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

PROJECT REPORT

EDITED BY LIVIA RALPH
FEBRUARY 2016

Contributors:

The voice of banking

Agency for Public Management
and eGovernment

Executive Summary

Customers of Norwegian banks have a very simple experience for opening a bank account. A customer can use a 'Bank ID' digital identity issued by one Norwegian bank to open or login to a bank account with any other Norwegian bank. They can also use it to access public services.

When Norwegians move overseas for work or education they expect opening a bank account to be almost as easy as it is at home. That is not the case.

This paper looks at the journey of opening a current account in the UK and reflects on how new UK and EU initiatives on digital identity might create a simpler life for the customer and reduce overheads for the banks.

Motivation / benefits

Approximately 50% of new bank accounts are opened by customers that have recently arrived in the UK to work or study and do not have an established footprint with local credit reference agencies. A digital identity, issued under a recognised national scheme that satisfies the verification requirements of the European Anti-Money Laundering Directive (AMLD) as transposed by the UK Money Laundering Regulations could be used to make opening a bank account easier.

EU and UK initiatives

There is a new EU Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS). eIDAS makes it possible to know how much trust sits behind a digital identity issued in any European country. It also makes it possible, at a technical level, for users to assert their digital identity wherever they go in Europe.

A federated digital identity scheme, GOV.UK Verify, has been created in the UK in line with the e-IDAS regulation. It meets high standards for identity verification and is being adopted across UK digital public services. How it might be adopted across the private sector is being considered.

The UK is rapidly becoming a digital economy. Customers increasingly expect to be able to open a bank account through digital channels easily and quickly without having to visit a branch. Regulators expect banks to maintain high standards for identity verification of new customers who, increasingly,

do not originate from the UK. Adoption by banks of digital identity services that meet high government standards presents a solution to these twin challenges.

Recommendations

Customer research conducted through this project showed that customers would be pleased to be able to use their domestic digital identity scheme to open a bank account when moving to a new country. This paper recommends further work to:

- Identify the practicalities of using a Norwegian Bank ID and / or UK digital identity as part of the bank account opening process through end-to-end testing,
- conduct detailed analysis on the potential benefits in terms of improved identity verification, compared to current practices, and reduced fraud.

Table of Contents

1. Introduction

The project tested the 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.'**

The project ran from August 2015 to October 2015 under the collaborative OIX framework. The British Banking Association (BBA), BankID Norge, Barclays, Cabinet Office, the Financial Conduct Authority's Innovation Hub (FCA), and the Norwegian Government (Difi) contributed towards this OIX project.

Over the period of three months the project consisted of a number of workshops and three rounds of user testing. The paper summarises the topics and findings from the workshops and findings from user research.

The scope of the discovery project was to:

- Explore ideal user journey(s) that would allow a user to open a bank account in another country using their national digital identity, with an exclusively online account opening journey,
- consider the practical, commercial, regulatory and privacy implications of such a service, and
- explore how identity works in the financial sector and how digital identity could contribute to how firms meet legal and regulatory requirements to identify and verify a customer's identity.

2. Background / context

Below, the paper notes a number of developments that relate to the subject of digital identity and provide context for this discovery.

a) GOV.UK Verify[1]

The UK government has developed GOV.UK Verify, a new way for citizens to safely and securely prove they are who they say they are entirely online when accessing digital public services provided by central government. GOV.UK Verify uses certified private sector companies to conduct identity verification checks according to published government standards. The user chooses which certified company they would like to use to establish their digital identity. A set of nine principles guides the design of the identity assurance system. A digital identity created with a certified company through GOV.UK Verify can currently be used to access an increasing range of central government services on GOV.UK. In principle, certified companies might also enable users to assert a digital identity that meets government standards in transactions with local government, NHS and the private sector. How this would operate in practice has yet to be established.

b) BankID

BankID Norge AS is an electronic ID organisation supplying all Norwegian banks, the public and private sector with an electronic ID, called BankID. BankID is used both for authentication and electronic signatures. 80% of the adult population in Norway has a BankID and is using it on average two times a week. The Norwegian BankID is a qualified eID, meaning it meets all national eID requirements for the highest level of security (level four) and the product is compliant with the EU regulations and requirements. Further information on BankID, including its history and a drawing describing business and reliability model can be found in Appendix A.

c) Electronic Identification and Authentication Services (eIDAS) Regulation[2]

The Electronic Identification and Authentication Services (eIDAS) Regulation 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.

