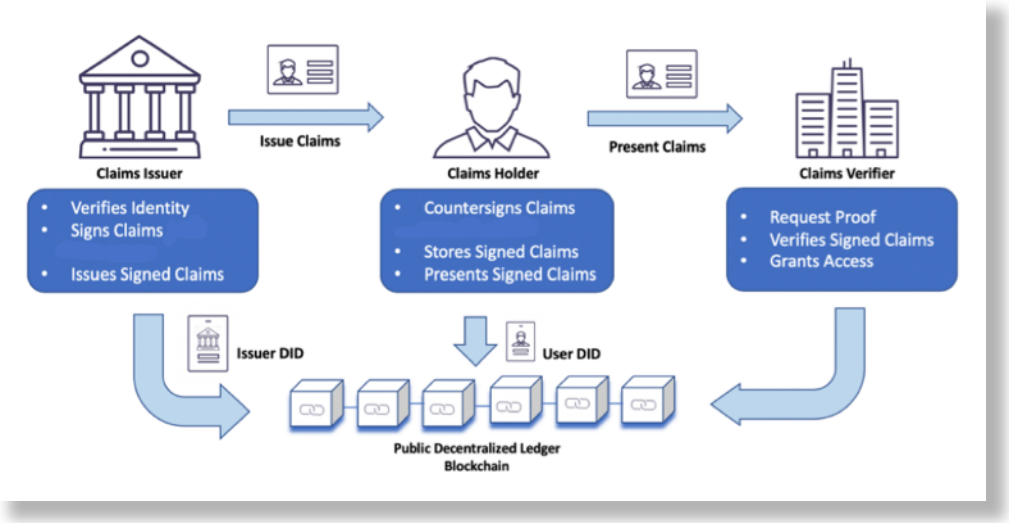



Figure 3

The high-level relationships within a generic self-sovereign network are shown in Figure 12, with the User / CH at the centre of the model, having a relationship with one or more IDPs along with one or more Verifier / RPs, all of whom are participants in the same scheme. The User / CH can request a claim to be issued by any of the Issuers / IDPs, and this claim can in turn be passed to the Verifier RP who can validate its authenticity.

More specifically, the key technical elements enabling SSI are: Decentralized Identifiers (DIDs) and blockchain technology. In a nutshell, the process goes as follows: the (necessary) wallet app installed on the user's device generates a Decentralized Identifier[11] (User DID) and a cryptographic private/public key pair. The private key is stored in the user's device; the public key is associated with the User DID which is stored in a global public decentralized registry, i.e a blockchain. In order to acquire validated identity claims, the user makes a request to the appropriate issuing authority. The latter issues verified credentials which contain PII data about the user in the form of claims and signs them. The credentials are then also signed by the user and stored in an encrypted form in the user's wallet app. When a service provider requests personal information about the user, the latter can provide them with the relevant claim contained in the verified credentials (or a subset of it). To validate the provided information, the service provider verifies the user and issuer signatures using the public keys associated with the User and Issuer DIDs.

The best-known current example of a self-sovereign identity scheme is **Sovrin**.

[11] DIDs are mathematically derived, unique, and random identifiers.

Sovrin's vision is to provide a decentralised, public global identity scheme, with data under the control of the individual, not any other third party, business or government. Several large organisations, including IBM, Infocert and T-Lab (the R&D arm of Deutsche Telecom) are actively engaging with Sovrin, and signing up to be stewards of the Sovrin ledger. The Sovrin protocol is based entirely on open standards and open source—the Hyperledger Indy Project, as the principles of self-sovereign identity transcend any "type of" blockchain or distributed ledger.

Most of the benefits proposed by Sovrin relies on the existence of a Public Global Blockchain.

Verified.Me is built on top of the IBM Blockchain Platform which is based on Linux Foundation's open source Hyperledger Fabric v1.2 and will be interoperable with Hyperledger Indy projects.

It is also expected that Verified.Me, which is based on IBM Blockchain technology, will switch to a self-sovereign architecture. Other identity technology suppliers are also starting to bring self-sovereign offerings to the market, such as the Trust ID Network recently launched by Gemalto, and Mastercard with Mastercard ID.

Research on the opportunities for SSI in the banking sector, like for leveraging KYC processes, has been undertaken by Rabobank since 2016. Banks have to put their customers through extensive KYC and CDD processes, gathering and verifying data from a variety of sources. These processes could generate value, if they could reuse the collected and verified data. This is possible with the use of SSI, if for example banks become issuers, or verifiers, of verifiable credentials.

A product of the Rabobank research was the design of a Universal Ledger Agent[12]: an SSI scheme realized by a component implemented by the wallet application and the verifier. The ULA allows the holder to retrieve credentials, and the verifier to validate credentials, issued under different standards (i.e. ERC-780, W3C and DIDs) and using different blockchains (i.e. Etherium, Indy, and X), with the help of plugins. This feature gives it a great advantage in supporting SSI-as-a-service (server issuing or verifying verifiable credentials).

[12] https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/topics-and-advance-readings/universal-ledger-agent.md?fbclid=IwAR1_GadSA_PZgtLrTPsYlgs7tv99v29PNw7uhGp5ByWfrXz43VWJekjShBg

# 4. Examples of European successful collaboration

As a matter of fact, the EU market is today shifting from siloed solutions to federated ID architecture with Trusted Third-Party attestation.

Models such as itsme®, BankID and GOV.UK Verify build on the self-attested model by incorporating verification of the identity being claimed. In this model, the value of the claim is in the level of assurance (LOA) of the data vouched for by the IDP based on their identity proofing processes.

In the GOV.UK Verify model the government plays the role of the core identity provider, who also defines the parameters of digital identity verification, delegated to government licenced companies. Government-issued credentials form the foundation of verification, which can also draw from other government sources such as police databases, as well as commercial sources like bank account savings, or a mobile phone contract. For example, IDPs participating in Verify typically request verification using three separate forms of trusted identification, e.g. passport, driving licence, bank statements etc. This model is appropriate for relying parties, as banks or financial institutions, who need a reasonable level of assurance that they are dealing with a specific individual. Furthermore, separating Service Providers from Identity verifiers in this way has the benefit of enabling secure digital access while ensuring minimal concentration of PII by either of the two entities.

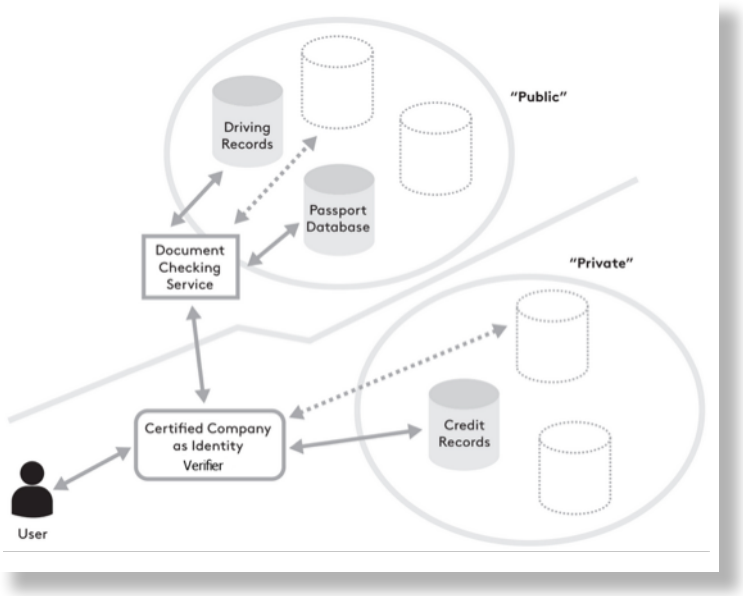



Figure 4[13]

[13] Alan Gelb, Anna Diofasi Metz(2018). *Identification Revolution: Can Digital ID Be Harnessed for Development?*, Center For Global Development

Self-Sovereign is still on study, as the pros/cons ratio must be clarified and the compliance of this architecture with the existing European Regulations and Directives, as well as with National provisions, must be discussed with EU Authorities. The Self sovereign model based on "self- attestation" is not suitable for the acquisition and management of information related to the identity of an individual or company in every situation in which such information must be used by regulated entities, or subject to quality control of the data acquired. There is also an issue of information management - expiry of identity documents, change of telephone users connected to open relationships only as an example - something that the SSI model does not automatically guarantee.

