ECA Standard - DRAFT 0.2

- Version control
- Introduction
  - Background
  - Key design principles
  - Use cases
  - Data model overview
  - Intellectual Property Rights (IPR)
  - Regulatory considerations (PSD2/GRPR)
- API Specification
  - The specification (OpenID for Identity Assurance)
  - Data Model
  - Attributes
    - Natural Person attributes
    - Verification attributes
    - Session attributes
    - Legal entity attributes
  - Use Case technical examples
    - Onboarding Use Case sequence diagram
    - Age Verification Use Case sequence diagram
    - Payment, Name and Address Use Case sequence diagram
- Customer Experience Guidelines (CEGs)
  - Example 1: Age verification
    - View prototype
  - Example 2: Onboarding for a service
    - View prototype
  - Example 3: Secure login via QR code
    - View prototype
  - Example 4: Persistent login
    - View prototype
  - Example 5: Account sign-up with AIS
    - View prototype
  - Example 6: eCommerce checkout with PIS
    - View prototype
- Implementation considerations/risks
- Appendix 1: ECA Intellectual Property Rights Policy

Version control

⚠ This is a draft standard published by OBIE. This standard is subject to change at any time and is optional for implementation by any firm who choses to use it.

Version	Date	Author(s)	Comments
DRAFT 0.1	15 Feb 2021	OBIE Standards Team	Initial draft for review by ECA Working Group
DRAFT 0.2	17 Feb 2021	OBIE Standards Team	Version for formal consultation
DRAFT 0.3	*TBC*	*OBIE Standards Team*	*Including updates from consultation for approval by ECA Working Group*
DRAFT 1.0	*TBC*	*OBIE Standards Team*	*Approved by ECA Working Group and ready for submission to OBIE and other standards bodies*

Introduction

Background

The aim of this work is to design an open Extended Customer Attribute (ECA) Standard to support the sharing additional customer data, which is not required under PSD2 nor the CMA Order, and which can be surfaced by ASPSPs and provided to relying parties on a commercial basis. This data can be used for a number of identity verification use cases and is of particular relevance to the UK government's work ("GOV.UK Verify") as well as the OpenID Foundation's eKYC & Identity Assurance work.

It has been agreed that a common, open ECA Standard such as that already developed by OBIE would be beneficial to support a number of use cases, providing clarity around the data elements, presentation of consent to the customer, and provision of this data to relying parties. The ECA Standard is modelled on the principles used the within the PSD2 customer journeys for TPPs, for example, gathering of consent and authentication at the ASPSP. The prototype journeys provided within this standard are designed to reflect ECA example journeys, some of which may sit outside the PSD2 framework. Certain journeys may demonstrate a combination of PSD2 and ECA data sharing in which case certain PSD2 principles will directly apply. Design of the standard needs to be inclusive and OBIE will ensure a wide range of participation in developing the ECA Standard so that it reflects views of both providing (ASPSPs) and relying parties (other entities and/or TPPs).

This ECA Standard is being developed on behalf of seven contributing members (the 6 largest UK ASPSPs plus TSB Bank). The scope will be limited to producing a standard based on extending the latest OBIE Standard (https://standards.openbanking.org.uk/) to meet the set of use cases as defined below.

This work is not covered by the activity defined by the CMA's Revised Roadmap but is an area of interest to many participants and it is hoped that extending the OBIE Standard to cover such data will allow the ecosystem to continue to innovate and flourish.

Key design principles

A number of key design principles were agreed for the development of the ECA Standard, namely:

1. Developed as an initial draft to enable any participating firms to launch MVP or pilot activity.
2. Aligned to the emerging UK Government Trust Framework model, albeit not necessarily initially constrained by this (as it still being drafted).
3. Published under the MIT Open Licence to ensure it is free from IPR claims so that it can be submitted to other standard bodies without issue.
4. Will be submitted to OBIE for inclusion (as an optional/premium API) into the OBIE Standard.
5. Out of scope of the CMA Order, thus OBIE will not mandate implementation for the CMA9 (or any other firms).
6. Must be aligned to (i.e. not conflict nor contradict) PSD2/RTS, CMA Order, GDPR or any other relevant regulation.
7. Should not re-invent the wheel, so should re-use rather than replicate other relevant standards wherever possible.

The initial ECA Standard will thus focus on a set of (relatively) simple extensions to the current OBIE Standard and Trust Framework as follows:

1. Be based on the current OBIE API interaction flows and FAPI security profile.
2. Make use of the existing OBIE Directory, so that the APIs can be accessed by existing authorised TPPs, without the need for OBIE (or any other body) to create nor validate additional roles or scopes (e.g. Digital Identity Service Providers). Albeit this should not necessarily restrict access by other firms under contract with an ASPSP.
3. Initially focus on the provision (not consumption) of additional data (beyond CMA Order/PSD2 data) by ASPSPs.
4. However, this should be extensible (e.g. in a future version) to enable:
    a. data consumption by ASPSPs and potentially both provision and consumption by other data holders; and
    b. use cases which require access to data from multiple sources (e.g. bank accounts and government services).
5. Cover both personal and business accounts, in particular considering data attributes which relate to both:
    a. the authenticating user; and
    b. the owner(s) of the account.
    c. but perhaps leaving more complex multi-user accounts out of scope for now.
6. Will generate value for people and small businesses and be designed to avoid harm.

