Connecting Europe Facility: Opening a bank account across borders

Discovery Phase Report

by Harry Weber-Brown

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 participants were:

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

Background

HSBC, Barclays, Government Digital Service (GDS), Morpho (trading as Idemia), Orange and Open Identity Exchange (OIX) UK formed a Consortium to deliver a digital identity

project[1] (hereinafter referred to as the Action) that developed and tested a prototype to enable an EU citizen to open a bank account in another European country using their national digital identity. This Action designed the service and operational framework that could facilitate a more trustworthy and efficient account opening process for EU citizens across Member States.

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

The Consortium has been awarded a grant by the European Commission's Innovation and Networks Executive Agency (INEA), under the Connecting Europe Facility (CEF) programme[2]. It is building a full end-to-end prototype, testing a strong authentication process by leveraging Mobile Connect[3] and validating the citizen's digital identity, across Member States, via the eIDAS[4]framework.

Discovery Phase

The Discovery Phase focused on undertaking the necessary research and planning to enable the Consortium to deliver the proceeding Alpha Phase. In this Phase, the Consortium agreed to focus on five key areas, which are:

1. Contractual and Commercial Models
2. Business analysis
3. Technical Architecture
4. Stakeholder Engagement
5. Design and user testing of paper based end-to-end customer experience

These are covered in turn below;

---

[1]http://bit.ly/2hrpwjU
[2]For more details https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom
[3]https://mobileconnect.io
[4]eiDAS is an EU regulation and sets the standards for electronic identification and trust services for transactions in the European Single Market.

Contractual and Commercial Models

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 the 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 their exposure to liability; this is covered in detail in the Alpha phase,

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. Morpho 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:

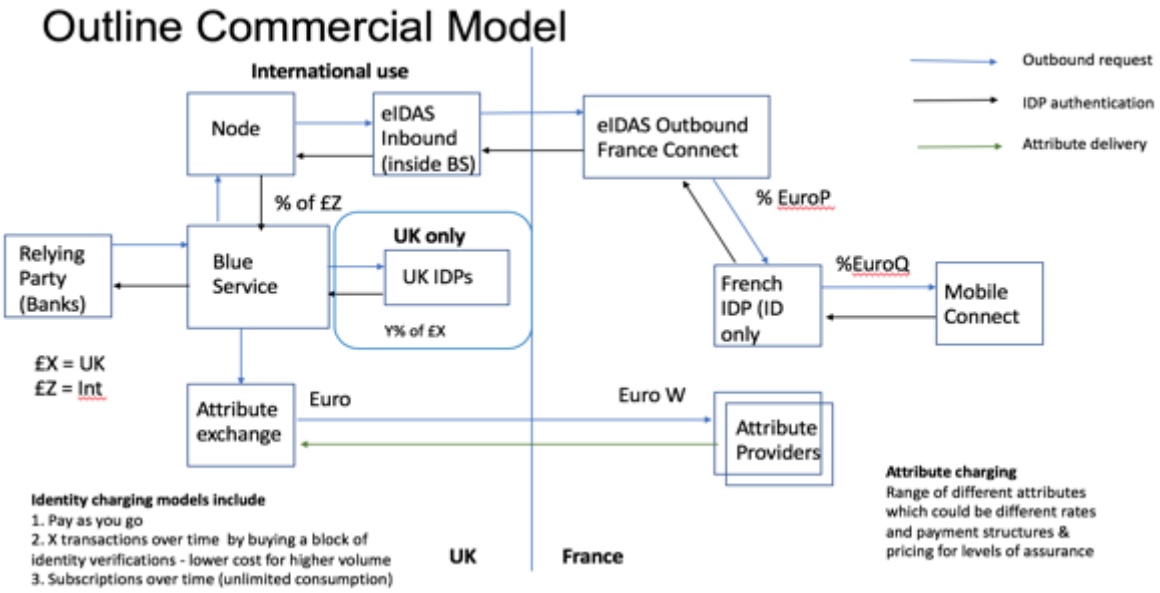
- Prices cannot be fixed by IDPs for either identity authentication or additional attributes: this has to be determined by the market as it would otherwise be anticompetitive.
- IDPs and attribute providers can have different prices, and these may be based on the available data sets (including eID and 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

Morpho 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. Morpho 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.