There are a few real-world use cases that indicate the rapid advancement and usage of blockchain for digital identity. However, industry standards for digital identity definitions and its interoperability mechanisms are just evolving, primarily driven by World Wide Web Consortium (W3C), and would need to be finalized to enable holders, issuers, and verifiers to securely transact using digital verifiable credentials.

Self-sovereign also does not mean customers have full rights to verify their own identity. There is still a need to rely on trusted authorities to validate and issue verified credentials. Users must be required to obtain such verified credentials from multiple trusted authorities and store it in a secure wallet on their device before they can transact. The scenario of how users can move their verified credentials from one device wallet to the other or when they lose their trusted device is another challenge.

There is also the important challenge about the right to be forgotten [14]. Though the presented claims are not expected to be persisted by the service provider, there can be several instances where they would want to store user attributes in their own data store for seamless and continued service. For instance, an on-line shopping retailer will require name, address, phone number to deliver an item ordered by the user. Even though they may have obtained this data upon express consent of the user, they may decide to store it in their own datastore for continued service or marketing needs. The data then is outside the self-sovereign identity realm which then breaks the very fundamentals of de-centralized identity and the concept of owning and controlling your own data. When the customer decides to revoke the previously granted claim, all that he has to do is request the claim be removed and forgotten by the service provider. There are no automated processes or standards in place to fulfil this right to be forgotten scenario, which could then lead to data breaches that self-sovereign identity was conceived to address.

Considering the above, in spite the great enthusiasm around SSI with standards rapidly evolving, there is a need to clarify and improve several aspects of it because we are still far away from the ideal world where customers can truly own, control and transact with self-sovereign identity.

In this context comes the eIB project.

[14] European Parlaments "Can distributed ledgers be squared with European data protection law? -Blockchain and the General Data Protection Regulation" July 2019


Figure 5[15]

## Digital Identity in the Nordics

There are already some good examples of digital identity schemes driven by the banking sector that are achieving success:

- BankID, in Norway
- BankID, in Sweden
- NemID, In Denmark
- Finnish Trust Network in Finland

The schemes were introduced initially to provide a common, secure approach to accessing on-line banking services. Now these identity services provide access to millions of users throughout the Nordics, with most of the citizens being regular users.

**BankID Norway** supports a mobile version called MobileID, with secure mobile authentication. According to research, soon after its launch, users were already transacting with MobileID an average of 3.5 times a week.

Indeed, the same research claimed that up to 75% of users would be willing to pay for MobileID, they preferred it so much to the non-mobile solution[16].

**BankID Sweden:** Sweden has a long history of robust federal identity ecosystem

[15] Thales

[16] https://www.gsma.com/identity/wp-content/uploads/2014/02/Case-Study-on-Digital-Identity-Norwegian- Mobile-Bank-ID.pdf

with a general-purpose identification system characterised by a unique ID number in place since 1974. This has allowed administrative frameworks and the broader public to adapt relatively easily to digitisation. The Swedish government opted to pursue a market-based digital ID system rooted in the financial services sector to spur competition between identity service providers, thus facilitating innovation and driving per transaction costs down, creating trusted identity integrations into a greater variety of e-services, and reducing initial implementation costs for the public sector.

First launched in 2003 and managed by a consortium of 10 Swedish banks, BankID is a bank-based identification system. All customers of participating banks are given a digital ID free of charge, which can be used to authenticate transactions across the private and public sector. Companies looking to integrate BankID with their services establish a contract with a bank in the BankID network, which facilitates a direct revenue stream to participating financial institutions. Identity credentials themselves are available in "hard" form—encoded on a smart chip or "soft" form, which is available on a user's personal computer, tablet, or phone.

BankID has integrated next generation identity verification and authentication mechanisms based on behavioural biometrics to minimise reliance on passwords. Six of the country's largest banks also cooperatively launched a common mobile payment app, Swish, in 2012, building on BankID's Swedes between 21-50 years of age have a BankID and 93% of BankID transaction volumes in Sweden are using Mobile[17].


## Focus on the Belgian Experience "eCard" and "itsme"

The eCards include the Belgian Citizen eCard and the Foreigner eCard (referred to as the Belgian eCards). The Belgian eCards satisfy the Level of Assurance 'high' for the context of the eIDAS notification. Municipalities / consulates and embassies are responsible for the enrolment, issuance, and delivery of the eCard.

17 https://www.bankid.com/assets/bankid/stats/2018/statistik-2018-05.pdf

The Federal Authentication Service (FAS) is responsible for authenticating users. The authentication flow between the citizen or foreigner and the FAS, using the eCard, is based on the TLS mutual authentication standard.

During this authentication flow, the internet browser sends the citizen or foreigner authentication certificate to the FAS. The FAS performs the necessary certificate verifications to ensure the integrity, validity and authenticity of the presented TLS client authentication certificate. This certificate can only be used by providing the PIN code, which is known only by the citizen or foreigner holding the eCard. Access to the requested government application is provided after the correct entry of the PIN code, a successful verification of the authentication certificate and completion of the authentication flow.

Today, almost all Belgian citizens and residents have an eCard, which now grants access to a wide range of over 800 eGovernment applications, including Tax-on-Web, social security and eHealth applications, Police-on-web, applications of regional governments, and online portals for municipalities.

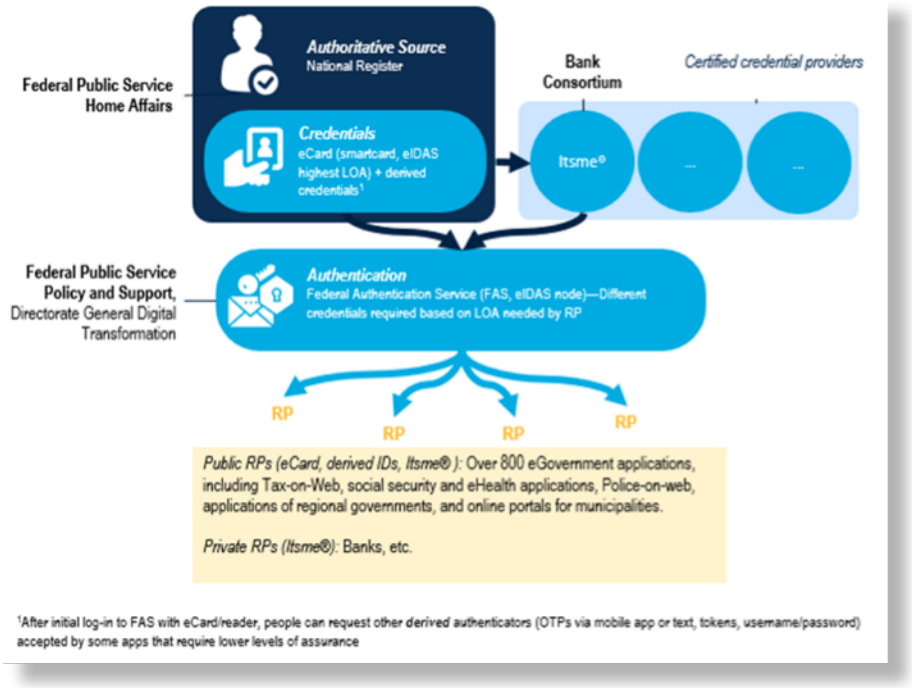



Figure 6[18]

Since January 2018, Belgian citizens have had the option to use a mobile identification means to authenticate themselves on public applications. "ItsMe®" (created by BMID, a private company owned by four major banks and three major telecoms operators) has been recognized by the Belgian government as a valid authentication means, with a Level of Assurance 'high'.