Use cases

The initial use cases have been prioritised based on the following considerations:

1. Do-ability: should be (relatively) easy for ASPSPs to build.
2. Market readiness: should meet one or more high priority, high value and/or high volume market needs.
3. Commercial value: should thus provide ASPSPs a strong commercial benefit (either directly or indirectly) which aligns to their commercial strategy/objectives.
4. Value for end users: use cases which help drive better outcomes and/or generate value for end (personal and business) users and/or bring broader societal benefits.

The following high level use cases have been identified as in scope for the initial ECA Standard:

ID	Use Case	Notes
1	Onboarding	Provision of one or more data attributes which can be shared with a relying party (e.g. a utility company) to facilitate account opening with that party.
2	Ongoing validation or data sharing	Provision of long lived consent to the relying party for either basic attribute validation and/or data sharing.
3	E-commerce	Provision of validation and/or data attributes specifically in the context of ecommerce, to include ‘PISP plus' and Gift Aid examples.
4	Authentication as a service	e.g. Register/Login with BankID
5	Attribute verification	No data provided back, rather a binary Y/N verification by ASPSP of data provided by relying party (e.g. Is the user over 18? Is this the correct postcode?).

Data model overview

To facilitate these use cases, the following data should be covered by the ECA Standard. This is further developed in the Attributes section below

Personal and Business	Personal	Business
• Full legal name (if not already provided as a PSD2 requirement) • Date first account opened • Has active account(s) - Y/N • Phone number(s) • Email address(es)	• Date of birth • Age (and/or over 18 flag) • Previous/maiden name • Current address (inc date moved) • Previous address(es) • Gender • NI Number • Passport number • Driving licence number	• Trading address(es) • Registered address • Company House Reg Number • VAT Reg Number

For each of these data objects, we will also consider:

1. The date/time the field was last updated.
2. The level of assurance at the time of update (e.g. the method by which it was checked), however, this should be aligned to emerging standards in this regard (e.g. GPG 45).
3. Whether the data relates to:
    a. the authenticating user; or
    b. the owner(s) of the account.
4. Not all providers will have all of these fields.
5. The above list of fields is not exhaustive and may change as the project progresses.

Intellectual Property Rights (IPR)

As per key design principle #3, any work produced as a result of this activity will be published under an open licence and may be shared with and submitted to other standards bodies. Therefore any contributions to this work must be made with the understanding that there are no IPR associated with any such contributions and the contributor warrants that their contributions are free from any IPR claims.

All contributions are made in accordance with the IPR Policy set out below in Appendix 1.

Regulatory considerations (PSD2/GRPR)

The ECA standard and ECA customer journeys have been developed to replicate the design principles of the OBIE Standard. OBIE has used a design approach which leverages on the current PSD2 principles and overlays them to support the ECA use cases. It is important to note that while the principles of consent and authentication will feature in each of the use cases, they may not necessarily be underpinned by a relevant regulatory requirement under PSD2 as they may not be linked to a payment activity within the regulation. It is the sole responsibility of participants to consider applicable regulatory obligations and ensure that they have been appropriate met for any of the use cases they are engaging in. This is especially important in use cases which combine payment services under PSD2 and data sharing under ECA. Participants must also ensure that they meet any applicable regulatory obligations under GDPR in relation to processing personal data.

API Specification

The ECA Standard will use the specification that is under active development by the OpenID foundation eKYC & IDA Working Group, namely, the “OpenID for Identity Assurance” specification. There is an associated specification that will add support for legal entity use cases called “OpenID for authority”.

Advantages of this specification include:

- Developed under the OpenID Foundation
- Builds directly on OpenID and FAPI so is sufficiently secure for data sharing.
- A fairly simple technical extension to OpenID and FAPI
- Privacy preserving through requests for specific claims in any combination
- Provides access to attributes directly from the OpenID provider via OpenID ID Token or UserInfo endpoint
- OpenID with eKYC & IDA Supports most use cases
- Age verification is in roadmap for Q1 2021 as part of eKYC & IDA Implementers Draft 3
- Will support use cases for both personal and business use cases
- eKYC & IDA base spec is already in production for similar use cases elsewhere in the world
- Can support use cases that require data from multiple sources
- Verified claims are presented in a JWT so a plethora of libraries are available

The OpenID for Identity Assurance specification already supports a majority of the use cases defined in the ECA scope and will support the remaining in scope use cases in the future. The specification has also been developed in a way that means it is highly flexible with regard to use cases and can be readily extended with new attributes. It also allows requesting parties to be very specific about which attributes are required thus addressing data leakage and privacy concerns at a protocol level.

