OPEN IDENTITY EXCHANGE
White Paper

Connecting Europe Facility: Opening a bank account across borders

Project Report and Findings

Co-financed by the Connecting Europe Facility of the European Union

The project reported within this document was awarded grant funding from the European Commission's Innovation and Networks Executive Agency (INEA) in May 2017. The coordination and management of the delivery has been performed by the OIX on behalf of the Consortium members.

The project consortium participants were:

Barclays
Government Digital Service (part of Her Majesty's UK Government)
HSBC
Morpho (trading as IDEMIA)
OIX UK (part of the Open Identity Exchange)
Orange

The project was supported through technology and services by:

ForgeRock
SecureKey
Ariadnext

Contents

Executive summary

The internet's commercial economy is dominated by a small number of marketplaces - Amazon, Facebook, Google, et al - under which people and organisations transact with one another on a fleeting, occasional or regular basis with low friction and a high degree of clarity on liabilities and consequences. These marketplaces operate smoothly across national boundaries and serve a limited - though growing - range of transactions and services.

Opening a bank account across a national border has been used in this project as an example of the challenges faced by traditional businesses in adapting to new customer behaviours in the digital age. More people than ever before spend time overseas to live, work and study. They need local access to financial services. But the growth of money laundering and criminal finance place greater onus on banks to validate information about people before and throughout their business relationship. With ever growing quantities of data to check, banks must continue to discern the 'truth' from what is fraudulent or misleading.

The Connecting Europe Facility project looks at the relay of 'trustworthy' data about a person across national boundaries. It is founded on innovation driving changes in European regulations.

The first is a change in the EU Anti-Money Laundering Directive to accept digital identities recognised under EU Regulation 910/2014 (eIDAS)[1] as appropriate for identity verification purposes when opening a bank account. The 5th Anti-Money Laundering Directive will be transposed into national laws by 10th January 2020.

The second is a change in a citizen's entitlement to his or her data as set out in the General Data Protection Regulation (GDPR)[2]. Citizens now have the 'right of data access' and 'right of data portability', as defined in the regulation. Given that businesses must now make this personal data available to their customers, the project has looked at how customers might obtain value from it and how that presents a commercial opportunity for the businesses supplying it.

How these changes in regulations will manifest themselves in new digital services for customers is as yet unclear. The market of digital identity services is at an early stage of maturity, fragmented and sensitive to context and culture. However, it is clear that people and businesses need better solutions for establishing the trustworthiness of data asserted in digital transactions and that government

[1] EU Regulation 910/2014 of 23 July 2014 on electronic IDentification, Authentication and trust Services https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[2] https://eugdpr.org/

endorsed standards have an important role in creating the trust environments for more efficient commercial transactions.

Project Synopsis

The objective of this project is to illustrate how a verified digital identity can be used to improve the current sometimes cumbersome, paper based, time consuming processes that EU citizens have to engage with to open bank accounts in another EU country. This process currently is a barrier to both citizen and bank alike.

The project specifically considers how a digital identity, created in a live digital identity service in France, can be transported through a technology infrastructure as described in the eIDAS regulation to a UK bank's customer onboarding service. The aim is to demonstrate how a digital identity could improve the customer's experience, as well as provide additional benefits to the banks through reduced operational burden.

The project was driven by a consortium of Barclays, Government Digital Service (part of Her Majesty's UK Government), HSBC, IDEMIA, the OIX (Open Identity Exchange) and Orange. ForgeRock, SecureKey and Ariadnext supported the consortium by providing a technology and services. The Consortium was awarded grant funding for the project from the European Commission's Innovation and Networks Executive Agency (INEA) in May 2017 to deliver the project and the Consortium's findings. The coordination and management of the delivery has been performed by the OIX on behalf of the Consortium members.

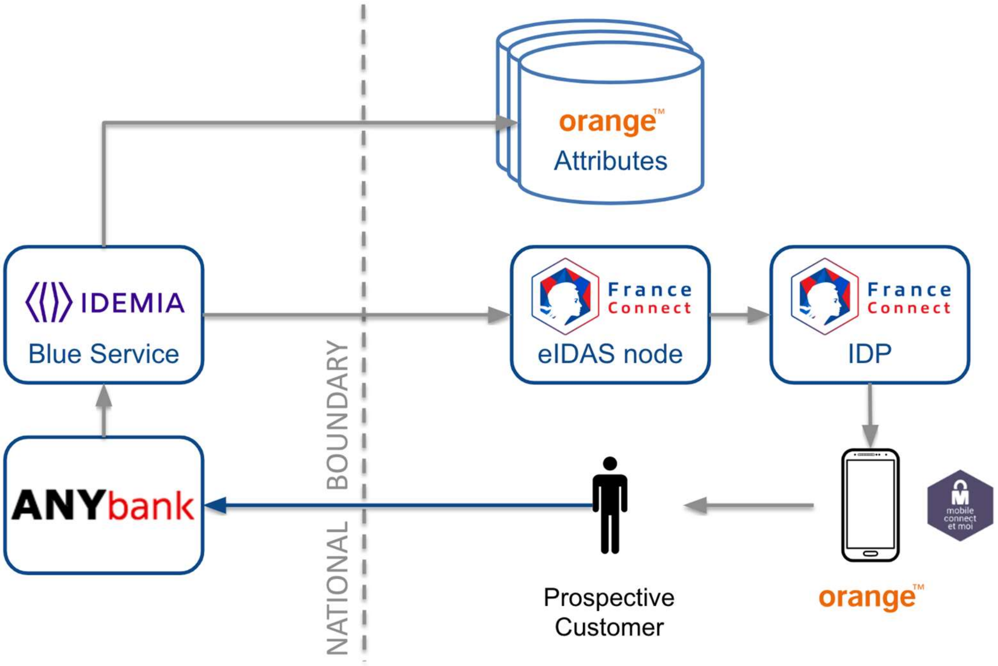
The project was initiated before the UK's decision to leave the European Union. However, it is expected that the legislation relevant to this project will be adopted by the UK. In either circumstance, the challenges of establishing trust in identity details when transacting across national borders remains pertinent.

The project delivered a technical prototype that demonstrated how a French Digital Identity (that is aligned with eIDAS) could be accepted by a UK bank, as part of the online process to open a bank account. The transaction was simulated in a prototype testing environment, to demonstrate a proposed customer journey. In addition to the technical work, operational factors were also considered, such as liabilities and commercials factors.

The technical prototype includes:

- a demonstration application of a customer journey (see narrated video)
- a technical specification for integration to the French eIDAS node
- the 'Blue Service' for consent management, digital identity and attribute orchestration

- a connector to the French eIDAS node and Identity Provider (France Connect) through which the user accesses Mobile Connect et Moi Identity Provider with Orange's Mobile Connect authentication service
- a mocked Attribute Provider.



Conclusions and recommendations

Digital technologies have reinvented many industries and spawned new methods of conducting business. Cryptographic solutions have improved the security with which data can be transferred and disseminated between people and organisations through digital channels. However, the challenge of establishing 'trust' in digital information is only partly solved through new technologies.

The Connecting Europe Facility project on opening a bank account across borders has used well established technologies and frameworks to consider how organisations can use the new regulatory environment in Europe to unlock the value of 'trustworthy' identity and personal data. A number of conclusions and recommendations can be drawn from its work.

1. It will take some time for new market offerings to be developed that leverage the new regulatory frameworks. Many trustworthy sources of personal data have not been made available for people to exploit through digital channels. Multiple organisations and stakeholders need to digest the operational implications of the regulations for their businesses and determine how they should adapt. The need for and commercial viability of new products and services will become apparent once the operational implications have been

tested. A ‘regulatory sandbox’ will provide the ideal testing environment for understanding how to deploy service innovations.

2. People have developed an expectation of how personal data is shared in transactions. The CEF project has developed a service based around a new model enabled through government grade digital identities. However, new language and service designs will be required to communicate this new approach to people in ways that convey the benefits. This is best done in specific contexts through real deployments.

3. Any number of technologies could be deployed to deliver innovative services such as those proposed through the CEF project. Though some technologies will doubtless prove more or less effective in some contexts, the greater challenge is to devise an implementation plan that allows scale to be achieved sufficiently quickly so that investors have confidence in the timeline to profitability. This will require solutions that are designed to be technologically and contractually interoperable. It will also require government bodies and regulators to encourage and facilitate collaboration between commercial organisations, including between rivals.

4. All parties will require clarity on their contractual liabilities. These liabilities should apply where organisations have not achieved the operational standards that they have declared. They may be capped. An organisation’s pre-existing liabilities are not displaced through the acceptance of a digital identity.

5. Commercially, a digital identity federation has many participants each of which provides value. An end beneficiary, such as the bank, will pay a single fee for this value which will be apportioned through a series of bilateral agreements.

6. Further work should be commissioned on protective monitoring. Any organisation that relies on a digital identity will require a system of alerts to be in place in the eventuality that the digital identity is compromised. Technologically, such a service is not complex to implement. However, agreeing how such a service should operate will be a challenge and should be facilitated by governments and relevant international organisations.

Whilst the European Union is the largest single market in the world, its growth is impeded by the lack of trade across national borders. Creation of a digital single market in which ‘trust’ transfers across borders will reduce the barriers to cross border trade and accelerate economic growth. Governments should build on the work of this project and encourage public and private sector adoption of commercial digital identity services.

Terms used in this document

ANYbank
A fictitious UK bank to which the French customer applies for a bank account before moving to the UK.

Attribute Provider
The organisation that the customer chooses to supply an item of his / her personal data to another party, in this case ANYbank.

Blue Service
The prototype name given for the service that connects ANYbank to the Identity Provider and Attribute Provider.

France Connect
France Connect is the French national digital identity scheme that allows French citizens to assert identity details in digital transactions.

Identity Provider
With the authorisation of the customer Mobile Connect et moi provides his or her identity details, validated under France Connect, to ANYbank.

Mobile Connect
This is a GSMA standard for authentication on mobile phone where users are identified by their mobile number.

Mobile Connect et moi
This is the French Identity Provider relying on Mobile Connect for authentication through a mobile phone. Mobile Connect et moi is available to any Orange France subscriber and in the near future to subscribers of other French operators.

Introduction

The value of the digital economy is restricted by a reluctance to buy and sell goods and services across national borders. Trust in the provision and acquisition of personal data through the internet is a major obstacle. Organisations must have confidence in the provenance and validity of personal data acquired and people must have confidence and control in how their personal data is shared. Removal of these obstacles across Europe could unlock many billions of Euros in value to commerce and the wider society.

The Digital Single Market aims to create the right environment for digital networks and services by providing high-speed, secure, trustworthy infrastructures and services supported by the right regulatory conditions. Creation of the Digital Single Market[3] is driven by the European Commission’s Directorate-General 'Communications Networks, Content and Technology' (DG CONNECT).

The EU Regulation 910/2014 of 23 July 2014 on electronic IDentification, Authentication and trust Services (eIDAS)[4] has created an interoperability framework between Members States on standards for identity verification in digital channels. Whilst the regulation only applies to public sector transactions, the national digital identity schemes that have been notified under eIDAS have the potential to be commonly adopted and trusted in private sector transactions in the same manner that passports and driving licences are accepted in face-to-face transactions. Interoperability between the public and private sectors is seen as critical for success of digital identity schemes as well as for successful development of the Digital Single Market.

This report provides an overview of the findings of a project funded by the European Commission to facilitate the adoption of eIDAS compliant digital identities by the private sector. The project focuses on one specific example of where the establishment of trust in a person from another Member State creates cost and inconvenience for all parties - opening a bank account in another EU Member State.

The project developed a prototype infrastructure and demonstrator application through which a digital identity, created in one country could be used in another country to expedite the opening of a bank account. Today, opening a bank account in another country can be very slow, sometimes taking several months. The project demonstrated how the end-to-end process could be done in minutes through the adoption of a digital identity infrastructure.

[3] https://ec.europa.eu/commission/priorities/digital-single-market_en
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

The project was conducted by a consortium of organisations brought together by the UK Government Digital Service: Barclays, HSBC, IDEMIA, the Open Identity Exchange, Orange and the UK Government Digital Service. It used the example of a French citizen who is planning to come to the UK to work or study and would like to open a bank account from France using his or her national digital identity.

Today in France Orange customers can use *Mobile Connect et moi* service which allows them to assert their French national digital identity, provided by France Connect, in digital transactions.

The project built an infrastructure that would enable a bank to accept this as evidence of identity when opening a new bank account. The 5th Anti-Money Laundering Directive[5] recognises eIDAS compliant digital identities as appropriate means of identity verification, stating in Article 13.1:

> *"Customer due diligence measures shall comprise:*
>
> *(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation EU 910/2014 or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities."*

The Directive has yet to be transposed into UK law, at which point industry guidance will be written by bodies such as the Joint Money Laundering Steering Group (JMLSG). It should be emphasised that the recognition of eIDAS compliant digital identities is not a requirement for banks to use or accept them. It is rather an option that banks can choose to verify identities of their potential customers.