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.

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, Price Waterhouse Coopers 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.

Technical Architecture

This work module initially assessed the principles and then the frameworks were considered for delivering the technical architecture. The specific recommended components for the workstreams were defined in this module.

Principles and frameworks for the technical architecture

In defining the components for the workstreams, the Consortium developed the principles to apply to the solution (e.g. open standards) and identified the technical frameworks that align to the principles.

Principles

The table below sets out three categories of principles and assumptions describing the market in which the Blue Service operates with regard to (A) the user experience, (B) the service architecture and (C) the commercial environment.

Principle	Rationale
A.1 User controlled • The User controls the release of his / her personal data to the Relying Party (RP)	• Compliance with the General Data Protection Regulation (especially the **Lawful Basis for Processing** of personal data) • The User is responsible for assertions that he / she makes to the RP
A.2 Transparency to the user • The User is able to view all personal data used or processed in a transaction and will be able to correct erroneous data	• If erroneous data is being used, then the User will correct it before costs are incurred (with implications for trustworthiness of the data to the RP). • A User should not be able to deny fraud by claiming that he / she did not know the assertion that was made in his / her name
A.3 User choice • The User should not be obliged to use the service of any party (IDP, Attribute Provider, Hub Service, etc).	• The User should not be obliged to have a relationship with any given private sector organisation.
A.4 Risk based • The RP will determine what services it will provide to the User at any given level of risk	• It is the RP's business decision.
A.5 Risk articulation • The User will be made aware of the level of assurance required to be achieved for a service	• The User needs to understand what he / she has to do in order to access a service through any given channel or mechanism.
B.1 Federated architecture • There will be no monopoly of operational function in the digital	• There will be no 'single point of weakness'

identity ecosystem by any one component	
B.2 Interoperability ● All elements of the ecosystem should be technically interoperable (i.e. open technical standards based)	● Poor performance by a component operator should not be protected by construction of bespoke technologies.
C.1 Standards based ● All processes should perform to agreed operational standards	● Government and the market will ensure that citizens' and society's needs are met through brokering reasonable standards across all stakeholders.
C.2 Certification ● Operators will be assessed against standards by independent certification authorities	● Trust that standards are being interpreted and met requires neutral interpretation through a transparent process
C.3 Commercially driven ● All parties act according to their own (commercial) interests	● The value of participating in the identity ecosystem, whether monetary or otherwise, must be clear to all parties for long term sustainability
C.4 Open ● Any IDP that is certified against Standards will be acceptable to any RP	● No artificial (commercial) barriers should be created to restrict user choice and control ● The RP should not know who the Identity Provider is for any specific transaction
C.5 Market of data ● Data sources used to corroborate personal details will compete with one another	● There are many sources of data that can be used by an individual. ● It is acceptable and inevitable that they will all have different trust weightings and different costs associated with using each.

Frameworks

The Discovery Phase focused on the eIDAS technical frameworks and reference architecture to assess how the private sector node could be connected.

The following frameworks were considered and used in developing the working prototype during the Discovery phase.

Functional components:

- The Prototype (labelled *AnyBank*) website
- ID federation hub
- eIDAS component
- France Connect
- Mobile Connect infrastructure
- Attribute exchange solution
- Database structure for attributes

Frameworks needed:

Physical infrastructure framework

- Hosting solution
- Cloud vs in-house
- AWS requirement
- Network requirements
- Network security

Operating systems framework

- Linux
- VM solution VMWare / Oracle
- Scaling
- Server solutions
- Server security
- Database solutions. MySQL, MS SQL
- Server Homologation - Idemia (Morpho) Corporate IT
- IPR protection

Application framework

- Server monitoring
- Application monitoring
- Web technology
- SAML solution
- eIDAS requirements and specification for federation hub
- SecureKey Exchange federation hub
- UK IDP for initial testing
- French IDP
- Mobile Connect
- SIM applications

Protocol framework

- OIDC
- SAML /Verify SAML
- eIDAS
- HTTPS
- Verify SAML
- GSMA Mobile connect
- UMA

