Identity & KYC Attributes

IDEMIA

FORGEROCK

Agenda

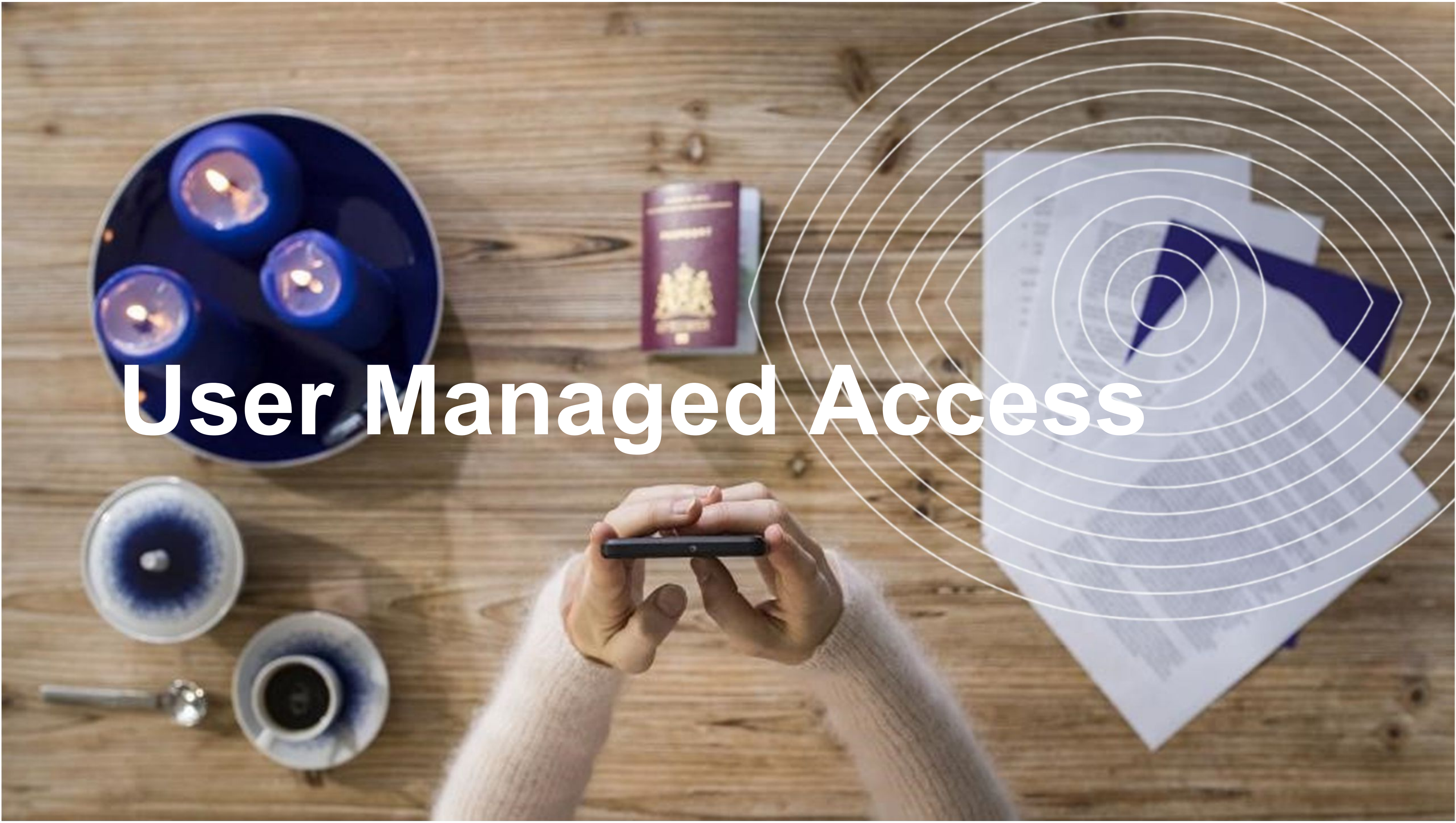
1. **Introduction** - David Rennie, Idemia (5 mins)

2. **User Managed Access (UMA) Protocol** - Maciej Machulak (20 mins)

3. **Connecting Europe Facility** - Andrew Potter (20 mins)

4. **EC Expert Group on KYC Attributes** - Stephane Mouy (20 minutes)

5. **Proposed next steps** - David Rennie (20 mins)

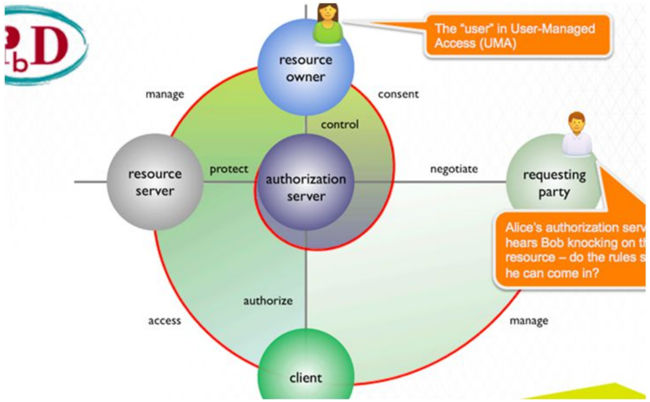


User Managed Access

Maciej to provide.

