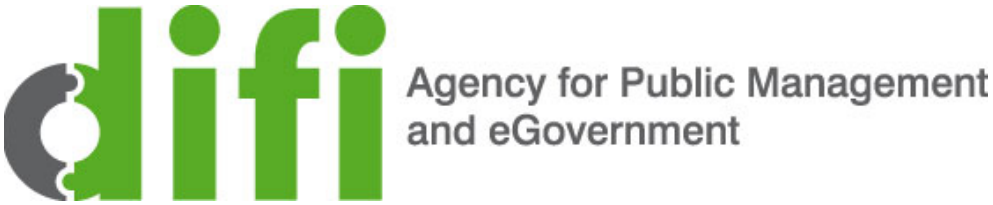
ALPHA DIGITAL IDENTITY ACROSS BORDERS: OPENING A BANK ACCOUNT IN ANOTHER EU COUNTRY

PROJECT REPORT

EDITED BY LIVIA RALPH
JANUARY 2016

Contributors:

The voice of banking

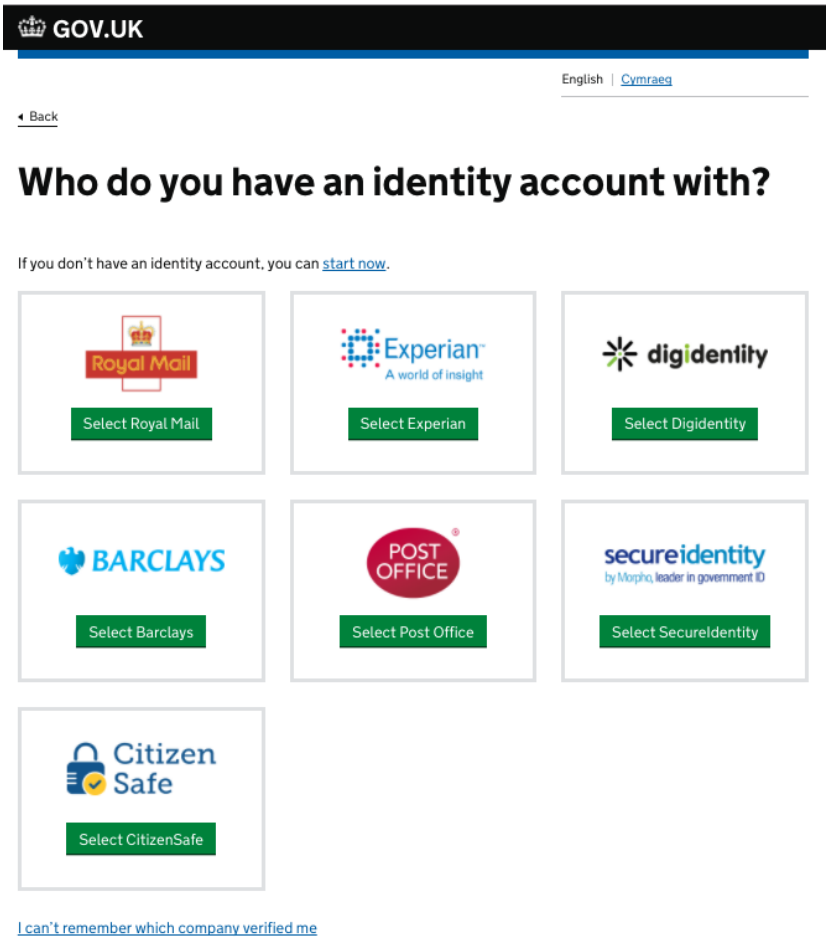


Executive Summary

As people use digital channels to access more and more services they are faced with a growing and unmanageable number of usernames and passwords. Federated solutions allow people to register and login to web based services through a third party such as a social network. However, the identity details passed to the web based service are those associated with the third party 'Identity Provider' account and have not necessarily been verified as a 'true' identity.

In the UK, the Government Digital Service (GDS) has developed a federated identity service to enable people to register for and access digital public services. The Identity Providers contracted under the GOV.UK Verify service must meet high government standards for identity verification so that the service provider has a high level of assurance of the person's identity. As increasing numbers of public services are delivered digitally a large part of the UK adult population will choose a private sector Identity Provider and create a digital identity through Verify.

Customers increasingly expect to be able to manage all aspects of their life through digital channels. However, proving identity in digital channels to the high standards required by banks remains a challenge. Pilot projects are being conducted to consider how digital identities created to government standards under Verify could allow people to make a trustworthy assertion of identity in any digital transaction in the private sector, for example when opening a bank account, in a manner that reduces identity fraud and meets regulatory obligations.



Federated identity schemes have been in place in Scandinavian countries such as Norway for a decade or more. In considering how Verify might be adopted by the UK banks there is a great deal to be learned from Norway's experience where the banks and government collaborated from the outset. This project has focused on three specific aspects:

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

Through the project the British Bankers Association (BBA) has commissioned PWC to survey British banks on their identity verification processes for new customers and compare them to government digital identity standards. The PWC report[1], published alongside this report, provides an objective view on the relative benefits and challenges of federated digital identity against in-house processes.

[1] http://bit.ly/2iZ0OqF

In 2015 the European Union's Electronic Identity and Authentication Services (eIDAS) Regulation came into effect. This requires Member States to recognise each other's digital identity systems for access to public services. It creates an interoperability framework so that equivalence between national digital identity verification standards can be established. In July 2016 the European Commission recommended that the fourth Anti Money Laundering Directive be revised to make direct reference to the agreed identity verification standards framework.

Pilot projects with UK financial institutions are being planned for 2017 that will define the governance and operational structures under which digital identities issued under the UK's Verify scheme or under other countries' digital identity schemes could be accepted by financial institutions. These 'alpha' projects will be followed by 'beta' pilots in which live services will be introduced.