The specification (OpenID for Identity Assurance)

The work of the eKYC & IDA Working group is still underway and currently has an approved Implementers Draft 2 specification.

Implementers Draft 2 supports the following use cases that the ECA Standard is intended to support:

1. Onboarding
2. Ongoing validation or data sharing
3. Ecommerce
4. Authentication as a service

The roadmap for the eKYC & IDA specification includes an Implementers Draft 3 which is scheduled for Q1 2021 and currently includes the addition of age verification features and could also include registration of additional attributes required for the ECA Standard. Roadmap items for the eKYC & IDA spec that are of interest to the ECA Standard are:

- Attribute verification
- Support for legal entity use cases
- Conformance testing facilities

Data Model

In the context of the OpenID for Identity Assurance specification attributes can be used in a flexible fashion but there are a set of attributes in the specification that are going to be registered into the IANA JSON Web Token Registry to ensure consistent use internationally. It is appropriate for globally relevant attributes identified as part of the ECA Standard to be added to that set.

There is discussion on-going within and between various bodies about how interoperability can be achieved with respect to more localised attribute requirements. The OIDF, IANA, OIX and other stakeholders are considering this matter. One suggestion is registration of a UK specific profile that contains attributes that are only relevant in a UK context (such as national insurance number).

The data model for ECA is being developed with four attribute types:

1. Natural person attributes
2. Verification attributes
3. Session attributes
4. Legal entity attributes

Attributes

Natural Person attributes

Description	attribute name	Registration context	Comments
Full Name	name	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
	given_name	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
	middle_name	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
	family_name	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
phone_number	phone_number	Registered IANA via OpenID Connect Core 1.0, Section 5.1	not strongly formatted
	msisdn	Proposed by OpenID for Identity Assurance in scope of Implementers Draft 3	Defined to use ITU-T E.164 format
Phone number(s)	phone_numbers		Re-use phone number and msisdn singular claims Establish a structured object that is an array including: • preferred flag • format (e.g. msisdn or phone_number) • capbilities (e.g. audio, fax, sms, etc) • tag (e.g. personal, work, mobile)
e-mail address	email	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
e-mail addresses	emails		Re-use email Establish a structured object that is an array including: • preferred flag • tag (e.g. personal, work, mobile)
Date of birth	birthdate	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
age	age		
age verification	age_is_at_least	Proposed by OpenID for Identity Assurance in scope of Implementers Draft 3	
age verification	age_is_at_most	Proposed by OpenID for Identity Assurance in scope of Implementers Draft 3	
Previous/maiden name	birth_family_name	Proposed by OpenID for Identity Assurance in Implementers Draft 2	is family name what is intended or should this be a structured object with given, middle and family?
Previous names	previous_names		is this needed? should it be a structured object with given names and middle names and family names? what about date periods?
Current Address	address	Registered IANA via OpenID Connect Core 1.0, Section 5.1.1	start date not supported in current definition

Previous address(es)	previous_addresses		suggest an array of address objects with additional date to and from for each
End-User’s place of birth	place_of_birth	Proposed by OpenID for Identity Assurance in Implementers Draft 2	The value of this member is a JSON structure
End-User’s nationalities	nationalities	Proposed by OpenID for Identity Assurance in Implementers Draft 2	in ICAO 2-letter codes [@!ICAO-Doc9303], e.g. "US" or "DE". 3-letter codes MAY be used when there is no corresponding ISO 2-letter code, such as "EUE".
Residence Status	residence_status		From gov.uk alpha on digital identity structured object with array of status and nations
End-User’s salutation, e.g. “Mr.”	salutation	Proposed by OpenID for Identity Assurance in Implementers Draft 2	
End-User’s title, e.g. “Dr.”	title	Proposed by OpenID for Identity Assurance in Implementers Draft 2	
Stage name, religious name or any other type of alias/pseudonym	also_known_as	Proposed by OpenID for Identity Assurance in Implementers Draft 2	
Gender of end user	gender	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
Qualifications	qualifications		From gov.uk alpha on digital identity structured object with array of qualification and level of attainment
Employment history	employment_history		From gov.uk alpha on digital identity structured object with array of job titles and employer
Income	income		From gov.uk alpha on digital identity
Citizen registration number			From gov.uk alpha on digital identity
Biometric information			From gov.uk alpha on digital identity
Details of authority that the end user has over another entity	authority	Proposed by OpenID for Authority draft	Structured object containing data about the authority the end user has over another entity (such as a legal entity) Includes sub-elements: • applies_to - the entity over which authority is held • permission - details of what may be done on behalf of the entity the authority applies to • granted_by - process and or entity that granted the authority