Whilst this wording is important in satisfying Customer Due Diligence officers within banks, there is still a requirement for banks to receive and verify other data about their new and existing customers, as discussed below and in greater detail in Annex B. For example, banks must maintain accurate contact details for their customers as well as information about their tax status and source of funds. The project proposed a solution architecture that leverages the citizen's right of data access and right of data portability defined under the General Data Protection Regulation (GDPR). It demonstrates how a digital identity can be used to access and pass personal data from one organisation to another in a manner such that its trustworthiness can be assessed by the recipient.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN

The problem of trusting personal data

The internet does not recognise national borders. It enables people from one country to engage and transact with people and organisations in any other country. For organisations, it means their goods and services can be made available to a far greater market of customers than ever was practical to consider before. For people, it means they can choose from a far wider range of suppliers and supplier offerings. The internet should drive efficiencies in both supply and demand for goods and services.

However, the development of trust across national borders takes place slowly. To a large degree, trust is established by understanding what will happen when things go wrong. In most commercial transactions, financial compensation is the appropriate remediation and this is most often facilitated by the banking and payments infrastructures.

However, financial compensation is often not appropriate, particularly in cases of criminal activity. National regulations require organisations to apply measures to safeguard against the risk of such outcomes. Frequently, these regulations necessitate identity verification processes. For example, banks are subject to ever tightening regulations to prevent money laundering and criminal finance. This requires them to conduct a number of Customer Due Diligence checks when opening and operating bank accounts.

Increasing volumes of people are moving to new countries to study, work and live. In 2017, Foreign citizens made up 7.5% of persons living in the EU Member States[6] and 3.8% of European Union (EU) citizens of working age (20-64) were residing in another Member State than that of their citizenship[7]; this share has increased from 2.5% ten years ago.

They need access to local financial services but the process of opening a new account locally can be time consuming and expensive both for the customer and the bank. In the UK some banks estimate that 50% of new bank account applications are from customers from overseas.[8]

The difficulty of opening a bank account is a source of frustration for both customers and banks. This is supported through high drop off rates in the application process. The requirement to present physical documents either in person or through the post, is an inefficient way of processing identity documentation. (Whilst a document and

[6] https://ec.europa.eu/eurostat/statistics-explained/index.php/Migration_and_migrant_population_statistics

[7] https://ec.europa.eu/eurostat/documents/2995521/8926076/3-28052018-AP-EN.pdf/48c473e8-c2c1-4942-b2a4-5761edacda37

[8] https://oixuk.org/opening-a-uk-bank-account-with-a-norwegian-bankid/

facial image can be presented online, this data needs to be validated by the bank.) Focus on 'traditional' forms of identity documents and data excludes certain user groups including international customers with limited or no local footprint.

Creation of eIDAS compliant digital identity schemes improves the efficiency with which people can assert verified identity details to organisations. The CEF project aims to develop an architecture that solves three residual problems facing the private sector when transacting with their customers digitally:

1. A customer might originate from any country and might therefore have a digital identity developed to a variety of national standards. So the private sector organisation needs to understand which national standards the digital identity aligns to and consider whether any risks need to be mitigated.

2. Verified identity details are necessary but not sufficient for most transactions; other data is normally required. In the context of opening a bank account this is often referred to as ‘Know Your Customer’ data. Whilst a core set of these attributes will be consistent from bank to bank, some will vary depending on the context of the transaction, a bank’s business processes and risk appetite.

   When a customer presents the evidence required, the organisation needs to be able to validate the evidence and ensure it is linked to the same identity as the person providing it.

   However, it is unlikely that the entity able to establish the identity of the customer to the required level of assurance is also able to establish the validity of all necessary attributes about that person.

3. Validating evidence presented by a customer through back office procedures is inefficient. The independent sources used to validate information may be out-of-date or may have been inaccurate to begin with. Ensuring that the data relates to the right person becomes the responsibility of the back office function and so the back office function may have to revert back to the customer to corroborate any information uncovered that doesn’t reconcile with the customer’s information. This can be frustrating for all parties.

Solution Design

The solution was designed around a number of service components. These included existing services as well as demo services created specifically for the project.

France Connect is the French national digital identity scheme. Orange France mobile customers can use a live service called **Mobile Connect et**

moi that allows them to authenticate and assert their French national digital identity in transactions. This service was launched November 2017; at time of writing, more than 60 000 Orange customers have created their digital mobile Identity. **Mobile Connect et moi** offers a strong two factor authentication and is in the process of being certified to the eIDAS *substantial* level.

The **ANYbank** application process was designed as a generic bank account opening process with the consultation of Barclays and HSBC. The ANYBank application was provided by ForgeRock using its Banking Demo application.

ANYbank integrated with the IDEMIA **Blue Service** to facilitate provision of trustworthy identity and personal data by the prospective customer.

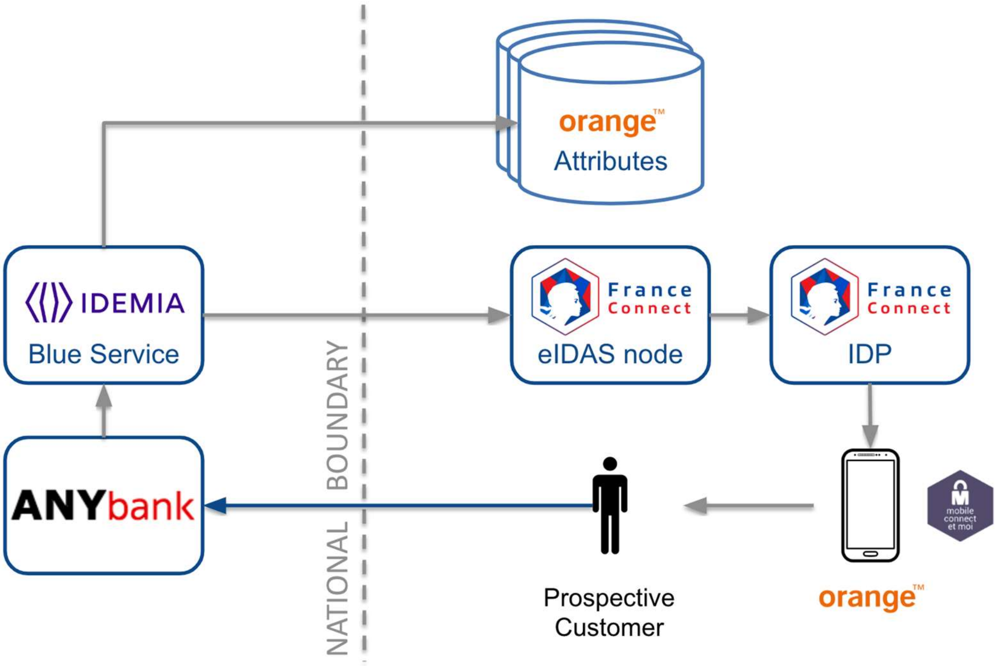
ANYbank chose to accept address details for French customers from three **Attribute Provider** services. These services do not exist and were fabricated for the project. Orange France, HSBC France and a French Authority were envisaged as Attribute Providers that ANYbank would accept (representing a mobile provider, financial institution and a government institution respectively).

A digital identity acts as the basis for trust in the proposed solution. Defined against government standards which are recognised internationally under the eIDAS regulation, the digital identity is considered as a satisfactory mechanism to recognise the customer in the digital transaction and for the Attribute Provider to accept consent to share data with ANYbank.

The project used the User Managed Access (UMA) protocol[9] as the basis for the Blue Service solution. UMA is a profile of OAuth 2.0 and has been developed to allow a person to control the sharing of his or her data with third parties (where the control can be realised through a central authorisation system). In UMA, a user can share his or her data between different applications (person-to-self sharing) but also with other users and organisations (person-to-service and person-to-person sharing).[10]

[9] https://docs.kantarainitiative.org/uma/ed/uma-core-2.0-01.html

[10] https://kantarainitiative.org/confluence/display/uma/UMA+Scenarios+and+Use+Cases



UMA defines a number of logical entities:

- The **Resource Owner**, the Prospective Customer, who manages his or her data and provides consent for identity and other details to be passed to ANYbank
- The **Client**, the ANYbank account opening application that will receive the data of the Resource Owner
- The **Requesting Party**, a party for whom data will be shared. In the CEF project, this is the same Prospective Customer who also plays the role of a Resource Owner. A Requesting Party controls the Client which asks the customer to provide evidence of address from one of the three accepted Attribute Providers
- The **Resource Server,** which has the customer data and from which the Attribute Provider will send that data
- The **Authorisation Server**, the kernel of the process which manages the sequence of dialogues which results in authorisation being given for the data sharing; it is where the consent for sharing the data is stored and managed.

UMA's goal is to address the complexities of data sharing described above in the digitally interconnected modern market. The project's manifestation of UMA through the Blue Service is intended to create a familiar, repeatable user experience for data sharing to facilitate the user's trust and understanding of the process (as the Blue Service can provide a single, common and intuitive user interface for establishing trusted connections between Attribute Providers and Clients). It is designed around core concepts of user-centric data sharing:

- **Context**; the Blue Service is presented within the ANYbank account opening process - sharing of the data is done during the actual transaction (and does not have to happen beforehand).
- **Choice**; consent for sharing the data is captured within the Blue Service - the customer could always review this consent and change it according to their wishes (e.g. having full control over the relationship between institutions which is in line with GDPR).
- **Control**; although not designed for this project the Blue Service would provide tools for the user to share data granularly (i.e. share the right amount of information required for a particular transaction).
- **Respect**; sharing of the data is done according to the customer's wishes and preferences - i.e. the Blue Service, which mediates access between ANYbank and respective Attribute Providers, makes sure that the shared data is used appropriately.

A more detailed mapping of the CEF project solution design and the UMA protocols can be found in Annex A describing how the identity details are matched before release of the data by the Attribute Provider.

Security and resilience

Confidence in the end-to-end security and resilience of the infrastructure is essential for trust by all parties. In the CEF solution design the Blue Service connects the customer's choice of Identity Provider and Attribute Provider to the bank. Its standards for security and resilience must achieve the highest common factors between the private sector banks and Attribute Providers with which it contracts and the inter-government agreements under eIDAS.

In the CEF solution only the customer's digital identity information is decrypted by the Blue Service. The identity details act as the key for permissioning the sharing of personal data between the Attribute Provider and the bank but the data is passed directly between these two end points. The Blue Service cannot therefore act as a point from which to harvest a customer's personal data.

Benefits of the solution

The CEF project has focused on the use of trustworthy identity and personal data across international borders. The majority of benefits described below apply equally within a country.

For a customer the solution represents a convenient way to provide evidence of his / her identity and personal details remotely through a digital channel. The association to government standards for identity and attributes, and implied alignment to regulations such as the General Data Protection Regulation provide reassurance that the data sharing methodology is trustworthy.

In practical terms, the solution would provide the tools that the customer needs to manage his / her data sharing arrangements with third party organisations such as ANYbank, (although fine grained data sharing permission tools were not developed for the project). Most importantly the customer needs transparency on the quality of information that he / she needs to provide to access a service, and how these quality standards can be achieved.

Familiarity with a workflow that is consistent from one transaction to another will increase the customer’s confidence to share personal data. In time this will drive customer demand for organisations to make customer’s data available through such services, in line with the rights set out in the General Data Protection Regulation.

For the bank the solution represents a simplification of its current identity verification processes and a set of standards that can be more easily evaluated against the bank’s risk appetite. By implementing consent based agreements with customers the bank can reduce its costs for ongoing Customer Due Diligence.

Recognition of eIDAS in the 5th Anti-Money Laundering Directive creates a simpler dialogue with regulators on how the bank meets its Customer Due Diligence obligations. Banks remain liable in the event of risks being realised but the agreement of industry wide, regulator approved standards presents an opportunity for the industry to address the challenges of rising fraud and money laundering collectively without collusion or anti-competitive practice. However, to realise this opportunity, cross jurisdictional regulators would need to work together to support adoption of the standards.

Under the second Payments Services Directive, Open Banking in the UK and the General Data Protection Regulation banks are being obliged to open up their customer data for their customers’ benefit, with their consent. There is substantial value to third parties, including other banks, in the data that banks have validated about their customers. As described below, this presents a commercial opportunity.

For society the increase in money laundering and criminal finance perpetuates and accelerates all manner of harm. Banks have important responsibilities and work proactively with regulators. But with the growing complexity of the financial systems and the vast quantities of data a bank must check, the current model appears unsustainable. For banks to fulfil their obligations in these three areas there will inevitably be an increase their operating costs.

The solution represents an opportunity for individual citizens to participate proactively in the reduction of criminal finance whilst taking greater control of their data sharing relationships.

Though not explored in the project, the economic benefits of facilitating the opening of accounts by customers from one country with financial service providers operating in another should be significant. Currently, so-called ‘passporting rights’ provide a licence which, once granted, has unitary effect throughout the European Economic Area. However, in effect, the difficulty of verifying the identity of people from other countries inhibits the realisation of this market.