The difficulty of opening a bank account is a source of frustration for both customers and banks. Federated digital identity presents an opportunity to increase competition in the financial sector and reduce fraud. New entrants will be quick to adopt federated digital identity schemes and policy makers will welcome the opportunity to facilitate greater openness and competitiveness across the sector. The financial sector is experienced in the collaborative development of open standards based infrastructures that enable competitive markets. It is therefore well placed to work with government to create a digital identity infrastructure that will be of benefit to all.

Table of Contents

Introduction

In 2015 an OIX discovery project was conducted that looked at the use of EU digital identities (specifically Norwegian BankID) to open a Barclays bank account in the UK[2]. The following were contributors to this project: The British Banking Association (BBA), BankID Norge, Barclays, Cabinet Office, the Financial Conduct Authority's Innovation Hub (FCA), and the Norwegian Government (Difi).

The discovery resulted in a project report[3] that included a number of recommendations. It recommended that a follow on alpha project should:

- Conduct further analysis to understand how EU levels of assurance for digital identities map against the existing processes that banks already have in place for identity verification.
- Conduct analysis of how digital identity could enhance fraud control processes.
- Consider technical practicalities of a digital identity being used by a bank to conduct checks against credit, sanctions, and other necessary databases at both national and international level.

These recommendations have been taken through into an Alpha project, the results of which can be found in this report.

The benefits of digital identity for customers and organisations

During both discovery and alpha stages the following hypothesis was the main focus of the research: **'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.'** and a number of potential benefits have been highlighted during the workshops for both end customers and organisations.

[2] http://oixuk.org/?page_id=2367
[3] http://bit.ly/2gVEVax

Benefits for Customers

Adoption of a digital identity service to enable account opening will bring a number of benefits for consumers. Customers would not have limited access to banks based on the proximity of the banks' branches to them but would have access to a much wider market (not only across one country but potentially across the EU or wider). Trusted digital identity would also allow those who lack a credit footprint in the country where they want to open a bank account to be able to identify themselves remotely.

Using trusted digital identity would also allow customers to complete an end to end account opening journey through their preferred channel, rather than breaking it into a number of stages including potentially a face to face visit in the branch.

Trusted digital identity will provide customers with a single, reliable tool they can use to confirm their identity, across both public and private sectors. This will increase customer familiarisation with 'normal' procedures for asking for their data and may make them less vulnerable to scams. Customers also may have more agility and be better placed to move between service providers, making them able to benefit from improvements a single market has to offer, and challenge suppliers to continue to improve services and products.

Benefits for Organisations

There are a number of benefits for financial sector institutions in adopting digital identity services that meet government standards.

Banks would have a method of identifying customers which is reliable and independently sourced, and more difficult to subvert which will reduce the risk of fraud at account opening. Using digital identities also means there is reduced reliance by organisations on manual processes, resulting in reduced staff error and reduced cost of associated quality assurance. Moving into digital space and away from physical evidence means that records would be electronic so easier and cheaper to store.

Use of digital identities would allow for customers to shift into a digital channel more easily, while leaving branch staff to help those that don't have digital identities or need assistance. During peak account opening times (such as student registrations) use of digital identities would move focus away from branches into an online channel, enabling better handling of the applications.

Banks would also be less reliant on having a large branch network in order to be able to have a significant market share, which could help increase competition in the retail banking space as customers would be able to be more agile.

Project approach

Methodology

The project was split into four workstreams, aligned to the recommendations in the discovery project report. The workstreams on Customer Due Diligence (CDD); and Fraud consisted of a number of workshops with relevant parties, exploring how digital identities fit into CDD processes and how digital identities and a federated model can help reduce fraud. The two workstreams are summarised below under the points 1. and 2.

The technical workstream included a number of meetings and a workshop where eIDAS infrastructure was explained. Based on these there is a short summary written under point 3.

And lastly, an independent analysis of how a digital identity that meets government standards compares with banks' current ID verification methods has been done by PWC. A short summary on this work (with a link to the full report) can be found under the point 4.

1. How digital identity aligns with banks' Customer Due Diligence processes

The developing context of 'digital identity'

Digital identities are being developed across Europe with a view to compliance with the eIDAS regulation. The regulation will require member states to be able to consume digital identities issued in other member states (where the other member state's scheme has been notified) in the same way they consume their own national digital identity for access to public services, if the service requires level of assurance that is 'substantial' or 'high' as defined under the regulation. The regulation also encourages member states to make these digital identities available for use in the private sector.

In December 2015 the European Commission published a green paper[4] on retail financial services, with focus on creating a true European market for retail financial services. This paper focused on increased cross border sales of retail financial products so that consumers could have access to the full market and increase competition driving up quality of products and services.[5] The ability to

[4] http://bit.ly/2gDyBUs
[5] http://bit.ly/2h882Yu

provide non face to face, cross border proof of identity is seen as a key requirement for the successful delivery of a true single market for financial services. An Action Plan is expected to be published by the Commission shortly, to set out a range of non-legislative proposals to improve cross border access to financial services, and digital identity solutions are expected to be a significant element of the solutions proposed by the Commission to open up the market.

Equally, banks in the UK are keen to provide services to consumers through their digital channels, with a number of new banks entering the UK market on a digital only proposition. For banks to be able to achieve these objectives there needs to be a standards based approach to identity verification for on-boarding customers through non face-to-face channels.

This workstream, under the Alpha project, looked at how BankID and similar national digital identity schemes can assist in this process. Specifically, this requires an examination of the Customer Due Diligence requirements. Customer Due Diligence goes beyond basic ID checks and includes some of the wider detail about a customer which banks collect, such as source of funds and purpose of the account.