Activation of this service on the mobile device is directly or indirectly bootstrapped with the Belgian eID card, to ensure proof of identity.

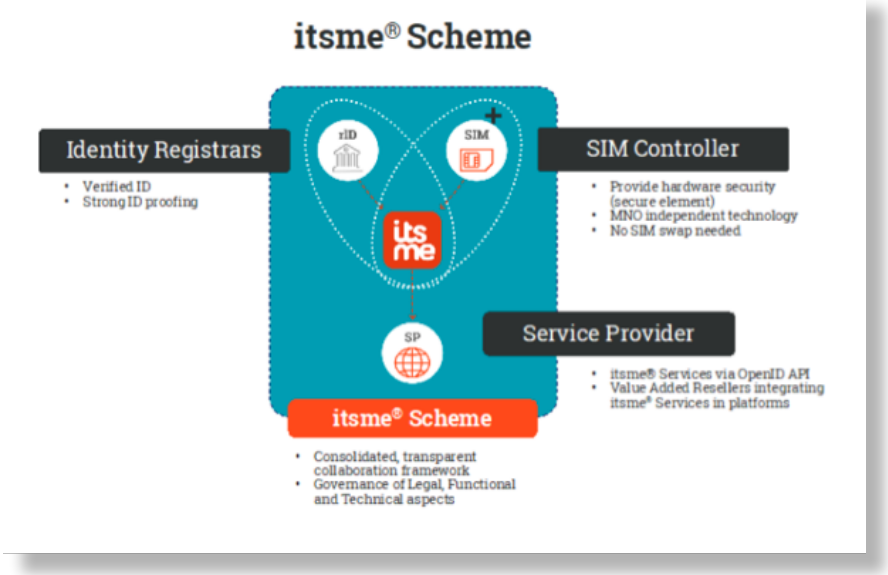
During the itsme® authentication flow, the browser redirects the itsme® users' browser

[18] FATF - Report

to the itsme® login page with the authentication context[19] where it requests the mobile phone number (MSISDN) from the itsme® user. The MSISDN is the unique identifier for this itsme® user, the itsme® app instance as well as the device on which it is installed (1 Unique itsme® user = 1 MSISDN = 1 Device = 1 App). The central itsme® service will request the itsme® app to answer a challenge for which the user enters the correct itsme® PIN (or uses the correct fingerprint if that was configured by the user).

The itsme® PIN is only known to the user. Based on the response received, including the device and/or SIM fingerprint information, the login transaction will be validated and approved.

itsme® has already expanded from usage across banking and government services to be used more widely, with the launch of support for itsme® by service providers in the health and insurance domains, claiming usage figures in 2018 of over 12 transactions per month per user on average, split across banking (50%), government and enterprise usage.




Key characteristics of the itsme success include:

- The smooth user experience offered
- A sound and sustainable commercial plan
- The ensured respect for the regulatory framework
- The technical platform alignment on which Digital IDs are built
- The creation of a strong ecosystem – encompassing close cooperation between market leaders and a common approach to governance

Of significance has been the active support, from the outset, of four major banks. This has delivered the reach and coverage necessary to swiftly establish itsme as a market standard for Digital ID in Belgium. At present, over 50% of all itsme-enabled transactions are in the banking sector, serving to underline the critical role that financial institutions fulfil in the launch of new ID initiatives.

[19] https://merchant.itsme.be/oidc/authorization/phone/confirmation

# Chapter Two eIB

The eIB Project aims at leveraging the potential of combining eIDAS based identification and e-signature technologies (especially remote e-signatures) to fully automate and secure the process of online registration with a bank.

So, its focus lies on developing an appropriate financial digital identity model

To achieve this, the action will develop a business process model for automating the process of opening a new customer and bank account cross – border (OBA c-b) by a user coming from another EU Member State. This business process model will combine the use of eIDAS eID for customer identification and e-signature (based on eSignature DSI DSS) for signing the necessary documents.

Moreover, the eIB project aims at creating a new generation of cross-border e-banking services.

Specifically, the action will create an eIDAS enabled value chain, where Banks and Retail Service Providers (operating in different locations across Europe) collaborate in real-time to unambiguously identify users with high level of assurance, via their eIDAS identifiers, exchange assets and information (KYC) and ultimately offer banking products and automated e-services.

The Project members are Athex (Managing), University of Aegean, National Bank of Greece and ABI Lab with its sub-contractor CBI.

An Industry Monitoring Group (IMG) has been established, under the coordination of ABI Lab, in order to channel the inputs for the feasibility analysis, roadmap and recommendations reports to maximize the eIB project outcomes uptake.

# 5. Financial Digital Identity and Digital Customer Onboarding in the Banking Sector: preliminary results of the survey done in Europe (FR, SP, GR, IT)

On-boarding processes represent one of the most critical aspects that banks must manage, as they directly impact on the user experience and the relationship between banks and customers. Banking customers expect simple, fast and innovative services because the first impression is the most important.

According to an ABI Lab survey on digital onboarding, 43% of the customers that have a negative experience on the onboarding phase are more likely to change bank.

Furthermore, digital customer onboarding plays a key role in automating bank account lifecycle management, leading to improved operational efficiency: it reduces customer cost-to-serve and operational costs, while raising productivity[20].

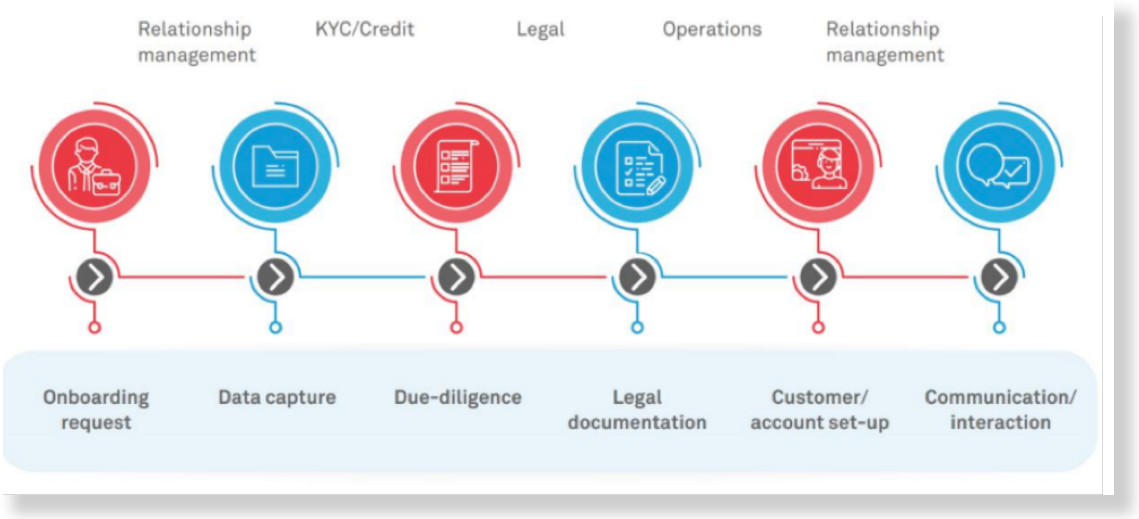



Figure 7: The various stages of a typical customer onboarding process[21]

At the same time, the increase in cyber fraud is requiring greater levels of customer verification and ongoing assurance of a customer's identity. In turn, this is creating further potential barriers to customer acquisition and retention.

