SIGNICAT

SIGNICAT INNOPAY REPORT

THE RISE OF DIGITAL IDENTITIES:

Plugging the 'digital gap' in financial services onboarding

THE RISE OF DIGITAL IDENTITIES:

Plugging the 'digital gap' in financial services onboarding

WHITE PAPER – JUNE 2017

The drive towards digital onboarding

For many financial services organizations (FSOs) today, onboarding is an analog process. It can be costly, prone to fraud and create unnecessary friction in the customer's experience. This old approach is simply not sustainable.

As the financial services landscape becomes increasingly competitive, FSOs must attract more customers at lower costs. New entrants challenge incumbents and the race is on to deliver innovations that meet the needs of these increasingly demanding and savvy customers. FSOs are having to find more ways of minimizing costs while maximizing the quality of their offering.

All this is driving a move to digital onboarding for new customers. As a result, digital technologies for identifying customers and assisting the customer due diligence (CDD) process are on the rise across Europe.

Onboarding is an analog process. It can be costly, prone to fraud and create unnecessary friction in the customer's experience. This old approach is simply not sustainable.

A new identity?

A digital identity is "the digital representation of attributes that are used to identify a natural (individual) or legal (company) person." There are many ways a person can identify themselves online with differing levels of assurance. A username and password is perhaps the most common example of attributes that make up a digital identity. Others include a national insurance or social security number. In many cases, the user only provides a username and password, which gives no assurance who the individual is. Often more information is needed and the user must provide some means of proving who they are.

In financial services, there is enormous scope for these digital identities to reduce inefficiencies by providing greater digital assurance in onboarding and for personalized services.

Not only do digital technologies streamline processes but also, they can reduce the regulatory burden. In particular, anti-money laundering (AML) and counter terrorism financing (CTF) requirements across Europe have become more stringent. For FSOs, Know Your Customer requirements (KYC) are more important than ever and they are under increasing pressure to comply. This demands greater confidence in customers' identities and cross-referencing between geographies and organizations – all of which is difficult and time-consuming to achieve manually.

Reducing friction

A digital-first approach is attractive from the customer's perspective. Signicat research shows that 40% of consumers abandon a banking onboarding process, mainly as a result of the time needed to complete the onboarding process or the need to provide too much personal information. Digital identities have the potential to transform this process and Norway is heralded as a prime example of success.

The Norwegian BankID, issued by the banks in Norway, is a means of personal identification and allows banks to authenticate individuals digitally. Some 3.5 million Norwegians have a BankID and the system is used by all the country's banks, as well as the government, insurance companies and the open marketplace. It removes the need for customers to re-enter detailed personal information every time they sign up for a new product, dramatically reducing the likelihood of them abandoning the process before completion.

Joining the dots

As FSOs switch to digital onboarding, they need to call upon a variety of tools to perform the CDD and verify the customer's identity. These include national electronic identity (eID) schemes, various digital assets and traditional ID documents such as passports.

While the theory is robust, in practice there are some major challenges. The information is not always readily available, there are inconsistencies across regions and different stages of onboarding require different levels of assurance.

For digital onboarding to succeed, FSOs must find ways to plug the gaps, ensure they have access to the right information in the right geographies, and deliver the high levels of assurance needed by regulators and customers alike.

Delivering assurance

Digital identities apply at various stages of the customer experience – so it's crucial for FSOs to understand when to enlist the various forms of ID and what it entails.

- **Initial onboarding:** digital identities at this crucial stage reduce friction and can help ensure a positive customer experience. However, most existing applications during initial onboarding offer low levels of assurance, which might limit functionality.

- **Step-up:** FSOs are now stepping beyond the limitations of the initial onboarding processes. Having proved the identity, they are accessing more forms of ID and adding more attributes to the overall digital identity. This provides higher levels of assurance so unlocks greater functionality, benefitting both the FSO and the customer.
- **Preservation:** digital identities remain valuable beyond the initial stages of signing a new customer. Over time, customers' identities expire, documents become invalid and new forms of identity are needed, which could include eIDs, for example. As digital identities degrade, FSOs must rebuild, refresh and reprove them to ensure they stay relevant and restore trust in their level of assurance.

eIDs: the first piece of the puzzle

The eID schemes play an important role in creating digital identities. Regulators themselves are advising that eIDs be used to improve the customer experience and reduce the burden of CDD processes.

On the surface, the regulators, FSOs and customers all seem aligned in terms of their goals. The problem is that eIDs are not uniform throughout Europe and the various countries are at different stages of adoption. Different schemes cater to different needs and require varying degrees of detail. This means that interoperability between schemes is difficult if not impossible to accomplish in their current form. Most eIDs were not intended for onboarding in financial services and most were certainly not intended for use across multiple geographies.

Regulators themselves are advising that eIDs be used to improve the customer experience and reduce the burden of CDD processes.

