OPEN IDENTITY EXCHANGE
White Paper

OPENING A BANK ACCOUNT CROSS BORDERS WITH A DIGITAL ID

Pre-Discovery - Market Intelligence report

By Harry Weber-Brown
(Project Coordinator)

Co-financed by the European Union
Connecting Europe Facility

Background

HSBC, Barclays, Government Digital Service, OT-Morpho, Orange and OIX UK have formed a Consortium to deliver a digital identity project[1]that will develop and test a prototype to enable an EU citizen to open a bank account in another European country using their national digital identity. It will build the service design and operational framework and will deliver a business case for the development of the fully operational service that will enable a more trustworthy and efficient account opening process for EU citizens across Member States.

The project is specifically focused on the use case of a French citizen wishing to open a bank account in the UK prior to moving into the country.

The project has been awarded a grant by the European Commission's Innovation and Networks Executive Agency (INEA), under the Connecting Europe Facility programme[2] and will provide a strong authentication process by leveraging Mobile Con[3]nect and validating the citizen's digital identity, across Member States, via the eIDAS[4] framework.

As part of the pre-discovery phase, the Consortium agreed to research and report on related projects and initiatives to understand the range of findings, data and use cases available, regarding the opening of a bank account in an overseas jurisdiction; the primary focus is within the European Community. This report captures this and this project will utilise the findings from similar projects in order to avoid any potential duplication.

Executive Summary

This CEF funded project will help deliver the European Commission's *Consumer Financial Services Action Plan*[5], which aims to increase consumer choice in financial services across Member States. This is will achieved by enabling remote customer identification so making it easier for banks to check customer identities by utilising digital technologies and the existing building blocks of the eIDAS framework.

This project is building on other OIX projects (including the Alpha Project on *Opening a Bank Account in another EU Country*[6] and the BBA PwC commissioned report[7]), both of which

[1] http://bit.ly/2hrpwjU

[2] For more details https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom

[3] https://mobileconnect.io

[4] eiDAS is an EU regulation and sets the standards for electronic identification and trust services for transactions in the European Single Market.

[5] http://bit.ly/2s6cgSk

[6] http://bit.ly/2w9rQ25

established that federated digital identities can enable the bank account opening process, however additional data elements are required.

There are a broad range of complementary initiatives within Europe with similar aims to this project and which are financially supported by the European Commission. These include the CEF funded *Everis* project and the H2020 funded research project awarded to *Signicat*; these both aim to define the digital building blocks required to deliver bank account opening capability across Member States by EU citizens, so supporting the Digital Single Market[8].

Although none are identical in their ambitions, there are key areas for alignment, coordination and shared learnings, which will be delivered through a programme of workshops and stakeholder management, as the projects develop.

Evidence of robust user testing is limited. Some of the existing OIX projects undertook user testing using workshops and a qualitative laboratory based approach with a modest number of test candidates; this digital identity project intends to adopt a quantitative approach to reach a larger cohort of users and track their behaviour to enable rigorous assessment of demand and take up of such services, as well being able to refine the customer experience of the account opening process through a digital channel.

The project and initiatives activities below clearly support the case for developing the capability for cross-border bank account opening using national digital identities, which is key pillar of the European Commission's *Consumer Financial Services Action Plan*. The benefits to financial institutions are well documented in the *World Economic Forum* report and the customer and organisational benefits of using Government approved digital identities, are presented in the final reports for the OIX projects detailed below.

However, none of the projects and initiatives have attempted to deliver detailed forecasting on the savings or additional income that could be generated by banks, from the use of digital identities in account opening and on-boarding. The STORK 2.0 e-Banking pilot report presents one bank's estimated cost savings; this is a key area that will be addressed in the business case for the operational service and will help motivate the broader financial sector to utilise the outcomes of this project.

The STORK 2.0 eBanking pilot highlights many of the questions that need answering, when developing a commercial model (including the need for a cost:benefit ratio to determine the value to service providers), however it does not detail how relationships would operate in a commercial environment.

Pilot studies have attempted to deliver cross border bank account opening with limited success; the exception being *Zveza* (Austria) from the STORK 2.0 pilot. The final report details a broad range of issues that need to be overcome in the development and delivery of cross border bank account opening capability, many of which this project will address with proposed solutions.

[7] http://bit.ly/2uZHkXP

[8] http://bit.ly/2nhiFL1

The Estonian e-Residency[9] programme promotes the Holvi[10] business current account, which can be opened remotely and relies on the applicant having an Estonian e-Residency ID card and a business registered in Estonia; the full registration and opening process can be achieved remotely through digital channels. Although the Holvi account service is defined as a payment institution (under the Finnish regulations), as opposed to a Bank, it does have similar KYC checks as required by banks.

Specific projects and pilots have highlighted the need for clarity around the liability model. Legal issues are well documented in the STORK 2.0 report, as these constrained the project. There isn’t clear guidance on how these should be approached; which is a key objective of this project.

The need for technical interoperability is highlighted through different research projects, with eIDAS delivering the national identity authentication between notified Member States, however additional components need to be developed to enable full opening process and banks’ approaches to assessing new customers is based on risk as opposed to standards; this is highlighted in the OIX projects below. There is also a need to check the interoperability of eIDAS, in the mobile environment, through Mobile Connect.