In a nutshell, the eIB has two challenges to achieve:

i. Provide a complete end-to-end digital customer application process, allowing the customer to have a frictionless experience for cross border onboarding.

ii. Assure identity to prevent frauds or misuse of the bank accounts eIB started

[20] See: Opening a Bank Account Across Borders with an EU National Digital Identity, at OIX UK-Europe (web ref: https://oixuk.org/opening-a-bank-account-cross-border-id-authentication/)

[21] 13 Wipro, 2019, The future of commercial customer onboarding in banks, available at https://www.wipro.com/content/dam/nexus/en/industries/banking/latest-thinking/the-future-of-commercial-customer-onboarding-in-banks.pdf

analysing the current process of opening a bank account, that typically involves some core processes[22]:

1. Verifying an identity and confirming the link between the applicant and the claimed identity (authentication)
2. Know Your Customer (KYC) and Customer Due Diligence (CDD) processes as a deterrent to protect the banks from being used by criminals for money laundering/terrorist financing activities, and to aid in better understanding their customers and their financial dealings to manage their risks prudently
3. Customer screening against reference data including Sanction and PEP lists
4. Enhanced Due Diligence (EDD) to further investigate applicants where an increased risk is identified
5. Product suitability for the applicant
6. Other data e.g. verified mobile number, location of device
7. Anti-impersonation requirements for non-face-to-face business

In order to understand if there are common datasets and/or procedures between the banks at European level, a relevant survey has been conducted.

The results are still preliminary[23] and will be part of the final eIB report, but a quick summary of them is presented below.

The data collected during digital customer onboarding by the surveyed institutions are of four types:

- core identity data
- KYC data
- other data
- identity and KYC verification data

Requested core identity data always include the identity data included in the eIDAS eID minimum dataset (First Name, Family Name, Date of Birth, Unique Identifier[24]), and other additional personal information like gender, email, phone number, and occupation. KYC data refers to information related to AML or other anti-Financial Crime purposes and vary as KYC processes used by banks are not harmonized at the EU level. KYC data includes information like the purpose of the account, source of funds, and Tax/Fiscal Residence.

Other data refers to various other information gathered during the onboarding process, like the customer's preferred communication channels. Finally, identity and KYC verification data are data required for the verification of the collected PI and KYC information, depending on the relevant mechanisms used, i.e. digital copies of ID documents like a national ID card or passport, pictures, resident permit, proof of address, or a statement from another bank in the EU.

---

22 Oix "Achieving Frictionless Customer Onboarding"

23 A detailed account of the information collected so far can be found in the appendix.

24 National identification number

| Common Core Identity Data | Divergent Core Identity Data |
|---|---|
| Family Name | Gender |
| First Name | Place of Birth |
| Date of Birth | Family Name at Birth |
| Unique Identifier (not for non-residents) | Email |
| Current Address | Occupation |
| Country of Nationality | |
| Country of Residence | |
| Phone Number | |

Just like identity data and KYC processes, authentication and verification mechanisms vary according to bank institution, as each Member State is free to translate the EU provision into local legislation, while also introducing additional checks linked to the cultural context of the country. Verification and authentication processes include uploading identity documents, local eID solutions, video conferencing, biometric identification, selfies taken by the customer using her smartphone's built-in camera device, and bank transfer.

From the above it becomes obvious that the employed concept of financial digital identity is better understood as a system comprised of an aggregate of data belonging to different types of identity (legal, physical, behavioural), and the processes of authentication and verification determining the trustworthiness of this data. Taking into account the common and variant elements of the systems of financial identity used by different bank institutions, eIB aims at suggesting a financial digital identity model that will allow cross-border digital customer onboarding, while being flexible enough to also be used on a national level in those countries which lack a collaborative digital id solution.

This approach is in line with the recommendation made by the KYC Expert WG[25] where the EC "recommends establishing a KYC framework primarily based on attributes, both for customer identification and customer due diligence matters, as a suitable approach for remote onboarding processes in the digital age".

[25] "Assessing portable KYC/CDD solutions in the banking sector" EC, February 2020

# 6. eIB Model Description

The Financial Digital Identity Model proposed by eIB[26] is presented in the following diagram:

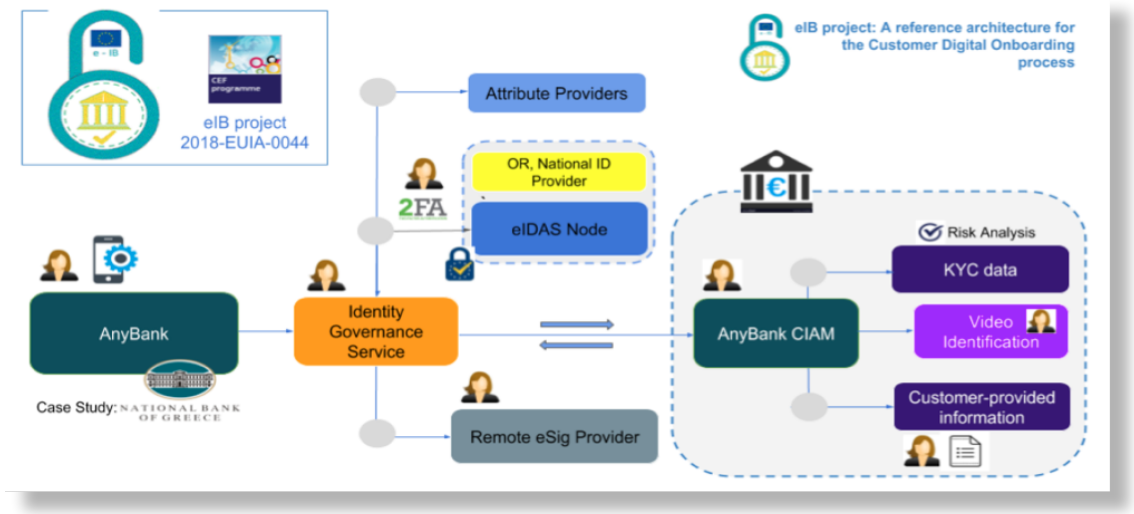



Figure 8

The main components of the model are as follows:

**AnyBank**, representing a generic digital onboarding process which allows cross-border opening of a bank account (i.e. the mobile app offering the possibility of remote account opening that will receive the data of the Customer) - or any other retail bank (in the context of eIB the proposed model was implemented using the National Bank of Greece mobile DCO application).

**Identity Governance Service**, the service connecting AnyBank to the Identity Provider, Attribute Provider(s), and remote e-signatures provider, which will provide digital identity and attribute collection and orchestration services.

**eIDAS Node**, the specific country's eIDAS Proxy Node. The eIDAS node is the connection point to the eIDAS network. eIDAS eID authentication allows cross-border digital account opening.

**National ID provider** provides authentication for a domestic digital account opening.

**2 Factor Authentication Service**, the service providing 2FA to the customer who does not have a credential with substantial or high LoA.

**Remote e-signature provider**, who provides one-time e-signatures to a customer and

[26] eIB D2.1 Opening Cross Border Bank Account with the use of eIDAS and e-signatures Technical Design Report

handles the remote signing of the contract documents necessary for cross-border or domestic digitally opening a bank account

**Attribute Provider(s)**, which corresponds to the organisation in possession of a customer personal attributes (i.e. PII data beyond what is included in a digital identity), supplying these attributes to AnyBank with the customer's consent (for example a provider attesting that a user is a student currently participating in an ERASMUS mobility program).