Signicat commissioned Innopay to analyze and understand this 'digital gap' between eIDs and the onboarding requirements in Europe. Innopay surveyed the onboarding landscape across seven European countries to understand the regulations within each, the eID schemes, and how far removed they are from each other.

Of the 13 eID schemes in Europe, only three provide all of the attributes required for onboarding natural persons and none provide all attributes for legal persons. Even if all attributes are covered, the scheme itself might be redundant because FSOs are unable to apply it in financial services.

In Austria, for example, identification of natural persons based solely on a digital identity is not enough for CDD purposes. The Belgium eID covers all the right attributes needed for onboarding but the scheme is only used in a consumer-to-government context. Meanwhile, in The Netherlands, the private scheme operated by banks falls short of delivering truly digital onboarding because it still requires banks to upload ID paper documents.

Breakdown by country

	EID OVERVIEW	% COVERAGE OF LEGAL REQUIREMENTS	SUITABILITY
Austria	**Bürgerkarte**: a citizen card using a facilitated identity model.	· Natural persons: 100% · Legal persons: 11%	For natural persons, identification solely based on a digital identity is not sufficient for CDD purposes. The scheme contains few attributes needed for the legal persons.
Belgium	**beID**: a government-issued electronic identity card required for all Belgium citizens. The scheme is organized in a facilitated identity model.	· Natural persons: 100% · Legal persons: 20%	For natural persons, all requirements are covered by beID – but the scheme is only used in a consumer-to-government context. For legal persons, the usability of the beID scheme is very limited.
Germany	**Personalausweis**: an official identification document with electronic data. It is organized as a facilitated identity model, operated by the Government. **Giropay-ID**: a private identity solution, operated by banks, which operates as a operated as a trust framework model.	· Der Personalausweis · Natural persons: 71% · Legal persons: 0% · Giropay-ID · Natural persons: 29% · Legal persons: 0%	For natural persons, Giropay-ID has limited potential but Personalausweis contains almost all attributes needed. There is no digital identity scheme for legal persons.
Luxembourg	**LuxTrust**: a privately-owned digital identity scheme, which is a (three-party) platform model. **Carte d'Identité Luxembourgeoise**: a public digital identity scheme developed by the Government, operated as a facilitated identity model.	· LuxTrust · Natural persons: 67% · Legal persons: 88% · Carte d'Identité Luxembourgeoise · Natural persons: 50% · Legal persons: 0%	For natural persons, LuxTrust is more suitable since it has greater coverage. For legal persons, only the LuxTrust scheme applies.

Breakdown by country

	EID OVERVIEW	% COVERAGE OF LEGAL REQUIREMENTS	SUITABILITY
The Netherlands	**digiD**: A scheme for accessing government services **Idensys**: a pilot scheme by the Government based on the trust framework model. **iDIN**: a new private identity scheme operated by banks. **EHerkenning**: intended for use by legal persons.	· digiD · Natural persons: 80% · Legal persons: 0% · Idensys · Natural persons: 80% · Legal persons: 0% · iDIN · Natural persons: 80% · Legal persons: 0% · EHerkenning · Natural persons: 0% · Legal persons: 80%	DigiD cannot be used for CDD purposes; Idensys and iDIN provide all the attributes necessary but with differing levels of assurance – and the sole use of a digital identity for verification purposes is not sufficient to meet KYC requirements in FS. For legal persons, the EHerkenning scheme can provide several attributes during a digital on-boarding procedure.
Switzerland	**SuisseID**: a national ID scheme using a facilitated identity model. **SWITCH Edu-ID**: an identity scheme which applies to educational institutions.	· SuisseID · Natural persons: 80% · Legal persons: 40% · SWITCH Edu-ID · Natural persons: 60% · Legal persons: 0%	SuisseID and SWITCH are suitable for CDD purposes but neither can provide all the information needed for natural persons. SuisseID is hardly useable for legal persons. It can be used to verify that a certain natural person represents that company. A specific scheme designed for legal persons is not available in Switzerland.
United Kingdom	**Gov.UK Verify:** a digital identity scheme, using a trust framework model, for accessing government services.	· Natural persons: 100% · Legal persons: 50%	Digital identities can support the CDD process but UK regulation requires additional verifications measures be performed in case the customer is not physically present.

Finding the missing pieces

The reality is that existing eID schemes were not designed for FSOs to use for complete onboarding. They are mostly non-bank schemes and there are clear disparities between these and the KYC requirements across Europe. They do, however, provide a starting point, from which FSOs can build a trusted identity. To do this, FSOs need to source the other vital pieces of the puzzle:

- **ID documents:** passport, driving license and social security number are just some of the existing, more traditional forms of ID. They are established and trusted forms of identification so are an important part of the overall picture. The challenge is that they can create friction in the onboarding process because End users must first find them then register them digitally.
- **Registry lookups:** FSOs can use registry lookups to verify a customer's identity, including postal address, utility data or credit information. The challenge is that there are multiple sources for this information, such as the electoral roll, credit reference agencies or central government registers, not all customers will be listed and some customers might be listed several times with differing or out-of-date details. Indeed, most of these registers were originally created for human lookup, before even the idea of APIs, and therefore are difficult to search.
- **Other digital assets:** there are a seeming endless variety of digital assets relating to any one customer. These include digital 'selfies', social media profiles and content, and SMS one-time-passwords (OTP). They all provide some information and assurance of a customer's identity. However, individually, they fail to provide any depth of insight or high level of assurance.