The questions asked by a bank during the CDD process depend on a number of variables, not least how their back end systems work, and what data they can use most effectively, the products they sell and their risk based approach to customer onboarding. Due to the variances not all CDD is the same.

CDD data is also used to ensure the customer is eligible for the product and is then used in the ongoing monitoring of the relationship to enable the bank to identify suspicious activity, or changes in behaviour which warrant an update in CDD.

How banks currently open accounts

Account opening experiences can be broadly divided into two groups, face to face and non face to face. Both journeys require the bank to collect data about the customer including:

- Name
- Date of birth
- Address
- Purpose of account
- Intended use
- Risk assessment
- Marketing

- Security

A description of an account opening process is also described in Figure 1 below, from the discovery project.

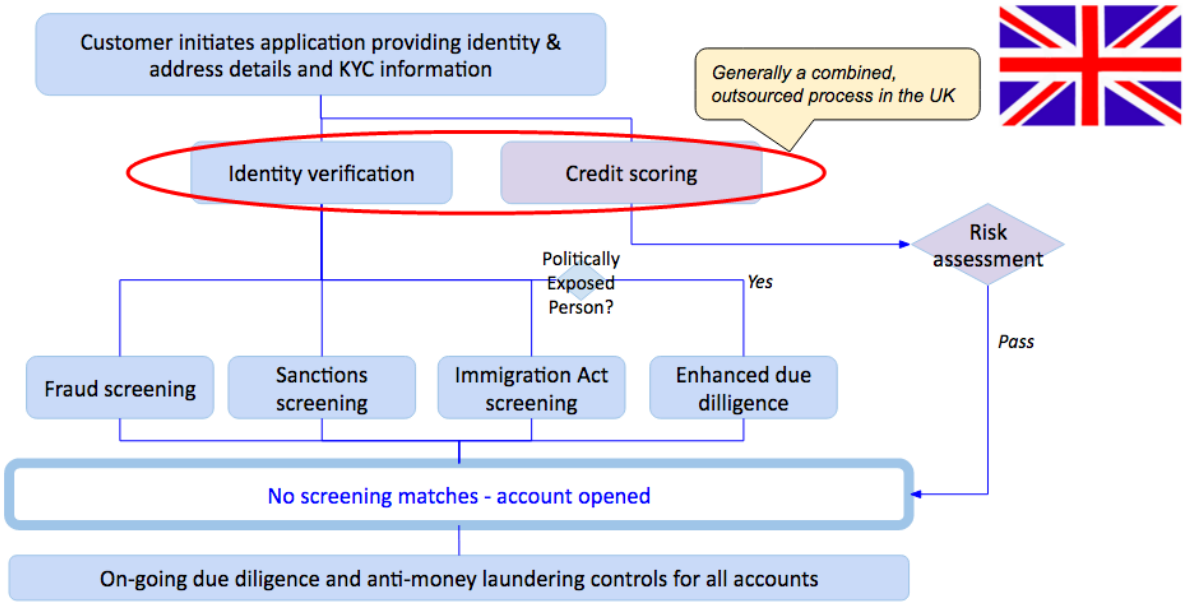


Figure 1 summary of a generic bank account opening process. Source: Digital identity across borders: opening a bank account in another EU country

The amount of information that a bank collects about a customer, and which data points need to be verified, is based upon the product type, services, and risk associated with the product and customer. It is only identity that the Money Laundering Regulations 2007 stipulate must be verified.

ID information needs to be based upon "documents, data or information obtained from a reliable and independent source;"[6], whereas CDD information is collected from the customer and does not usually require to be verified with documentary evidence (assuming a standard risk customer opening a standard risk product).

The aim of Identification and Verification (ID&V) is to be comfortable that the identity exists and that the customer is the owner of that identity. Essentially the bank must be sure they know which unique individual they are entering into a relationship with. This identity is key to then managing the associated account opening processes, and managing the account throughout the lifetime of the relationship. This can include for example ongoing screening and monitoring, managing court orders, and managing data about people who have died. As such, it is important that this process is correct at account opening to ensure the smooth onward running of the account.

[6] Money Laundering Regulations 2007 (5 (a)) http://www.legislation.gov.uk/uksi/2007/2157/regulation/5/made

Whilst there is no regulatory requirement to obtain proof of address alongside proof of identity, most UK retail banks are understood to require proof of address at account opening. This additional control is in place to help manage the risk around impersonation fraud.

In a face to face journey ID and address will normally be proven through the customer presenting documentary evidence. The industry guidance by Joint Money Laundering Steering Group (JMLSG)[7] highlights that there is a hierarchy of sources of these documents which differ in their independence, reliability and integrity. With government issued photographic documents sitting at the top of the list. Account opening organisations each have a list of documents they accept, to support an account opening which seeks a balance between the reliability of the documents, access to the documents and ensuring that potential customers do not become financially excluded due to lack of access to specific documents.

In a non face-to-face account opening journey banks tend to rely on electronic identity verification (eID&V). This is where a customer is identified through confirming that they have a length and breadth of personal data held at their declared address, traditionally this has been completed through use of data compiled by credit reference agencies. For example, the search may confirm that the customer is on the electoral roll, and has a number of other financial services registered to them at their address. Each account opening organisation will have a minimum requirement to be met for this process. Where customers have insufficient data they will then be required to complete their account opening through a face to face journey. This may be an unsatisfactory journey for the customer as they have not been able to complete their account opening at the time they wanted to, or indeed through their preferred account opening channel.

This model causes a number of challenges for genuine customers trying to open new financial services products, for example many customers do not have ready access to standard identity documents. In May 2016 the FCA published Occasional Paper 17: Access to Financial Services in the UK.[8] This identified that 9.5million consumers in England and Wales do not have a passport and 1 in 4 residents in England do not have a driving licence. Where they do not have these documents customers are more likely to face challenges in opening products.