Verification attributes

Description	attribute name	Registration context	Comments
Date first account opened	first_account_open		
Has active account(s) - Y/N	has_active_account		
Time the End-User's information was last updated	updated_at	Registered IANA via OpenID Connect Core 1.0, Section 5.1	
There has been account activity seen in this 3 month period consisting of inbound our outbound payments or customer login	account_activity_3months		derived from GPG 45 discuss are these verification claims in reality

There has been account activity seen in the 3 to 6 month period consisting of inbound our outbound payments or customer login	account_activity_6months		derived from GPG 45 discuss are these verification claims in reality
There has been account activity seen in this 6 to 12 month period consisting of inbound our outbound payments or customer login	account_activity_12months		derived from GPG 45 discuss are these verification claims in reality
Evidence used in verification process	evidence	Proposed by OpenID for Identity Assurance in Implementers Draft 2	Structured object containing data about the evidence used when verifying the end-user's identity e.g. details of passport, details of driving license, details of utility bill, details of any vouch
	uk.nino		is it a verification evidence attribure or a natural person attribute? perhaps a typed structured object might be more appropriate? - like “document”?

Session attributes

Description	attribute name	Registration context	Comments
Authentication Context Class Reference	acr	Registered IANA via OpenID Connect Core 1.0, Section 2	Trust framework possibly appropriate to define valid values for this claim
Authentication Methods References	amr	Registered IANA via OpenID Connect Core 1.0, Section 2	Trust framework possibly appropriate to define valid values for this claim

Legal entity attributes

Description	attribute name	Registration context	Comments
Company name	organization_name	Proposed by OpenID for Authority draft	
	organization_type	Proposed by OpenID for Authority draft	discuss
	trading_as	Proposed by OpenID for Authority draft	
Registered address	registered_address	Proposed by OpenID for Authority draft	
Trading address(es)	trading_addresses		array of address objects
Company Registration Number	registration_number		Structured object that contains issuing body, country and registration number
VAT Reg Number	tax_details		structured object with types?
Legal Entity Identifier	lei	Proposed by OpenID for Authority draft	
Name of regulatory Jurisdiction under which the legal entity is registered	registered_jurisdiction	Proposed by OpenID for Authority draft	
Legal status of legal entity	organization_status	Proposed by OpenID for Authority draft	
Date of incorporation of the legal entity	incorporation_date	Proposed by OpenID for Authority draft	
Date last accounts were submitted	last_accounts_date	Proposed by OpenID for Authority draft	
Turnover	last_annual_turnover		From gov.uk alpha on digital identity

Standard Industrial Classification (SIC) code	uk.sic_code		From gov.uk alpha on digital identity
Economic Operators Registration and Identification (EORI) number	eu.eori_code		From gov.uk alpha on digital identity
Excise Authorisation Verification (SEED) number	eu.seed_number		From gov.uk alpha on digital identity
Data Universal Numbering System (DUNS) number	uk.duns_number		From gov.uk alpha on digital identity
data protection registration number	dprn		From gov.uk alpha on digital identity Structured object that contains issuing body, country and appropriate data protection registration number

Use Case technical examples

Relying Party is any entity that is permitted to interact with a provider so could be an intermediary or end consumer of data attributes.

OpenID Provider is the entity that has data about the end user and will

It is anticipated there will be a contractual arrangement between the relying party and the OpenID provider

The end User has an established relationship with the OpenID Provider but not necessarily with the Relying Party

Onboarding Use Case sequence diagram

Onboarding use case requires delivery of specific verified claims and specific verification metadata including some details of evidence used for verification of the end user and requests those claims to be delivered via the ID Token.