Purpose: to explain how UMA overcomes challenges of sharing data

- User authorised / controlled
- creation of **bilateral** data sharing arrangement direct between entities
- Privacy
- Built on proven technical protocols


The "user" in User-Managed Access (UMA)
resource owner
manage
consent
control
resource server
protect
authorization server
negotiate
requesting party
Alice's authorization serv hears Bob knocking on t resource – do the rules s he can come in?
authorize
access
manage
client

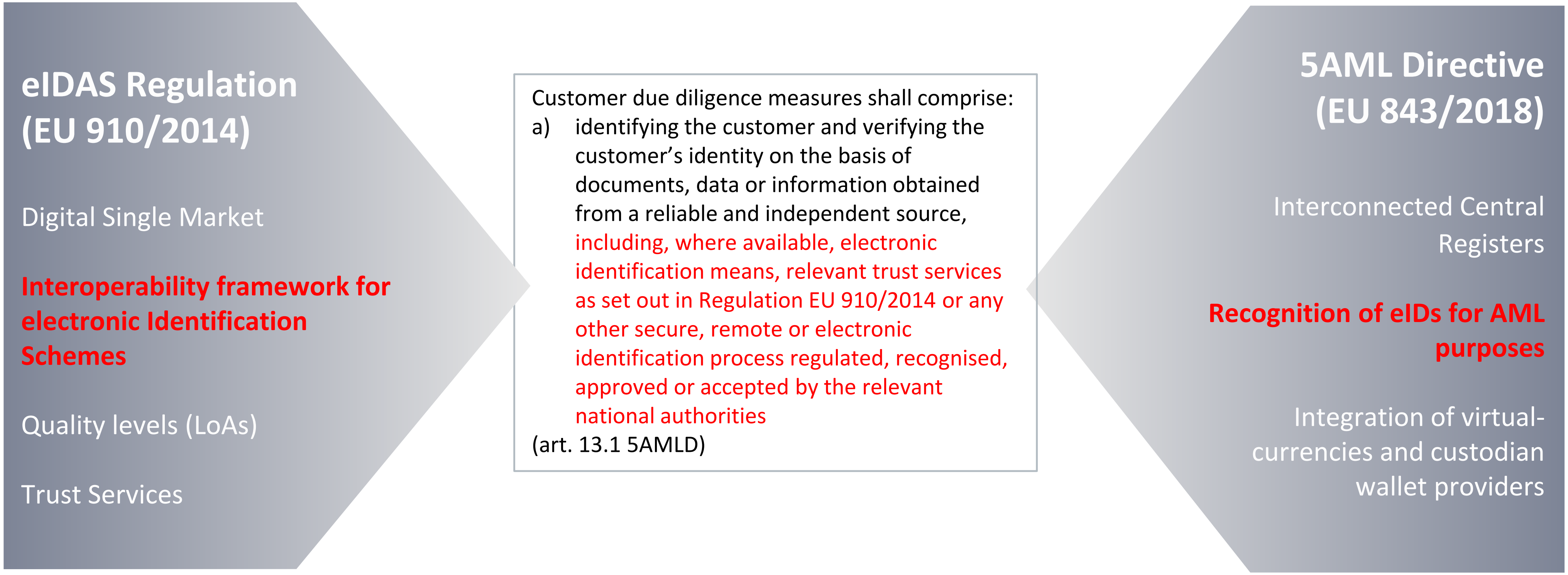
Connecting Europe Facility

Andrew to provide.

- Walkthrough wireframes and explain how UMA was used
- https://oix-proto.herokuapp.com/

EC Expert Group on KYC Attributes

When 5AMLD meets eIDAS : KYC Regulatory Impact



eIDAS Regulation (EU 910/2014)

Digital Single Market

Interoperability framework for electronic Identification Schemes

Quality levels (LoAs)

Trust Services

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

(art. 13.1 5AMLD)

5AML Directive (EU 843/2018)