That obligation does not apply to services provided in the private sector, whose uptake of secure digital identities remains a question for the market to determine. However, the Regulation does

[1] bit.ly/1ASQBil
[2] bit.ly/1QdPqOs

include recital 17 under which Member States should encourage private sector parties to use eID schemes notified under the Regulation to facilitate the secure provision of services to users. Recital 17 and Article 7(f) also make it clear that member states can set conditions (for example a charge) for private sector re-use of authentication capabilities.

The eIDAS Regulation does not therefore create any obligations for the private sector, but it does two specific things that make it easier for the private sector to consume digital identities from across the EU: (i) it creates a set of European Assurance levels (high, substantial and low) and (ii) it sets out an interoperability framework. Further information on (i) and (ii) is in Appendix B.

The Regulation also includes provisions on liability for notifying Member States, which private sector service providers could consider when starting to look at when relying upon digital identities under notified schemes. It does not address some of the other questions which need to be handled, such as the question of commercial models - where it makes identification and authentication free to a service online provided by a public sector body, but leaves to Member States how they establish the regime applicable to the private sector.

d) Payment Accounts Directive (PAD)[3]

The EU Payment Accounts Directive (PAD) must be implemented by September 2016. Its main aim is to further develop the EU internal market for payment accounts, by seeking to improve transparency of fee information, enhance the ability of EU citizens to switch their current accounts, and create a right of access to basic bank accounts in any Member State for consumers legally resident in the EU, subject to certain conditions.

In the UK, the provisions of the directive on basic bank accounts will only apply to those payment account providers that are designated by HM Treasury as providers of basic bank accounts. Neither Payment Accounts Directive nor the UK Payments Account Regulations 2015 make any statements about how banks should conduct identity verification. They do, however, make clear that existing UK and EU regulations and rules on anti-money laundering continue to apply.

e) Payment Services Directive 2 (PSD2)[4]

The second Payment Services Directive (PSD2) looks to extend the harmonisation of European Economic Area payments to ensure consistency of how payments are processed, and to open up the payments marketplace to new entrants. This is intended to increase competition and therefore the level of choice for consumers and businesses.

[3] http://bit.ly/1PCrSV8
[4] bit.ly/1PqBwXu

Much of PSD2 is founded on a need for transactions to have 'strong authentication' – essentially requiring payment providers and banks to be better able to verify the identity of the consumer. The drive to find ways to simplify and yet strengthen the process of authentication are increasing, accelerated by changes to customer behaviours, the take-up of mobile and alternative payment methods, digital banking and the use of new technologies.

As such, there are clear potential benefits and future opportunities for digital IDs to play a much greater role in providing a customer friendly, practical and more secure means of providing authentication and validation as part of the evolution of payment services and the roll-out of PSD2 over the next two years.

f) The European Commission's Green paper on Retail Financial Services[5]

The European Commission's Green Paper on Retail Financial Services is a new initiative launched in September 2015 which aims to uncover the obstacles that providers and consumers face when offering or purchasing financial services across the EU. The main aim is to identify means of increasing competition and its benefits for consumers, and to enlarge the market for existing providers of these services.

The PAD is an example of legislation that aims to move the retail banking sector in this direction. The Green Paper itself subsequently seeks to identify the residual issues that exist – either in the form of barriers, or the need for additional actions. For PAD, this will largely relate to the underlying 'infrastructure' needed to provide retail banking services across EU borders.

Digital IDs may be one potential solution relevant to this particular problem, and is likely be explored in more detail by the Commission as part of the Green Paper discussions.

g) BIS review of Anti Money Laundering (AML) regulations[6]

The Government launched a review of the impact on business of the current Anti-Money Laundering (AML) and CTF regime as part of the Cutting Red Tape Review programme in August 2015. The call for evidence closed on 6th November and a report is expected in the near future.