Major themes considered by the project

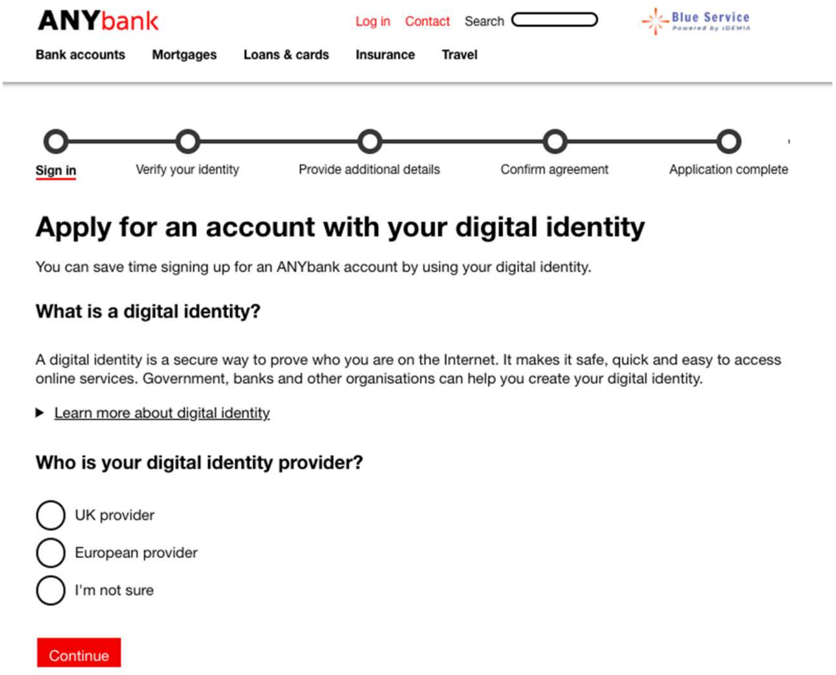
Adoption requires a number of aspects of the federated digital identity to be addressed. A summary of the findings on each aspect is provided below.

1. The user experience must be comprehensible

A prototype was developed through which the project team demonstrated the user journey for opening an account with a UK bank called ANYbank. The first iteration of the journey is illustrated at points within this document and the access to the later online version is available upon request. A narrated video of the user journey can be found on the internet.[11] The design of the user journey has a number of challenges.

1.1 Maintaining the prominence of the interaction with the bank

The customer has chosen to apply to ANYbank for his or her account. It is the expectation of the customer that the application process will happen on the ANYbank website.



Apply for an account with your digital identity

You can save time signing up for an ANYbank account by using your digital identity.

What is a digital identity?

A digital identity is a secure way to prove who you are on the Internet. It makes it safe, quick and easy to access online services. Government, banks and other organisations can help you create your digital identity.

▸ Learn more about digital identity

Who is your digital identity provider?

○ UK provider

○ European provider

○ I'm not sure

The user journey was therefore designed to maintain the prominence of the ANYbank brand even though ANYbank is using a third party service, the Blue Service, to enable its customer to share digital identity and personal data from trustworthy third parties.

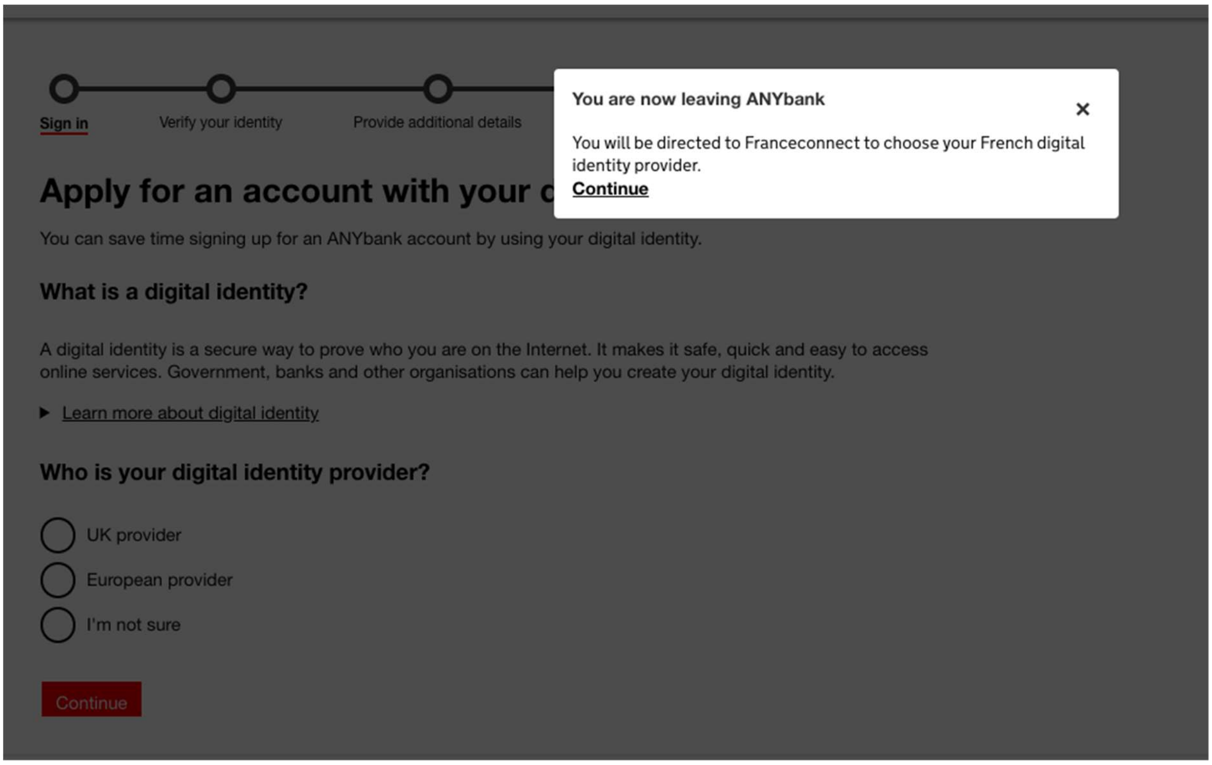
[11] https://vimeo.com/297324209/b1c287a577

The Blue Service brand appears discreetly on the ANYbank page in the top right hand corner. It is assumed that the role of the Blue Service will not be apparent - or of interest - to the customer until he or she has used it a number of times.

1.2 Redirection to the Identity Provider

The customer chooses to assert identity details to ANYbank through his or her French national Identity Provider. This requires a redirection to an authentication service under the France Connect scheme, such as the *Mobile Connect et moi* service.

On first use of a digital identity the customer might well be surprised to be redirected from the website of the organisation requiring proof of identity. The user journey was designed to cater for the unfamiliarity of the experience with text intended to explain what is happening. An overlay box explains that the customer will be directed away from the ANYbank website.



You are now leaving ANYbank

You will be directed to Franceconnect to choose your French digital identity provider.

Apply for an account with your d

You can save time signing up for an ANYbank account by using your digital identity.

What is a digital identity?

A digital identity is a secure way to prove who you are on the Internet. It makes it safe, quick and easy to access online services. Government, banks and other organisations can help you create your digital identity.

▸ Learn more about digital identity

Who is your digital identity provider?

○ UK provider

○ European provider

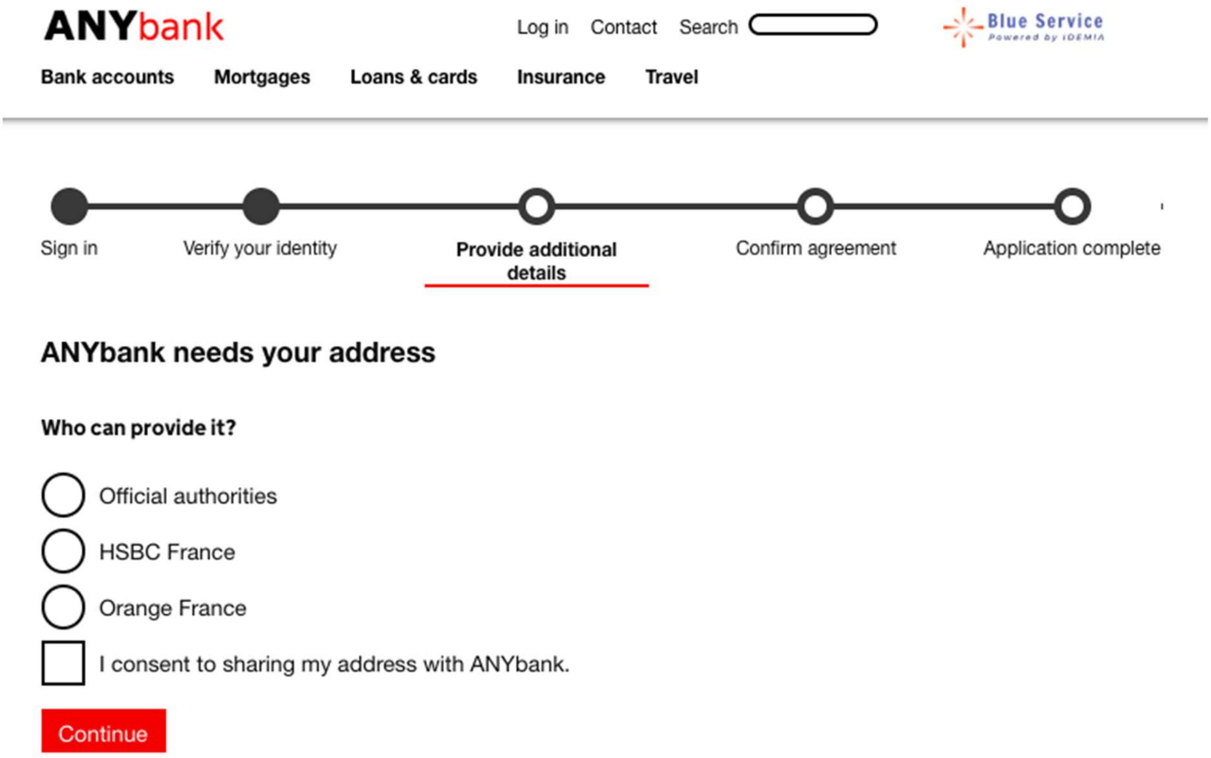
○ I'm not sure

The *Mobile Connect et moi* service is currently in live operation so was deployed in the prototype in a manner that closely reflects the current service. However, the project team recognised the potential confusion to the customer from this element of the customer journey, in particular in the first few times it is used.

After choosing Mobile Connect et moi, the customer has to enter his or her Orange France mobile number to initiate an authentication transaction on his or her mobile to share digital identity details.

1.3 Linking trustworthy sources of data through the Blue Service

The prototype considered how a single attribute that is not contained within a digital identity could be shared with ANYbank through the Blue Service. The example used was 'address' which is not part of the digital identity definition under France Connect.



ANYbank needs your address

Who can provide it?

○ Official authorities

○ HSBC France

○ Orange France

□ I consent to sharing my address with ANYbank.

The project imagined that three "Attribute Providers" were available to the customer in this transaction. Each one must be considered as appropriately trustworthy sources of evidence of address for ANYbank, although each will have different characteristics. ANYbank must have configured the Blue Service so that these three organisations appear, each of which has met its threshold level of trustworthiness. In reality many more organisations might, so this part of the user journey might look quite different.

Likewise, the customer may not have a relationship with the three organisations presented as options. For the user journey to be satisfactory the customer must be able to link a source of address with an organisation with which he or she has a relationship. The Blue Service therefore needs to broker agreement between multiple Attribute Providers to share attributes and multiple Relying Parties to accept them. The design of the user journey might look quite different to the one developed in this circumstance.

1.4 The fragmented digital identity and personal data market

The digital identity market is at an early stage of maturity and highly fragmented. As a result customers are uncertain of the concept of a digital identity or which provider they might use to get one. The situation is mirrored for organisations: most of which do not know what the benefits of a digital identity are or, if they do, how best they can access digital identities. The market for user controlled attribute provision is less mature still. The plurality of early stage options and paucity of general understanding mean that it will be some time before a viable market is established.

2. The design must evolve based on user research

The consortium conducted user research in the form of a small survey[12] in which employees of consortium members were asked to watch a video[13] of the prototype and then answer question about their experiences opening a bank account in another country. Respondents were mostly, but not exclusively, referring to opening a bank account in the UK. (The sample size was small and the results are therefore not statistically significant.)

When asked about their experience of opening a bank account, two described it as ‘very easy’, ten as ‘easy’, eight as ‘neither hard nor easy’ and seven as ‘difficult’, and one as ‘very difficult’. Some explained that their expectation was that opening an account would not be easy: *“You need to ensure that your documents are in the right format and have the right attestations.”*

When asked what a digital identity is, one respondent from Romania replied: *“That's why Google exists - but, my understanding of it after watching the video is that it is a virtual way of identifying your personal details to accredited institutions for various purposes, with your consent.”*

However, when asked “Would you have created a digital identity if it had made opening a bank account easier?” 26 respondent replied ‘yes’ with two responding ‘maybe’ and no people responding ‘no’. Also, when asked if they would use a digital identity if they already had one, 24 said ‘yes’, two ‘maybe’ and only one said ‘no’.

[12] https://www.surveymonkey.co.uk/r/79YQT2G
[13] https://vimeo.com/297324209/b1c287a577

Respondents were more cautious of sharing personal data. When asked “Would you have shared other personal data in a similar way?” only 13 replied ‘yes’, eight ‘no’ and seven ‘maybe’.