Interconnected Central Registers

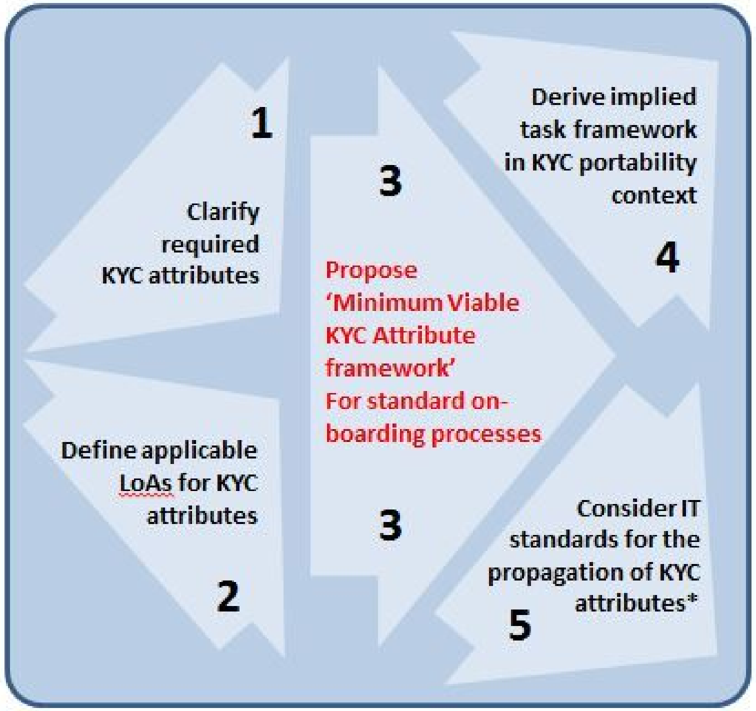
Recognition of eIDs for AML purposes

Integration of virtual-currencies and custodian wallet providers

The rationale for a common eKYC framework

Key considerations

- We are far from a digital single market : How do we deal with a fragmented landscape?
- How should innovative on-boarding solutions be recognised?
- How do we provide a level playing field for service providers?
- How do we facilitate KYC transfers & KYC mutualisation?


1
Clarify required KYC attributes
2
Define applicable LoAs for KYC attributes
3
3
Propose 'Minimum Viable KYC Attribute framework' For standard on-boarding processes
4
Derive implied task framework in KYC portability context
5
Consider IT standards for the propagation of KYC attributes*

Early consensus on the following

- A common standard is needed
- Focus on individuals rather than corporates
- Identify KYC attributes and related LoAs
- Propose a 'minimum viable' framework
- Address liabililty implications upfront

First assessment : the major hurdle does not appear to be on the technology side – solutions are available

eKYC framework proposal explained

Clarify KYC attributes & ID documents

CEF Eid Building block - Architectural Solution Document (March 2018)

- Defines KYC attributes

PwC Study on eID and digital on-boarding (April 2018) : offers a classification for ID documents

- Type 1 : physical document not machine-readable
- Type 2 : physical document machine readable
- Type 3 : physical document machine and electronically readable
- Type 4 : 'logical' document implemented in digital media only

Distinguish 3 main blocks

- **Identification attributes – Core ID**
- **Status & due diligence attributes (PEP, Sanction, Origin of Funds, Tax residency status, etc)**
- **Risk profiling attributes (not covered by proposal)**

Reuse the eIDAS LoA Framework

Identification attributes

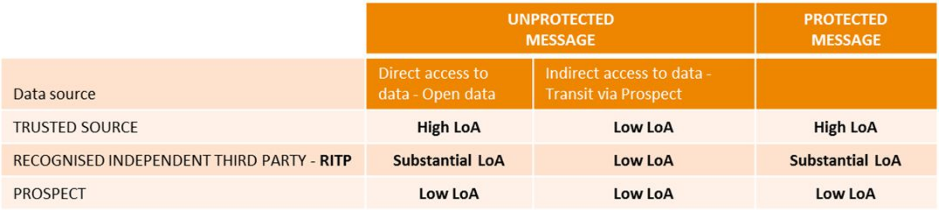
Attributes communicated through eIDs : eID LoA

Attributes remotely extrated from ID documents

- Type 1 ID Documents : Low LoA
- Type 2 ID Documents : Low or Substantial LoA
- Type 3 ID Documents : Low, Substantial or High LoA
- Type 4 ID Documents : High LoA

Status & Due Diligence attributes

- Trusted source : High
- Recognised Independent Third Party : Substantial
- Prospect (self-declaratory) : Low



	UNPROTECTED MESSAGE		PROTECTED MESSAGE
Data source	Direct access to data - Open data	Indirect access to data - Transit via Prospect	
TRUSTED SOURCE	High LoA	Low LoA	High LoA
RECOGNISED INDEPENDENT THIRD PARTY - RITP	Substantial LoA	Low LoA	Substantial LoA
PROSPECT	Low LoA	Low LoA	Low LoA

Overview of an Minimum-Viable LoA-rated KYC framework

ON-BOARDING JOURNEY – CURRENT ACCOUNT OPENING BY INDIVIDUAL

	LoA - Low	LoA – Substantial	LoA – High
Core ID attributes	NO	OK	OK
Status & Due diligence attributes	NO/OK	OK	OK

‘Minimum-Viable’ means

- Minimum requirements set for regulatory purposes
- Financial institutions are always in a position to require more attributes or higher LoAs, especially for credit-related and fraud-prevention processes

Key benefits

- Standard approach offering visibility and predictability
- Key element for the lowering of intra-EU barriers
- Can easily be packaged into existing IT protocols (including OpenID Connect)
- Greatly facilitates the transferability of KYC attributes – key step towards KYC portability