Messaging flow

- Bank web to Hub
- Hub to eIDAS
- eIDAS - French IDP

- Mobile Connect to Smartphone

User Interface

- HTML 4/5
- JavaScript
- CSS

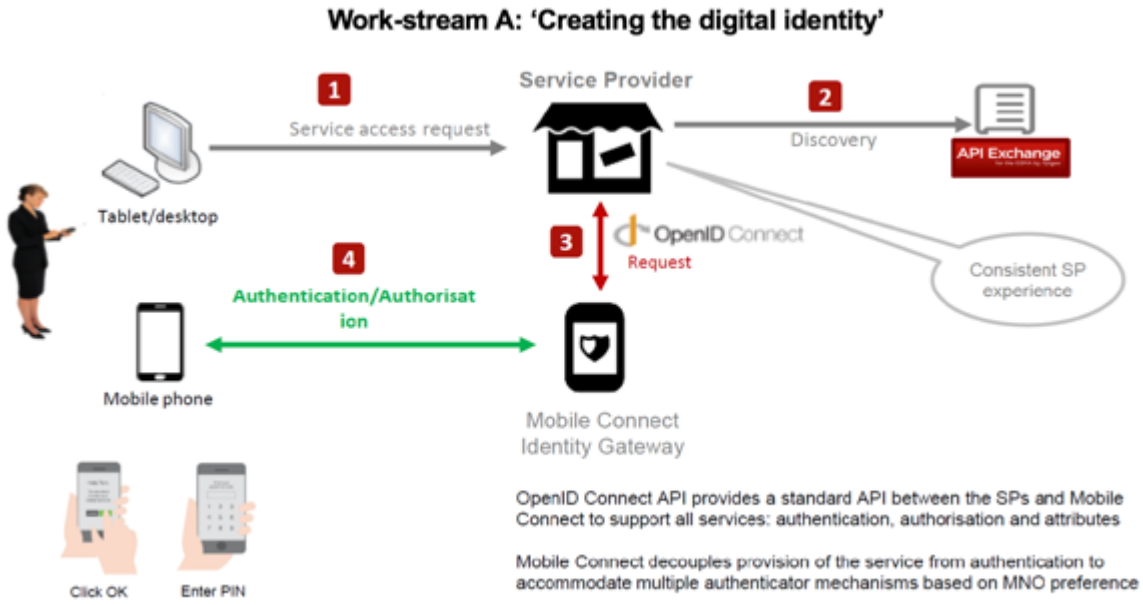
The Consortium decided to use the User Managed Access (UMA) framework and identified what exists and what additional components would be required, which are detailed in the Alpha report.

Detailed components planned for development during the Action

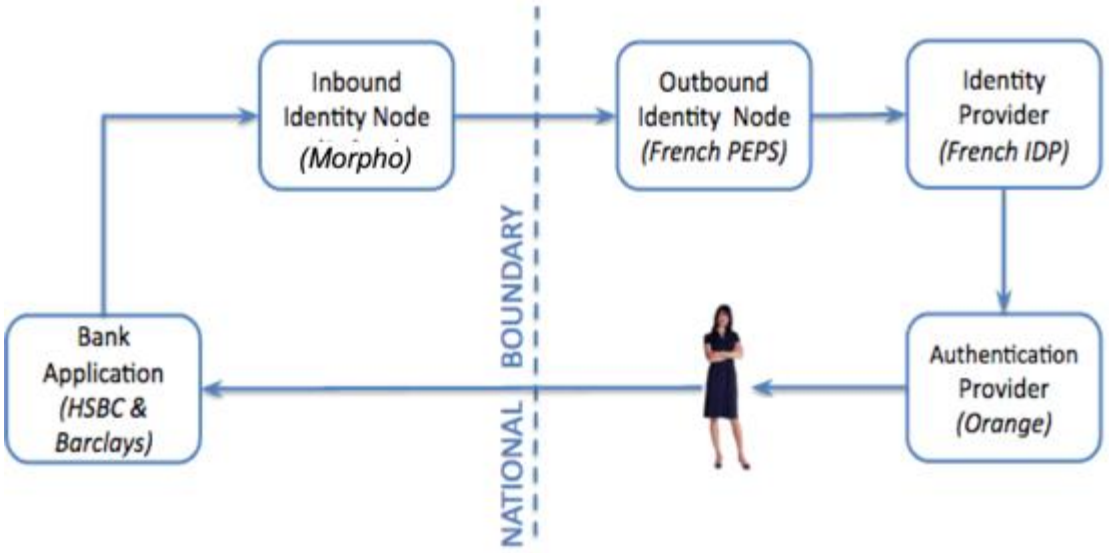
Defining the components required for Action was achieved by splitting the Action into three distinct stages, with the aim of demonstrating the creation of a digital identity, assertion of the digital identity to the service and the use of that digital identity to access other necessary attributes about the user in order to access the service (i.e. opening a bank account) which were set up as work-streams. These were:

1. Workstream A - Creating the Digital Identity
2. Workstream B - Asserting the Digital Identity
3. Workstream C - Using the Digital Identity

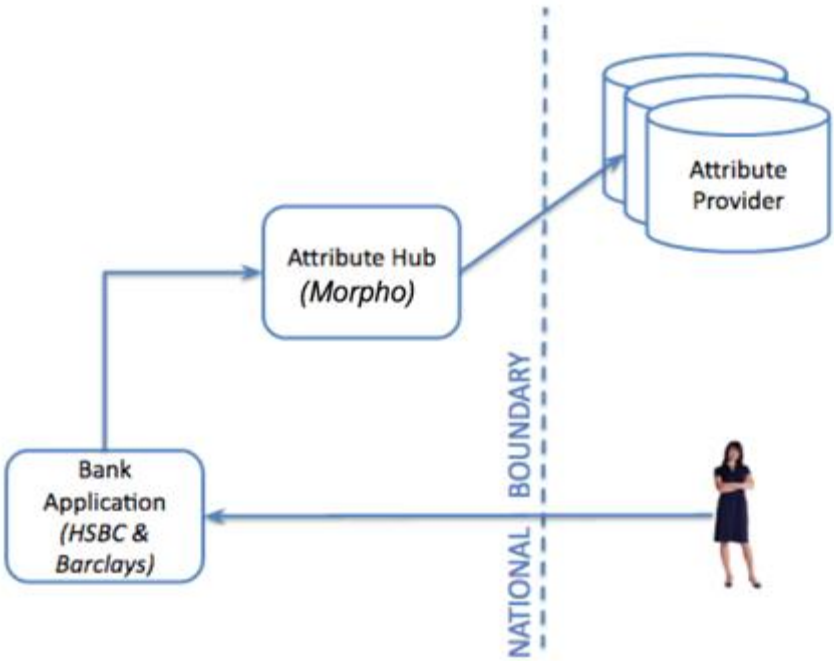
The components of each of the Work-streams were analysed by working through the following high-level process flows:



Work-stream B: 'Asserting the digital identity'



Work-stream C: 'Using the digital identity'



The Consortium agreed the Action should not attempt to change the existing flow of data into a Bank and the current process of opening a bank account, as any changes to existing systems would be a major blocker. The Action focused on the outputs of the Discovery and Alpha phases, rather than a Live Phase which would require integration into live banking services.

The Consortium therefore agreed to build the prototype outside of the banking infrastructure and deliver this as a simulator, however it would need to understand the flow into the Bank and how the Banks regard identities provided through the eIDAS framework.