There is a need to maintain stakeholder involvement across the various projects and take critical learnings from other large scale projects that have attempted to address cross-border banking (such as the STORK 2.0 pan-European e-Banking Pilot).

As the project progresses, it is recommended that this Pre-Discovery report is continuously updated as other ‘live’ projects develop and new projects and initiatives are identified. Key stakeholders have been identified from the other projects and these will form part of the stakeholder management programme.

Pre-Discovery Report

The following project and initiatives were identified as potentially having information that would be useful for this project, as they cover issues relating to cross-border bank account opening and digital identities.

Projects/Initiatives included are:

- EC Consumer Financial Services Action Plan
- Everis (CEF funded) project on eID Solution Architecture for Banking and University Education Domains
- Stork 2.0 e-Banking pilot (pan-Europe)
- Signicat (Horizon 2020 funded)
- GSMA Mobile Connect pilot (eIDAS interoperability)
- TISA ID pilot
- Signicat (Horizon 2020)
- World Economic Forum: *A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity*

[9] http://bit.ly/2rZwPCC

[10] http://bit.ly/2vlor2C

- Norwegian Bank ID papers (OIX projects)
- BBA PWC paper
- Estonian e-Residency/Holvi

Title: EC Consumer Financial Services Action Plan

As only 7% of consumers, living within a European Union Member State, currently buy financial services from another Member State, the European Commission has developed and published an Action Plan (March 2017) that aims to achieve three core objectives, which are:

1. Provide more consumer choice and trust
2. Remove cross-border obstacles for business
3. Harness digital technologies to increase choice and remove trust obstacles for businesses and consumers

The Action Plan states: "*The use of electronic identity schemes, as set out in eIDAS, would make it possible to open a bank account on-line while meeting the strong requirements for customer identity proofing and verification for know-your-customer or customer due diligence purposes,"*

The Action Plan aims to achieve its objectives by delivering:

- Remote customer identification to make it easier for banks to check customer identities remotely.
- Greater transparency on currency conversion fees.
- Easier product switching and consumer credit.
- Better car insurance conditions for consumers.

As digital ID solutions are developed within the EU, the Commission is setting up an expert group to "develop common guidelines" to ensure the tools "are safe and secure and do not introduce new risks to consumers or the system and comply with EU data protection laws". The group will comprise regulators, supervisors, financial institutions and the existing group of identity experts from Member States.

Description of the Action Plan

For the Remote Customer Identification work strand, the Action Plan has spawned funded projects, through the INEA funding instruments (including this CEF funded project and another outlined below delivered by *Everis*) that are assessing and defining the required technical architecture to enable the banking industry to utilise the eIDAS framework for remote identity authentication and customer due diligence across the EU.

The Commission is also developing an implementation plan to develop a specific e-Banking building block that will meet the requirements of remote identification of bank customers.

Key findings

These are contained within the individual projects, funded by the INEA funding instruments, rather than in the Action Plan.

What are the outcomes?

One of the key proposed outcomes of the Action Plan is the Commission will make it easier for firms to get credit information about potential customers living in other EU countries. This will be achieved by developing common criteria to assess consumers' creditworthiness and define a minimum set of data to be exchanged between national credit registers.

Points to consider and references

The findings from this project will feed in to the implementation plan (outlined above) Action Plan.

Action Plan summary:

https://ec.europa.eu/info/sites/info/files/factsheet-consumer-financial-services-action-plan-23032017_en.pdf

Full Action Plan:

http://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0003.02/DOC_1&format=PDF

Title: Study on eID Solution Architecture for Banking and University Education Domains

Participants: Everis (part of NTT Data), banks and universities across the European Union.

Description

Everis (Belgium) has been awarded a CEF grant to investigate the requirements for developing eID Building Blocks for the banking and educational sectors, which complements the work being undertaken in *"eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the European Union"*. [11]

The objective of the study is to integrate eID in eBanking and eStudent services, across Member States. This is a 12 month project that commenced in March 2017.

Key findings

The project has completed its Discovery Phase, which investigated the technical and legal issues regarding eIDAS.

As of August 2017, it is in the Knowledge Phase, which involves defining the scenarios that would build value of eIDAS and proposing a solution that will make it easier to use eIDs for cross-border banking and for students wishing to study at another university in a different member state. There aren't any key findings at the time of preparing this report, however it will be updated as the project progresses.

[11] http://bit.ly/2wraX27

What are the outcomes?

The outcome of this project will be a report detailing a high-level and aspirational view of the required architecture that will utilise the existing eID building blocks and integrate these with digital services used in the higher education sector (e.g. universities) and online banking systems for customer on-boarding across EU Member States.

It will propose an implementation plan including timings, estimated costs, resources and a roadmap to make the solution a reality with recommendations on how move to live environment.

Contacts:
Alice Vasilescu (alice.vasilescu@ec.europa.eu)
Mario Cabellos: mario.cabellos@everis.com

Title: Stork 2 e-Banking Pilot

Participants: this Pilot was implemented (2012-15) by a large consortium of 58 participating partners (included banks and financial institutions) from across 19 European countries within the European Community. The countries most actively involved included: Austria, Greece, Iceland, Italy, Portugal and Slovenia. The UK involvement was limited and no UK bank was actively involved in the pilot.