One respondent from Pakistan wrote: *“I am quite sceptical about sharing such personal data cross border or within the country especially after hearing how governments have spied on their own people in the past and that nothing is safe. I'd rather go through some trouble the traditional way than risk my data being tracked and potentially stolen.”*

3. The bank’s liabilities must be clear

Annex C provides a description of a bank’s liabilities when opening and operating a bank account for a customer today and how these liabilities would change under the model proposed in the project. It makes the following conclusions:

> Banks are exposed to potential losses when opening and operating accounts for their customers. These liabilities can be placed in a number of categories. Verification of the identity of the account holder and personal details about the account holder is an important mechanism for mitigating the risk of these liabilities being realised. Banks also have a regulatory obligation to verify the account holder in a manner commensurate with the circumstances.
>
> There is no universal, foolproof identity verification solution. Banks provide themselves with assurance of the identity of the customer to a level that the bank considers appropriate in the context. They use a variety of third party services for this purpose. A study conducted by PwC for the European Commission found that typically banks conduct identity verification to a lower level of assurance than defined as ‘Substantial’ under the eIDAS regulation.
>
> Acceptance of a customer’s digital identity, as proposed in this project, can be viewed as a useful identity verification solution which may reduce a bank’s risks. It has been accepted as an appropriate solution in the 5th Money Laundering Directive but it does not change a bank’s liabilities. However, a bank may wish to place contractual liabilities on third party providers of digital identities.

4. The market must be commercially viable

Data and trust are the two raw ingredients of a digital transaction. Both can be sourced from many different locations and in many different ways. The solution design recognises this variety. Its value is in allowing people to connect the buyers and sellers of trustworthy data and in calibrating the data such that its value can be understood and remunerated.

Whilst the value of such a service is easily comprehended at a macro level, the service must work at the micro-transaction level; a market in which many transactions containing small amounts of personal data and shared between organisations at low price points. The commercial challenge for adoption is therefore to be able to scale the service rapidly so that transactions can be priced appropriately.

A number of assumptions have been made about the commercial design of the mature solution:

- Customers will not pay for setting up the capabilities to share trustworthy identity and personal data. Today customers self assert identity and personal data at no cost to themselves. The data is then validated in the back office at the organisation's expense. It is unlikely that customers would pay for a service that delivered reduced costs of on-boarding to the organisation.

- Although the General Data Protection Regulation 'right of data access' and 'right of data portability' oblige organisations to make customer data available digitally, they are more likely to proactively develop such services if there is a compelling commercial rationale.

- The value of the data to the receiving organisation is a factor of how it will be used and the extent to which the receiving organisation can trust it. As discussed above, for a digital identity the receiving organisation may require some contractual liabilities to be in place but these cannot be so large as to inhibit the market for Identity Providers. (Furthermore, public sector Identity Providers are unlikely to accept any liability.)

- For personal data linked to a digital identity, such as 'residential address', the level of trust - and therefore value - placed by the receiving organisation will be based on what the Attribute Provider claims to have done to validate the data. For a utility company the address might be validated by the meter but the identity details will be self asserted.

A key role for the Blue Service will be to establish a commercially attractive model under which organisations will buy and sell data from each other, facilitated by the customer to whom the data pertains. The project did not estimate the scale of the commercial flows.

Annex D provides a more detailed review of the contractual and commercial considerations for implementation of the service.

5. Banks will require proactive threat intelligence and transaction monitoring to guard against compromised digital identities

In a digital transaction, assurance of the identity details is necessary but not sufficient for a bank. A bank's decision on whether to open an account for a prospective customer requires evidence of his or her suitability for the product. The bank must also be vigilant against fraud, not just at the point of opening the account but on-going throughout the life of the customer relationship. Three categories of data required by a bank in addition to identity data have been considered;

- **personal data** such as address, income details, employment, etc as described in Annex B
- secure storage and transmission of the relevant **metadata** allowing for confirmation of provenance of the identity and personal data received
- **security information** and check digits such that enables the bank to have confidence in the end-to-end security of the transaction and assurance in its integrity. Audit information can also be considered within this class of data.

It is an established fact that identity theft is on the rise and malicious actors are using increasingly sophisticated tools and techniques to harvest identities and attributes. In order to protect the ecosystem a nuanced approach to threat intelligence and alerting will be required. This is a combination of human analysis and automated mechanisms. This function is critical and provides banks a timely alerting mechanism of suspicious or compromised digital identities, but also provides proactive awareness of potential risks and threats to the methods and sources used.

Important considerations as part of this will include but not be limited to:

- A clear threat intelligence picture built upon collection of relevant and actionable intelligence from sources such as Open Source Intelligence (OSINT), DarkWeb and Underground Forums (DARKINT) and Cyber Threat Intelligence (CYBINT).
- Ensuring that dissemination and feedback is presented in a timely manner and that information is placed in the correct hands will require a degree of automated mechanisms to "share signals"
- As part of a shared signals approach, the appropriate technical and legislative constructs will be designed/documented and implemented. This will also consider the complexities of sharing data, and potentially evidence across multiple jurisdictions.

6. The solution must be technically and operationally robust

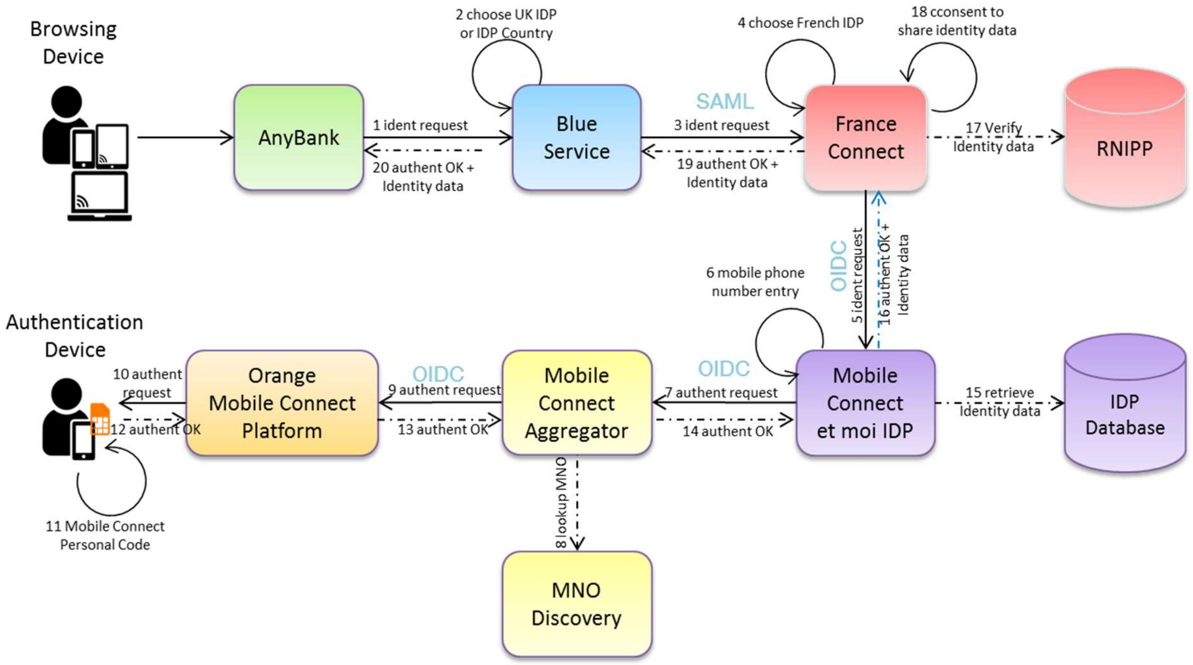
As discussed above under Solution Design, the infrastructure for establishing trust by the bank in the prospective customer's assertions is comprised of three components:

- **Mobile Connect et moi**, the customer's chosen Identity Provider, which uses France Connect to provide a trustworthy digital identity
- the infrastructure used by ANYbank to acquire identity and personal data (the **Blue Service**)
- the **Attribute Provider** service selected by the customer and approved by ANYbank.

Implicit in the design is the assumption that each component is technically and operationally of a standard that safeguards the trustworthiness of the data. Appendix A provides an overview of the technical design of the component parts. This section provides an overview of design of the components of the trust infrastructure and how they comply or align to standards and approved schemes.

Mobile Connect et moi

The following diagram depicts the full identification and authentication flow:


Browsing Device
2 choose UK IDP or IDP Country
4 choose French IDP
18 cconsent to share identity data
AnyBank
1 ident request
20 authent OK + Identity data
Blue Service
SAML
3 ident request
19 authent OK + Identity data
France Connect
17 Verify Identity data
RNIPP
OIDC
5 ident request
16 authent OK + Identity data
6 mobile phone number entry
Authentication Device
10 authent request
12 authent OK
Orange Mobile Connect Platform
OIDC
9 authent request
13 authent OK
Mobile Connect Aggregator
OIDC
7 authent request
14 authent OK
Mobile Connect et moi IDP
15 retrieve Identity data
IDP Database
8 lookup MNO
MNO Discovery
11 Mobile Connect Personal Code

After being guided to Mobile Connect et moi, the user enters his mobile number and is then redirected to the Mobile Connect platform of his mobile operator (Orange) thanks to the MNO Discovery database managed by a Mobile Connect Aggregator (currently Orange Applications for Business). The user is then notified on his mobile to enter his Personal Mobile Connect PIN Code stored on his SIM Card.

Once successful authentication occurred, the Mobile Connect et moi service retrieves the user identity from its database and returns the information to France Connect. France Connect verifies the given identity against the French National Identity Database (RNIPP - Registre National d'Identité des Personnes Physiques) and checks that the declared identity sent by Mobile Connect et moi is a real and validated identity. Finally, the user consents to share his identity data with Blue Service. Blue Service then aggregates with other data attributes and send them to AnyBank.

All communication in the French context are performed thanks the OpenID Connect (OIDC) protocol[14].

The Blue Service and Attribute Provider

The Blue Service maintains a number of bilateral contractual agreements to facilitate the customer in sharing trustworthy data from one organisation to another. The customer's digital identity acts as the 'trust anchor' that all parties recognise as the representation of the customer throughout the end-to-end transaction.

The Blue Service operates under a contract with ANYbank as an operationally secure means of enabling the customer to assert his or her digital identity to the bank and for linking it to attributes provided by Attribute Providers that ANYbank trusts. It maintains a list of the organisations that ANYbank will trust to act as an Identity Provider and provider of the 'address' attribute (and other attributes) for nationals of different countries.

The Blue Service also operates under a contract with Identity and Attribute Providers as a conduit for people to control the sharing of their personal data with third parties such as ANYbank.

Steps of the transaction:

1. ANYbank requests via the Blue Service that the customer provides a trustworthy digital identity and address attribute. It has previously established with the Blue Service that the Mobile Connect et moi Identity Provider is trustworthy as a means of verifying a prospective

[14] https://openid.net/connect/

French customer's digital identity details on the basis that it is recognised under France Connect, the national digital identity scheme.

2. Following authentication the Blue Service receives an encrypted token from France Connect which it is able to decrypt the customer's digital identity details. The Blue Service maintains rules for how long these digital identity details can be accepted as representation of the customer's authorisation of the following steps.

3. The ANYBank client asks the customer to select the Attribute Provider for their address and requests the address attribute from the Attribute Provider's Resource Server.

4. The Resource Server requests an authorisation ticket from the Authorisation Server within the Blue Service using a secure identity token representing the user that was previously established between the Resource Server and Authorisation server.

5. The Resource Server returns the ticket to the ANYBank client. The client uses this ticket, in conjunction with the digital identity token to request an authorisation token from the UMA Authorisation Server within the Blue Service.

6. The Authorisation Server sends the client an authorisation token containing permissions it has for the address attribute at the Resource Server.

7. The ANYBank client requests the attribute from the Resource Server, this time submitting the authorisation token along with the request,

8. The Attribute Provider's Resource Server validates the authorisation token and sends the address attribute directly to the ANYbank client.

7. The implementation strategy will require rapid adoption

The economics of digital identity require scale. The business case for organisations to accept digital identities when opening a bank account is dependent upon a critical mass of potential customers having - and knowing that they have - a digital identity and assurance that the end-to-end solution meets regulatory conditions.

Review of the digital identity markets across Europe show a marked difference between successful and less successful markets. The markets tend to be at either end of the spectrum - either very high take up, or low take-up rates. Few markets are in the middle of the spectrum, which may support the idea that the network effect[15] is integral to the success of digital identity.

Markets with high take-up rates, for example in Scandinavian nations, tend to be in countries where digital identities can be used in transactions within both the public and private sectors. And, where digital identities can be used across both sectors, the private sector tends to provide the majority of transactions. Once users become familiar with using their identities it is easier to transact with them - thereby encouraging more services to accept them. In this way, identity markets appear to work as ecosystems, with frequency of use key to catalysing the system.

With the exception of the Netherlands[16], markets with lower take-up rates tend to be associated with public sector use only. As transactions with the public sector tend to be fewer, this appears to lower the perceived value to users - they undertake registration journeys with relatively high barriers, for an identity they may use once or twice per year. In the UK, the public sector has catalysed the creation of over 3 million digital identities through public services. However, until October 2018 they could not be used outside the public sector. As a consequence, there are still challenges in establishing the mental model of reusable digital identity.

This analysis suggests that, when an identity is only usable in the public sector, it is more challenging to trigger the network effect of users and services needed for a successful identity ecosystem.

Creation of a digital identity needs to be the by-product of some other transaction. In most European countries today this transaction will come from an interaction with the public sector. De facto identity verification documents in the pre-digital world, passports, identity cards, driving licences, etc have been issued by the state. However, the most successful examples of digital identity schemes have seen collaboration between the public and private sectors. In the Norwegian Bank ID system the state establishes the basis for trust through standards but awareness of the scheme is generated mainly by the private sector.