The Review will help to identify those parts of the regime where reform is most likely to deliver increased efficiency and consistency. It has specifically sought evidence on the role of supervisors in the regime and will examine the potential to tackle financial crime more effectively and efficiently, by identifying aspects of the supervisory regime that appear to be unclear, inefficient or unnecessarily

[5] bit.ly/1HYMFBz
[6] http://bit.ly/1NE1H0o

cumbersome. The aim of this review is to identify scope for better regulation that makes the regime more effective and less onerous where there is unnecessary red tape.

h) The Anti-Money Laundering Directive (AMLD)[7]

The Anti-Money Laundering Directive (AMLD) creates a common European legal basis for the implementation of the Financial Action Task Force's 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation'.[8]

Article 13(1) of the AMLD requires financial institutions within its scope to identify their customer and verify the customer's identity on the basis of documents, data or information from a reliable and independent source. Financial institutions can adjust what they do to verify a customer's identity on a risk-sensitive basis, but must be able to demonstrate to their supervisor that what they do is commensurate to the money laundering and terrorist financing risk associated with the business relationship. The European Supervisory Authorities are currently consulting on Guidelines for financial institutions and their supervisors, which set out what firms should do to satisfy the Directive's requirements.[9]

Financial institutions must normally apply the measures in Article 13(1):

- Before the establishment of a business relationship, or
- before carrying out an occasional transaction (i.e. a transaction that takes place outside of an established business relationship) that either exceeds EUR 15000 or constitutes a person-to-person transfer of funds in excess of EUR 1000.

Financial institutions cannot enter into a business relationship and must terminate an existing one where they cannot apply the measures set out in Art 13(1).

Member States have to transpose the AMLD by 26 June 2017.

European AML/CTF legislation is implemented in the UK through the Money Laundering Regulations and Proceeds of Crime Act 2002. The Money Laundering Regulations 2007 set out the current Customer Due Diligence (CDD) requirements. The UK will consult shortly on updating these regulations to transpose AMLD.

Banks in the UK also have to comply with the Financial Conduct Authority (FCA)'s financial crime systems and controls requirements in SYSC 6.1.1R and SYSC 6.3, and may have regard to both the

[7] Directive (EU) 2015/849
[8] http://www.fatf-gafi.org
[9] http://bit.ly/1NDTvg0

FCA's regulatory guidance, Financial Crime: A Guide for Firms[10] and the Joint Money Laundering Steering Group's AML/CTF guidance.

3. What we tested with customers

The project tested the 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.**'

[Image 1 Bus stop sign - Barclays proposition]

The project specifically considered a user journey of a Norwegian individual opening a UK bank account online with Barclays Bank, prior to coming to the UK, using their Norwegian digital identity - BankID Norge.

The user research consisted of three user research sessions, each having six participants in structured one to one usability interviews, to understand users' attitudes, opinions and understanding of digital identity in general. The first user research session took place in the UK, while the other two took place in Norway.

The recruited participants in the UK were 11 Scandinavian nationals and one German national while those participating in the user research sessions in Norway were Norwegian nationals.

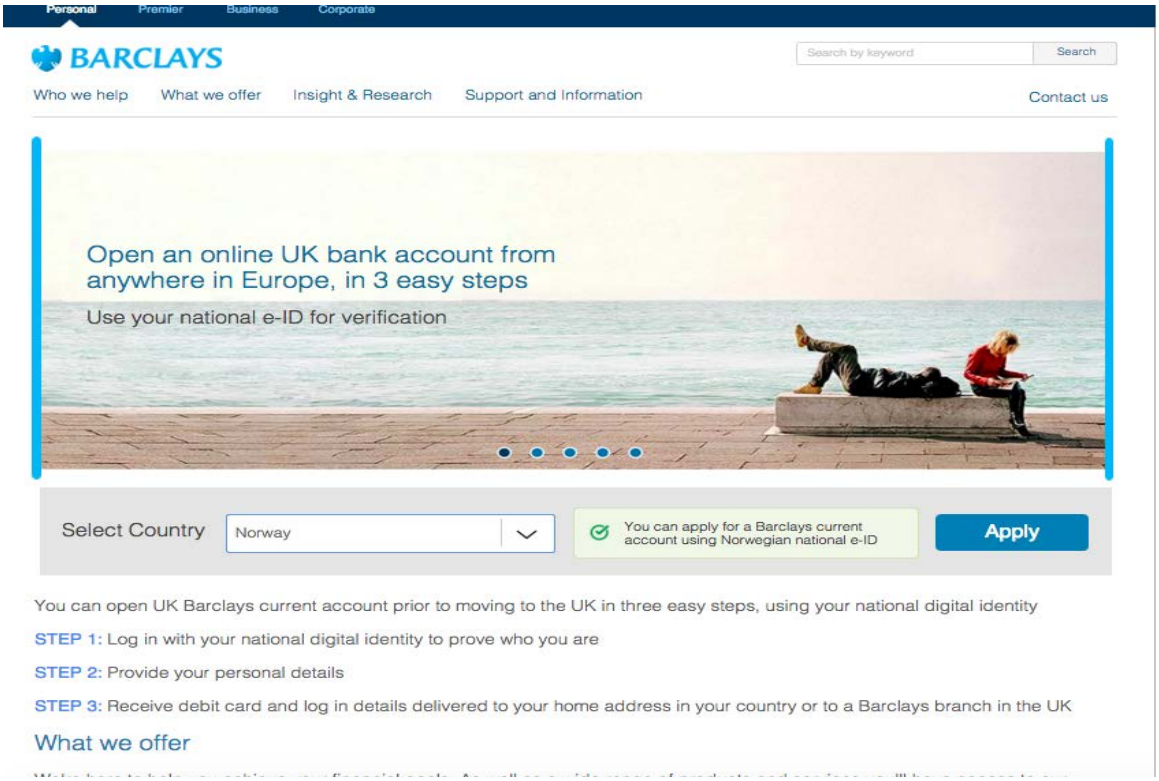
The sessions were split into two segments:

- The first segment was a discussion and inquiry into user motivations and beliefs around their experience of opening a bank account in their home country and user expectations of opening a bank account in UK.

[10] http://bit.ly/1NDTM2t

- The second segment included usability testing and research using the Barclays prototype (clickable front end wireframes). Participants went through the scenario of imagining they are moving to the UK from Norway and need to open a UK bank account. The participants were taken through one of the user journeys designed; one of them going through eIDAS interoperability infrastructure, the other staying in Barclays environment and assuming a bilateral agreement between the bank and national digital identity provider.

The full user research report can be viewed here.



[Image 2 A wireframe used in the user research - Barclays landing page]

4. Findings from the User Research and benefits for the User

Overall, the findings from the user research sessions can be split into the following themes:

- User reactions to the concept
- User journey experiences
- Experience of opening a bank account in the UK
- Expectations of opening a bank account in the UK
- Users' understanding of digital identity
- Sharing of personal data
- Reactions to the partnership between UK and Norway

"Bank account opening is the real point of entry to this country. I made three trips to the branch. I went to two different branches and got different information from them." (Tom, 27)

"I would expect to share only my identity, to open an account. It should take a short time - a few hours. Today you can open an account in the same bank straight away. If it took longer than a day it would be too long (off putting)". (Jorn 56)

Full findings can be found in the user research report.

Based on the user research, below are potential user benefits of using a national digital identity across borders to open a bank account:

a) Easier for the end user to provide credentials through a trusted channel.

The working hypothesis of the project was that recognition of digital ID would make it easier for users to apply for a bank account and would improve the overall experience of moving to another country and remove the need for corroboration of their physical credentials on arrival.

The research indicates that people are comfortable using their national digital identity and confident that their information would be in safe hands, across entities; they trust both the service (BankID Norge) and the bank (Barclays), to protect their identity.

The findings suggest users prefer seeing the eIDAS environment log in because this is a familiar and trusted service. However, the Barclays environment did not pose any serious concerns, but would require the user interface to be designed in more detail.

b) Users are receptive to the concept

The people were surprised but open to a partnership between UK & Norway that supports a federated approach in the exchange of identity data.

Being recognised in a foreign country is a very important first step for those moving overseas. The initiative not only offers individuals instant status, but also reduces anxiety and time involved in establishing oneself in a new place.

Being able to access the service on mobile is an important factor. Users prefer to access the service via their one time password on mobile, rather than by code generator. Consideration could also be given to what form of authentication is used most widely in the local country and the user experience this supports.

" National e-ID, I am confident that this is something I already have or can get easily, which is worth having if it makes the process easier. " (Tom, 27)