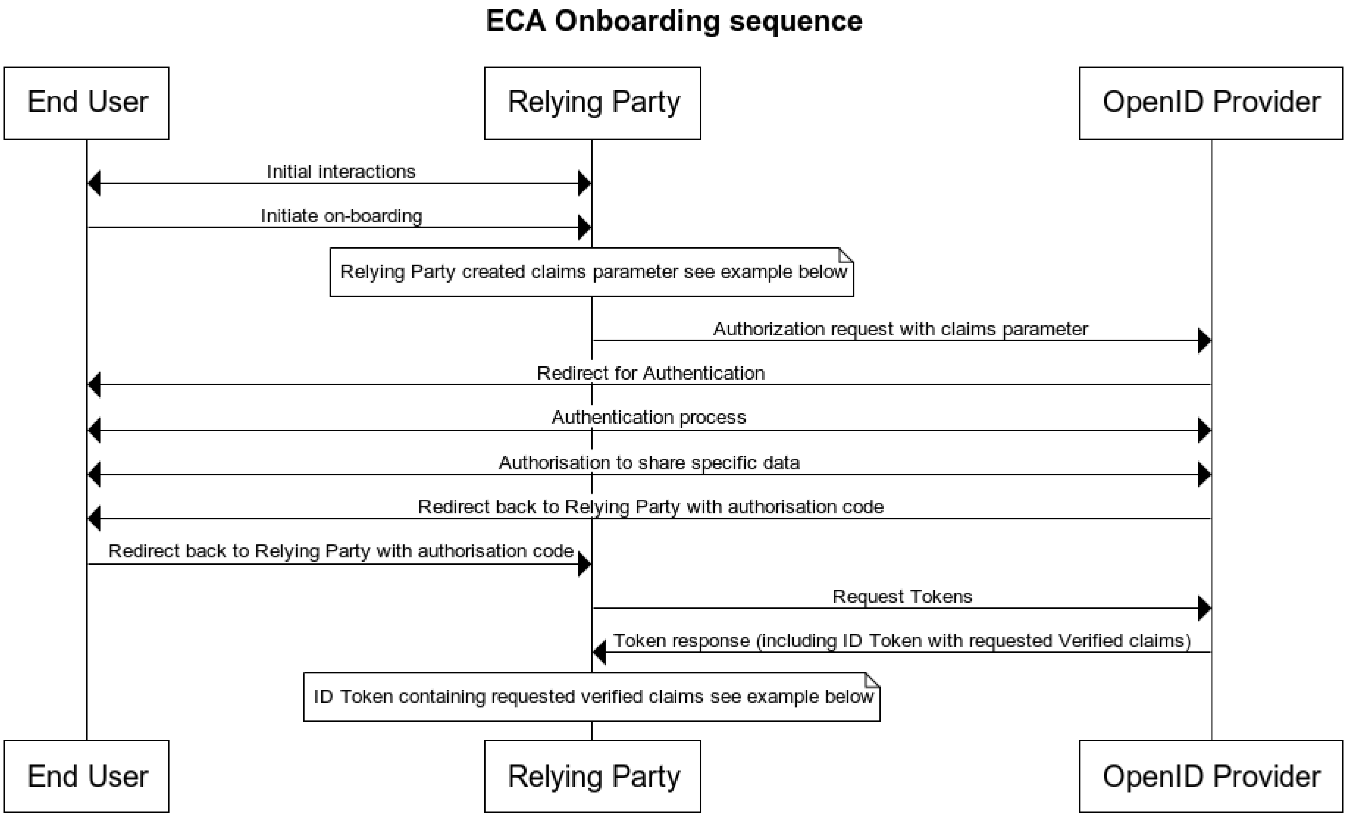

ECA Onboarding sequence
End User
Relying Party
OpenID Provider
Initial interactions
Initiate on-boarding
Relying Party created claims parameter see example below
Authorization request with claims parameter
Redirect for Authentication
Authentication process
Authorisation to share specific data
Redirect back to Relying Party with authorisation code
Redirect back to Relying Party with authorisation code
Request Tokens
Token response (including ID Token with requested Verified claims)
ID Token containing requested verified claims see example below
End User
Relying Party
OpenID Provider

Diagram source

title ECA Onboarding sequence

participant End User
participant Relying Party
participant OpenID Provider

```
End User <-> Relying Party: Initial interactions
End User -> Relying Party: Initiate on-boarding
note over Relying Party
Relying Party created claims parameter see example below
end note
Relying Party -> OpenID Provider: Authorization request with claims parameter
OpenID Provider -> End User: Redirect for Authentication
End User <-> OpenID Provider: Authentication process
End User <-> OpenID Provider: Authorisation to share specific data
OpenID Provider -> End User: Redirect back to Relying Party with authorisation code
End User -> Relying Party: Redirect back to Relying Party with authorisation code
Relying Party -> OpenID Provider: Request Tokens
OpenID Provider -> Relying Party: Token response (including ID Token with requested Verified claims)
note over Relying Party
ID Token containing requested verified claims see example below
end note
```

Onboarding use case Claims request

```
{
 "id_token": {
  "verified_claims": {
   "verification": {
    "trust_framework": null,
    "time": null,
    "verification_process": null,
    "evidence": [
     {
      "type": null,
      "method": null,
      "document": {
       "type": null,
       "issuer": {
        "country": null,
        "name": null
       }
      }
     }
    ]
   },
   "claims": {
    "given_name": null,
    "family_name": null,
    "address": null
   }
  }
 }
}
```