The need for a clear customer experience has been explored above. Evidence from other markets such as Canada indicates that transactions through smartphones and tablets is significantly driving growth. This can lead to a different user experience and conceptualisation by the customer of how the transaction is conducted. The role of mobile devices is clearly important in developing an implementation strategy.

[15] https://en.wikipedia.org/wiki/Metcalfe%27s_law

[16] The Netherlands has nearly full take up of digital identity but it can only be used in the public sector.

Annex A: Technical Summary

This is published separately.

Annex B: Attribute Exchange

The Connecting Europe Facility: Opening a Bank Account project (CEF) has developed a prototype for a service under which a user is able to provide personal data digitally in order to open a bank account - and make it operational - in real time without the need for further background checks.

Opening a bank account is a specific example of a generic challenge: how a person can share data with another party in a manner that is sufficiently trustworthy to both parties and so reduces the ‘friction’ often associated with digital transactions.

This annex provides an overview of methodology on which the project was based. It draws upon work conducted under the Open Identity Exchange[17], the UK Government Digital Service[18] and by the European Commission’s Expert Group on Know Your Customer Attributes[19].

Overview

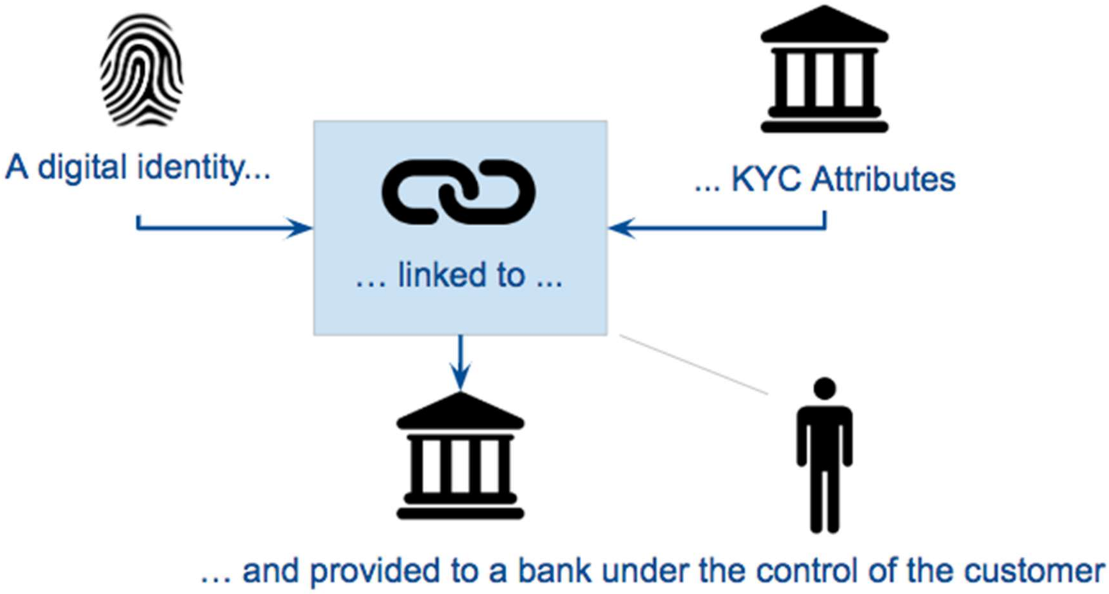
Trust is a multi-faceted concept. It is a value judgement which a person or organisation will make based on its own criteria. In digital transactions the result is that people are frequently requested to repeat mundane tasks like providing personal data, creating new passwords and downloading new apps. The complexity - or tedium - can often cause people to fail to complete transactions. Furthermore, the current systems for establishing trust are both inefficient and leave opportunities for fraud which are increasingly being exploited by criminals.[20]

The CEF project has proposed a generic solution based around four logical functions and applied to the scenario of opening a bank account across a national border:

- The customer’s **digital identity** as defined through the eIDAS regulation (Regulation EU 910/2014)
- A set of the remaining **‘Know Your Customer’ (KYC) attributes** (i.e. not defined above as ‘identity’) currently being defined by an Expert Group set up by the European Commission and made available for the customer by an **Attribute Provider** in a manner compliant with the General Data Protection Regulation (GDPR)
- The organisation to which the customer wishes to provide the identity and KYC attributes; in this scenario, ANYbank, but generically described as the **Relying Party** (or in UMA terminology, the Client Application)

[17] https://oixuk.org/?s=Attribute+Exchange&lang=en
[18] Further information will be published by Government Digital Service in due course
[19] Priority Group 2 under eID and KYC expert subgroup
[20] https://www.unodc.org/unodc/en/money-laundering/globalization.html

- An **Attribute Exchange** service that allows the customer to control the sharing of the data between the different participants through a consistent user experience and in a manner compliant with GDPR.



For this process to be trustworthy to the Relying Party that receives and uses the data it is necessary for the basis of trust to be analysed and understood by all parties. The customer has a relationship with three organisations. All three must have confidence that person conducting the transaction in the digital channel is the person that he or she claims to be and the person to whom the data relates.

The basis for trust between all parties, sometimes referred to as the **"trust anchor"**, is the digital identity. It is clearly necessary that the digital identity is created to high standards and in a manner that all parties accept. The eIDAS regulation (Regulation EU 910/2014) has created the interoperability framework between governments for this trust anchor in the context of public services.

The liability model for this trust framework is critical. It is described in Appendix C.

The Attribute Provider is likely to have had a relationship with the customer that predates the creation of the digital identity. The Attribute Provider must therefore establish that the digital identity refers to the correct customer. This process is described as 'matching' or 'rebinding' the digital identity to the customer account. It may occur after the customer has authenticated to the Attribute Provider using his or her normal method. Once matched, the digital identity can be used by the customer to access and share data held by the Attribute Provider.

Having linked the digital identity to a customer account held by the Attribute Provider, the User Managed Access (UMA) protocol describes the sequence of calls and responses between defined actors which leads to the release of data to the Relying Party (or Client Application). These are described in the Solution Design description above..

To be able to open a bank account in real time through this process the bank must be able to satisfy two conditions:

1. It must be able to acquire all the elements of data about the applicant required under its Customer Due Diligence process
2. It must have sufficient confidence in the validity of the data received to meet its risk appetite.

The remainder of this document considers these two facets.

1. Data requirements to open a bank account

In 2017 PwC conducted a study for the European Commission researching banking practices when opening an account for a customer. These practices are driven, to a large degree by the Anti Money Laundering Directive[21]. The PwC report[22] defined two categories of data (attributes) collected by a bank:

A. The **identity attributes** required for a natural person or for a legal person are defined by Member State legislation. For natural persons it includes, among others: Name, Address, Date of Birth, Nationality, and Occupation. For legal persons it includes, for instance: Legal name, Address, Unique Identifier.
B. **KYC attributes** are required for risk, anti-fraud or suitability evaluations for natural or legal persons. This includes politically exposed person (PEP) status, Source of funds, Tax and Fiscal residence for natural person; and Beneficial Owner Identity, Source of funds and Brand name for legal person.

A. Identity attributes

In 2018 in the 4th Anti-Money Laundering Directive was revised (now known as the 5th Anti-Money Laundering Directive). Article 13(1), point (a) refers to the means of identity verification and has been replaced by the following text:

> *"(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent*

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

[22] https://publications.europa.eu/en/publication-detail/-/publication/139abc5b-49c6-11e8-be1d-01aa75ed71a1/language-en

> *source, including, where available, electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council (*) or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities;"*

Whilst not prescriptive, the new wording acknowledges the potential role of digital identities as defined under eIDAS and aligns with the summary from the preceding PwC report:

> *"The analysis performed demonstrates that it is reasonable to conclude that eIDAS compliant means can support the verification steps of the on-boarding processes for the electronic identification of natural and legal persons. The appropriate level of assurance can be selected by the financial institutions, according to their risk management.*
>
> *[...]*
>
> *For cross-border on-boarding, a fully digital process can be envisaged. This would make use of the network of eIDAS nodes which is currently being constructed."*

This project has aligned its approach with the process described in the PwC report. The 'Attribute (Friendly) Name for the 'identity attributes' provided through eIDAS and set out in the SAML specification[23] are reproduced below. The 'KYC attributes' are discussed in the next section.

Mandatory attributes

Current Family Name
Current First Names
Date of Birth
Unique Identifier [This uniquely identifies the identity asserted in the country of origin but does not necessarily reveal any discernible correspondence with the subject's actual identifier (for example, username, fiscal number etc)]

Optional attributes

First Names at Birth
Family Name at Birth

[23] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile?preview=/46992719/47190132/eIDAS%20SAML%20Attribute%20Profile%20v1.1_2.pdf

Place of Birth
Current Address
Gender

B. KYC Attributes

An Expert Subgroup has been set up by the European Commission, under the eID and KYC Expert Group, to consider a framework for KYC Attributes. The Expert subgroup is drawing on work previously conducted, including the PwC report.

The framework will consider a set of attributes that are commonly required by banks and the confidence in the validity of the data, or ‘level of assurance’, as discussed in the section below. It will publish its proposals in the Spring of 2019.

The attributes under consideration by the Expert Subgroup as common across banks in the draft framework are set out below.

Core ID Attributes (in addition to those set out above)

Country of Nationality
Maiden Name

Identifier Attributes

Social Security Number
Fiscal Number
Existing Bank Account Code

Contact Attributes

Current Address
(Mobile) Phone Number
Email Address

Status and Due Diligence Attributes

Occupation (Profession)
PEP
Source of Funds
Sanctions Lists Status
Fiscal Residence
Marital Status
Qualification level in higher education (QAA level)

Independently of the Expert Subgroup, the CEF project researched the attributes commonly collected by UK banks and provided a representative view of which ones are typically:

- **Verified** by the bank
- Considered **valuable** by the bank
- Provided as **self-asserted** by the customer
- Created in the bank's **back office** through a process and without necessarily involving the customer directly.

Personal Details	Email address
Personal Details	Title
Personal Details	Forename(s)/Given Name(s)
Personal Details	Surname/Family Name
Personal Details	Previous/other first name(s) (up to 5)
Personal Details	Previous/other surnames(s) (up to 5)
Personal Details	Date of Birth
Personal Details	Country of Birth
Personal Details	Customer's Nationality(ies) / Citizenship(s) held
Personal Details	Gender
Personal Details	Country of permanent residence
TAX Details	Customer's Jurisdiction of Tax Residency
TAX Details	Tax identification number (TIN)
Contact Details	Home telephone number

Contact Details	Mobile phone number
Contact Details	Work telephone number
Contact Details	Customer's Residential Address
Contact Details	Date moved in
Contact Details	Address History (3 years)
Employment Details	Employment status
Employment Details	Employment role
Employment Details	Occupation
Employment Details	Employer/business name
Employment Details	Business type / industry classification
Employment Details	Employer address
Employment Details	Gross annual salary
Employment Details	Earnings
Background Checks	Credit / Over indebtedness Check
Background Checks	PEP / Sanctions
Background Checks	Mortality Warning
Background Checks	Fraud Warnings
Background Checks	Velocity Warning

2. Confidence in the validity of KYC data

A number frameworks have been proposed for a third party such as a bank to measure the confidence in the validity of an attribute from an Attribute Provider. To date none have been adopted within either the public or the private sector. The Expert Subgroup on KYC Attributes will publish its work on this subject later in 2019.

A summary of the UK Government Digital Services (GDS) proposals on establishing confidence in the validity of an attribute is set out below. The GDS proposals consider cultural, legal, commercial and business aspects to the establishment of trust in an attribute. However, this summary focuses only on the technical aspects, i.e. the facets of the provenance of the attribute that need to be understood by a recipient in order to appraise its trustworthiness.

The GDS approach defines that an attribute is always held by an ‘Attribute Provider’ which may be an individual or organisation. It is service, technology, and situation-agnostic and has defined five categories to define the trust in an attribute:

- Enrolment
- Validation
- Rebinding
- Data Processing
- Management and Organisation

Enrolment

Enrolment describes the processes an Attribute Provider has conducted when associating an attribute to an identity at the outset. The two primary processes are:

- How the Attribute Provider assured the identity of the person
- How and if the uniqueness of the attribute to the person was established

Validation

The quality of the checks an Attribute Provider has done to validate if an attribute is true. The trust in the validity of an attribute increases with the checks done by an Attribute Provider. An attribute could be:

- Not checked
- Self-asserted
- Checked against a third-party source
- Checked against a reliable source
- Checked against multiple reliable sources
- The attribute provider is the issuing source

Rebinding

How an Attribute Provider has matched a returning (digital) identity to a customer account under which the attribute has been enrolled. The quality of the rebinding process is determined by:

A. The quality measure of the returning (digital) identity
B. The quality of the matching process to the identity details of the customer account

Data Processing

An attribute provider must have a sound legal basis to process and retain data. The attribute provider must be compliant with UK legislation for:

A. Right to share data or metadata, eg consent (eg GDPR)
B. Data retention; the attribute provider must
   - record and maintain relevant information
   - retain and protect records for as long as they are needed for auditing and investigating security breaches
   - securely destroy records when no longer needed

Management and Organisation

These are measures of the Attribute Provider itself, in particular its declared policies that allow third party organisations to trust in the integrity of the Attribute Provider and the attributes it asserts. The measures are categorised as:

A. **General Management;** the organisation has sufficiently trained staff and subcontractors, protects against damage that may affect security, protects personal, cryptographic or other sensitive information, complies with legal requirements, complies with an agreed liability policy and fulfils its own and any outsourced contractual commitments
B. The strength of an attribute provider's **Information Security Management System** (ISMA) which may impact the likelihood of data compromise
C. The **technical controls** implemented by an Attribute Provider's to protect data security over time and the confidentiality, integrity and availability of their information, the electronic communication channels against impersonation, eavesdropping, manipulation and replay, and the storage, transport and disposal of personal, cryptographic or other sensitive information

D. **Compliance and audit processes** that give trust in the integrity of an attribute, for example, periodic internal audits, periodic independent internal or external audits under a certification scheme.