**AnyBank CIAM (Customer Identity and Access Management)**, the internal AnyBank service which controls the roles and access privileges of individual customers to AnyBank's resources.

**KYC Data** and supporting documents collected during the onboarding application process composing the customer's financial profile. KYC data include legal and risk attributes, together with specific attributes required by AnyBank.

**Video Identification**, or other identity verification mechanism used by AnyBank, verifying the customer's identity (authentication check of the customer's ID document and customer's identity check via a video chat or biometric photos).

**Customer-provided information**, AnyBank performs a risk analysis for opening a bank account to an applicant on the basis the collected KYC data, video identification, and customer-provided information.

The eIB model follows the Federated ID TTP attestation approach, being the best choice - among currently accepted digital identity solutions - for high-touch services; the eIDAS network acts as the Core Identity provider for cross-border account opening, substituted by a National ID Provider for the purposes of digital onboarding addressed to citizens of the specific EU Member State. In this way, a single customer experience covers both cross-border and nationally offered digital customer onboarding, and financial services in general.

But the eIB model's true novelty lies in adding to the Federated ID approach a multi-source identity feature, to deal with the variance of additional identity, KYC and verification data required by different EU banks. This feature allows multiple credentials from multiple providers - connected via an Identity Governance Service - to be shared flexibly and conveniently. In this way a dynamic, service-specific model of financial digital identity is created, and with it a service value network on top of which an eIDAS enabled value chain can be easily realized.

# 7. Implementation Model - Identity Governance Service (IGS)

In the eIB the Identity Governance Service (IGS) will mediate between SPs (banks) and IDPs, with the aim to facilitate the exchange of customers' financial identity data, and their verification.

Banks are de facto FDI (Financial Digital Identity) consumers as Service Providers (e.g. Digital Customer Onboarding), but they are also potential FDI providers or Attribute Authorities[27], and could function as a trusted third party issuer, verifier, or seller of financial identity data (provided they have obtained the consent of the data owner). The high level of trust banks enjoy gives them a competitive advantage in these new markets.

The IGS supports a financial identity model which:

- Is based on the Pan-European Civil DI Infrastructure (eIDAS eID)
- supports a risk-based approach to FDI verification
- holds no customer data, but will dispatch the request of Relying Parties to the right FIDP(s) (Financial Identity Data Provider(s))
- will act as a utility to integrate the Trusted Identity with the KYC data owned by FIDPs
- Can support both B2B and C2B services
- will have no direct relation to the final customers, or if strictly needed the IGS will try to minimize them

The IGS will act as a typical 4 corner Governance Entity Scheme, providing:

- "contract/licence" for the Service participants that will define economics, liabilities and SLAs, avoiding the multi bilateral agreements between RPs and KYC data owners as planned in the CEF project
- Standard "contract/information module" for the Customer using IGS containing GDPR provisions, and other relevant rules, in order to have one easier/shared/ European customer experience

Additionally, the IGS will unify National and EU level digital identification processes.

The IGS should work in a very similar way to a card payment scheme switch, dispatching authorisation requests received by acquirers to the right issuer as illustrated in the following diagram.

[27] Reference to the eSENS pilot (www.esens.eu)

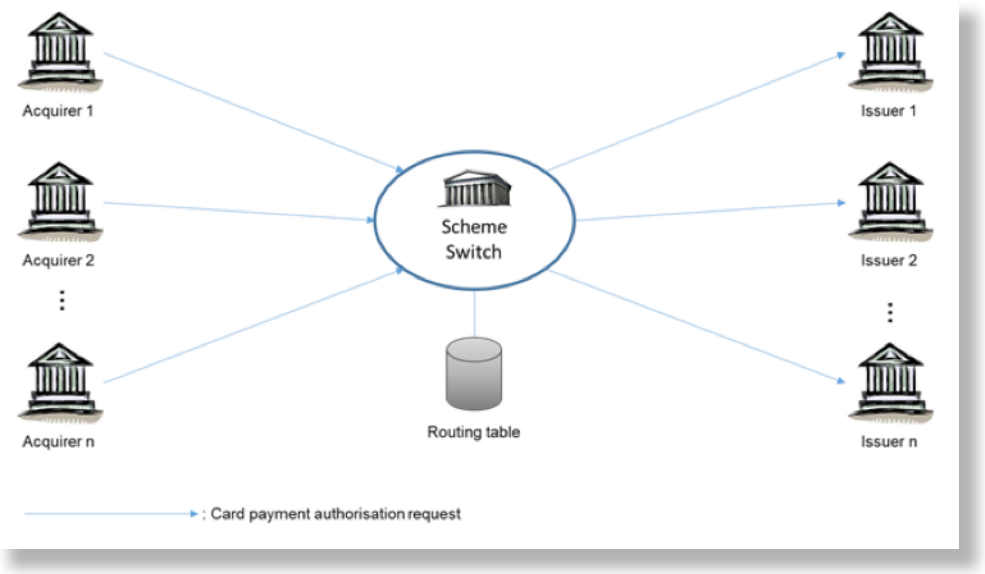



Figure 9

The IGS model is also similar to the Proxy Databases used by the mobile P2P (person to person) and P2B (person to business) services to derive an IBAN using an identification code linked to the mobile user (typically the phone number, but also an email address or car registration plate number).

Instead of having a centralised IGS routing switch, switching information could be made interoperable through a blockchain infrastructure, as in the following diagram:

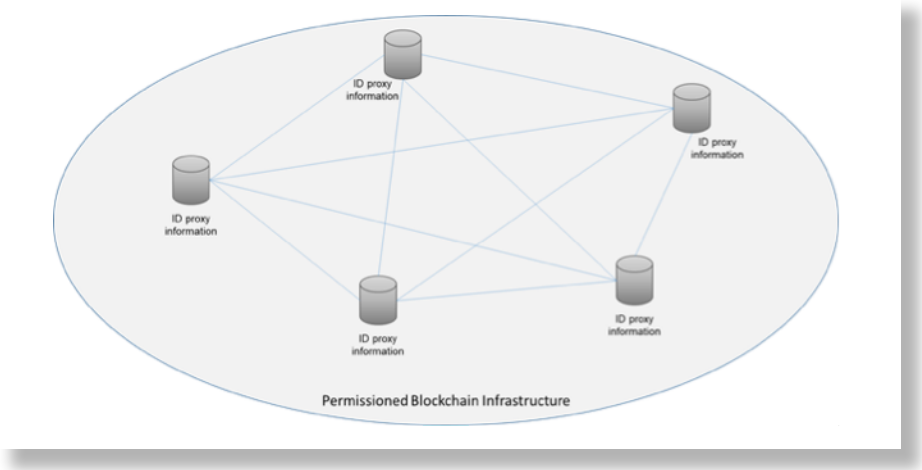



Figure 10

The main advantages of such a solution are an easy implementation with no need to change existing infrastructure, it is enough to interconnect all the ID Proxy functions of the different schemes. That also makes governance easier by defining the common interoperability rules. The technical and organisational impacts are therefore limited to existing ID management schemes.

The IGS role could be played by an already existing infrastructure for the eIDAS infrastructure like an ID Provider.

# 8. The business cases

There is value in allowing a smooth buyer connection.

In the eIB model, the sellers of trustworthy and updated data are creating a market in which many transactions containing small amounts of personal data are shared between organisations at low price points.

Customers will not need to pay for sharing trustworthy identity and personal data.

Today customers self-assert identity and personal data at no cost to themselves (e.g. In the Self assessed models described before).

The onboarding organisation (Relaying Party-RP) then has 2 (costly) alternatives:

1. to validate the personal data in a back office at their own expense
2. or a fraud risk is taken, if possible (certain organisations are not enabled to take risks).