Attribute Exchange specification

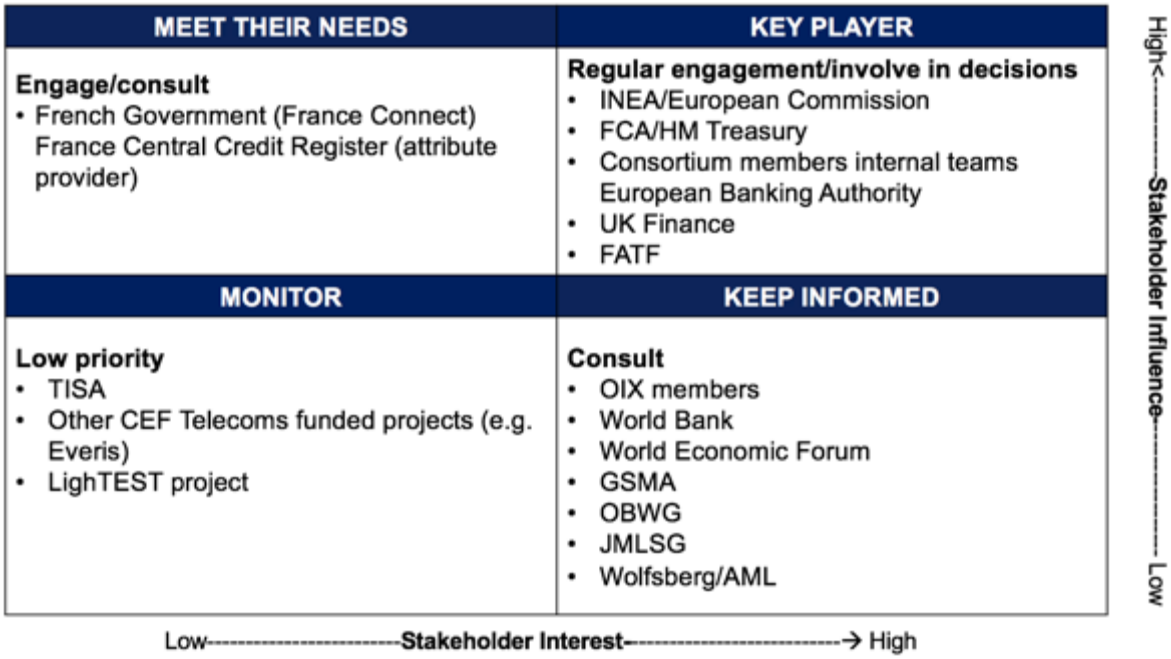
The Morpho team were responsible for defining the specifications for the attribute hub and the eIDAS node These were detailed in the implementation requirements ensuring the components comply with the eIDAS specifications for the Message Format and SAML Attribute Profile. These are detailed in the attached schedule.

Investigate how interoperability (as per eIDAS standards) has been achieved by the GDS team with other member states and look at best practice.

The Consortium convened a number of workshops that focused on eIDAS standards, with expertise provided from the technical and standards GDS leads on eIDAS. The workshops considered the eIDAS technical architecture and standards in detail, and the necessary requirements in order to develop an interoperable prototype, as specified under eIDAS. The architecture and standards were then adopted within the Action to ensure interoperability with France Connect, for the end to end prototype testing.

Stakeholder Engagement

The Consortium identified the following stakeholders in the Discovery Phase and these were segmented according to their influence within this field (based on low to high) on the vertical axis and the stakeholder interest (based on low and high) on the horizontal axis. These organisations were progressively engaged through the delivery of the Action.



The Consortium gathered feedback from relevant stakeholders on the different workstreams outlined above, including the contractual and commercial principles. The feedback is contained in the sections above.

During the Discovery Phase, OIX developed a dedicated section of the OIX website to include pre-discovery report and a LinkedIn discussion thread was created. Updates on the

Action were included in the quarterly OIX membership bulletin newsletter. Please note that the opportunity for Government communications was limited, especially concerning Europe.

Communications

The British Bankers Association (BBA) agreed to communicate this Action to its member panels, and BBA engaged with its European counterpart banking associations on behalf of the Action.

GDS and OIX developed a PowerPoint deck for internal communications, within the participating organisations, and for external stakeholders. This included assessing the size of the addressable market (based on migration data across member states) that highlighted the opportunity, the use case, an overview of the Action and the benefits.

This was widely shared and used for presentations to a broad range of interested organisations including the European Commission, the GSMA and OIX members. More details of the stakeholder engagement, through the development of the Action, will be included in the Final Report.

Design and user testing of paper based end-to-end customer experience

Define the user testing required of the end-to-end customer experience and high-level technical architecture for Alpha phases.

During the Discovery Phase, the Consortium built an end-to-end customer experience (in PowerPoint) which is contained in Schedule 3 below and further iterations were built in the Alpha Phases which the Consortium members shared into their respective organisations and gathered feedback on the user experience and flow. OIX/GDS presented this to the OIX membership, through events.

The Consortium convened a number of workshops to develop personas, which outlined the types of people who may be interested in using such a service. These included the following personas and their intended user journeys. Full details of the personas are contained in Schedule 4.