5. Challenges and Opportunities

How digital identity helps

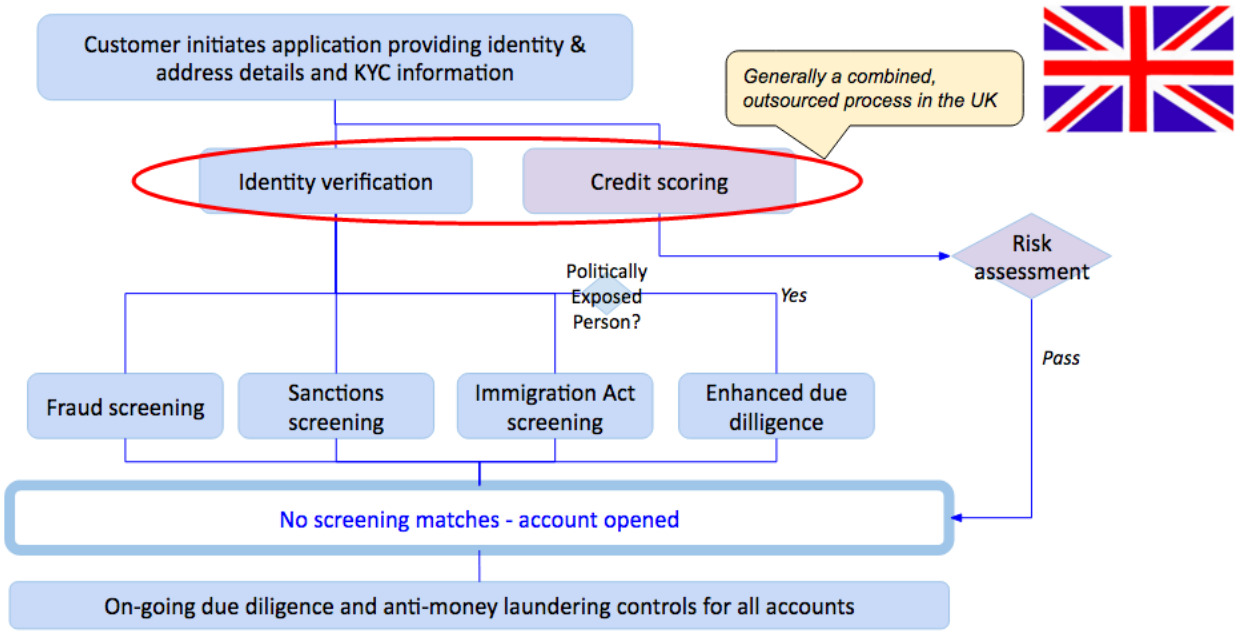
As described in section 2 (h) above, banks must identify a customer on the basis of documents, data or information obtained from a reliable and independent source. A digital identity established through national schemes recognised under the e-IDAS regulation should be constituted to meet these regulatory criteria.

Currently, UK banks use third party services to verify customers' identities. Where customers don't have 'biographical footprint' in the databases that these third parties use, either because they have recently arrived in the UK or because they do not have a credit history, then it is unlikely that their identity can be verified. Banks will then require new customers to conduct a face-to-face verification process in branch using documentary evidence such as a passport and utility bill.

Banks must also conduct a number of back office regulatory and risk management processes when opening a new account. A bank account opening process that leverages a digital identity scheme must enable the bank to reduce costs in all aspects of the account opening process if it is to be adopted. These aspects are considered in the sections below.

Current processes

The diagram below sets out the generic processes undertaken when opening a bank account in the UK.



[Figure 1: summary of a generic bank account opening process]

Banks complete identity checks, sanctions screening, immigration checks in the normal course of their due diligence procedures. Where customers have a higher risk profile, for example if they are identified as 'Politically Exposed Persons', banks are required to go further than this, and conduct enhanced due diligence. Credit checks and fraud screening are processes that enable the bank to exert its own risk appetite, and best place the bank to have robust systems and controls to prevent it from being used to further financial crime.

Banks are required to verify the identity of a customer so as to check the eligibility of the customer for the banking services they will receive. Eligibility is determined by:

- Whether the customer meets regulatory requirements such as those to prevent money laundering,
- whether the customer meets the bank's risk profile so as to prevent losses to the bank.