So, we can assume that the relying party would pay for the identity and related attributes if this is cheaper than the current costs previously described.

In our case, this process should reduce a bank's costs of opening a bank account and onboarding a new customer as her Digital Identity will already be verified. This means that the bank can choose not to develop and implement its own identity verification solution, which implies considerable cost reduction.

Relying parties would prefer to contract with a single entity (such as an ID federation hub like the IGS) that addresses all of the required ID data to enable the account to be opened, rather than having to shop around to gather identities and relevant attributes (such as address) from multiple entities.

# 9. Standardising ID APIs: the collaboration with the Berlin Group

The PSD2 has created a framework for open banking.

API standardization is crucial for building a fully-functioning, interoperable open banking ecosystem – and the Berlin Group's NextGenPSD2 Task Force has emerged with the NextGenPSD2 as the leader among several PSD2 API standardization initiatives to create uniform and interoperable communications between banks and TPPs.

The Berlin Group consists of almost forty banks, associations and PSPs from across the EU. The objective is to define open and common scheme- and processor-independent standards in the inter-banking domain between creditor banks (acquirers) and debtor banks (issuer).

To achieve this objective, the Berlin Group has established a pure technical standardisation body, focusing on detailed technical and organisational requirements.

The NextGenPSD2 is no longer focused solely on PSD2 and the banking world: the initiative has been opened up to enable FinTechs, consulting firms and software companies to contribute enhancements.

As eIB eIDAS enabled i-Banking has several common points with PSD2 services, APIs to manage eIB services are likely to be similar to PSD2 Open Banking APIs.

The proposed methodology for a collaboration with the Berlin Group is the following:

The eIB-IMG analyses and defines the use-cases functional requirements of eIB APIs

When the analysis is complete, the eIB-IMG files a change-request with the Berlin Group's NextGenPSD2 TF

The NextGenPSD2 TF, with the participation of eIB-IMG members, designs the APIs specifications

# 10. Application on the e-commerce frauds

According to ECB data, e-commerce fraud is the largest category of fraud in absolute value and the only one to record an increase (of 2.1%) compared to the previous year[28] (Report 2018).

Evidently, this is an area of interest for banks, PSPs, merchants and all the stakeholders in the industry.

Some common specific types of e-commerce fraud affecting the market are:

i. **Clean Fraud**: when a fraudster successfully impersonates the legitimate owner of a payment card, e.g. obtained through a data breach like that in Equifax that affected more than 140 million pieces of customer data). According to a 2019 data threat report[29], more than 14.7 billion data records have been compromised since 2013, many of which included PII.

ii. **Synthetic Identity Theft Fraud**: when a fraudster creates a "synthetic" person by applying for credit cards using legitimate (stolen) identity information and a legitimate (untraceable, like a postal box) address. This "synthetic" person can then make purchases using these fraudulently obtained credit cards

iii. **Triangulation Fraud**: when a fraudster opens a fake online store, and then uses it to sell merchandise purchased with stolen credit cards

iv. **Account Takeover Fraud**: when a fraudster uses the stolen personal information of a bank or online store account holder to fraudulently gain access to the account. The fraudster then uses the account to make purchases the actual account holder did not authorize.

Now we can imagine a situation where:

- eIB is a (FTTP) trusted identity service integrating also KYC information that enables biometric features, in line with SCA requirements
- both the merchant (business) and the cardholder (customer) have an eIB profile

[28] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html

[29] https://www.thalesesecurity.com/2019/data-threat-report

Continue to imagine the customer login to the ecommerce website using the eIB profile (yellow one) as shown in figure 11 below:

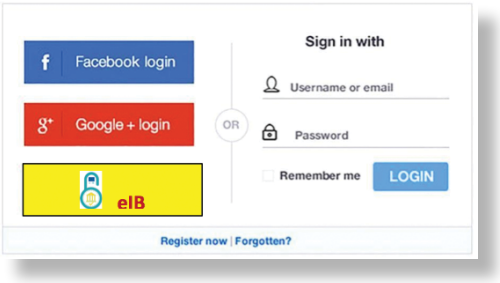
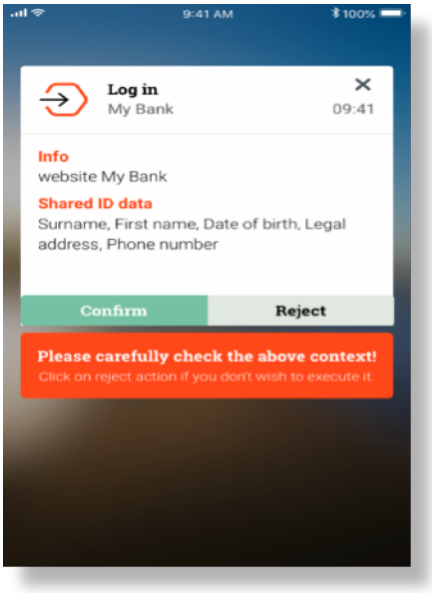



Figure 11

The login information will allow the merchant to know the user identity via their own digital identity issued by a government-authorised entity; at the same time, the customer will be informed where they are accessing (via eIB) with their own Digital Identity and what the data sent to the business/ merchant are. In the image below the customer is accessing to "My Bank" (thanks to itsme for the picture)




When, and if, the customer decides to buy something the payment will be performed via the usual means of payments (e.g. SCTinst, payment card, etc.) with Strong Customer Authentication as requested by the EBA, in a simpler way thanks to the eIB App.

This practise is very welcomed by customers, in fact considering the BankID experience:

> "Only 10 % of our customers still use normal password and username, 90 % of the customer identifies themselves with BankID."[30]

[30] Signicat, "Federated e-IDs" 2020

In such context we are minimizing the fraudsters' chance to continue to work like in the past, in fact:

| Type of Fraud | What eIB could do to prevent fraud |
|---|---|
| Clean Fraud | Via the SCA this type of fraud should be avoidable. |
| Synthetic Identity | To create Synthetic Identity will be much more complicated (if not impossible), because of the FTTP architecture of eIB that will link the customer profile to a Governmental Issued Identity |
| Triangulation | To create a triangulate context (with a fake ecommerce website) will be much more complicated, because of the FTTP architecture of eIB that will allow the customer to know where he is (really) logging in |
| Account takeover | Via the SCA this type of fraud should be avoidable. |

Some application of this methodology is already in place: in 2019, Telia Norway required all new mobile users signing up through their web page, to verify their identity digitally using the Norwegian electronic identity (eID) BankI[31].

To become a customer of Telia, the customer journey is short and simple: the customer types in their existing mobile number and date of birth, and then choses BankID or BankID on Mobile.

Since the launch, Telia Norway has reduced fraud cost by ca. 400K €.

The user experience is simpler than in the past and the steps to become a new mobile customer has been reduced significantly.

Telia has been able to redeploy two full time equivalent people devoted to manually following up and verifying customer data, to tasks that create more value.

Furthermore, although Telia Norway required all new customers to present their digital identity during onboarding, this has not impacted the completion rate, which remains at over 70 %.

[31] https://www.signicat.com/resources/telia-norway-reduced-fraud-with-digital-identity

# 11. The way ahead

For the next months of activity, the eIB will proceed on:

- finalizing a survey on the digital onboarding practises in use at European level for opening a bank account
- to enhance the collaboration with NextGenPSD2 TF in order to propose a European wide standardized approach to the digital onboarding for financial services that will leverage eIDAS
- comparing the FTTP model with the SSI one, in term of technical, regulatory, governance and economic sustainability aspects
- evaluate a possible newer approach combining the FTTP and SSI models

While using blockchain technology (or decentralized storage of data onto a distributed ledger) and issuance of anonymous verified claims is one way of creating an identity management system, there is still a long journey in terms of having concrete examples and measurable results on a large scale level when it comes to the use of this technology in electronic identity programs created or managed by the public sector.