Annex C: Bank liabilities when accepting a digital identity from a government identity scheme

Context

The OIX Connecting Europe Facility (CEF) project is investigating a model under which a prospective customer of a bank in another country could use the digital identity from a digital identity scheme notified by a member state under the eIDAS framework[24], as a means of verifying identity details, during the application process. The project is using the example of a French citizen opening a bank account in the UK with their France Connect eID. In order to limit complexities it has been decided that credit products are out of scope for this project.

This paper considers the generic risks to a bank when opening a bank account with a new customer, the potential liabilities that the bank is exposed to in the process and how these liabilities are managed by a bank.

It then describes the process proposed by the CEF project, and considers the functionalities necessary for the process to be operationally feasible and the liabilities of the various parties involved.

Risks to a bank when opening an account with a new customer

Banks face risks when opening a new customer relationship. For the purposes of this document there are four categories of risk to be considered:

- **Credit risk;** that the (honest) customer is not able to repay any loans that he / she is provided by the bank. [However, credit products and how a bank manages credit risk are not considered within the scope of this project.]
- **Fraud risk;** that the customer supplies false information (including identity details) and is able to commit either:
  - 1) First party fraud – whereby the individual defrauds the bank
  - 2) 3rd party fraud – whereby the individual creates a mule account. This may use a real identity, but the purpose of the account is to defraud other people.
- **Legal risk;** the risk of loss or imposition of penalties, damages or fines from the failure of the firm to meet its legal obligations including regulatory or contractual requirements.
- **Operational risk;** the risk that the bank has inadequate or failed processes in place e.g. for managing personal data.

[24] https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/

If a bank fails to correctly mitigate the above risks associated with identifying potential customers, then this may result in fines, paying damages, being defrauded and reputational damage which might have significant financial costs. On the other hand, if a bank's processes are far too difficult for people to meet, resulting in a significant number of real, honest people being turned down, this then this may result in them turning away potentially profitable custom which is not viable in the long term.

Bank liabilities differ in each of the risk scenarios above. A bank will have mechanisms to mitigate the risks:

1. Develop internal operational processes that manage the risk cost effectively by acquiring information about the customer and his / her transactions and by validating this information with independent and reliable sources.
2. If a bank isn't able to acquire sufficient information to satisfy its processes, either from the customer or from other sources, then the bank will no longer proceed with the account opening.

In practice, acquiring and validating information automatically may prove complex leading to a less 'black and white' outcome. A hybrid online and offline bank process may result.

Risks associated with identity verification

The bank must establish confidence about the identity of the Prospective Customer as, without this it is not possible to validate the assertions that he or she makes about the context for the new banking relationship and any relevant personal information.

There are two principle types of identity fraud:

- **Identity 'theft'** where a fraudster impersonates another person
- **Identity fabrication** where a fraudster establishes a new or amended set of identity details

To mitigate the risks of identity fraud the bank must assure itself to an appropriate level of certainty that:

- The identity details asserted by the Prospective Customer can be corroborated against independent and reliable sources so as to confirm that they describe a 'real' person.
- That the identity details have not been reported as being associated with identity fraud.

- That the identity is a ‘developed identity’ i.e. the evidence for the identity does not appear to have originated at a specific point in time indicating an abnormal existence.
- That the person asserting the identity details can demonstrate that he / she is the person described by the identity.

Traditionally, these mitigations are performed by inspecting paper documents such as passports, driving licences and utility bills or by checking the personal data asserted by the Prospective Customer with independent and reliable sources.

Currently there are no Europe-wide standards for the financial sector describing the level to which identity assurance should be achieved. Instead, a risk-based approach applies: banks are obliged to ensure that the level of Customer Due Diligence is proportionate to the context of the business transacted by the bank. Additionally, some countries may have ‘national guidance’, for example in the UK the Joint Money Laundering Steering Group (JMLSG) provides guidance around the interpretation of Money Laundering directives. Across Europe the nature of the national guidance varies with some countries having more detailed guidance than others, creating a lack of consistency in the application of Money Laundering regulations.

Bank liabilities today

The liability of a bank in any given scenario is dependent on the circumstances in which a party seeks redress. For example, if a fraud has occurred in the context of a payment scheme then the protections of the different parties will vary between a Direct Debit and a push payment based upon the rules of the specific scheme.

Where a party seeks redress from a bank then the question that is asked is, essentially, did the bank do the right thing? In answering this question, part of the judgement test may be to consider whether the account associated with the fraud was opened using documents and identity verification processes that are compliant with regulatory requirements and industry best practice.

The models for identity verification permitted in the UK under current HM Treasury industry Guidance are:

- the bank requests particular documents to be presented by the customer, tests that the documents are genuine and keeps a copy of them
- the bank asks a Credit Reference Agency to give it data which it uses to determine whether the identity assertions of the customer are valid
- the bank places reliance on a third party – which does the end to end identity verification process. The bank tests the third party for compliance on a regular basis.

In each model liability for the identity verification process resides with the bank. All banks accept government issued documents, such as a passport or driving licence, as a proof of identity and / or address but the government suffers no liability if the document has been issued to a fraudulent identity and then used to open an account for illegal purposes.

It is possible to investigate fraudulent identity details that have come to light within a country but, at present, the process is more complex across borders. Identity fraud data is shared between organisations within the UK, but international services are less mature.

Where a bank has determined there to be a breach with regard to an identity document then the bank would be considered to be on notice and hence in a position of 'constructive trust' making the bank liable for related third party losses that might arise.

Management of liabilities today

Bank liabilities are managed through risk models that depend upon information about the customer. Without high assurance of the identity details it is difficult for the bank to have confidence in the data about the customer.

Banks therefore mitigate the risks from identity verification in proportion to their liabilities associated with the business transacted with the customer.

Liability to regulators for compliance with money laundering regulations
Banks minimise their legal risks through internal processes agreed with regulators. As criminals become more sophisticated, the Customer Due Diligence regime for banks becomes more stringent, for on-boarding of new customers, for monitoring of existing customer relationships and for monitoring the counterparties of the banks' customers. In recent years banks around the world have incurred penalties from regulators, even in cases where no fraud has occurred but bank Customer Due Diligence processes have been shown to be inappropriate.

Liability for losses to the bank
Banks will minimise their exposure to losses from either:

- *bad debt;* by collating sufficient quality information about the customer's circumstances and business transactions to model the risk of exposure to loss to the bank and price the risk accordingly
- *fraud;* by validating information about the customer and the customer's circumstances was insufficient to detect the likelihood of loss.

Liability to the bank's customer

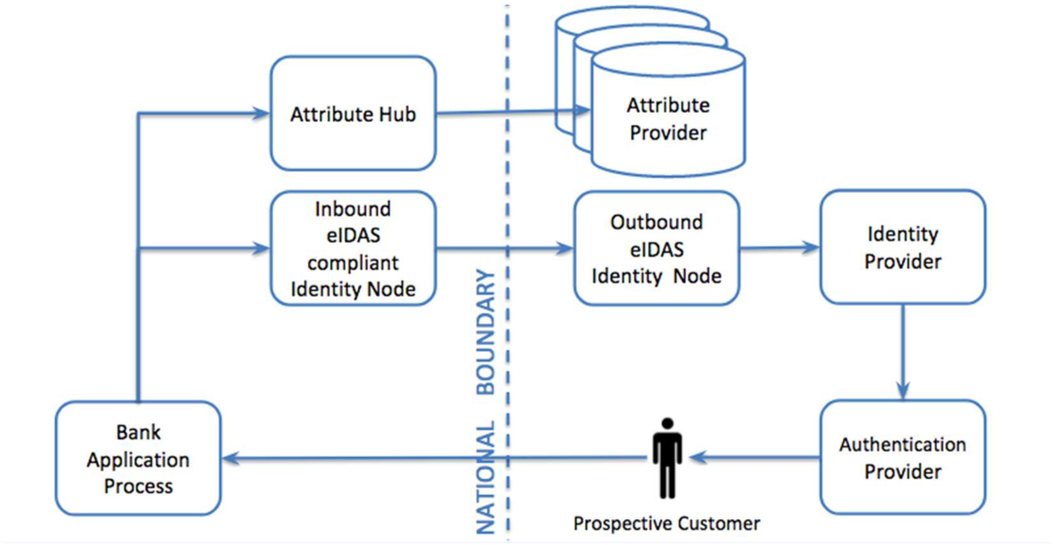
In some circumstances, banks will be liable to their customers for losses incurred. Banks manage the risks of loss through clarity of the contractual responsibility between customer and bank and by investment in internal operational capabilities to detect fraudulent transactions.

Liability to third parties
In some circumstances, banks will be liable to third parties for losses incurred through fraud.

Liabilities passed by the bank to third parties
Where banks use the services of third parties there may be contractual terms that pass some liabilities to the service provider. For example, where identity information is being passed through an infrastructure from the source of evidence to the relying party bank, then there is a risk of 'man in the middle' attack. The contractual terms may pass liability in the event of such an attack onto the infrastructure supplier. However, the conditions of the liability will be clearly defined and capped.

Process proposed through the CEF project

The user experience for opening a generic bank account in another country proposed under the CEF project is described through a set of wireframes. The diagram below describes how the applicant's identity and associated personal data is relayed to the bank.



1. The bank invites the Prospective Customer to verify his or her identity digitally through an Identity Provider that is recognised under the eIDAS regulation
2. The Prospective Customer navigates to his / her national Identity Provider and authenticates using the Identity Provider's credentials.

3. The Identity Provider requests permission from the Prospective Customer to pass to the bank his / her identity details and any additional personal data requested by the bank.
4. The bank receives the identity details and additional personal data through the eIDAS compliant infrastructure and populates the Prospective Customer's application form with them.

Changes to bank liabilities under the process proposed

In the context of banking and the Money Laundering Regulations discussed in this document it is not envisaged that liabilities associated with identity verification will move from banks that accept digital identities as proposed through the CEF project. [The EU General Data Protection Regulation has liability implications for organisations of all types. These are not considered within this document.]

The commercial market for digital identities that meet government standards will vary from one country to another. In markets where a public sector entity is responsible for the digital identity and the infrastructure through which it is asserted, it is unlikely that the public sector Identity Provider will accept any liability should the identity prove to have been inaccurately or fraudulently asserted to the bank. The bank must therefore judge the risks of identity fraud based on its own sources of intelligence about the issuing country's national digital identity issuance processes.

In markets where private sector Identity Providers are certified as able to make identity assertions on behalf of a person according to government standards then it is anticipated that the commercial contract between the Identity Provider and the bank will require the Identity Provider to take a clearly defined liability in specific circumstances, for example where the defined standards and processes have not been met. However, although this may cover bank financial losses it will not remove ultimate liability from the bank.

For a federated digital identity scheme such as the one proposed in the CEF project to be adopted there will need to be a mechanism for sharing identity fraud data. If a digital identity is discovered to be fraudulent there must be a mechanism to revoke it and alert those organisations that may have been exposed to fraud as a result.

Benefits to banks under the process proposed

The European Commission has agreed wording in the 5th Money Laundering Directive that recognises digital identities under the eIDAS framework.[25] To date it is not known how this change will transpose into national law and national guidance.

[25] http://data.consilium.europa.eu/doc/document/ST-15849-2017-INIT/en/pdf

However, this regulatory change will provide confidence to banks to explore the operational practicalities of digital identity schemes.

Notwithstanding current regulations, for banks there is a need to enable new and existing customers to transact and assert personal and identity information through digital channels. Traditional physical documents are more easily spoofed by sophisticated fraudsters and face-to-face interactions in branch are becoming less common. New services and technologies make it quicker, easier and potentially more secure for customers to access financial services digitally and a range of new market entrants are leveraging these.

The principal benefits for banks in adopting a digital identity scheme that meets internationally recognised government standards will be:

- That the bank can have greater confidence in the accuracy and currency of the identity details of the customer him or herself thereby reducing potential fraud and demonstrably complying with identity verification requirements for Customer Due Diligence
- That the bank can assess information about the customer in terms of the government identity verification standards and develop more automated and less subjective methods of assessing data, as explained in the section on Attribute Linking below
- That remote account opening will be dependent upon a digital identity scheme and not on a credit footprint which excludes some customer demographics
- That it facilitates the creation of a truly European market for financial services[26].

Attribute Linking

In meeting Customer Due Diligence requirements banks are obliged to gather and monitor information about their customers. For example, the customer's current residential address is an example of an attribute of information that most banks require from their customers.

In some, but not all national digital identity schemes the customer's current residential address may be available from the Identity Provider. In such circumstances the bank can be assured that the current residential address will have been verified to a defined standard against the name and date of birth of the customer.