Onboarding use case ID Token

```
{
 "iss": "https://server.example.com",
    "sub": "24400320",
    "aud": "RP-client-id-s6BhdRkqt3",
    "nonce": "n-0S6_WzA2Mj",
    "exp": 1311281970,
    "iat": 1311280970,
    "auth_time": 1311280969,
    "acr": "urn:mace:incommon:iap:silver",
     "verified_claims":{
      "verification":{
        "trust_framework":"UK_ECA_Example",
        "time":"2021-01-02T18:25Z",
        "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
        "evidence":[
         {
           "type":"id_document",
           "method":"pipp",
           "document":{
            "type":"utility_bill",
            "provider": {
              "name": "First Combined Utilities",
              "country": "GBR",
              "address":{
                "locality":"St Albans",
                "postal_code":"AR1 3ZZ",
                "country":"GBR",
                "street_address":"98 Electric Road"
               }
             },
           }
         },
         {
           "type":"id_document",
           "method":"pipp",
           "document":{
            "type":"driving_permit",
            "issuer":{
              "name":"Driver Vehicle Licencing Authority",
              "country":"GBR"
            }
           }
         }
        ]
      },
      "claims":{
        "given_name":"Jon",
        "family_name":"Smyth",
        "address":{
         "locality":"Norwich",
         "postal_code":"NR1 3QP",
         "country":"GBR",
         "street_address":"31-33 St. Stephens Street"
        }
      }
     }
   }
```

Age Verification Use Case sequence diagram

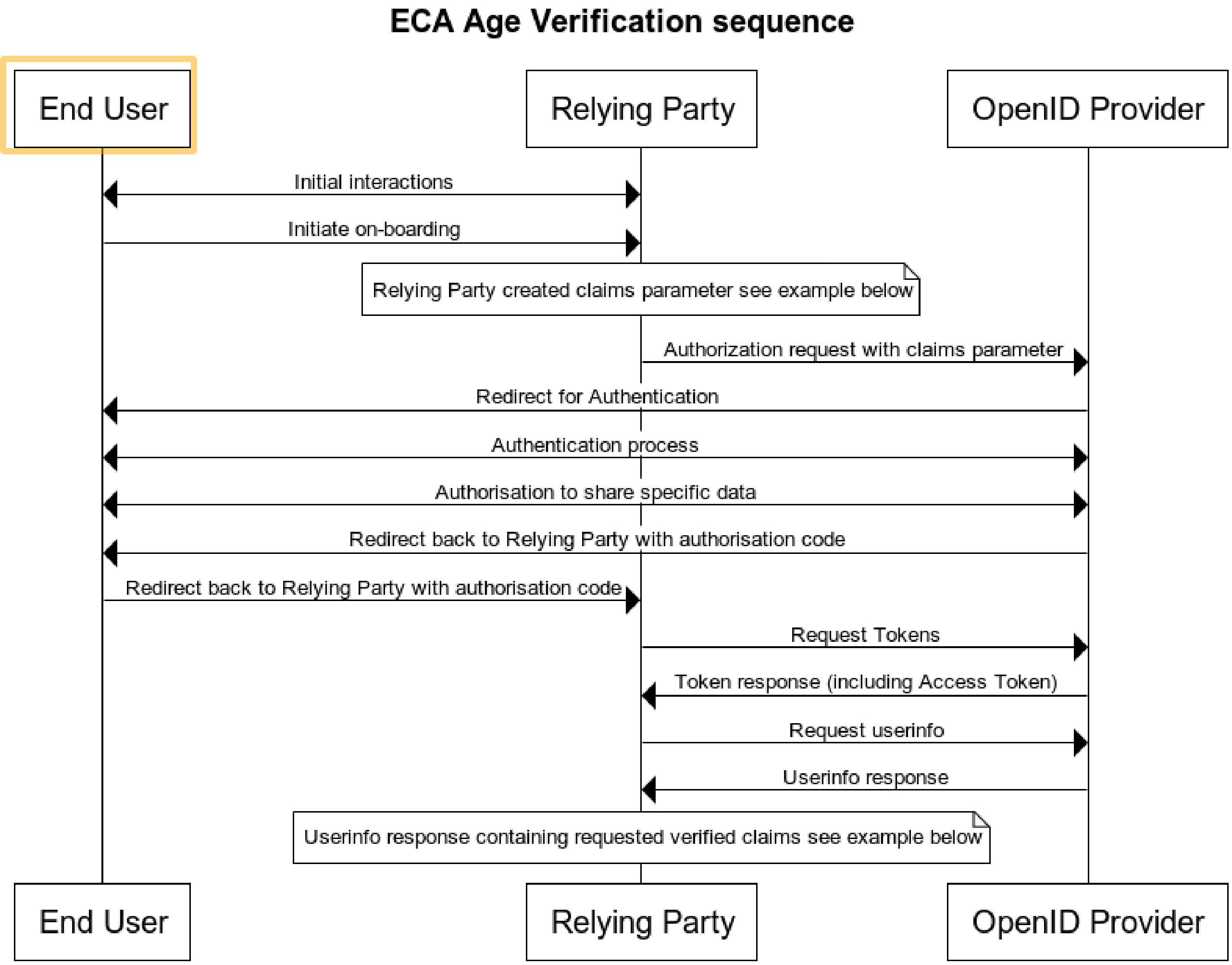

ECA Age Verification sequence
End User
Relying Party
OpenID Provider
Initial interactions
Initiate on-boarding
Relying Party created claims parameter see example below
Authorization request with claims parameter
Redirect for Authentication
Authentication process
Authorisation to share specific data
Redirect back to Relying Party with authorisation code
Redirect back to Relying Party with authorisation code
Request Tokens
Token response (including Access Token)
Request userinfo
Userinfo response
Userinfo response containing requested verified claims see example below
End User
Relying Party
OpenID Provider