Customers who have little history of credit (thin file) are less able to be identified through non face to face electronic identification. This may apply to younger people who have only recently gained access to credit, people who are new to the country and have not yet built a footprint, and also people who are in a post credit phase in that they have paid off all their credit. In these cases the customer will be forced out of the online process and instead be required to attend a branch and complete a face to face account opening presenting documentary evidence for proof of ID and address.

[7] http://www.jmlsg.org.uk/what-is-jmlsg
[8] http://bit.ly/2h8gtTG

For many consumers there is a challenge with attending branch, either due to personal circumstances where travel may be less possible, or where working hours are such that the customer cannot get to the branch or due to the lack of proximity of a branch.

All of these challenges lead to customers either not being able to complete an account opening at the time of their choosing, through the channel of their choice, or indeed prohibits them from being able to open an account completely.

Recent research completed by Signicat indicates that "40% of consumers have abandoned bank applications[9]:

- More than 1 in 3 (39%) abandonments were due to the length of time taken to do the application
- A third (34%) were due to needing too much personal information"

The evidence presented in the FCA Occasional Paper 17 and the Signicat research indicate that there is consumer demand for improved means of identity verification which is not currently being met.

How digital identity can help to solve the account opening challenges for consumers

BankID[10] provides the customer with a means of providing evidence of their name, date of birth and a social security number. (In Norway the social security number can be used to cross reference another database to confirm the customer's residential address). This eases the amount of time taken in an application, provides a secure channel to verify personal data and ensures that the customer is not forced to leave their digital application.

The information is supplied by the customer, and the BankID allows the account opening bank to check the information against a reliable and independent source. Whilst digital identity is not explicitly mentioned as a means of identity verification in either JMLSG or Money Laundering Regulations, it does arguably meet the principles defined by the Money Laundering Regulations 2007. Further, the European Commission's proposal amending directive (EU) 2015/849[11] - the 4th Anti Money Laundering Directive[12] - has provided explicit acknowledgment of digital identities delivered in compliance with eIDAS as being comparable to face to face identity verification processes. Acceptance of this proposal would provide clarity to the regulated sector in terms of acceptance of

[9] Signicat Onboarding Report The battle to on-board: Why 40% of consumers abandon banking applications, http://bit.ly/2gpJNkA
[10] Description of BankID can be found in appendix A, p18, in the discovery report: http://bit.ly/2gVEVax
[11] http://bit.ly/2gQXl9I
[12] http://bit.ly/2gpHDBC

digital identities issued by other member states. This will allow customers in both the face-to-face and non face-to-face groups to meet the ID&V requirements for new financial products, without requiring them to hold documentary evidence of their ID.

BankID has two factor authentication, which acts as an additional control as it enables the bank to confirm that the person using it has ownership of the identity. The ownership test is important as it provides the account opening financial services provider to be comfortable that they are dealing with the owner of the identity. There remains a risk that customers would allow a third party to have access to their security details, however this risk is expected to be low as this would then compromise their full identity including access to all other savings and payment accounts they hold. Also background security and anti fraud controls would provide additional comfort around this risk.

Challenges that digital identity does not address

In the UK most banks seek to verify the customer's address as well as their identity. The eIDAS Regulations provide a framework for digital identities to be used across EU borders. The core data set under eIDAS does not include address data so banks may need to determine whether the value of a digital identity and the security it offers offsets the risks around not verifying address, or find an alternative means of verifying the address. In the Norwegian model there is a central register of addresses for people who hold a social security number. Banks are able to verify their customer's social security number using BankID and then use the verified number to check the associated address. As the address is not part of the eIDAS core attributes (but is optional) there is a risk that each member state will have local solutions for this which will continue to make cross border account opening challenging.

When opening an account, a customer will be asked to answer a number of questions beyond confirmation of name and address. For example:

- Eligibility questions – to ensure that the selected product is suitable for the customer.
- Consent – ensuring that the customer understands what checks will be completed and how their data will be used.
- Personal data – including name, address and date of birth.
- Address history – to enable a credit check to be completed (both to enable lending and also identify customers in distress for whom alternative products might be more suitable.)
- Employment / income details – to enable the bank to understand what transactional activity they can expect to see on the account and facilitate ongoing transaction monitoring.

BankID or a similar digital identity will not solve all of these question sets, and thus, will not address the abandonment rate which is due to customer perception of too much personal information being required. Thought fewer questions being asked about identity may positively impact this figure.

It will only solve the issue around verification (based upon a standard risk retail personal account being opened).

When opening an account, the bank completes a number of checks. BankID or another digital identity providing standardised trusted identity verification will assist in accuracy of checks the bank has to do when onboarding a customer as well as reducing false positives.

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.

Under the Payment Account Directive EU citizens are able to open certain types of account in any member state. Take up of this will provide some initial indication as to whether there is cross EU appetite and may add weight to the need to progress with digital identity solutions.

Learnings from The Norwegian BankID system

BankID was developed by banks in Norway, and was focused on being an identity solution, which has since been leveraged for digital services. The solution has evolved with the needs of the industry and in light of their experience. This evolution has led to some challenges.

There is a declining number of bank branches in Norway and low population density. To ensure the availability of BankID non bank staff were used to collect a copy of the passport and issue the physical BankID token. This led to a small number of instances in which BankID was issued on invalid documentation. Procedures have been enforced to ensure proper controls are now in place.

Most banks only issue BankID to customers that hold a Norwegian passport. This led to migrants having a different experience around access to banking than Norwegian nationals. Though full cross border use of all national digital identity schemes would ease this challenge.