Proposed next steps

IDEMIA

FORGEROCK

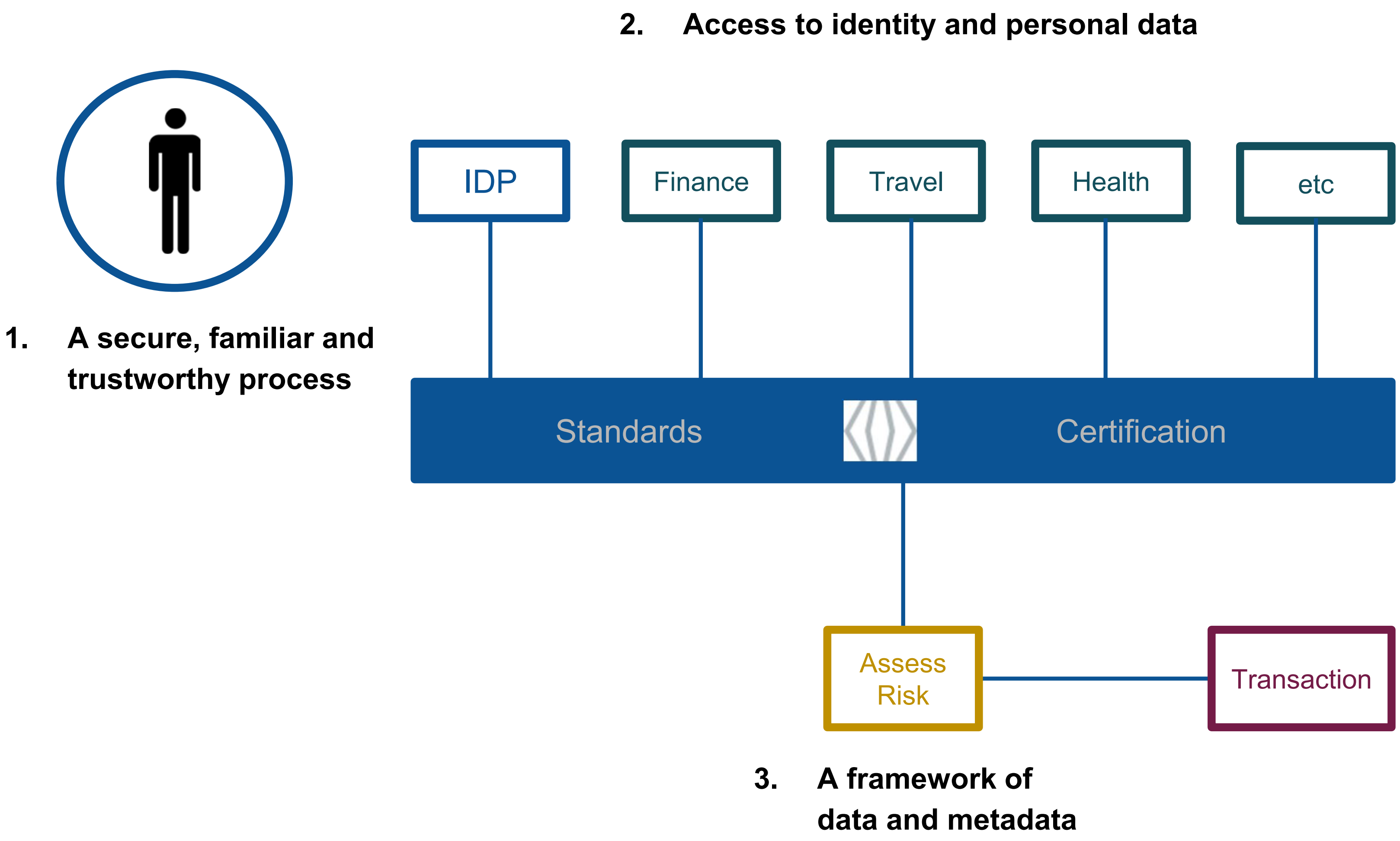
Summary

Banks’ customers:

- are multinational
- have different ways of proving identity
- have different sources of ‘KYC attributes’
- and multiple banking relationships

Banks invest significant resources **validating** personal details about customers in order to meet on-going Customer Due Diligence requirements.