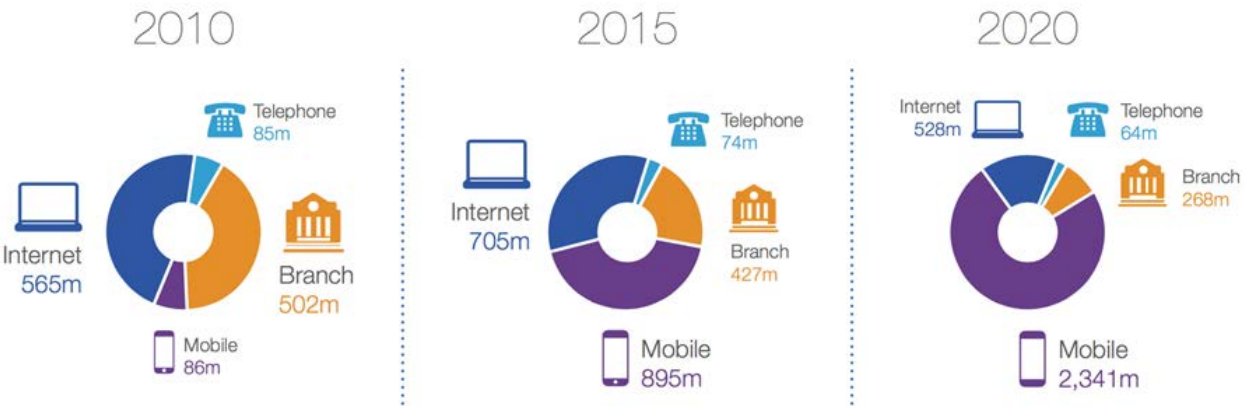
Banks match the customer's identity details against information held by third parties, including Credit Reference Agencies, fraud databases and public domain data. These banks will match the customer's identity details against appropriate databases or systems and return information for interpretation. The bank will make a risk assessment, based on the returned information, as to whether the customer is eligible for the banking services.

There are few instances where the bank is faced with certainty. The bank develops its account opening processes to a level of assurance that meets internal compliance procedures and the bank's risk appetite. These are honed to minimise risk to the bank in the current environment from fraud, bad debt or the risk of being utilised to further financial crime or money laundering.

In the UK, as in many other countries, matching of the customer's identity against the various databases and systems for account opening tends to hinge on the history of address asserted by the customer. This creates a challenge for customers who have not lived in the UK for very long and so cannot associate their identity details to an address, or where customers have little credit history such as those without debt or younger people. The bank is therefore unable to access data about the customer and therefore requires the customer to provide documents to verify their identity; this usually means the account opening process cannot be completed online, and instead the customer is required to use branch to open the account.

Opportunity from digital identity

The findings from the research above indicate that Norwegians would welcome an online process for opening a bank account. Statistics, as per the Figure 2 below, indicate a general move by UK customers to online and mobile banking. It is assumed that UK customers would also welcome a purely online account opening process as much as those new to the UK.



[Figure 2: Copyright BBA Annual Retail Banking Conference, 2015. Data copyright CACI Limited, 2015]

A federated digital identity that meets agreed government standards might also provide benefits to banks in the account opening and switching process above and beyond customer experience. At a domestic level, identity assertion through a digital identity - and the matching of the identity details to third party databases - will become standardised. This will improve match rates and therefore reduce uncertainties, risks and additional costs that are incurred in the current systems.

For 'new to country' customers, a common understanding of digital identity would permit the appropriate questions to be asked of fraud prevention and credit scoring systems in the customer's country of origin or most recent domiciled country. If structured in the right manner such questions can be answered easily and without provision of personal data across international boundaries. If the identity is known and can be referenced correctly then questions such as "does this customer appear on a Sanctions list?" can be answered with a simple 'Yes' or 'No'. Having a standardised digital identity scheme would mean fewer false positives in the screening as the name and address would be presented in a uniform way.

For the customers the win is having a digital identity which is readily verified and can be used by them across borders and across multiple parties.

To achieve this outcome then international agreement and standardisation around federated digital identity is required. There are three reasons for hope that this can be achieved in the UK:

- The UK Government is introducing a federated digital identity scheme, GOV.UK Verify, under which a number of private sector Identity Providers will establish and authenticate digital identities for customers to published government and industry standards,
- the European Union has introduced the eIDAS Regulation under which Member States' digital identity schemes will be aligned against common standards and recognised by each other,
- the UK's FCA has recently published a report setting out options for establishing regulatory "sandboxes" and proposing to set up its own sandbox by next Spring. This may afford an opportunity for the hypotheses set out in this paper to be tested in a practical manner.

Reduction in internet banking fraud

During the course of discussions on this project it was noted that Norwegian banks have very low levels of internet banking fraud. The BankID system allows a single credential to be used for access to multiple online bank accounts. The BankID system provides capabilities to detect fraudulent information about an identity between platforms and relying parties. That information is shared with the banks in the form of a warning light and some reasoning data for the light. It is up to the bank to act upon the information. The banks take action based on information received from the BankID anti-fraud system and many other sources. It is the totality that prevents the fraud becoming successful, not one single activity. It was proposed that the federated approach adopted in Norway might prevent or deter online banking fraud compared to countries where each bank issues and manages credentials for its own customers.