As national schemes for digital identity are established there must be steps taken to ensure coverage is not limited to those who already hold robust identity documents, and instead ensure coverage is as near to 100% as possible, this will ensure that all consumer groups benefit from the schemes equally.

2. How digital identity could enhance fraud control processes

During the Discovery project it was noted that internet banking fraud is significantly lower in Norway than in the UK. This could be for a number of reasons however it was recommended that further analysis be done on how digital identity as demonstrated through the BankID system could assist fraud reduction.

Fraud Environment in the UK

A review of fraud data in the UK in 2015 showed that "Financial fraud losses across payment cards, remote banking and cheques totalled £755 million in 2015, an increase of 26 per cent compared to 2014"[13] and in September 2016 Action Fraud released statistics that indicated financial fraud had increased in Q1 2016 by 53%.[14] Similarly CIFAS has released statistics on identity fraud, which has

[13] FFAUK - Year-end 2015 fraud update: Payment cards, remote banking and cheque
[14] http://bit.ly/2gDLUo5

increased by 52% in 2015 amongst the young (under 30s).[15] The figures confirm that fraud is a significant issue within the UK and it is growing. The aim of this workstream was to understand how the use of a digital identity and its supporting controls in banking may impact upon the financial fraud losses that are being experienced and drive up the fraud prevention rates.

The UK financial services sector has an established fraud reporting and data sharing ecosystem in place. This enables clear sight of high level fraud figures, and understanding of the associated fraud typologies.

Many of the fraud types which occur in the UK are linked to customer identification both at on-boarding where the financial services provider uses identification & verification services to determine whether the person they are opening an account for is a genuine person, and they are the owner of the identity and during on-going relationship with the customer, where the account provider needs to be sure that each instruction on the account has been initiated by the genuine account holder for example through telephone banking, being able to authenticate that it is the genuine customer being spoken to.

As discussed in the customer identification section, currently financial services use a variety of different means to identify their customers; the means of identification is usually reflective of what the customer can reasonably do, commensurate to the risk, and the channel through which the company is engaging with the customer.

The two key methods of customer identification are face to face using documentary evidence of an identity such as a passport, or remotely using credit reference data. Both solutions have control issues which can be manipulated so that accounts are opened in incorrect or illegitimate names.

Once a customer has been identified financial services providers tend to then apply additional fraud controls which include:

- Reviewing against internal data. Looking at account opening details such as the customer's declared address, name and contact details to determine if these have been used previously in a fraud against the bank.
- Reviewing against external data. Many UK banks are members of data sharing groups such as CIFAS, SIRA and Hunter. These tools enable the industry to identify confirmed frauds and share this information with their counterparties to protect the industry as a whole from repeat frauds.

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

Credit Reference Data may also be reviewed to understand whether the customer has attempted fraud by misrepresentation by failing to disclose bad debt or previous address history. The data can also assist in determining whether the application represents an identity takeover as inconsistencies in application data may be identified.

On-going Controls in the UK

During the relationship with the customer, financial services will use a variety of different means to authenticate customer activity, from voice recognition through telephone banking to use of PIN numbers for debit card activity, and two factor authentication for online banking. The method will reflect the channel and the risk associated with the activity being undertaken. Financial services providers walk a tightrope between ensuring that there is a good customer experience and ensuring that customers and their money are kept safe.

Whilst there is some cross industry collaboration on fraud controls such as the introduction of Chip & PIN, many of the controls are bespoke to each financial services company and hence there is potential inequality of quality of controls between smaller and larger firms and there is a duplication of resource used across the industry to build robust fraud controls.

Current Norwegian Bank Account Opening Controls

Customers wishing to obtain a BankID digital identity are required to attend a bank face to face (or linked supplier) and present their Norwegian passport, they must also have a Norwegian social security number or equivalent.

Once a successful application has been made the customer is issued with a password generator and a temporary password. First time used the certificate and private public keys are generated, valid for 2 years.

They can then use their National Security Number and their one time password to activate a transaction through their Norwegian BankID.

Once a BankID has been issued then the customer can use it to open other Financial Services products with any bank within the BankID network.

The bank that issued the ID retains some liability around fraud, the liability amount encourages banks to have robust on boarding processes but would not cover the full losses of most fraud cases.

Equally the issuing bank holds the documentary evidence to support the BankID, this is an issue as once the customer exits that relationship then there will be a need to purge those records, though the BankID may still be active elsewhere.

How the Norwegian BankID is used

BankID is used as a means of authenticating payments for Norwegians. The process is as follows:

1. Customer logs into Online banking using their BankID as a secure login. The certificate is validated against revocation/suspension list.

2. Customer initiates a payment to a third party.

3. Before processing the payment the bank checks that the BankId is live and has not been reported as compromised.

4. Most banks ask the customer to sign or self administer the change.

5. Payment is processed.

The key benefits are that there is a real time check to confirm that the BankID digital identity is live and has not been reported as compromised. The banks must have a 24/7 support desk to allow customers to report BankIDs that they wish to close or believe have been compromised. This is of significant value for customers, in the UK if a customer has an identity takeover they will usually only realise this when they are denied credit and then check their own credit report.

Once they have identified themselves as a victim they have to then liaise with each institution to advise them of the fraud and work with them to get back to their original position.

In the Norwegian model, as soon as a consumer identifies they may have been a victim of an identity theft or account takeover they can report this to one central location, which will halt all transactions. The customer can then establish a replacement BankID and they will not be at immediate risk of being targeted again, as the new BankID will have separate security features from the original.

Ongoing Fraud Controls under BankID

BankID provides a suite of centralised controls which are in place to identify activity of concern and

flag them to the bank the customer is transacting through. This enables the bank to verify with the customer whether or not the transaction is genuine.