ID	Name	Digital ID use	Level of Assurance	Additional Attributes
1	Noemie	Registration	Substantial / LoA2	All
2	Dylan	Registration	Proofing Failure	N/A
3	Celia	Re-use	Substantial / LoA2	All
4	Emily	Re-use	Substantial / LoA2	Some
5	Enzo	Re-use	Substantial / LoA2	None

The aim of the User Testing was to understand whether a purely digital process would be used by those people from overseas who have recently opened an account and what blockers may arise. A clickable (html based) prototype and video have been produced for testing in the Alpha Phase.

The Consortium agreed that the User Testing would focus on a mix of key stakeholder presentations of the prototype, which simulates the user journey, and quantitative (rather than lab based) research that includes the development of a video that explains the Action and demonstrates the use case of opening a bank account from another member state. User research data, for the quantitative study, is being gathered using a Survey Monkey poll.

Schedule 1

CEF hub service - eIDAS node implementation requirements

Idemia developed the eIDAS components to comply with eIDAS specifications:
i) eIDAS Message Format_v1.1-2.pdf
ii) eIDAS SAML Attribute Profile v1.1_2.pdf

The incremental features to the Idemia ID hub are outlined in Table 1.

Table 1

#	FEATURES	Feature and Implementation Comments
General Feature		
1	<md:EntitiesDescriptor> Support	Need to support loading of metadata from <md:EntitiesDescriptor> (multiple entities) both RP and credential service provider ("**CSP**") sides. Should be supported according to security assertion markup language ("**SAML**") 2.0 spec.
2	Adding urn:oasis:names:tc:SAML:2.0:nameid-format:transient support	Transient flow should be fully supported according to SAML 2.0 spec. Currently support persistent flow.
3	Adding urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified support	Unspecified flow should be fully supported according to SAML 2.0 spec.
4	<eidas:SPType> support	Custom extension - general description from the eIDAS profile: For indicating whether an authentication request is made by a private sector or public sector service provider ("**SP**"), the defined element <eidas:SPType> MUST be present either in the <md:Extensions> element of SAML metadata or in the <saml2p:Extensions> element of a <saml2p:AuthnRequest>. If the SAML metadata of an eIDAS-Connector contains a <eidas:SPType> element, SAML authentication requests originating at that eIDAS-Connector MUST NOT contain a <eidas:SPType> element. The <eidas:SPType> element can contain the values "public" or "private" only. Exchange Implementation Requirements: 1>if Received from RP, should be passed to the CSP. 2>Should be definable per CSP (provider files). If the switch is present and value defined should send the parameter with the authentication request to that CSP.
Requesting Attributes		Requesting attributes by an eIDAS-Connector from an eIDAS-Service MUST be carried out dynamically by including them in a <saml2p:AuthnRequest>. Instead of using AttributeConsumerServiceIndex and similar to the way we pass attribute expression from federation to broker eIDAS requests attributes using custom extension with <eidas:RequestedAttributes> element and listing all

		requested / optional attributes in that extension that resembles attribute statement SAML elements.
5	Adding Attribute Request Extension support with listed required/optional attributes - <eidas:RequestedAttributes> \	Custom SAML extension with optional and required attributes requested dynamically. Exchange implementation requirements: SECUREKEY Exchange should be able to receive eIDAS AuthRequest with requested attributes extension
6	Adding Attribute Request Extension support with listed required/optional attributes - <eidas:RequestedAttributes>	Custom SAML extension with optional and required attributes requested dynamically. Exchange implementation requirements: SECUREKEY Exchange should be able to receive eIDAS AuthRequest with requested attributes extension: Exchange broker should be able to send authentication request to the CSP(based on CSP provider settings) with <eidas:RequestedAttributes> describing the requested attributes
eIDAS SAML Attribute Format		
8	Support Attribute value with custom eIDAS type definition All verify attributes must be mapped to eIDAS attributes and vice versa (CF. GDS specification)	<saml:Attribute FriendlyName="FirstName" Name=" http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"> <saml:AttributeValue xsi:type="eidas:CurrentGivenNameType"> Sarah</saml:AttributeValue> </saml:Attribute> Exchange implementation requirements: Exchange should be able to pass custom attribute value type for the attribute from CSP to RP
9	Supporting eIDAS SAML Attribute Profile encoding and Attribute Structure requirements	General customization work to support required and optional eIDAS attributes with requested encodings Exchange implementation requirements: pass-through from CSP to RP
10	Supporting basic eIDAS attribute types	
11	Supporting complex eIDAS types with encoding	pass-through from CSP to RP
SecureKey Development Eng and Project Support		
12	SecureKey Development Engineering	builds, package, deploy, performance tests, performance reports, operations handover + Docs
13	Product / Project Management, Integration support, Solution Architecture support	