[26] http://ec.europa.eu/finance/consultations/2015/retail-financial-services/docs/green-paper_en.pdf

In some countries the current residential address is maintained by a separate public sector scheme. The national digital identity system may be used by the person to give consent to sharing of the address with the bank. Depending on the rules under which the public sector scheme requires that current residential address must be updated by the citizen the bank can assess the likelihood of its inaccuracy.

In other countries the customer may use a third party source as evidence of current residential address, for example a utility bill. The bank can then assess:

- How the third party source has verified the address against the identity of the customer, which in the case of a utility company may be a very lightweight process
- How current the information is likely to be; for example a utility billing system may have been set up several years ago
- How secure the mechanism of assertion of customer’s residential address is in the current context.

A standardised framework can be developed to assess the trustworthiness of the attributes asserted by the customer based on the source against which they have been validated. Data about the attributes, so called ‘metadata’ can be defined using the same definitional framework as established in the eIDAS identity verification standards. This would allow the attributes to be appraised in terms of:

- how the source for the attribute verified the identity of the person at registration
- how the attribute itself was validated
- when the attribute was last validated
- how the digital identity in the current transaction has been verified by the source and associated to the attribute.

Based on such a system of metadata, a bank could achieve a high degree of automation both in processing information received from the customer and in scheduling when to review information based on risk.

A similar approach could be applied to other data that has not been asserted by the customer but checked independently, such a listings for Politically Exposed Persons and those to whom sanctions apply.

The subject of attribute linking and attribute exchange is further discussed in Annex B.

Conclusions

A system that enables people to use their national digital identity scheme when opening a bank account will not change the bank's liabilities. However it will improve risk mitigations and provide a number of advantages to a bank; reducing fraud and enabling automation and improved customer service. More widely, it may foster innovation in banking services, potentially mutualising customer on-boarding processes, and creating greater international competition.

To accept digital identities banks will require clear visibility on the liability implications. Banks are usually liable when on-boarding processes are not implemented appropriately - there should be no attempt to change that principle in a digital environment. However, there is need to clarify what the key tasks are for banks, especially when dealing with information or data which are not or cannot be fully verified. This is typically the case of 'residential address' and the assertion of the 'origin of funds'.

A number of additional features of such a scheme will be required if it is to be become operational and deliver its potential benefits:

- a contractual framework describing the responsibilities of each party in various circumstances as currently being explored by the European Commission's Expert Group (and discussed in Annex B).
- a system for detecting and alerting participants when fraud is detected
- a metadata framework by which each Relying Party can assess the trustworthiness of attributes it receives associated to the digital identity.

Annex D: Contractual and commercial models

This annex outlines the contractual and commercial considerations the consortium have made and the conclusions for a realisable service. The analysis was conducted during the Discovery Phase and the sections below are mostly repeated from the associated report.

Contractual Model

The Consortium decided that the most relevant issue to be addressed in the Contractual Models workstream was the liability of data as it passes between parties. There is no existing liability model, in the UK, regarding the use of Digital IDs for data providers, other than the one that formally exists between Identity Providers (IDPs) and GDS, as part of the GOV.UK Verify scheme. The identity assurance model adopted by Credit Reference Agencies wasn't in scope, however could be considered in a further stage of the project.

By utilising public sector recognised entities and relevant infrastructure, this may ensure that the private sector, as well as consumers, can have confidence in the system and use it to its full capacity.

The Consortium identified that liability levels differ depending on the products it is related to. This was determined by mapping the flow of identity and other relevant data across the onboarding process for a broad range of products. Typically, banks assess the risk on the inflow of data and are ultimately responsible for ensuring the right checks have been instigated in the identity verification process.

As part of the Discovery phase, the Consortium defined the principles and options for the high-level contractual model by reviewing existing liability models, which included those used in eIDAS, STORK II, GOV.UK (Verify) and the Bank ID Norwegian Model.

The pilot identified a range of liability issues regarding:

- The process chain,
- Organisational constraints,
- Security of the infrastructure
- The need for a liability model that underpins the exchange of digital identity data.

eIDAS

A Member State can choose to notify an eID scheme that operates within the territory of that Member State. However, for other schemes to be eligible for notification they must be under a mandate or recognised by the government within the Member State. Full details for notification eligibility can be found in Article 7 of the eIDAS regulation. It should be noted that the use of eIDAS is only mandated for public sector (Article 6) services.

Liability under eIDAS is defined as unlimited, under specific conditions (Article 11). The liability model for the use with private sector services is yet to be defined.

Proposed model

The Consortium identified liability arising from the reliability of the data, passed from one party to another. This would be defined in a trust framework or the scheme rules. Three different scenarios were proposed to define where the liability would reside when an eID is relied on:

1. If standards are adhered to, then the party providing the data should have no liability.
2. If standards are not followed by the party providing the data, then that party is liable. This could be agreed to be capped within the contract with the relying party.
3. If there is a cyber-attack, or other force majeure, the liability could be handled by insurance providers (such as Lloyds of London), who can provide identity related insurance schemes.

The development of the Governance structure and Trust Framework were not in scope in the Action and could be considered, if such a service was made available to private sector. This would also need to define the requirements to cover any insurance and cyber security controls.

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

STORK II

STORK II was an EU co-funded project that aimed to establish a European eID Interoperability Platform to allow citizens to establish new e-relations across borders, by presenting their national eID.

The eBanking Pilot Final 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.

Other contractual requirements were highlighted in the STORK II report. This included a range of security issues, and Banks would require Service Level Agreements if they are relying on third party data and services for identity verification. This may preclude some Banks from connecting their live services to the eIDAS infrastructure 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.

GOV.UK Verify scheme

The Consortium reviewed the GDS/IDP liability model in the UK, which now allows for the reuse of Digital Identities verified in the scheme, for commercial private sector use, so long as those IDs haven't been created using the Government Document Checking Service (DCS).

Currently in the UK case, the flow of liability from one party to another relies on contract law, which is detailed in the contract between the UK IDPs and the Government in the Verify scheme. This differs across schemes within other Member States. For example, in Germany, eID is managed and produced by the state, so they would most likely rely on legislation.

The liability model, in the Verify scheme, strongly favours the relying party and is focused on the public sector, so the Consortium didn't propose replicating this for the commercial sector.

Bank ID (Norway)

This Consortium investigated how the Norwegian Bank ID model works and how liability flows across the participants of the scheme. BankID (Norway) manages the liability issue by capping the liability at 100,000Kr/€10,000 as an upper limit per transaction, however it is understood that this is likely to increase to €100,000 per transaction; this liability cap is stated in the certificate issued by the scheme.

Recommendations

The Consortium recommends the following liability model:

- if the IDP follows the scheme rules and can demonstrate that the rules were followed in the event of a claim, then there is no liability flowing back to the IDP.

- Conversely, if an IDP does not follow the scheme rules, it is liable for any resulting claims, which the Relying Party and IDP may agree to cap within the contract.

- The IDP would also seek insurance against instances where it had followed the scheme rules, however a fraud has occurred.

If relying parties wish to consume digital identities delivered through eIDAS, then they would need clarity on the exposure to liability; this was worked up in a paper in the Alpha phase and published for review.

Commercial Model

The eIDAS framework does not propose any commercial terms for the use of eIDAS infrastructure or the provision of identities from Member States for use by commercial entities. Each Member State is free to decide how it may charge for the provision of national identities through the eIDAS framework.

During the Discovery phase, this workstream focused on the development of the principles and outline framework of a commercial model. IDEMIA led a range of workshops, and an outline commercial framework was developed; this was shared with the other consortium members, stakeholders (such as Experian, the GSMA) and presented at events (including OIX open industry events).

Proposed principles

The group agreed to work on key commercial principles and proposed the following:

- It will be free to the consumer, when they wish to have their national identity verified through the eIDAS core service.
- The relying party would pay for the identity and related attributes; the aim is for this to be cheaper than the current methods that use a mix of digital and manual processes. This process should reduce a bank’s costs of opening a bank account and onboarding a new customer as the Digital Identity will already be verified.
- Pricing would be determined by open market forces, to align with competition legislation.
- Member State National Identity scheme providers are free to determine the cost for delivering the eID, through eIDAS, when a user is authenticated.

- Relying parties would prefer to contract with a single entity (such as an ID federation hub) that gathers all of the required IDV data to enable the account to be opened, rather than having to gather identities and relevant attributes (such as address) from multiple entities.
- Money would flow across countries with different currencies, so it assumed that a currency exchange was required, which added in uncertainty.

Issue identified in stakeholder feedback:

- Prices cannot be fixed by IDPs for either identity authentication or additional attributes: this has to be determined by the market as it would otherwise be anticompetitive.
- IDPs and attribute providers can have different prices, and these may be based on the available data sets (including eID and related attributes), levels of assurance ascribed to the data and quality of service.
- A potential issue was identified that if the % of transactional model is applied (please see more below under Pricing) and attribute providers wish to charge more than the IDP is prepared to pay, then this would disrupt the commercial model. For example, a French attribute provider wishes to charge a fixed amount that is more than the UK Bank is prepared to pay.
- Price structures may be a mix of fixed, variable (as in a % of the price paid by the Relying Party) and a mix of both.
- The development and maintenance of a Hub that the Relying Party connects into (labelled the ‘Blue Service’ below) can be costly, this would need to be factored into pricing and the percentage of revenue shared with the organisation delivering such a Hub.
- Identity verification is more expensive than authentication. Any Commercial Model should reflect this so Identity Providers, who undertake the initial identity verification, should be compensated for any subsequent use of that identity.

Existing models

IDEMIA researched different commercial models used by existing businesses (such as the PayPal model, mobile network operators international roaming charging structures) and developed the outline framework below.

The Consortium agreed that the mobile network roaming model was the most appropriate model to design the Commercial Model for the Action. IDEMIA and OIX mapped out the model based on the exchange of data, across the following process map, with the financial flow passing back at each point in the process and as data is exchanged and flows in the opposite direction.

In this model, the Relying Party requests an eID and related attributes from the Blue Service, which acts as an aggregator of both identity data and related attributes. The Consortium agreed that the Identity authentication needs to be initially delivered, before other attributes are requested, to ensure the relying party is not paying for attributes if an identity fails the authentication process.

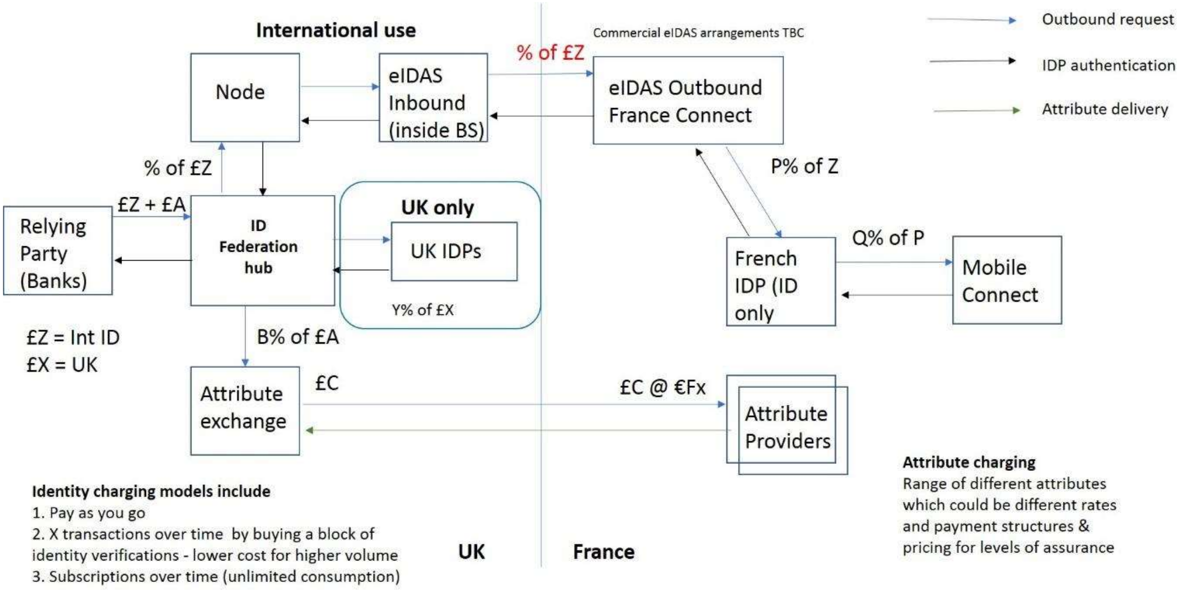

International use
Commercial eIDAS arrangements TBC
Outbound request
IDP authentication
Attribute delivery
Node
eIDAS Inbound (inside BS)
% of £Z
eIDAS Outbound France Connect
% of £Z
P% of Z
£Z + £A
Relying Party (Banks)
ID Federation hub
UK only
UK IDPs
Y% of £X
French IDP (ID only
Q% of P
Mobile Connect
£Z = Int ID
£X = UK
B% of £A
Attribute exchange
£C
£C @ €Fx
Attribute Providers
Attribute charging
Range of different attributes which could be different rates and payment structures & pricing for levels of assurance
Identity charging models include
1. Pay as you go
2. X transactions over time by buying a block of identity verifications - lower cost for higher volume
3. Subscriptions over time (unlimited consumption)
UK
France

Figure 1 - Commercial model

The pricing in the commercial model (outlined above) is based on percentage share of transactional revenue flowing from the Relying Party, through the technical infrastructure, and shared at the different points where the data is exchanged.