For example if the BankID has been used though a Norwegian IP address and on the same day is then used through a foreign IP address in a location the customer doesn't usually visit, this might flag for the bank to contact the customer to verify that they are using the BankID, or confirm that it has been compromised.

In order to support the collaborative approach to managing fraud, the BankID members also have regular contact meetings to share emerging threats and scams, this enables the banks to identify their local controls and test them to ensure that they will not also become victim to the threats.

This approach means that the entire Norwegian financial services sector becomes more hostile to fraud, rather than each bank increasing their protections in a silo, leading to fraudsters potentially hitting other banks in the system but not being forced out entirely.

To try to ensure that BankID remains secure and trusted by consumers there is constantly work being done to enhance the tool and the background fraud checks to try to combat such abuse.

There is a need to ensure that as the use of a digital identity increases then there must be supporting public awareness delivered to ensure that consumers are best placed to identify high risk situations and avoid them, and also understand when they should and should not disclose their security details. The value of there being a single identity solution which may also be used for customer re-verification is that this message becomes much more simple to deliver and understand.

Fraud Prevention Benefits of Digital Identity Governance

The eIDAS regulations invite ongoing engagement between countries with notified schemes so that countries can be made aware of identified weaknesses in a similar approach to how numbers of stolen passports might be shared.

If digital identities are used in the private sector, and the private sector assumes losses for frauds that are perpetrated in this space, there will need to be a mechanism for the private sector to feed into this process, perhaps through their government body, and also receive intelligence back out so that they can manage identified risks accordingly.

This public / private information sharing will ensure that the private sector can share their wealth of knowledge in the fraud space, reducing the risk of fraud in the public sector, but 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. There are established models for such information sharing and collaboration between the public and private sector in the UK which can be learnt from to ensure that digital identity solutions remain secure both for the consumers and the industry.

Liability Model Definition

Banks currently use government issued identity documents as a means of identifying customers for example passports, driving licences and passport.

In the UK industry guidance, approved by HM Treasury it suggests that "If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned."[16]

Where banks accept these government issued ID documents and a fraud loss event occurs, the issuing authority i.e. government has no liability for the loss. As Digital Identities are both used and issued by the private sector a clear approach to liability will need to be understood by all parties to ensure that the parties accepting or issuing the digital identity understand the risks associated with the process, and manage their risk accordingly.

Back office fraud controls

The Norwegian model is able to centrally identify activity which may be indicators of fraud. Similar controls would be needed in the UK to replicate controls which are already in place through current solutions.

For example where a customer is being verified through the identification and verification the service provider may identify that the same customer has had a number of searches in the same day, this information will feed into the decision engine to determine whether or not the application is genuine.

A robust suite of back office controls is vital, as whilst the Norwegian model shows the number of fraud cases is minimal, when a fraud does occur a customer's whole banking identity becomes vulnerable, and hence the scope for losses is much higher.

[16] Joint Money Laundering Steering Group Guidelines November 2014, Part 1, Section 5.3.61

As GOV.UK Verify could be used by many private sector companies, it may become a requirement for customers to be able to see a dashboard of their identity use, which can empower them to proactively monitor the use and ensure that it is only being used where they have initiated the transaction. This would be a similar control as currently exists which allows consumers to review their credit profile.

The model for cancelling a GOV.UK Verify identity account and ensuring that all the private sector partners are aware of the cancellation will need to be developed. In Norway this is managed through the identity being used as a customer verification tool as well as an account opening identity verification tool. A similar model could be developed in the UK to ensure that the customer has a single point of contact to report identity takeover to and all linked services can react accordingly.

Information sharing

The industry will need to identify how to use digital identity data in their existing fraud data sharing tools to ensure that customers who have committed fraud are not able to move between providers of identity and financial services and then become undetectable.

There may also be demand to use the network to share other customer data at significant points with the private sector, for example when a customer passes away the Verify identity could be updated accordingly putting each bank on notice and enabling them to protect the funds and be on notice of helping to pass the account through the estate settlement process. Equally where a customer changes their name, they can do this centrally rather than with each institution and each bank then pick up on the name change from the GOV.UK Verify identity. This reduces the risk of people having multiple legal identities which can be used to manipulate fraud controls.

Further the model of information sharing between the public and private sector will need to be reviewed to ensure control weaknesses in GOV.UK Verify identified in the Private sector are addressed by the Government, and that fraudulent identities can be shut down and potentially a collective approach taken to prosecution.

There are established methods of information sharing between Government and the Financial Services sector such as the Joint Money Laundering Intelligence Taskforce, learnings can be taken from this model and applied to engagement models for GOV.UK Verify.

3. Technical architecture needed for cross border use of digital identities in the private sector

The Discovery project 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.' Based on this hypothesis the Discovery explored the following user journey:

1. User started at Barclays landing page for opening an account
2. User indicated they are from Norway and have Norwegian digital identity
3. User got passed to the page - norwegian eIDAS node - where they chose one of the digital identities, specifically BankID
4. User logged in with their BankID and gave BankID permission to share the necessary information (name, date of birth, address…)
5. User moved back to Barclays website, where they were presented with partially filled out form based on the information Barclays received from BankID
6. User completed the registration process
7. User successfully opened a basic bank account with Barclays

The below image shows high level flow of the explored user journey, reusing infrastructure built under eIDAS regulation.