Exhibit 2

#	FEATURES	Feature and Implementation Comments
CEF Requirement for UK		
14	Create Exchange product extension mechanism(plug-in) that will allow SAML to SAML translation (from one SAML profile to another including attribute format transformation)	SecureKey will provide configuration and interface description for the "SAML to SAML IDP Response translation" plug-in mechanism.
15	eIDAS - UK Verify translator based on plug-In mechanism	Exchange implementation requirements: 1> Part of UK Verify private sector Exchange based Hub 2> Receives assertion from eIDAS CSP (eIDAS attributes and eIDAS response message format) 3> Generates UK Verify response message with UK verify attribute statement from the received eIDAS assertion 4>Sends the message back to RP that requested the authentication SecureKey will provide "eIDAS - UK Verify Translator" source code as an example of "SAML to SAML IDP Response translation" plug-in implementation.
16	UK Verify - eIDAS Translator based on Plug-In mechanism	Exchange implementation requirements: 1> Receives assertion from UK VERIFY (UK VERIFY attributes and UK VERIFY response message format) 2> Generates eIDAS response message with eIDAS attribute statement from the received UK VERIFY assertion 3>Sends the message back to RP that requested the authentication SecureKey will provide "eIDAS - UK Verify Translator" source code as an example of "SAML to SAML IDP Response translation" plug-in implementation.
17	SecureKey Development Engineering	
18	Product / Project Management, Integration support, Solution Architecture support	

Schedule 2

An Overview of a typical Customer Due Diligence based on 2017 data.