It is assumed that the Bank connects into the Blue Service, which is the single point hub that is responsible for gathering authenticated identities, by connecting into the Node that is connected into the eIDAS framework. For the purposes of this model, it is assumed that the other attributes will not be served within the eIDAS framework, so a separate attribute exchange is developed, which gathers the additional attributes required by the Relying Party to open the bank account.

Charging models

Different charging models were considered, these included:

- Payment based on users clicking on specific actions in the model
- Payment based on the percentage of transactional value, where a percentage of the identity transaction is shared by the different parties that handle the data.
- An agreed subscription (based on an annual arrangement)

- An estimate of the aggregated cost for developing and maintaining the different services (such as the Blue Service) and the related infrastructure (including the Attribute Exchange and the Nodes connecting into eIDAS) and then share this cost between the IDPs and relying parties.

The Consortium proposed that the percentage share of transactional value, paid by the relying party, was the most equitable and had the broadest support when presented to other stakeholders. Please note the consortium did not propose pricing, however it did gather market intelligence on national pricing structures.

Commercial structure for ID authentication

The following diagram illustrates how a digital ID federation service would charge a relying party for the provision of a service to authenticate digital IDs from an IDP connected to the hub. One point of the commercials is that there are none set for the exchange of ID verifications between countries at this stage. This could mean that the Federation hub could hold a contract directly with the IDP for ID authentications and the French IDP would charge accordingly to the hub's legal entity. Charges made in this contract would be for all relying parties connected to the federation hub in any commercial sector.

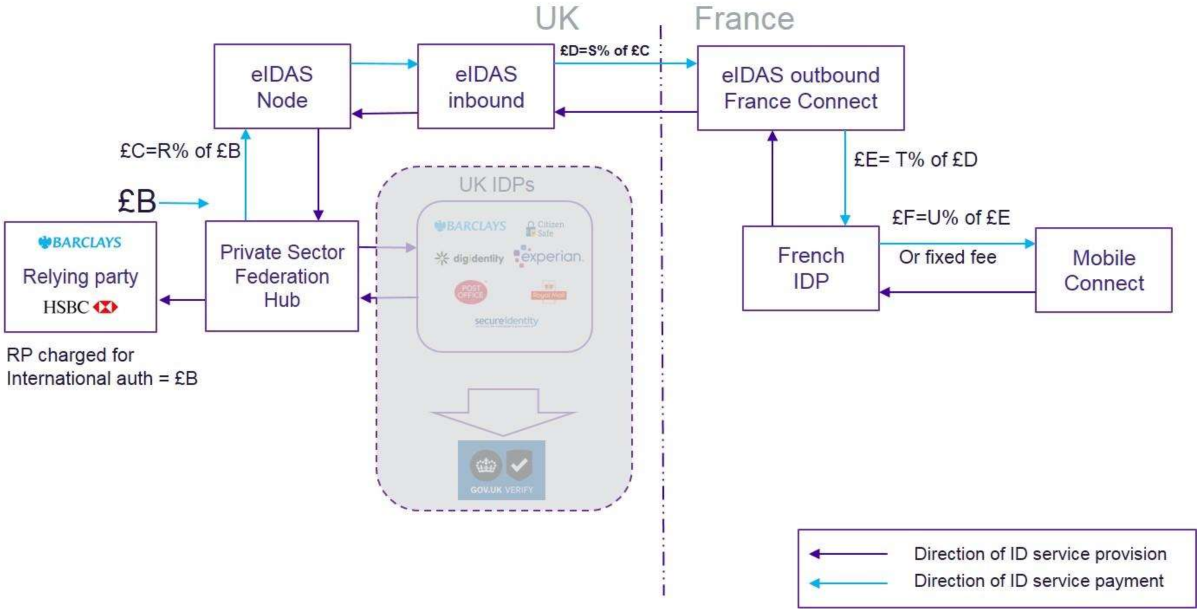


Figure 2 - ID verification charging.

Explanation of charging

Charge point	Description

B	The price that the hub charges the bank for verifying an ID
C	The price that the hub pays to the provider of an eIDAS service un the UK
D	Price paid to pass ID verification between eIDAS service providers in nation states.
E	Price which the French IDP charged for verification of the ID they created against their scheme ruled
F	Price that the MNO charges the IDP for use mobile connect.

Table 1

If there is no charging of the eIDAS interchange the charge point 'C' is the same as 'E' because the federation hub provider would contract directly with the French IDP.

Commercial Structure for attributes

The diagram below shows a similar approach to the construction of a commercial model for the acquisition of attributes. In analysing this part of the commercial model, there are simple commercial structures today for data that are operated by credit rating agencies. It was felt that the charging for this element of the Action should be adopted for simplicity at the outset.

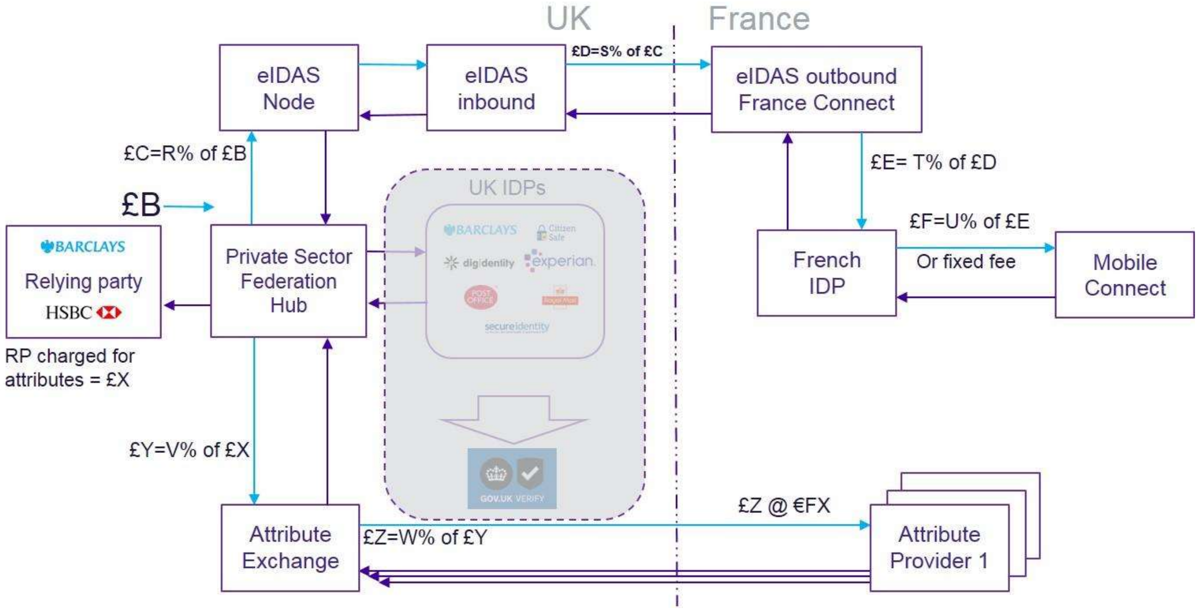


Figure 3 - Attribute exchange commercials

Figure 3 above shows simply how a French attribute provider would contract with the attribute exchange provider for the supply of an individual's data. In this illustration, the entity that operates the attribute exchange need not be the same entity that operates the hub. It is anticipated that both hub and attribute exchange will be operated by the same entity in production services.

Explanation of attribute charges, in addition to these detailed in table 1 above.

Charge point	Description
X	The price that the hub charges the bank for attribute data
Y	The price that the hub pays to the attribute exchange provider in the UK
Z	The price the French data provider charged to release the verified data for consumption.

Table 2

When considering the prices for attributes it is expected that the market for a particular attribute will be priced on its commercial value as attributes that provide good detail of an individual would command higher prices. For example an individual's address might be priced higher than the same individual's shoe size.

It is assumed that the Bank connects into the Federation Service, which is single hub that is responsible for gathering authenticated identities, by connecting into the Node that is connected into the eIDAS framework. For the purposes of this model, it is assumed that the other attributes will not be served within the eIDAS framework, so a separate attribute exchange is developed, which gathers the additional attributes required by the Relying Party to open the bank account.

Business Analysis

Currently, in the UK there is no standard way of identifying individuals, in the private sector context, so organisations use a mixture of data and documents to check whether the user is who they say they are. Most commonly used documents include (a combination of) a passport, or a driving licence, but may also include utility bill and others. Often these are not available in a digital format, resulting in face to face interactions.

UK Banks are regulated for Anti-Money Laundering (AML) by the Financial Conduct Authority, and the Joint Money Laundering Steering Group (JMLSG) provides practical guidance regarding AML requirements to banks to enable their on-boarding requirements. The Consortium decided to focus on the onboarding requirements for UK Personal Current Accounts, with no credit facility.

The participating banks provided details of the different data sets and attributes required to enable them to verify and validate an identity and the examples of other data required from an applicant to open a Current Account. These are detailed in Schedule 2 below and are supported by previous research work.

Research findings

The Consortium reviewed existing research into the identity verification approaches of UK Banks, including an OIX project called; How Digital Identities Which Meet Government Standards Could be Used as Part of UK Bank's Customer On-Boarding and KYC Requirements.

In 2016, PwC were commissioned, by the British Bankers Association (now part of UK Finance), to survey a range of UK Banks on the methods they use for verifying the identity of their customers. The research found that there is significant variation in the identity verification approaches used, and this depended on the size and type of bank.

The study reports that there is a correlation between the size of the bank and the data required of the customer. Larger, more well-established banks require the most data, whereas mid-tier banks require significantly less data and some new challenger banks seek significantly less than the other two categories.

Stakeholder feedback

The Consortium met with AML and Legal teams in the participating banks. Feedback included concern about accepting digital identities and associated attributes from other countries that may not have such rigorous approaches, to the identity verification and validation, used by UK financial institutions in their Know Your Customer (KYC) checks. Also, the reliance on data from organisations based in other countries may cause issues unless there is a standard developed that attests the validity of different types of data (such as attributes and credit checks) and due diligence of such organisations can be rigorously applied on an ongoing basis. In addition, it was noted that there would be a need for regulatory collaboration and industry alignment around the issue of liability in a digital identity ecosystem.

Through research, it was noted that financial institutions in other Member States rely on different data sets and approaches for verifying identities and assessing an applicant's credit worthiness. The availability of attributes and related services vary considerably in a digital format. This will prove challenging for UK Banks, who have very rigorous requirements in identifying a potential customer and the defined attributes required to assess their application, which are required to comply with UK AML regulation.

France research

To open a retail bank account in France requires the provision of a lot of paperwork, however banks will accept documents that are scanned and presented in an electronic format. Currently, there is no national identity database that can be used to verify identity credentials.

Identity verification requires the customer to present documents for both proof of identity and proof of address. The individual's identity can be checked through the presentation of an ID card (which may be a scanned copy) and transfer of money from another bank account (under the same name) is commonly required.

Fraud checks, relating to what the applicant declares in their forms, are achieved by checking the individual's tax claim with the Government. In France, it is not mandatory to declare your address to the Government, so the bank account opening relies on copies of recent bills, in the name of the applicant, to be provided. This could include a mobile phone bill, however the Consortium noted this raises the potential issue of accounts not being registered at the home address of the individual wishing to use their bill as form of address validation.

The ability to share credit data is very complex. For example, Credit Reference Agencies do not exist in France, so to check if the individual has had bad debt in another account may be achieved by checking the applicant's name against a register, held by the French Bank Association (FBA), of French citizens who have previously had debt problem. The FBA will provide a yes/no response, however the FBA will only currently only deal with French Banks, which may be an issue for UK Banks wishing to undertake credit reference checks.

Recommendations

The Consortium recommended that further detailed mapping is required, including how credit history data is reported, by which organisation and how reliable it is considered to be. The relying parties can then take their risk-based decisions as to whether to accept the credit history or not.

Annex E: project methodology and delivery issues

Project methodology

The project was initiated by Government Digital Service (GDS) in 2016. It brought together organisations under the consortium which then successfully bid for the EU funding under the CEF 2016 Telecoms funding round. The organisations in the consortium were Barclays, HSBC, IDEMIA, the Open Identity Exchange (OIX), Orange and the UK GDS.

The project was run by OIX, under OIX rules of openness and transparency. It also implemented an agile approach of running projects, with pre-discovery, discovery, and alpha stages.

The project has completed the stages and produced a number of reports, which were shared widely for comments, and input from relevant stakeholders, prior to being finalised. The relevant documents can be found on the OIX website.

The methodology applied by the consortium consisted of the agile approach, as mentioned above, including division of work into workstreams and assigning a lead for each of the workstreams.

The consortium created a project steering group, composed of the lead contacts from each of the organisations, which met on a regular, monthly basis. The leads reported on the progress of individual tasks, while the general tasks were discussed as well.

The OIX provided the coordination and project management role to the project.

Delivery issues

As the project progressed and the consortium delivered pre-discovery and discovery stages of the project, it became apparent that some elements won’t be delivered within the originally suggested timeline. A number of changes took place during the life time of the project both externally, with the UK’s decision to leave the European Union, and within organisations, with changes of strategy, focus and personnel. Most notably one of the consortium members, Morpho, merged with Oberthur Technologies. The company now trades as IDEMIA. The key role of this consortium member led to a delay in the project and a 6 month extension for its completion was granted by the European Commission.