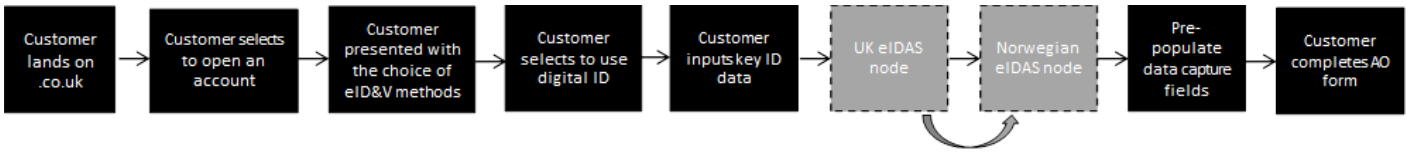


Figure 2

eIDAS includes EU rules for the recognition of digital identity schemes and means across borders. Specifically, it includes a rule that online services provided by the public sector in one EU country, which require a digital identity for the user to get access to the service, must recognise notified digital identities issued by any other EU country. While it is focused on the public sector services, this project explored how eIDAS could be reused in the private sector context.

eIDAS does two main points (i) it creates a set of European Assurance levels (high, substantial and low) and (ii) it sets out an interoperability framework. From a technical perspective the interoperability framework is crucial. It provides an easy way for service providers to recognise the identities being asserted by any notified scheme, no matter what authentication means is used. Interoperability under the Regulation is achieved by communication between nodes - single points which send and receive messages between the identity provider and the service provider. The existence of the architecture means that service providers can consume identities from any notified scheme under just one technical implementation. They could even share that technical implementation with other service providers if desirable.

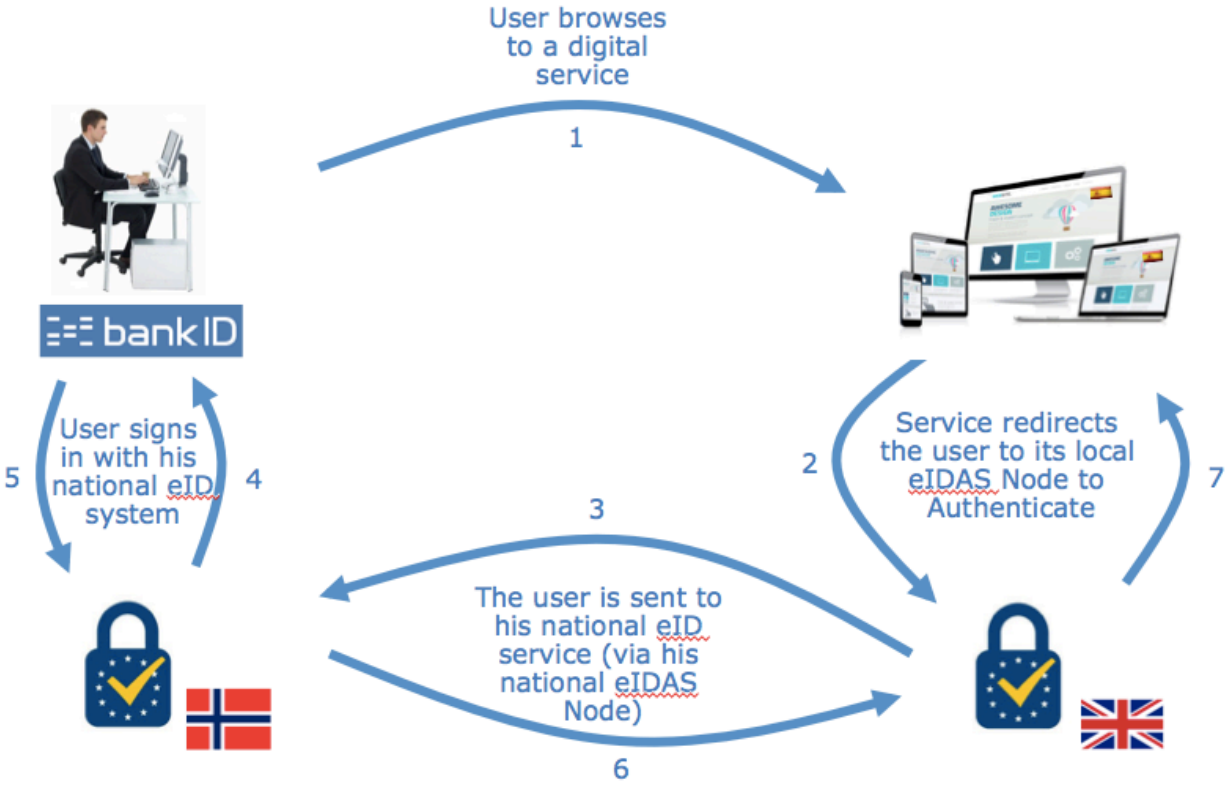


Figure 3 eID authentication under eIDAS - user accessing a UK service with a foreign (in this instance Norwegian) eID

The above diagram provides a high level architecture flow of the user journey, where the user is using their national digital identity when verifying with a digital service in another EU country. The user journey explored in the discovery project replicated this flow, as shown above.

Technical specifications developed under eIDAS have been published and include:

- eIDAS interoperability architecture,[17]
- eIDAS SAML attribute profile,[18]

[17] http://bit.ly/2by1IFd

- eIDAS message format,[19] and
- eIDAS cryptographic requirements for the interoperability framework.[20]

For Barclays being able to reuse this infrastructure they need a service that is able to connect to the national node, and make a call and receive a digital identity as per specifications under eiDAS.