Idemia will operate a service to bank rules

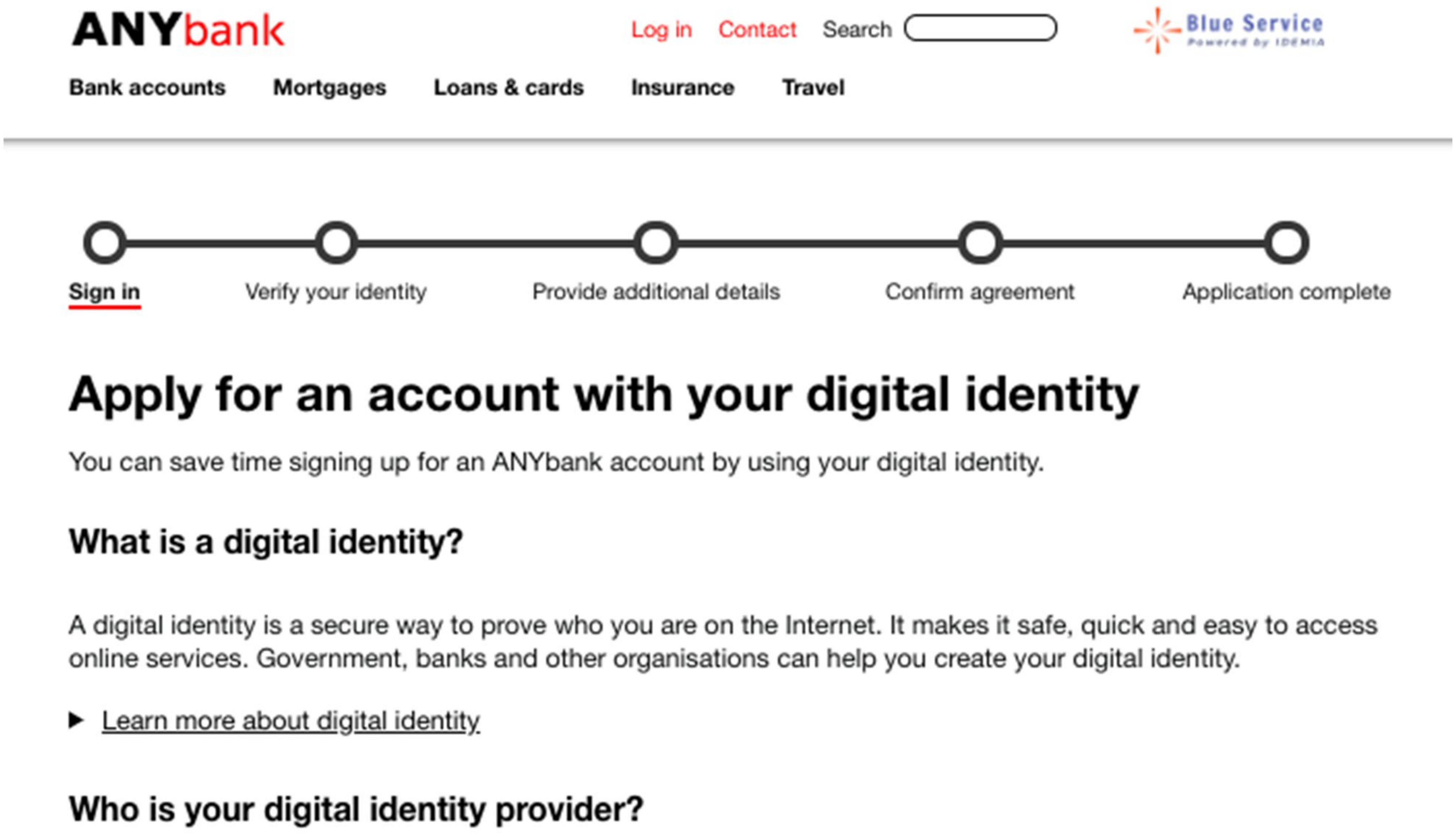


2. **Access to identity and personal data**

1. **A secure, familiar and trustworthy process**

3. **A framework of data and metadata**

1. A secure, familiar and trustworthy process



Apply for an account with your digital identity

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

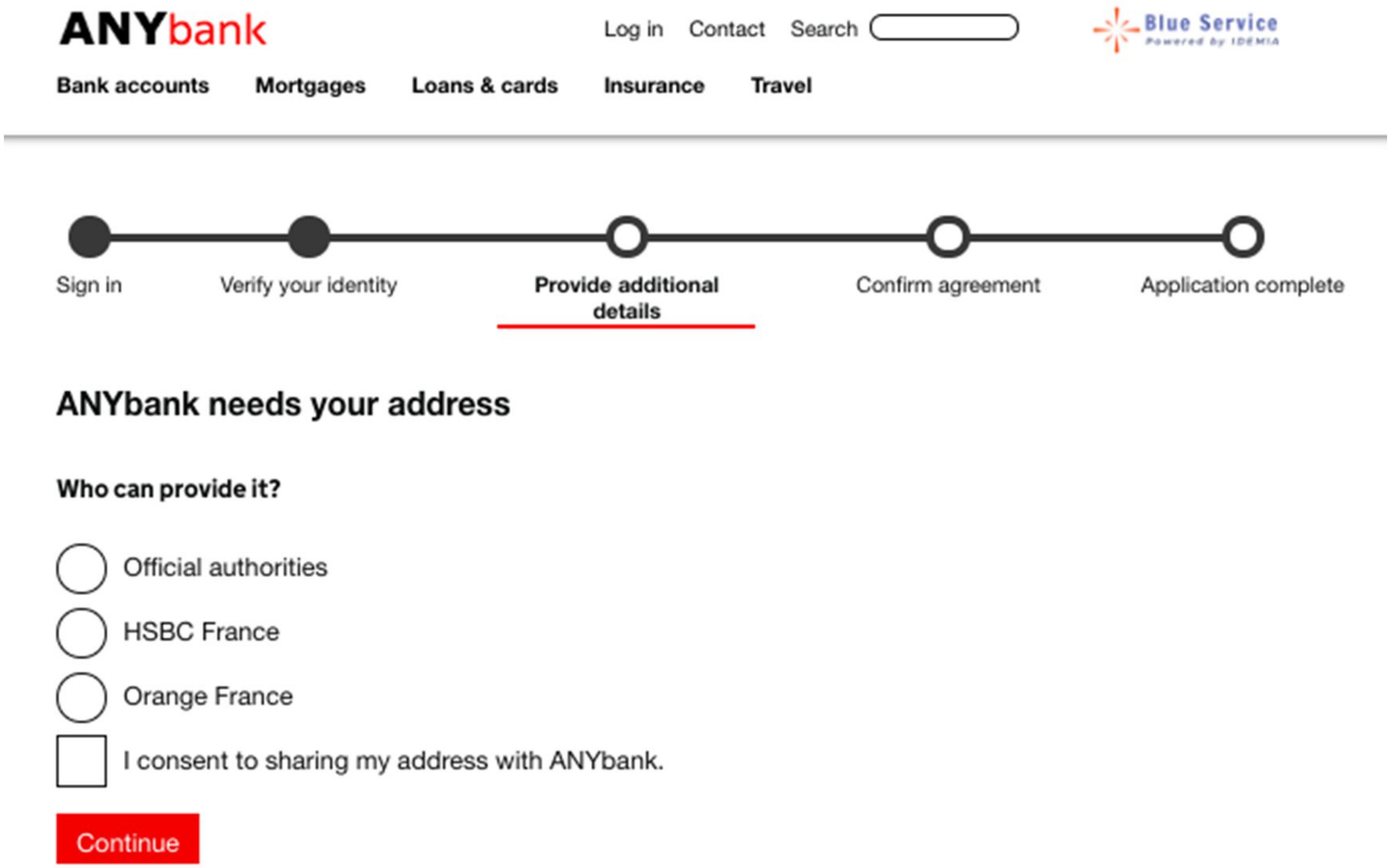
What is a digital identity?