The greater protection might come from a number of causes:

- Norwegian banks pool resources to prevent online banking fraud through BankID and other common initiatives.
- When a compromised credential is detected it is disabled preventing any further fraud with any of the banks that use it. In comparison, a fraudster that attacks and compromises a UK customer must be detected and prevented from attacking each bank account that the customer has individually.
- Intelligence to prevent fraud that is passed between the banks in Norway flows through the single BankID system and the common FinansCERT platform, and can therefore be applied more efficiently than in the UK systems.

It is proposed that these hypotheses are also investigated in greater detail in a further project to understand if and how federated digital identity might address forms of identity fraud. Within the BankID rule set a BankID which is detected as compromised can be suspended immediately and will not be possible to use at any location from that point in time.

6. Conclusions and recommendations

The project was successful in exploring the stated hypothesis. It considered user expectations of opening UK bank account as well as user attitudes towards the tested user journeys. It also addressed challenges and opportunities associated with the use of digital identity, both cross border and within a country, by financial institutions.

The project concluded with a number of recommendations based on the discussions and findings.

Recommendations

It is recommended that an 'alpha' project is conducted:

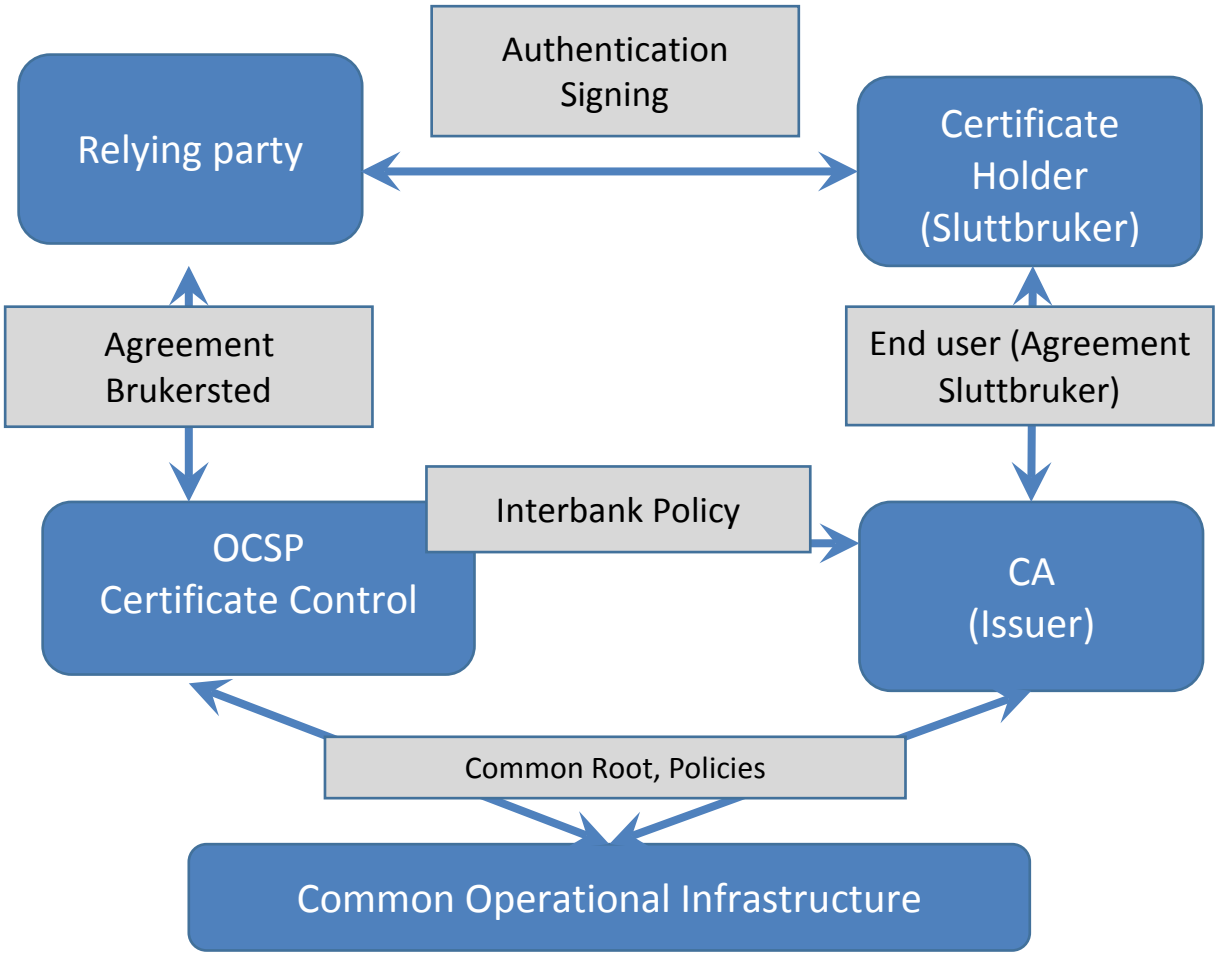
- that will consider technical practicalities of a digital identity being used by a bank to conduct checks against credit, sanctions, and other necessary databases at both national and international level,
- that conducts further analysis to understand how EU levels of assurance for digital identities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