The reality is that existing eID schemes were not designed for FSOs to use for complete onboarding. They do, however, provide a starting point, from which FSOs can build a trusted identity.

The eIDAS: another cross-border solution?

The eIDAS is an EU regulation on eIDs and services in Europe and, in part, aims to standardize eIDs in the single European market. Today, if Austrians (who only need four identity "elements" for a government eID) wanted to open a bank account in Germany (eight elements), they would quickly find they need further paper-based checks. According to eIDAS, an eID which is issued by one country (at a given assurance level: low, substantial or high) shall be recognized by other countries. That doesn't guarantee AML compliance in the short-term but does deliver a more flexible, interoperable approach for onboarding in general.

There is one major problem. As of today, eIDAS is only for government-to-consumer services. It is uncertain when or if it will become available for businesses but there is some hope. The Law Society has endorsed business-to-business use of eIDs and the European Commission also stated:

> *"Indeed, rolling out eIDAS means higher security and more convenience for any online activity such submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another Member State, authenticating for internet payments, bidding to online call for tender, etc."*

As of today, eIDAS is only for government-to-consumer services.

A combined strength

Each part of the puzzle, whether an eID, a passport or a social media profile, is valuable. However, on its own it has limited use in the onboarding process. The real strength lies in combining the various assets to create a complete and validated digital identity.

Different scenarios will require different combinations. Therefore, the true efficiencies are in understanding how and when to use different combinations. This will depend on several factors, including:

- **Geography:** each region has different requirements. These include local KYC and AML interpretations as well as national eID schemes and other forms of identification. Much of this will not easily transfer for use in other territories.
- **Market:** financial services, government-based schemes and health services all need varying levels and types of authentication. Again, these might not interoperate easily. For FSOs, for example, a government-based eID scheme won't be sufficient but it could be a crucial starting point.
- **Level of assurance:** various services, stages of onboarding, geographies and regulations all demand different levels of assurance. What's important is that FSOs can satisfy all levels up to the highest.
- **Risk-level:** certain customer transactions are less risky to an FSO than others. A purchase using a contactless card, for example, will require lower levels of assurance than taking out a mortgage.
- **Regulations:** the European Anti-Money Laundering Directive (AMLD) includes specific requirements around CDD, including rules for when to apply 'simplified due diligence' (SDD) and 'enhanced due diligence' (EDD). The latest update to the directive removes customer absent cases from the high-risk category, meaning FSOs can apply SDD in most cases of digital onboarding. What's encouraging is that this all paves the way for greater adoption of digital identities. However, the challenge is that each national interpretation differs and there is no one form of identification to satisfy all requirements.

Harnessing support

This is a fragmented landscape. Digital identities rely on FSOs being able to navigate a complex array of ID schemes, regulations and digital assets. Often, they need specialist support in order to access all this information and reduce the complexity. As such, many are working with a digital identity services provider (DISP) to help join the dots.

A DISP makes it easier for organizations performing the onboarding to connect to different schemes and source all aspects of the identity puzzle. It does this by facilitating connections with various platform models, trusted frameworks and other verification networks through one single technical interface.

To ensure success, a DISP must be country-aware and collect user information in accordance with each country's specific requirements in order to provide a robust and truly cross-border solution.

Realizing the full potential of digital identities

Partnering with DISPs is the most effective way for FSOs to take full advantage of the current landscape for onboarding. They can facilitate interoperability and connectivity in a fragmented European market and build a complete and trusted picture of the customer.

FSOs can meet the regulatory requirements but, perhaps more importantly, they can establish a digital relationship with the customer from the outset. In a post-PSD2 landscape, efficient onboarding will be particularly crucial. FSOs will need to create new services to capitalize on the new mandate and their success will rely on an effective process for new customers to sign up.

Complete digital identities are central to not just ensuring compliance in a complex regulatory landscape but also enabling FSO's digital transformation. However, not all FSOs will be able to move at the same pace – so those that can step ahead and deliver a superior onboarding experience today will be in the best position to win greater customer loyalty tomorrow.

Incumbents won't necessarily have the advantage either. Instead, efficient use of resources, greater innovation and strategic partnerships with the likes of DISPs will be the important factors in the next leg of the digital race.

To find out more about moving to digital onboarding, or to read the full research paper, "Possibilities of meeting AML and KYC requirements using digital identities" please **GET IN TOUCH.**