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?

2. Access to identity and personal data



ANYbank needs your address

Who can provide it?

○ Official authorities

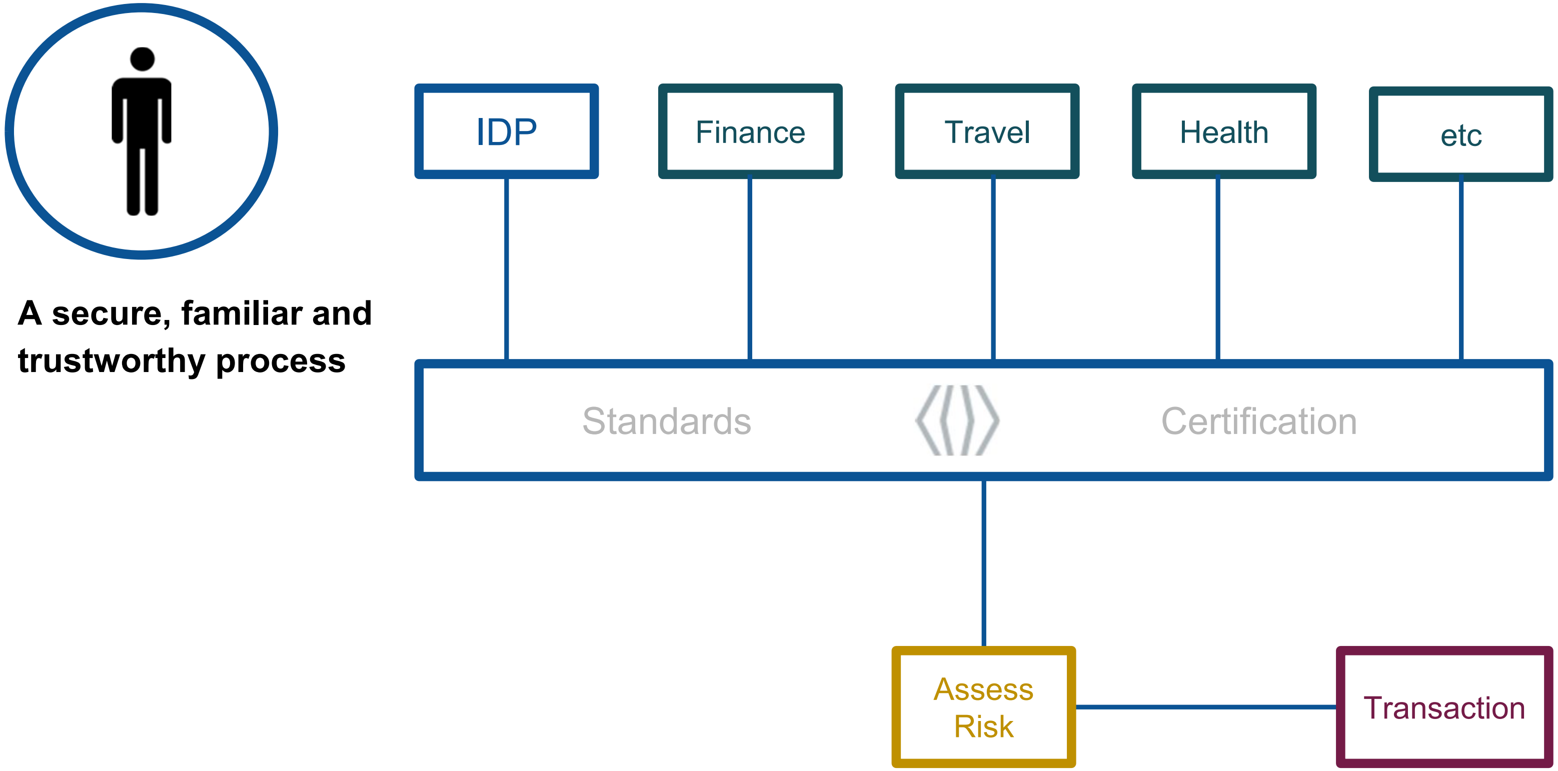
○ HSBC France

○ Orange France

□ I consent to sharing my address with ANYbank.

3. A framework of data and metadata

2. Access to identity and personal data