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

Schedule 3 - paper based end-to-end user journey

1

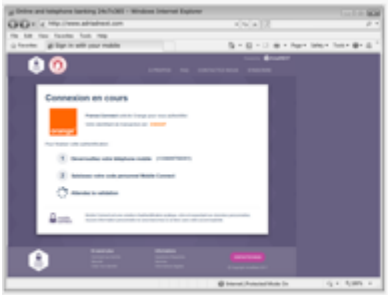
2

3

4


5


6



7


8

9

10

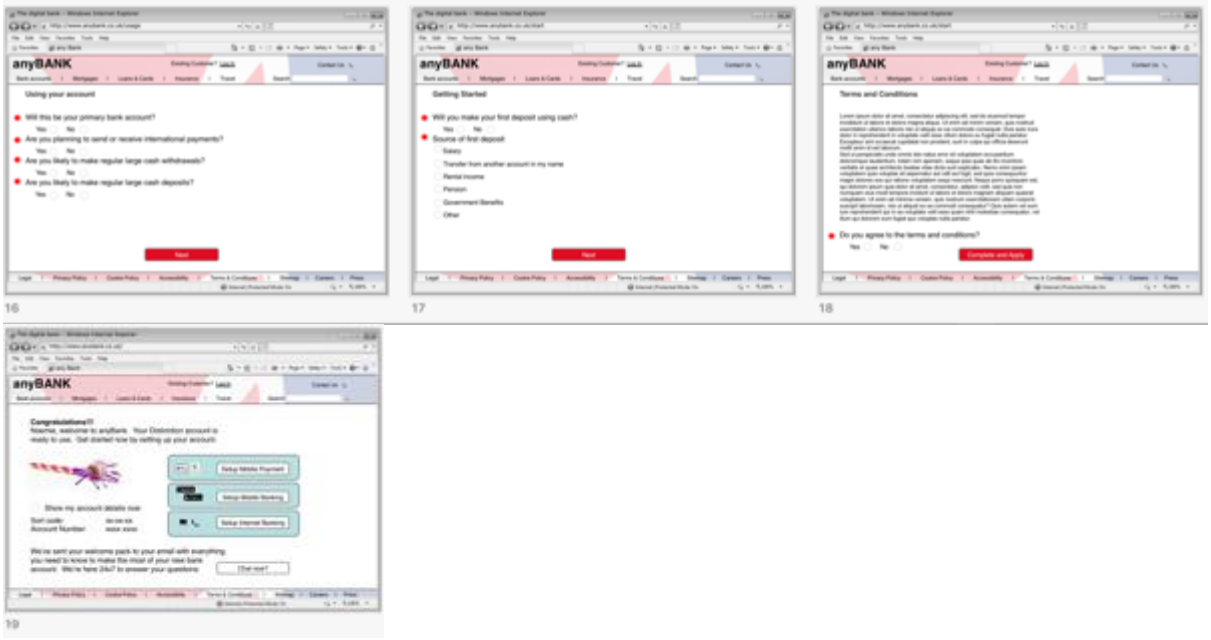
11

12

13

14

15



Schedule 4 - Developed Personas

Meet Noemie

Name	**Noemie Ismael**
DoB	3rd January 1990
Place of Birth	Lille
Current Address	11 Place du Colonel Fabien 75010 Paris France
Nationality	French
Bio	Living with long-term girlfriend; is planning to marry in the next year or two Is a manager in a large department store, she enjoys her career Though she moved out relatively young, she enjoys a close relationship with her parents
Demographic	Millennial (1980 – 1995)
Formative Experiences	1 Ubiquitous technology and the rise of social media Liberalisation of religious and social views
Characteristics	Lives each day to the fullest Expects immediate results and is easily frustrated by bureaucracy Confident, upbeat, optimistic and determined Willing to try new ways of approaching tasks in the digital age

Meet Dylan

Name	**Dylan Bernard**
DoB	1st August 1973
Place of Birth	Lyon
Current Address	46, Avenue Jean-Jaurès 69007 Lyon France
Nationality	French
Bio	Divorced, now dating online Two children whom he sees regularly, financially supports and co-parents Rebuilding his financial assets following his divorce Works in technology sector
Demographic	Generation X (1961 – 1979)
Formative Experiences	Boom and bust economy Increased workforce mobility and changing industry Rising divorce rates 24 hour news and game consoles
Characteristics	Self-reliant Mistrustful of institutions Willing to change rules and beliefs if he can see the benefits Tribal Strong, traditional parenting values

Meet Celia

Name	**Celia Bonnet**
DoB	19th March 1938
Place of Birth	Paris
Current Address	13 Rue des Cloutiers 17000 La Rochelle France
Nationality	French
Bio	Widowed Living on her pension and dwindling savings; still has a small mortgage on her home Healthy, mobile and active in her community
Demographic	Silent Generation (1928 to 1945)
Formative Experiences	World War II and the early days of the Cold War Booming Post-War economy Growth of suburbs Increased availability of consumer goods
Characteristics	Actively joins new clubs and societies Loyal to institutions and brands Accepting of hierarchy and rules Respectful of positional authority Sees financial worth as a metric of success

Meet Emily

Name	**Emily Duval**
DoB	26th July 1987
Place of Birth	Troyes
Current Address	Flat 8a, 97 Camden Gardens London NW1 9PQ UK
Nationality	French
Bio	Small business owner who lives in the UK, though maintains a second home in France Puts her career first in her life, works hard and reaps the rewards Passionate about mentoring others to help them made the best of themselves
Demographic	Millennial (1980 – 1995)
Formative Experiences	Parents love of art and design Rise of the internet marketplace Globalisation powered by technology
Characteristics	Always active, loves to explore new things and learn about how they work If something doesn't work how she expects she will find ways to fix it An entrepreneur Generous and altruistic with her time, money and knowledge

Meet Enzo

Name	**Enzo Lopez**
DoB	15th September 1999
Place of Birth	Saint-Paul-de-Vence
Current Address	77 Chemin des Rosiers 97460 Saint-Paul-de-Vence France
Nationality	French
Bio	Studies Economics at local college Career goal is to become an economic journalist Lives with his parents, though considers himself to be 'self-reliant'
Demographic	Re-Generation (born after 1995)
Formative Experiences	Grew up with mobile phones and reality TV Parents both work, providing a stable family life Used to earning his own money and contributing to family life
Characteristics	Expects ubiquitous access to information and services Believes in conservation and renewal Behaves in a frugal and pragmatic manner, is willing to make tradeoffs and compromise He believes he can make a difference in the world