Diagram source

```
title ECA Age Verification sequence

participant End User
participant Relying Party
participant OpenID Provider

End User <-> Relying Party: Initial interactions
End User -> Relying Party: Initiate on-boarding
note over Relying Party
Relying Party created claims parameter see example below
end note
Relying Party -> OpenID Provider: Authorization request with claims parameter
OpenID Provider -> End User: Redirect for Authentication
End User <-> OpenID Provider: Authentication process
End User <-> OpenID Provider: Authorisation to share specific data
```

```
OpenID Provider -> End User: Redirect back to Relying Party with authorisation code
End User -> Relying Party: Redirect back to Relying Party with authorisation code
Relying Party -> OpenID Provider: Request Tokens
OpenID Provider -> Relying Party: Token response (including Access Token)
Relying Party -> OpenID Provider: Request userinfo using access token
OpenID Provider->Relying Party: Userinfo response
note over Relying Party
Userinfo response containing requested verified claims see example below
end note
```

Age Verification use case Claims request

```
{

"userinfo": {

"verified_claims": {

"verification": {

"trust_framework": null

},

"claims": {

"age_is_at_least": {
"age": {
"value": 21
},
"on_date": {
"value": "2021-02-05"
}
}
}

}
}
```

Age Verification use case UserInfo response

```
{
"verified_claims": {
"verification": {
"trust_framework": "ezid_example_framework"
},
"claims": {
"age_is_at_least": {
"age": 21,
"on_date": "2021-02-05",
"result": true
}

}

}

}
```