Description

The e-Banking pilot attempted to integrate the STORK 2.0 cross-border authentication infrastructure into existing e-Banking services to allow citizens to use their electronic IDs to enable cross-border bank account opening and accessing bank services.

It was a three-year European Large Scale Pilot project that aimed to extend eID interoperability and help convergence of eID in both the public and private sectors, including the secure transfer of extended identity attributes and the opening of eID-based operations for authorised legal representatives.

The Pilot had 3 explicit aims, that were:

- Establish a range of cross-border online banking services utilising national eIDs and broadening eID acceptance within the EU.
- Enable businesses and citizens to open a bank account across borders, use online services and electronic management of mandates across European member states.
- Increase transparency and security in cross-border banking by including further identity attributes.

Key findings

The pilot had limited opportunity to engage real external users and integrate the front-end applications into ‘live’ banking services, so the majority of pilots were limited to demo accounts to closed groups of users, due to legal reasons or the decision of banks.

Many users involved in the tests had difficulty in authenticating their identities for different reasons including forgotten PIN numbers, not having high enough quality assurance for the eID and Member State infrastructure certificates expiring so stopping the cross-border authentication.

The pilot did, however, generate a significant amount of learning for the stakeholders and raised issues that need to be addressed, including in the areas of liability, usability, support, security, long-term operations, pricing and legal constraints regarding cross-border opening of a bank account.

Relevant key findings are detailed below:

Standards/Contractual/Liability models

The final report stated that there is a need for an organisational and contractual framework, which should regulate the terms & conditions and service levels between the different parties involved in building and delivering cross-border bank account opening.

The pilot identified a range of liability issues regarding the process chain, organisational constraints, security of the infrastructure and the need for a liability model that underpins the exchange of digital identity data. The pilot report suggested that the eIDAS regulations could help define the liability model (under Article 11 Recital 18 of the regulation), however this liability coverage does not extend to private sector usage of the Digital Service Infrastructure and eIDs.

The pilot highlighted a range of security issues such as banks to require Service Level Agreements, if they are relying on third party data and services. This may preclude some banks from connecting their infrastructure to open source solutions, which could prevent the pilot from using real bank accounts in selected countries. Banks also work to certain Standard Certifications (such as PCI-DSS, ISO27001 and ISO20000), which may be required for any technology to be integrated into their core–systems.

Technical Interoperability

The final pilot report stated that any third party infrastructure or building blocks need to be stable and rigorously tested before Banks will connect such into their infrastructure. During the pilot, the STORK infrastructure was evolving, which made it difficult for banks to rely on it. Also, for any integration to occur, there needs to be a clear testing procedure and conformance guidelines that would be mandatory to pass in an assurance audit.

Private sector usage

The pilot highlighted that eIDAS does not address the legal acceptance of eIDs in the private sector as the scope of the mutual recognition obligation is limited to public sector usage. Although access to electronic identification and authentication, through national eID schemes, means that it is possible for private sector organisations to use eIDAS, it remains subject to specific access terms (including pricing) defined by the notifying Member States.

Commercial model

The pilot didn’t provide detailed savings or increased revenues that banks could generate by using eIDs for account opening and on-boarding. The final report did quote SIBS (in Portugal) who estimated that banks might reduce operational costs by 50%, through utilising STORK 2.0 eIDs in the opening of a bank account and subsequent on-boarding; however additional work is required to accurately estimate cost savings, which may vary considerably between banks.

The pilot delivered attributes free of charge, so there is no knowledge to be gained on the likely commercial model of attribute provision. It also highlighted that attributes will have different values to different service providers in different countries; these need to be competitively priced and be less expensive than other channels (such as in-branch) to drive usage of eIDs. It stated that Banks require certainty in pricing models.

A key recommendation was that national eID schemes should advertise their services (that rely on eIDs) to drive eID registration, which would motivate the private sector to build services using eIDs.

Attributes

The pilot report recommended that attributes should be collected through a singular transaction, with broad range of consents provided, as opposed to being collated on a case-by-case basis. The report proposed developing a central contracting body responsible for managing and issuing attributes, and managing the relationships amongst different attribute suppliers.

It recommended the need for a simplified model to kick start the market. It also highlighted that the quality of attributes obtained from other sources may not be as trustworthy, or of the same data quality, as those delivered and assured by the Member States national identity schemes.

Despite that fact that the pilot was focused on cross-border bank account opening, it did recommend that eIDs should be available for opening domestic bank accounts, as banks' primary interests are still on their domestic markets.

What were the outcomes?

The pilot developed a simple, transparent and cross-border operational means to allow citizens and businesses to open a bank account in another EU Member State. It involved mapping all the different processes and different legal requirements in the Member States participating in the pilot; this included defining the process flows, data structures and requirements for each Member State.

The mapping of the processes enabled participants to build front-end applications for opening bank accounts, logging in to bank accounts and for cross-border e-Invoicing. These could then be integrated into demonstration services or the live services of the banks.

The pilot provided the first cross-border bank opening, utilising eID and a digitally signed KYC, however only one bank managed to build and deploy STORK 2.0 eID within its operational bank account opening process for cross-border identity authentication; this was Zveza in Austria. The test service was offered to Italian, Slovenian and Austrian Customers.