1. A secure, familiar and trustworthy process

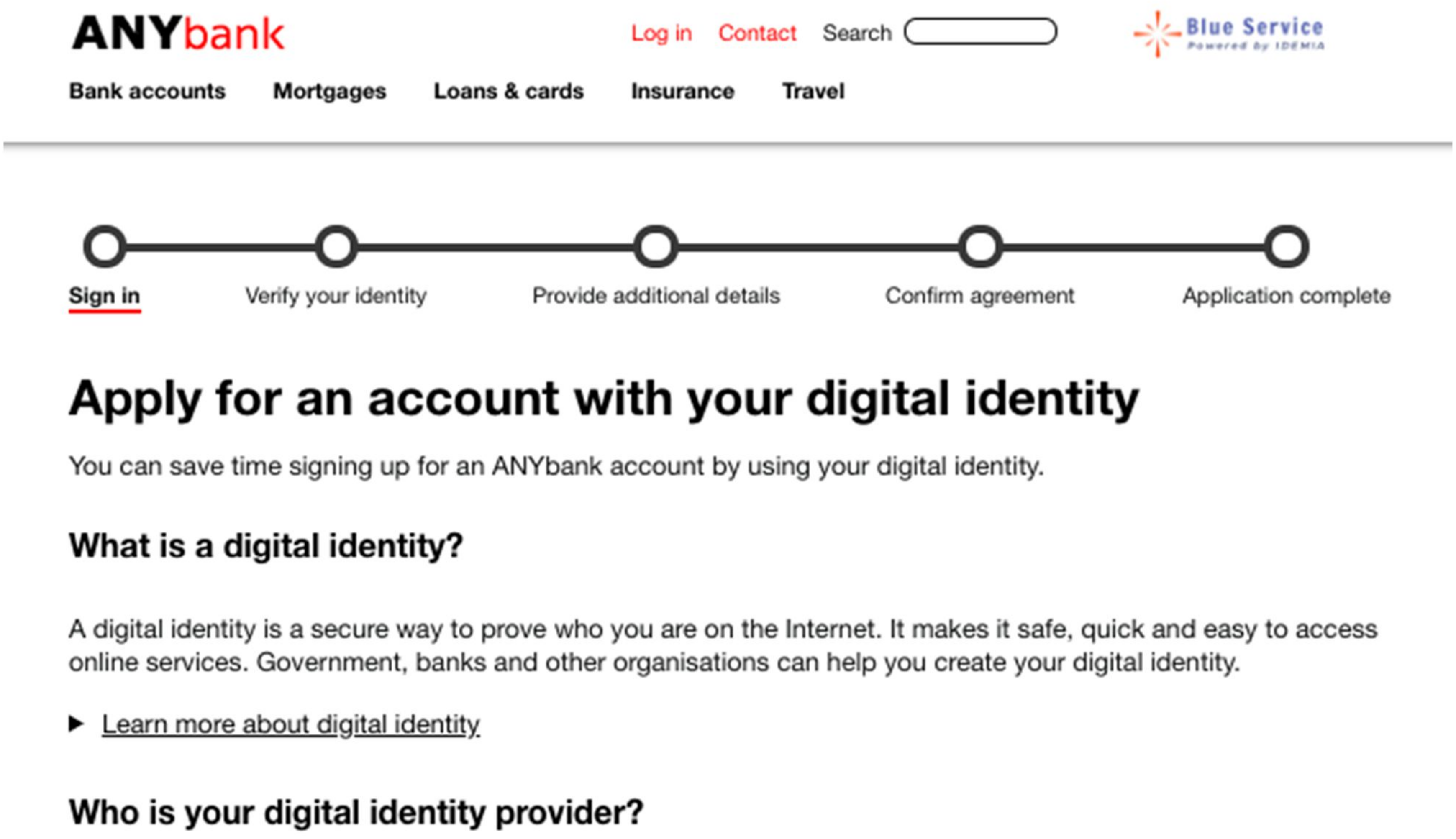
3. A framework of data and metadata

Metadata

Address:

- Type of address (main residence, second residence, temporary residence)
- Validating source & date
- LoA for identity linked to the address
- Validating source for link of identity to address
- Date of link of identity to address

Moving from ‘concept’ to ‘design’...