A solution can still be extremely decentralized, function very well and ensure the integrity of data without needing blockchain technology or run as a self-sovereign identity. There is also still a lack of knowledge on the possibilities of blockchain based identity management as there are many different consensus protocols and different types of ledgers one can create with blockchain, which also include permissioned ledgers that might be a better fit for managing identities than public blockchains.

Per se, the use of a blockchain does not remove completely the control from governments or remove the need for initial registration on public databases, it rather eliminates the constant need to interact between the ID providers, the user and the central database, which makes the complete system more secure and more efficient.

DLT makes it possible to create digital identities that can verify and authenticate individuals without having a continuous technical connection to a database of records and operate as a standalone to solve complex identification problems.

However, from a national Government perspective, digital identity management systems really depend on the specific public context and therefore should be technologically agnostic, for several justified reasons: the “trust in the code” approach is also a very narrow way of looking at blockchain.

For the success of a solution, the key source of trust must continue to derive from institutions, the complete digital ID ecosystem or via a reliable public-private partnership.

In the eIB' way ahead, we are evaluating a new approach that consists in combining

the FTTP and the SSI architectures in a way that takes advantage of the special benefits offered by each of them.

The eIB model is flexible and generic enough to accommodate such an approach, a case that will be further explored by the project.

IGS, for example, can function as a proxy verifier in a Financial Digital Identity model following an eIDAS-based SSI architecture. This hybrid architecture and its benefits are described below.

The Self-Sovereign Identity architecture is based on the use of globally unique identifiers (DIDs) which are registered in a DL, and thus not requiring a centralized registration authority (Id Provider or Certification Authority). Instead they are fully controlled by the *DID subjects* - the entities identified by them. DIDs do not contain user information; they point to *DID documents* which are sets of data describing the DID subject, including authentication mechanisms the subject can use to prove her association with the DID (I.e. public keys, pseudonymous biometrics). DIDs and their associated DID documents are created, read, updated, and deactivated on a specific distributed ledger through specific mechanisms called DID methods.

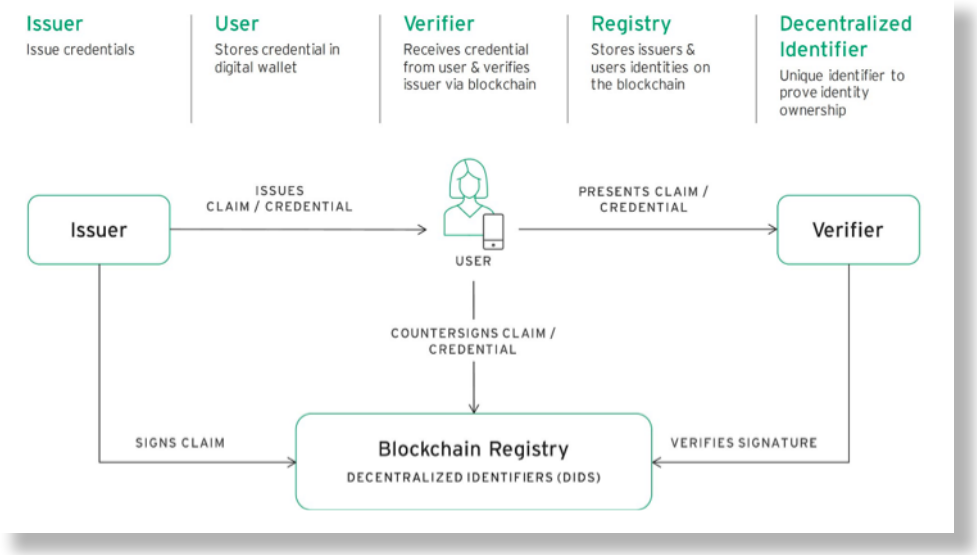



Figure 12

In digital interactions DIDs are used in combination with Verifiable Claims (VCs) to prove to a third-party that the DID subject has ownership of certain attributes or attestations. This proof is based on the cryptographic link between the VC, the corresponding DID subject and the VC issuer, which can be either the DID subject itself (self-attestation), or a third trusted party, like in the case of FTTP attestation models.

In this framework, the verified claims presented by the user are trustworthy to the degree that the issuing authority can be verified. But this trust is built outside of the system through bilateral relationships, trusted lists, or any other means. There is no SSI specification for binding the DIDs with real-world entities. This shortcoming can be addressed using the eIDAS network as a trust base for the SSI model.

Linking the identity provided by an eIDAS eID scheme with the Decentralized Identifier (DID), binds the latter to a real-world entity, to the extent that eIDAS eID authentication

does so. The link can be achieved by adding the eIDAS Minimum Dataset to the Verifiable claims of the DID at the moment of its creation, or at some later time.

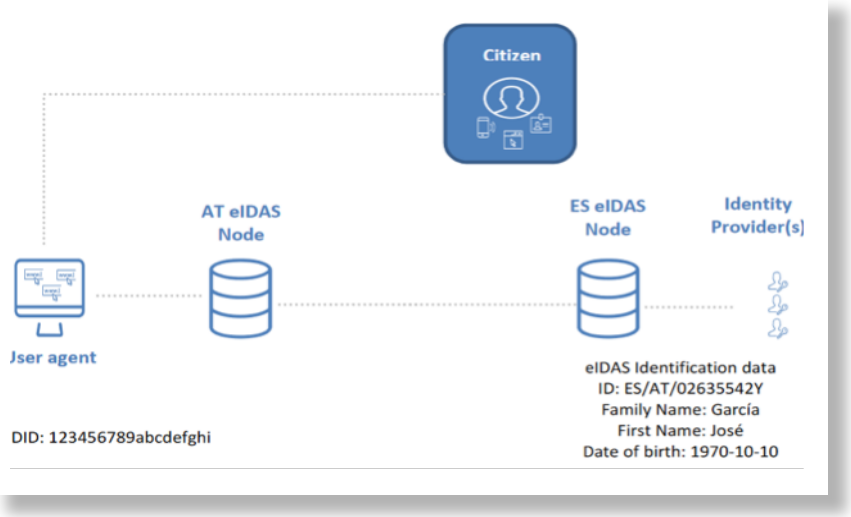



Figure 13[32]

SSI Verifiable Credentials can also be used as an electronic identification means under eIDAS regulation, enabling transactions with the public sector, and with private sector entities, for AML/CFT and other uses[33]. This means that banks could issue KYC VCs to their customers, to be consumed by other Service Providers requiring such data.

The eIB project is studying a (technology independent) public-private sector use case that hopes to gather support from all actors in the identity ecosystem and in helping them to reach the tipping point where identity management systems based on this technology become viable enough to implement.

Cases such as business registries that make it easier to do business and issue licenses (e.g. through a blockchain ledger) are opportunities where the public and private sector can get together to create the strongest business cases.

The DLT technology could also eventually allow a person's identity and authentication to become a standalone and remove the need for multiple federated models to talk to each other, but this can also be done via other solutions (e.g. IGS based on a federated approach or on Open ID Connect infrastructure).

For this reason, we believe that the eIB could be considered "technology independent": eIB is looking to achieve a smarter customer onboarding process for Financial and enhanced services via an enriched Digital Identity (with KYC data) combined with the level of confidence and legal effectiveness given by the eIDAS infrastructure, considering the DLT a tool, and not a goal.