Other participating banks were hampered from integrating 'live' cross-border services by a variety of issues including differing national legislations in respect to the acceptance of electronic identities, some banks were unable to accept e-Signatures, bank policy requiring the physical presence of the customer, and internal technical skills.

Points to consider and references

Digital signatures and the trusted attribute provisioning provided the most value to the banks, however few countries had deployed any PDF signature creation solution in their production infrastructure. They recommend DocuSIGN.

The scalability and service extensibility are also crucial issues to consider.

The report identifies specific banks, who are progressing with building cross-border capabilities, which would be useful to involve in developing the business case for this project and for take-up across Member States.

See **https://www.eid-stork2.eu/pilots/ebanking/index.php/en/**

The Final Report can be obtained from the INEA (European Commission).

Title: Signicat - pan-European Identity Assurance hub

Participants: Signicat (H2020 awarded grant) and Innopay (commissioned research) and a range of national eID schemes.

Description: This is a Horizon 2020 funded project whose purpose is to scope a simplified and cost effective online service for identity assurance that can be used in regulated industries, such as financial institutions across Europe.

This is a two phased project:

- Phase 1 (October 2016 to May 2017) investigated how eIDs are currently used to onboard consumers to financial services across seven pre-selected European countries which were Austria, Belgium, Germany, Luxembourg, the Netherlands, Switzerland and the UK.
- Phase II (subject to H2020 official announcement) will be the implementation of a revised business plan based on the findings, with available funding reaching an amount quoted as €200m[12].

Key findings

For Phase 1, Innopay were commissioned to deliver a report (entitled; *The Rise of Digital Identities*[13]) that investigated the legal onboarding requirements and compliance with KYC and AML, then mapped the eID schemes to these requirements. While current schemes do cover

[12] http://bit.ly/2iueDwn

[13] http://bit.ly/2v2oOhC

the majority of information needed by financial institutions to confirm a prospective customer's identity, gaps exist.

It reported that when conducting onboarding, the required information is not always available, there are inconsistencies across countries with different attributes required at different stages of onboarding; these also may have different levels of assurance as required by the regulators.

As customers' identities expire documents become invalid, banks may have duplicate listings and new forms of identity are needed, which could include eIDs, for example. The research recommends that financial organisations need to maintain and update their customers' identity details and attributes on a regular basis, to ensure that they are reusable and can deliver the requisite level of assurance. The research also highlighted that the European national e-Identity schemes differ, with regards to needs and interoperability with the private sector, and are at varying stages of adoption.

What are the outcomes?

Signicat aim to develop a comprehensive platform for a connected identity hub, with "complex integrations to be centralised." The firm wants to let European banks integrate with its hub, accessed through a single API, which is connected to all authorised national schemes.

The research suggests that the national eID schemes are at the starting point on which to build a trusted identity and can be the key foundation for a full on-boarding of new customers of financial products. It states that eIDAS, with its mutual recognition of citizen's identities across EU borders, is useful for banks to collate the data required for onboarding, especially being AML compliant, however there is still much disparity across Member States in the requirements of varying levels of identity elements for authentication.

The research recommends combining identity elements to deliver a validated identity with connections to multiple sources and trusted frameworks; this would be through a single technical interface for cross border identity verification, defined as *Identity as a Service*, which Signicat could deliver.

Points to consider and references

More information and the report can be requested at: https://www.signicat.com/press-release/research-innopay/

Title: World Economic Forum: *A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity (August, 2016)*

Participants: World Economic Forum and Deloitte with a large range of stakeholders across the financial services sector, innovation community, technology organisations, academia and the public sector.

Description of the Project

This research project (2016) explored the potential use of digital identity for financial services (across different products) and proposes a blueprint for the implementation of an effective digital identity system. It offers a detailed exploration of digital identity and its importance to financial services, and scans the landscape of current efforts to build digital identity solutions.

It provides recommendations on the roles that financial institutions should play in building a global standard for digital identity, however it does **not** focus on the creation of the actual standards around identity. It is a useful guide on the structure of identity and calls for action by financial institutions to build a transformational digital identity system, as it claims current identity systems are hampering innovation.

Key findings

It is a comprehensive analysis of the purpose of identity systems, the landscape, different uses for digital identity for financial institutions across a variety of products and different types of organisations. It proposes digital identity systems for different needs and presents a two-tiered approach to developing the identity ecosystem with: (1) the development of natural identity networks which evolve around user groups with similar needs and characteristics and (2) building the interconnections between these networks.

There is much useful background information on the different components of the digital identity market and it categorises the elements of the digital sectors (such as attributes in three groups: inherent, inherited and assigned attributes). It doesn't contain any detailed analysis on cost savings, user testing or propose the design of solutions.

What are the outcomes?

There is a strong business case for financial institutions to lead the development of digital identity systems, which could derive significant advantages such as efficiency, new revenue and development of new products and services. The benefits are clearly presented, however it doesn't provide any estimated cost savings or additional revenues that could be generated.

The Blueprint recommends that consortia of financial institutions form identity networks that cover large, contained oligopoly economies (such as Canada or Australia).

Points to consider and references

There was no distinct follow up by the World Economic Forum report.