7. Appendix A - BankID

a) History and overview

BankID was started as a project in 2001 and put into production in January 2004. Once in production Norwegian banks started to enrol their customers and by 2006-7 they had enrolled more or less 100% of their customers onto the BankID. In 2014 BankID was turned into a shareholding company with the banks as shareholders and from January 2015 the organisation took over the marketing and sales responsibilities from banks.

b) Business and reliability model



[Figure 3: Business and reliability model for BankID]

8. Appendix B - eIDAS

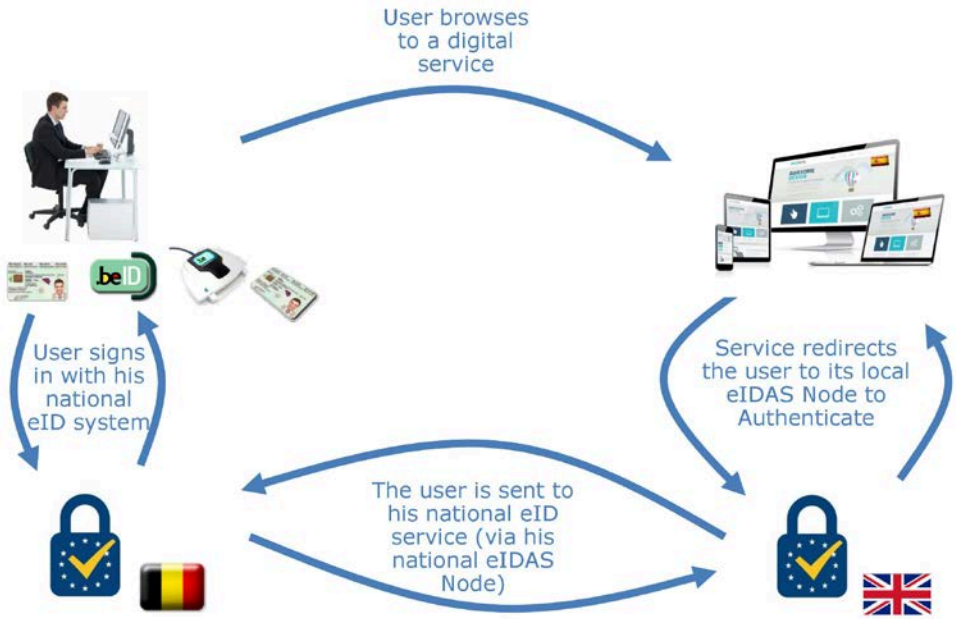
Further information on the assurance levels and the interoperability framework

a) The assurance levels are a way for service providers to be able to trust digital identity schemes notified (formally presented for use to the EU Commission and other Member States) under the Regulation (to the level at which they are notified) without the service provider having to do their own examination of each.

   There are three European assurance levels: low, substantial and high that have been further specified in the Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means. They are outcome based. They do not set one way to do identity assurance across the EU, but they do set requirements for a level of trust which must be met before a scheme can be notified under the Regulation. During the notification process, all Member States have the opportunity to peer review the scheme being notified.

b) The interoperability framework, that has been further specified in the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework, 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.

   This is comparable to the technical architecture used for GOV.UK Verify, with the part of the service that's on GOV.UK being replaced by nodes sending and receiving the cross-border request. 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 4: eID authentication under eIDAS - user accessing a UK service with a foreign eID]

9. 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)