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.

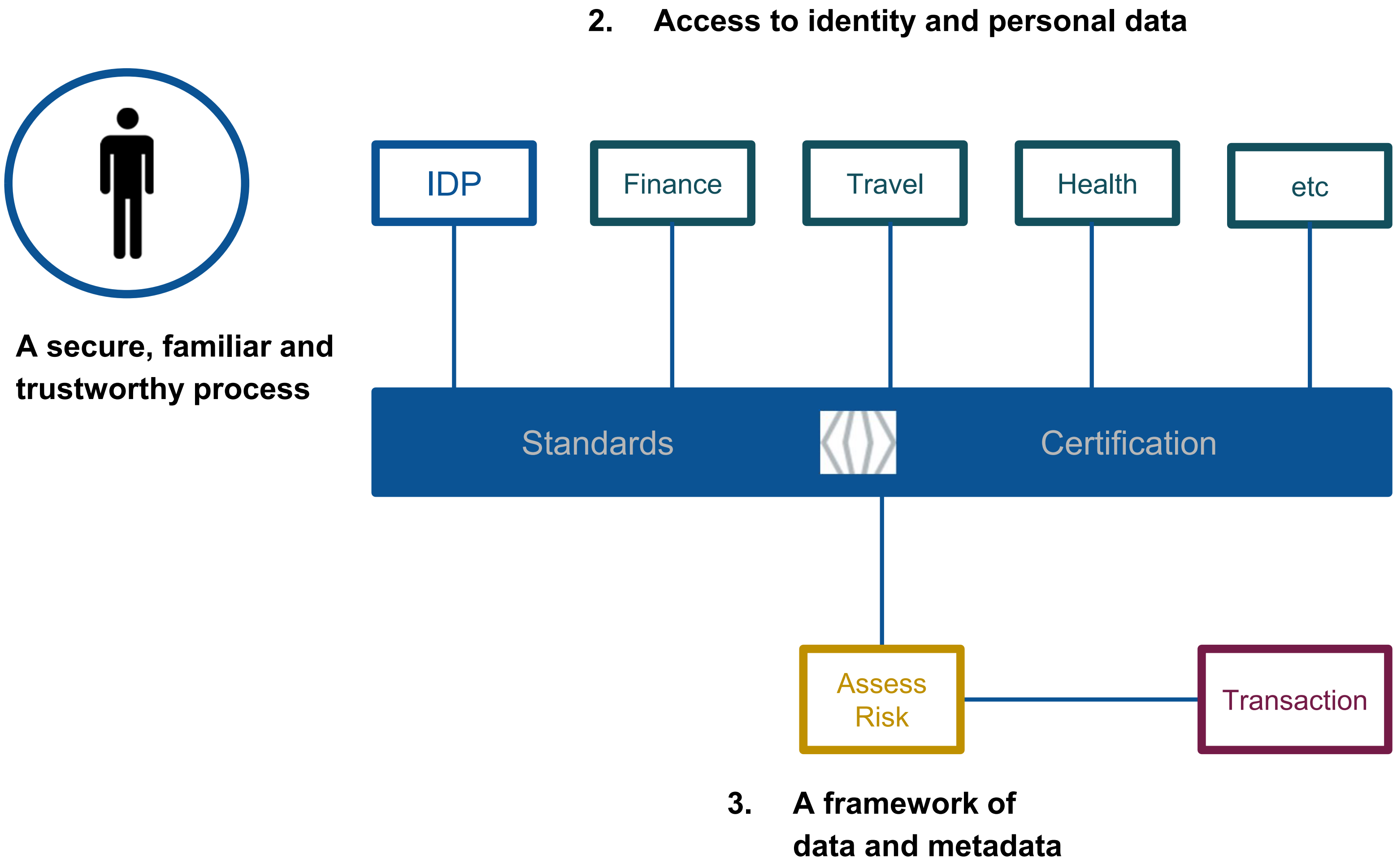
▶ Learn more about digital identity

Who is your digital identity provider?

...requires governance to be provided by banks

	GOVERNANCE	OPERATIONS
ATTRIBUTES	Attribute sharing schemes	Scheme operation
IDENTITY	Identity schemes	Scheme operation

Idemia will operate a service to bank rules


2. Access to identity and personal data
IDP
Finance
Travel
Health
etc
1. A secure, familiar and trustworthy process
Standards
Certification
Assess Risk
Transaction
3. A framework of data and metadata

Proposal - 8 week alpha project

Objectives:

1. design and test an MVP operational service
2. leverage emerging ‘trust frameworks’
3. assess feasibility of implementation

Proposal - 8 week alpha project

Starting in January 2019

Week 1 - user journey
Week 2 - Customer Due Diligence benefits and issues
Week 3 - technical integration
Week 4 - liability framework
Week 5 - commercial design
Week 6 - branding
Week 7 - governance
Week 8 - overall feasibility