The report can be found at:
http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Title: Mobile Connect pilot of cross-border identity authentication

Participants: This managed by the GSMA with organisations and national identity providers from different Member States including Estonia, Finland, France, and Norway.

Description

The GSMA has developed and is promoting Mobile Connect as a solution to identify an EU-citizen of one Member State to gain access to a public service in another, using the eIDAS framework. Mobile Connect aims to offer a simple way of achieving pan-European identity federation of cross-border services for the EU governments, compatible with the eIDAS regulation.

It has focused on a project with two phases:

The initial phase was a 2 month pilot (2015) between Spain (Catalunia) and Finland. The pilot established a proof-of-concept for cross-border authentication enabling the use of e-Government services, in line with eIDAS regulation. It allowed customers of participating Spanish mobile operators to log-in to a Finnish e-Government service. On the Catalunia side, the user could log-in, through a digital identity validator, to access Finnish public services.

The second phase was announced in March 2017, which will deliver a commercially viable, government backed, pilot demonstrating how mobile operators can support (via Mobile Connect) the deployment and scaling of eIDAS across two or more European countries. It aims to position Mobile Connect as the first private-sector cross-border service authentication solution that meets the technical and regulatory requirements of eIDAS.

Participants include eID schemes and mobile network operators in Norway, Finland, France and Estonia. The aim is to integrate Mobile Connect into the eIDAS nodes of the national eID schemes and build a range of test cases, which includes a technology company (such as an IoT company) and education institutions (e.g. an online university); the GSMA is keen to have a financial use case to include opening a bank account, which this CEF project could deliver as it is utilising Mobile Connect.

The timeline for delivery includes:

- Stage 1: defining the minimum viable product, business modeling and define main architecture options and use cases (completed July 2017)
- Stage 2: eIDAS pilot stage use cases and deployment including country level node integration with Mobile Connect and cross border integration between eIDAS nodes and Mobile Connect (June 2017 to January 2018)
- Stage 3: Launch and demonstration (key target is Mobile World Congress in February 2018), Communications & Post-launch.

Key findings

Nothing to report yet, but will keep in contact with the GSMA regarding development of this project and the sharing of information between the two.

What are the outcomes?

There are no outcomes at the time of preparing this report as the project is in the early stages of development; this will be updated as the project progresses.

Points to consider and references

It will cover a variety of use cases and will align with this CEF project on cross-border bank account opening.

Contact: Marta Ienco mienco@gsma.com

The second pilot can be tracked on the http://bit.ly/2wdrU0S

Title: TISA Digital Identity project

Participants: This is managed by TISA and open to its members. A sub-group of the TISA Digital ID Steering Group will be formed to oversee, fund and manage the pilot phase.

Description:

The TISA Digital Identity pilot aims to build a fully-fledged Digital Identity that will enable consumers to open new ISA accounts, pensions and bank accounts. It will use the same identity to access information on funds, and to securely transfer money between accounts. It intends that the identity can be used globally.

The Digital Identity will comply with all current and forthcoming regulatory requirements to meet the industry's needs to effectively onboard customers and manage their online relationship.

The initial phase of the project involved building an emulator, which consisted of a set of wireframes that simulates the process of asserting a digital identity in an account opening process; two versions were developed: (1) using a Verify ID and (2) creation of a new Digital Identity account.

The project is now entering the development stage, which consists of building an AML compliant KYC emulation, and aims to having a working solution within this current financial year, which be delivered as an industry application.

Key findings

The pilot aims to investigate consumer need, technical and operational requirements to develop this Digital ID, changes to current operational procedures required to use Digital IDs, the commercial model and any changes required of the legislation (especially GDPR).

What are the outcomes?

TISA's vision is for the Digital Identity, and the underlying data management, to become an enabler for the industry, which can be applied across a range of financial products and to provide access to additional value added services, such as more effective personal data management. This pilot is viewed as stepping stone to enable 'Identity as a Service' so moving towards a TISA titled 'Digital Trust Ecosystem'.

The current phase will deliver a report of the findings from the Pilot (including the consumer research, provider research and commercial model options) and recommend a strategy for the roll out of the Digital ID. It plans to develop accreditation standards, which will initially be Guidance, and this is currently underway. It is unclear if this will utilise the Government ID standards and Verify ID.

Points to consider and references

The project is aligned with the ICO Data Sharing Principles and is working closely with the FCA's Regulatory Sandbox. It will employ interoperable standards, working with UK Finance and the British Standards Institution to provide governance and will work with Verify to *'facilitate interoperability between private and public sector initiatives.'*

Contact: Andrew Churchill

Title: Digital Identities Across Borders: Opening a bank account in another country (Discovery and Alpha)

Participants: Government Digital Service, Barclays, BBA, FCA, Difi Norway and BankID

Both discovery and alpha projects tested the following hypothesis:

'Individuals coming to the UK will be inclined and able to open a UK bank account online, prior to arriving into the country, using their national digital identity.'

Discovery Project

The objective of the discovery project was to:

1. Explore an ideal user journey that would allow an individual from Norway, using their BankID digital identity, to open a bank account with Barclays, prior to their move to the UK.
2. Consider practical, commercial, regulatory and privacy implications of such a service.
3. Explore how digital identity could help banks meet their regulatory and legal requirements when identifying and verifying their customers' identities.