---

32 From eIDAS Observatory: SSI and eIDAS: a vision on how they are connect, available at: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

33 From a presentation by Dr. Ignacio Alamillo on Using SSI Alogned with eIDAS Regulation: Cases of Money-Laundering or Terrorist Financing available at: http://2019.eurofiling.info/wp-content/uploads/2019-06-19_IgnacioAlamillo_Logalty.pdf

# Appendix

## 1. Survey on DCO in European Banks

The survey on the digital customer onboarding processes followed by different European banks, conducted by eIB, has hitherto collected information for Greece, Italy, Spain and France. The tables below show the steps of the relevant processes.

| Steps | Greek Bank Digital Customer Onboarding Process[33] |
|---|---|
| 1 | Open the DCO mobile application |
| 2 | Select "Become an NBG Customer" |
| 3 | Provide phone number and email and verify them (via OTPs sent to phone and email respectively) |
| 4 | Acceptance of Terms and Conditions |
| 5 | Identification by providing personal details, or using an eID provider (redirection to eID provider to authenticate) |
| 6 | IF eID is used: Provide additional personal details (not contained in eID) |
| 7 | Upload tax statement and utility bill |
| 8 | AML step - provide KYC data (financial and occupation data) |
| 9 | Upload proof of occupation |
| 10 | Set credentials for the account access channels |
| 11 | Identity verification - live video session with the bank (show ID document) |
| 12 | Contract signing |
| 13 | Customer could use the bank account |

[34] The Greek bank onboarding process is analyzed in the eIB D2.1 report (see footnote 13 above)

| Category | Greek Bank – Data Collected | Source |
|---|---|---|
| Identity Attributes | Name | Customer or eIDAS eID authentication |
| Identity Attributes | Surname | Customer or eIDAS eID authentication |
| Identity Attributes | Date of Birth | Customer or eIDAS eID authentication |
| Identity Attributes | Country of Nationality | Customer or eIDAS eID authentication |
| Identity Attributes | Unique Identifier | eIDAS eID authentication only |
| Identity Attributes | Level of Assurance of eIDAS attributes | eIDAS eID authentication only |
| Identity Attributes | Father's Name | Customer |
| Identity Attributes | Mother's Name | Customer |
| Identity Attributes | Gender | Customer |
| Identity Attributes | Place of Birth | Customer |
| Identity Attributes | City of Birth | Customer |
| Identity Attributes | Residential Address | Customer |
| Tax Details | Tax ID | tax statement - OCR |
| Tax Details | Annual Income | tax statement - OCR |
| Tax Details | Tax Reference Year | tax statement - OCR |
| Tax Details | Source of Funds | tax statement - OCR |
| Tax Details | Fiscal Residence | tax statement - OCR |
| Financial and Job Data | Additional Financial Data | Customer |
| Financial and Job Data | Occupation | Customer |
| ID Document Attributes | ID/Passport Number | Customer |
| ID Document Attributes | ID/Passport Issuing and Expiration Date | Customer |
| ID Document Attributes | ID/Passport Issuing Country | Customer |
| Document | Tax Statement | Customer |
| Document | Utility Bill | Customer |
| Document | Proof of Occupation | Customer |

| Steps | Italian Bank Digital Customer Onboarding Process |
|---|---|
| 1 | Access the bank's website |
| 2 | Customer needs and product configuration |
| 3 | Access the login screen – New subscriber registration |
| 4 | Provide personal Details |
| 5 | Identification through eID provider (e.g. authentication via token by phone) |
| 6 | Upload Identity document |
| 7 | Fatca step |
| 8 | Privacy step |
| 9 | AML step |
| 10 | Identity verification via video or bank transfer |
| 11 | Contract signing |
| 12 | Bank acceptance of the Contract |
| 13 | Customer could use the bank account |

| Category | Italian Bank - Data Collected | Source |
|---|---|---|
| Identity Attributes | Name | Customer and eID authentication |
| Identity Attributes | Surname | Customer and eID authentication |
| Identity Attributes | Date of Birth | Customer and eID authentication |
| Identity Attributes | Place of Birth | Customer and eID authentication |
| Identity Attributes | Residential Address | Customer and eID authentication |
| Identity Attributes | Mobile phone number (verified with OTP sent to the phone) | Customer |
| Identity Attributes | Email Address | Customer |
| Tax Details | Fiscal Code | Customer |
| Financial and Job Data | Occupation (In the CDD phase) | Customer |
| Document | Identity Document | Customer |

| Category | Spanish Bank – Data Collected | Source |
|---|---|---|
| Identity Attributes | Phone number | customer |
| Identity Attributes | Email address | customer |
| Identity Attributes | Personal Details | Customer and eID authentication |
| Identity Attributes | Residential Address | Customer and eID authentication |

| Steps | French Bank Digital Customer Onboarding Process |
|---|---|
| 1 | Access the bank's website |
| 2 | Select "Open An Account" |
| 3 | Choose account type (individual or joint account) |
| 4 | Choose associated credit card type (gold or classic) |
| 5 | Confirm possession of account in another bank |
| 6 | Identification by providing personal details, or using an eID provider (redirection to eID provider to authenticate) |
| 7 | Provide occupation information with possibility to use an external data provider |
| 8 | Confirm product configuration |
| 9 | Upload RIB[34] (of account in other bank, as confirmed in step 5), Identity, Address, and Income documents |
| 10 | Authentication device registration/enrolment |
| 11 | Contract signing |
| 12 | Bank acceptance of the Contract |
| 13 | Customer could use the bank account |

[35] RIB is a document containing a user's bank account details: name and address of the accountholder, the bank code (5 figures), the sort code (5 figures), the account number (11 figures or letters), the "RIB key" (2 figures between 01 and 97), the name of the bank, the branch and the city, the IBAN (for International Bank Account Number) code,and the BIC (for Bank Identifier Code).

| Category | French Bank – Data Collected | Source |
|---|---|---|
| Identity Attributes | Personal Details | Customer or eID authentication |
| Financial and Job Data | Occupation information | Customer or external data provider |
| Document | Identity document | Customer |
| Document | RIB document | Customer |
| Document | Income document | Customer |
| Document | Proof of Address | Customer |

## 2. Comparison of prominent eID schemes

In a recent Mobey report[36] seven prominent eID schemes[37] are analysed and compared, offering insights to banks on how to leverage the opportunities presented to them in the digital identity market. The report presents - in a set of tables - the similarities and differences of the various schemes regarding their level of collaboration, uses, marketing, monetization, cross-border potential, and technology choices. The following points sum up some of these results:

- There seems to be a strong preference for private sector led initiatives.
- Most of them provide national eID services, lacking any cross-border feature.
- All of them serve the private sector, with the most prominent offering being authentication to e-banking services. Other common uses include identity data sharing, and qualified e-signatures
- The most successful schemes, in terms of adoption by the population, seem to be the ones which have been around longer, except for itsme which has been introduced in 2017 and presents an adoption rate of 80.000 persons per month.
- Branding the scheme as an individual entity is a practice followed by all initiatives
- All schemes rely on service provider fees for support. Monetization of data does not take place under any scheme.
- Challenges to cross-border identification derive from cultural, technological, and mentality differences between different EU Member States, and the sovereign nature of identity (each State wants the Identification service to be accountable locally). The key is understanding the nuance in identity management between countries.
- All schemes have cross-border potential; Interestingly, blockchain-based models are inherently cross-border
- All schemes are based on PKI, or blockchain technology.

[36] https://www.mobeyforum.org/mobey-forum-banks-big-opportunity-in-digital-id-wont-last-forever/

[37] Alastria (Spain), Itsme (Belgium), e-Estonia (Estonia), NemID (Denmark), BankID (Norway), Verimi (Germany), Verified.me (Canada)

## Consortium participants:

ABI Lab

ATHEXGROUP
Όμιλος Χρηματιστηρίου Αθηνών

NATIONAL BANK OF GREECE

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ · UNIVERSITY OF THE AEGEAN ·