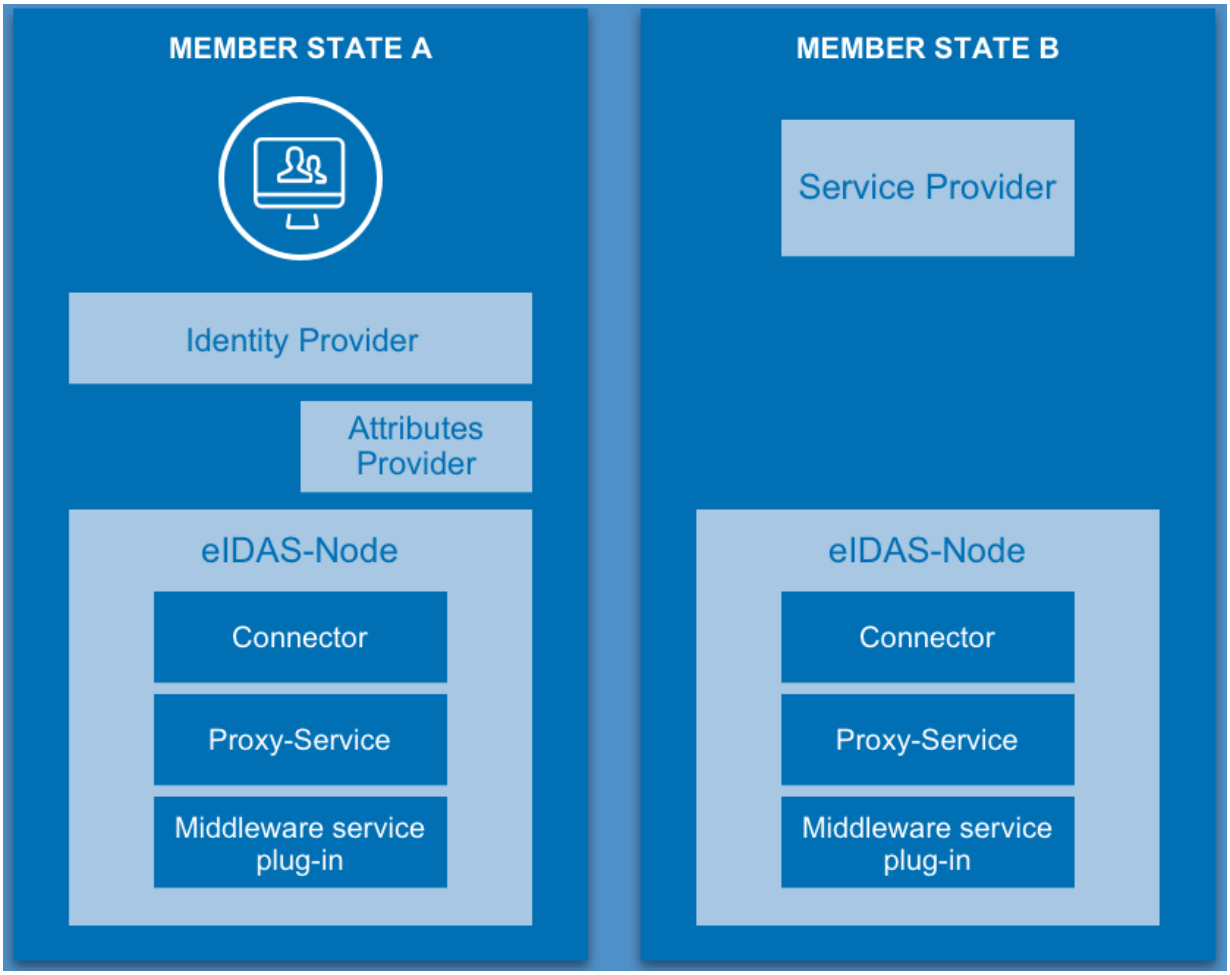


Figure 4

The diagram above 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.

[18] http://bit.ly/2eAReZi
[19] http://bit.ly/2g8QBp9
[20] http://bit.ly/2gQVD7Y

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

Following a number of project workshops PWC were commissioned by the BBA to conduct an independent survey and analysis of the current on-boarding practices across a range of UK financial institutions, ranging from the largest high street retail banks, to new entrants to the market, mutuals, and credit unions. The report can be found here.
It includes analysis of mandatory legal requirement and regulatory expectations, and other industry best practice. It provides a current and detailed view of current onboarding practices and the KYC landscape for personal current accounts amongst a wide range of bank account providers.

It then provides an analysis of digital identities that meet government standards (under GOV.UK Verify, and by extension other digital ID schemes developed in line with eIDAS regulations) against the regulatory requirements and other industry best practise.

Conclusions

The project considered how digital identities that meet eIDAS standards can benefit both customers and financial sector institutions, how they play into the regulations financial institutions have to comply with when onboarding new customers and how they could help reduce fraud. It also considered high level technical architecture and components that are needed for a service from a financial institution to be able to consume an eIDAS compliant digital identity.

Currently financial institutions use a risk based approach when onboarding customers. This is in contrast to the one applied under the eIDAS scheme, which is standards based approach. Moving to a standards based approach is not an incremental change for financial institutions but rather a step change, however, it is also a big opportunity. Because of this ongoing conversations need to continue with relevant organisations including regulators and different parts of the industry and government, as well as the EC, to ensure there is alignment around digital identities and what role they play in different initiatives.

As adoption of eIDAS, specifically notification of different schemes across the EU, is not going to be uniform it is crucial that work on this continues with the likeminded countries and organisations in order to explore the opportunities and lead the development of the identity ecosystem.

Glossary

Digital identity	The digital representation of a user that's authenticated through the use of a credential
Identity assurance	The ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity. Proving you are who you say you are to a certain level of confidence
Open identity exchange (OIX)	A non-profit trade organisation of market leaders from competing business sectors driving the expansion of existing online services and the adoption of new online products. Business sectors include the internet (Google, PayPal), data aggregation (Equifax, Experian) and telecommunications (AT&T, Verizon)
Identity provider (IDP)	Private sector organisations paid by the government to verify a user is who they say they are and assert verified data that identifies them to the relying party The organisations are certified as meeting relevant industry security standards and identity assurance standards published by the Cabinet Office and CESG (the UK's national technical authority)