Alpha Project

The Alpha Project focused on:

1. How federated digital identity aligns with banks' Customer Due Diligence processes and regulatory requirements
2. How digital identity contributes to Norway's low levels of internet banking fraud
3. How banks would adopt federated digital identity into their customer on-boarding process technically.

Key findings

The Discovery project recommended the key areas to be addressed in the Alpha project and the BBA (PWC) report.

The project recommended that an alpha should:

- Conduct further analysis to understand how EU levels of assurance for digital identities map against the existing bank processes for identity verification; this was addressed in the PWC report.
- Conduct analysis of how digital identity could enhance fraud control processes.
- Consider technical practicalities for bank to use a digital identity to conduct checks against credit, sanctions and connecting with other databases that store attributes, at both national and international level.

The Alpha project had four workstreams, which delivered the following findings:

1. **How digital identity aligns with banks' Customer Due Diligence processes**
   This workstream investigated how BankID and other similar national digital identity schemes can assist in the Customer Due Diligence (CDD) process. It analysed the information that a bank collects about a customer, and which data points need to be verified; it investigated how national identity schemes can assist in this process. Banks have a list of documents they accept and there is variation in requirements depending on the product type, services and the different risk based approaches adopted by banks. BankID provides the customer with a means of providing evidence of their name, date of birth and a social security number, which eases the amount of time taken in an application. It also provides a secure channel to verify personal data and ensures that the customer is not forced to leave their digital application.

   The table below (from the Alpha report) details the key findings including the checks that the digital identity solves or doesn't solve:

Bank Check	Impact of BankID / Digital Identity
Identity verification	Digital identity solves
Credit Scoring	If unique identifiers are shared with credit reference agencies this may improve the ease of data matching and hence tracing a customer's credit profile for assessment. It may also reduce errors such as erroneous deceased markers and split files, providing an improved match rate where credit data is required.
Fraud screening	Details of identities linked to confirmed fraud could be added to fraud data sharing systems, reducing the risk of false matches against genuine customers and the fraudster developing alternative identities (assuming that there are controls around the number of digital identities a person can hold, or a means of linking all identities a person holds).
Sanctions Screening	Use of a digital identity would mean the bank is sure the customer has used their genuine identity which will assist in screening and managing potential matches.
PEP Screening	Use of a digital identity would mean the bank is sure the customer has used their genuine identity which will assist in screening and managing potential matches.
Immigration Act	Use of a digital identity would mean the bank is sure the customer has used their genuine identity which will assist in screening and managing potential matches.
Risk Assessment	No impact
Ongoing due diligence	Bank ID completes regular checks against the Norwegian address file to ensure this data is kept up to date for the banks. There will need to be a definition of how such ongoing controls are completed cross border to ensure that a digital identity issued in one member state offers the same level of security when consumed in another member state.

   Where banks accept government issued ID documents and a fraud loss event occurs, the issuing authority (i.e. government) has no liability for the loss.

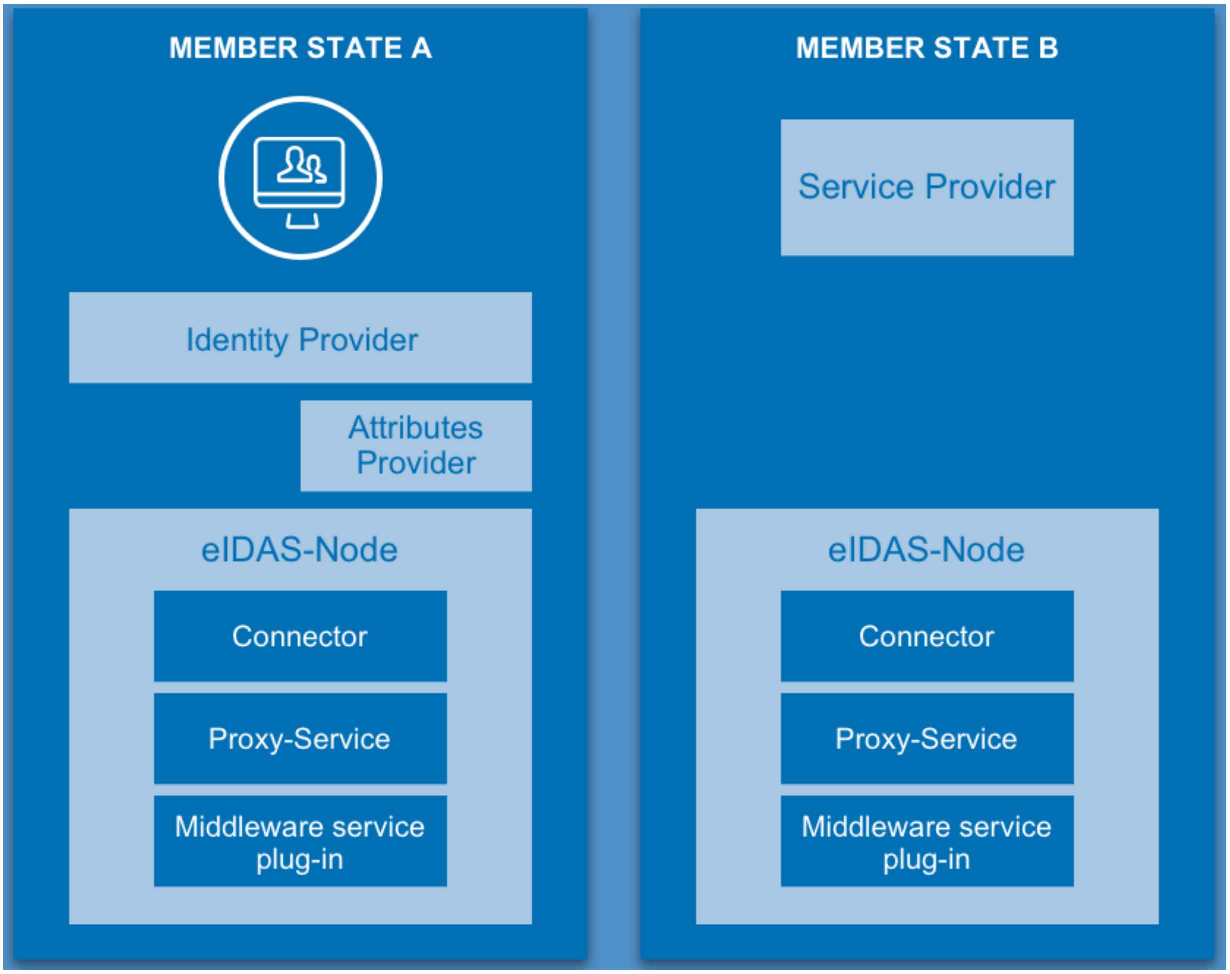
2. **How digital identity could enhance fraud control processes workstream.** This workstream investigated how the Norwegian model works and facilitated information sharing amongst the participants of the scheme.

   Sharing public / private information, by using national digital identities is mutually beneficial with the private sector sharing their wealth of knowledge in the fraud space so reducing the risk of fraud in the public sector. This will also ensure that the private sector and consumers have confidence in the system and use it to its full capacity, providing the critical scale to ensure the tool is a success.

   This workstream highlighted that if banks accept government issued ID documents and a fraud loss occurs, the issuing authority has no liability for the loss, which is an important consideration when devising the liability model for this project.

3. **Technical architecture needed for cross border use of digital identities in the private sector workstream**.
   The report outlines the use of eIDAS and its key benefits which are that it creates a set of European Assurance levels (high, substantial and low) and defines an interoperability framework, which is crucial from a technical perspective and is achieved by communicating between the points (or nodes) that send and receive messages between the identity and service providers.

   This project explored how eIDAS could be reused in the private sector context and the diagram below illustrates the core components of the eIDAS architecture. In this case both countries are proxy countries (the most common case) i.e. they do not operate middleware solutions for authentication. In general, when a user in member state A attempts to access a service in member state B, the “Connector” in member state B connects the user to their eID issuing member state Proxy-Service allowing them to sign-in, and for any additional attributes to be provided.



For any bank wishing to reuse this infrastructure, a private sector connection is required into the national node, which can then make a call and receive a digital identity using the eIDAS specifications. This is a key deliverable for this project.

4. **Analysis of digital identities against banks' current practices for identity verification**

This was delivered in the PWC report commissioned by the BBA, with the results outlined in the next section below.

The Discovery and Alpha projects identified a number of potential benefits for both the customers and banks, when utilising a digital identity that meets government standards. These benefits include:

For the customer

- Access to a wider market, not only within a country, but potentially across the EU, with the ability to prove they are who they say they are in the online channel when trying to access the service.

- Allowing the customer to access the service via their channel of choice and avoiding the need to present identity documents in a branch or switch across channels.
- Enable switching between different suppliers that leads to greater competition and better service.

For the bank:

- Identification and verification of an individual in a standardised, reliable way with a potential reduction in fraud.
- Reduced reliance on manual process and therefore reduction of staff errors and reduced cost associated with quality assurance.
- Reduced need for branches and therefore potential cost savings
- International interoperability.

Discovery

Findings from discovery included:

- It is easier for the end user to provide credentials through a trusted channel.
- Users were receptive to the concept of using their national digital identity to open a bank account in another country prior to their arrival.
- There is a general move by UK customers to online and mobile banking.
- Using a standardised way of identifying and verifying individual enables matching that identity in third party databases. This will improve match rates and therefore reduce uncertainties, risks and additional costs that are incurred in the current systems.

Alpha

Findings from Alpha included:

- The project considered how digital identities, which meet eIDAS standards, can benefit both customers and financial sector institutions, how they align with the financial regulations required for onboarding new customers and how they could reduce fraud.
- The report recommend that a high level technical architecture and components are needed for a service that allows a financial institution to consume an eIDAS compliant digital identity from another Member State.
- As financial institutions use a risk-based approach when onboarding customers, whereas the eIDAS scheme is a standards based approach; any changes to the risk based approach requires a step change, but presents a big opportunity.

What are the outcomes?

This project aims to tackle many of the issues that were delivered in the findings from the Discovery and Alpha projects, and utilising such in the design of the prototype and technical architecture.

Points to consider and references

The full reports can be found at:

Discovery report http://oixuk.org/blog/2016/02/28/digital-identity-across-borders-opening-a-bank-account-in-another-eu-country/

Alpha report http://oixuk.org/blog/2017/01/13/alpha-digital-identity-across-borders-opening-a-bank-account-in-another-eu-country/

Title: How Digital Identities which meet Government Standards Could Be Used As Part of UK Banks' Customer Onboarding and KYC requirements

Particpants: BBA, PwC and Government Digital Service (Cabinet Office)

To help to better understand the potential benefits and challenges in using a GOV.UK Verify identity as part of a non face-to-face on-boarding process, PWC were commissioned by the BBA to undertake objective research in two parts:

1. Survey a range of banks on the methods they currently use for the identity verification of their customers, &
2. To compare their existing requirements against an assertion of a digital identity that meets the currently implemented government standard, Level of Assurance ("LOA") 2.

Key findings

The research uncovered significant variety in the identity verification approaches used across different sizes and types of banks and financial institutions. The report distinguishes identity verification from the other processes that banks conduct to test a customer's eligibility for a product or service.

The report identified that there is a broad correlation between the size of the bank and the level of data sought from the customer, with larger banks seeking the most data, mid-tier banks seeking substantially less (perhaps more targeted) information, and some new banks requiring significantly less. New and smaller banks seek less data direct from applicants, as substantially more information is collated by using technology driven processes.

The report found that the government LOA 2 standard for identity verification (under GOV.UK Good Practice Guide No 45[14]) is equal to or exceeds the level of assurance currently achieved by the majority of banks in a non face-to-face on-boarding environment. A significant proportion of the banks interviewed were seeking to achieve higher levels of assurance in the future, with a number working towards LOA3.

Financial institutions utilising such Government assured identity would still require additional data and checks to meet their obligations under AML legislation, JMLSG guidance, and to undertake credit risk assessment.

What are the outcomes?

Given the alignment of GOV.UK Verify to the EU's eIDAS standards, national digital IDs could be used to apply products or services across Member States, however the report clearly identifies some significant challenges that need to be addressed:

[14] http://bit.ly/1BSkznK

- Firstly, a standards-based approach to establishing identity and its verification is a departure from current ‘business as usual’. Banks will need to be better informed of the standards that underpin the provision of digital identities, and to have confidence in the information they receive. Using digital identities requires banks to rely on third party data in a way that they do not currently. It would also reduce their ability to compete in the way that they identify their applicants, which some banks consider to be an important part of their offering.
- At present the use of digital identities is not well described in the JMLSG guidance, which guides banks’ on-boarding requirements. However this may change as part of the upcoming JMLSG review. Similarly efforts are ongoing in the Commission to ensure that the revisions to 4th EU Money Laundering Directive[15] reflect the opportunity to utilise digital identities, which has been supported by BBA and the European Banking Federation.
- While there is an established liability model for use of GOV.UK Verify identities for accessing public services, there is currently no such regime in place for use of digital IDs by the financial services sector. This will need to be addressed before any form of adoption will be possible, which is a key component of this project.
- There is also no current commercial model for the reuse of GOV.UK Verify identities. The cost of adoption, at a time of significant change for banks, is critical, and must be considered fully and be attractive to the industry for adoption to take place.

Points to consider and references

Many of the points raised above (such as the liability model and commercial model) are to be addressed in this project.

The report can be found at:

http://oixuk.org/blog/2017/01/09/how-digital-identities-which-meet-government-standards-could-be-used-as-part-of-uk-banks-customer-on-boarding-and-kyc-requirements/

PWC is in the process of preparing a second report, for UK Finance, that will be included in future version of this report.

Title: Estonian e-Residency/Holvi

The Estonian Government offers an e-Residency programme that allows foreign nationals to apply for a Government issued digital identity card. This allows e-Residents to open companies in Estonia, without the need to have a physical presence. The identity checking is managed by the Estonian Police and Government departments; it does not rely on the eIDAS framework.

Based on regulatory changes in 2017, opening a bank account is now possible online using an e-ID or e-Residency card. With an e-Residency and business registered in Estonia, it is possible to apply for a business bank account. Banks are developing the technical solutions that will allow clients to open an account from anywhere without a face-to-face meeting.

[15] http://bit.ly/2hfqnDp

Currently, the Estonian Banks require e-Residents to still physically present identity documents in branch, however Holvi offers a business account that can be opened remotely without the need to physically present identity documents in Estonia.

Holvi is a Finnish based start-up (owned by BBVA) that is regulated in Finland and provides a business current account that offers a range of features (such as online management of finances, invoicing and bookkeeping tools and IBAN functionality, access to Holvi MasterCard), however the organisation is defined an regulated as a payment institution, and not a bank, as it doesn't have a banking licence.

To be eligible to apply, business owners require an Estonian e-Residency ID card and ID card reader (provided as an e-Resident) and a Business register extract for the limited company in Estonia. The checking relies on the Estonian ID card for identity and it uses registries in different countries to authenticate the company and the directors.

Points to consider and references

The Estonian e-identity and e-Residency programme: https://e-estonia.com/solutions/e-identity/e-residency

Holvi Bank offer to Estonian e-Residents: https://about.holvi.com/e-residents/