Payment, Name and Address Use Case sequence diagram

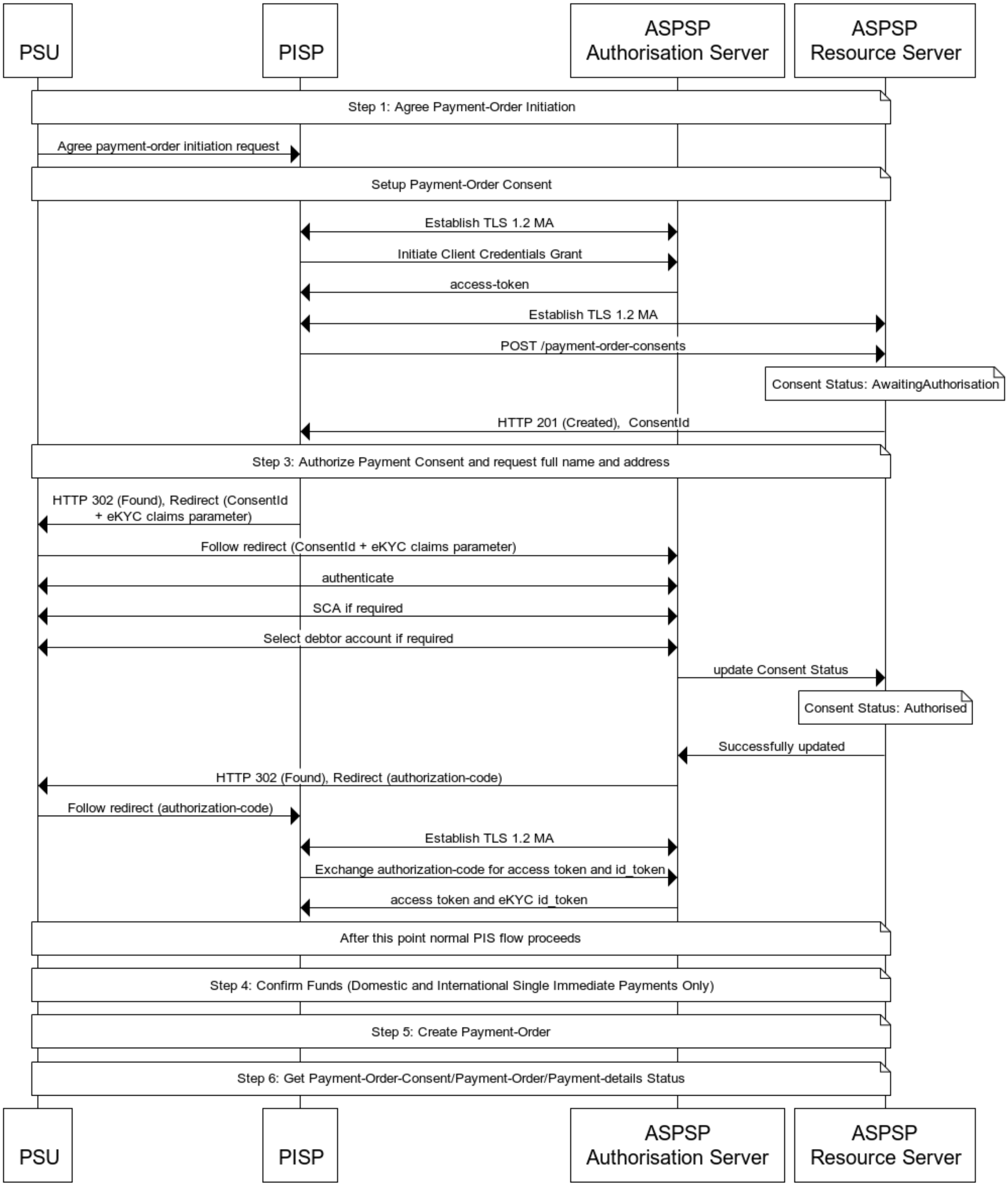

PSU
PISP
ASPSP Authorisation Server
ASPSP Resource Server
Step 1: Agree Payment-Order Initiation
Agree payment-order initiation request
Setup Payment-Order Consent
Establish TLS 1.2 MA
Initiate Client Credentials Grant
access-token
Establish TLS 1.2 MA
POST /payment-order-consents
Consent Status: AwaitingAuthorisation
HTTP 201 (Created), ConsentId
Step 3: Authorize Payment Consent and request full name and address
HTTP 302 (Found), Redirect (ConsentId + eKYC claims parameter)
Follow redirect (ConsentId + eKYC claims parameter)
authenticate
SCA if required
Select debtor account if required
update Consent Status
Consent Status: Authorised
Successfully updated
HTTP 302 (Found), Redirect (authorization-code)
Follow redirect (authorization-code)
Establish TLS 1.2 MA
Exchange authorization-code for access token and id_token
access token and eKYC id_token
After this point normal PIS flow proceeds
Step 4: Confirm Funds (Domestic and International Single Immediate Payments Only)
Step 5: Create Payment-Order
Step 6: Get Payment-Order-Consent/Payment-Order/Payment-details Status
PSU
PISP
ASPSP Authorisation Server
ASPSP Resource Server

Diagram source

```
title

participant PSU
participant PISP
participant ASPSP \nAuthorisation Server AS ASPSPAS
participant ASPSP \nResource Server AS ASPSPRS
```

```
note over PSU, ASPSPRS
Step 1: Agree Payment-Order Initiation
end note
PSU -> PISP: Agree payment-order initiation request

note over PSU, ASPSPRS
Setup Payment-Order Consent
end note
PISP <-> ASPSPAS: Establish TLS 1.2 MA
PISP -> ASPSPAS: Initiate Client Credentials Grant
ASPSPAS -> PISP: access-token
PISP <-> ASPSPRS: Establish TLS 1.2 MA
PISP -> ASPSPRS: POST /payment-order-consents
note over ASPSPRS: Consent Status: AwaitingAuthorisation
ASPSPRS -> PISP: HTTP 201 (Created), ConsentId

note over PSU, ASPSPRS
Step 3: Authorize Payment Consent and request full name and address
end note

PISP -> PSU: HTTP 302 (Found), Redirect (ConsentId\n + eKYC claims parameter)
PSU -> ASPSPAS: Follow redirect (ConsentId + eKYC claims parameter)
PSU <-> ASPSPAS: authenticate
PSU <-> ASPSPAS: SCA if required
PSU <-> ASPSPAS: Select debtor account if required
ASPSPAS ->ASPSPRS: update Consent Status
note over ASPSPRS: Consent Status: Authorised
ASPSPRS -> ASPSPAS: Successfully updated
ASPSPAS -> PSU: HTTP 302 (Found), Redirect (authorization-code)
PSU -> PISP: Follow redirect (authorization-code)
PISP <-> ASPSPAS: Establish TLS 1.2 MA
PISP -> ASPSPAS: Exchange authorization-code for access token and id_token
ASPSPAS -> PISP: access token and eKYC id_token

note over PSU, ASPSPRS
After this point normal PIS flow proceeds
end note
note over PSU, ASPSPRS
Step 4: Confirm Funds (Domestic and International Single Immediate Payments Only)
end note
note over PSU, ASPSPRS
Step 5: Create Payment-Order
end note
note over PSU, ASPSPRS
Step 6: Get Payment-Order-Consent/Payment-Order/Payment-details Status
end note
```

Name and Address ECA use case Claims request

```
{
 "id_token": {
  "verified_claims": {
   "verification": {
    "trust_framework": null,
    "time": null
    }
   },
   "claims": {
    "name": null,
    "address": null
   }
  }
 }
}
```

Name and Address ECA use case ID Token response

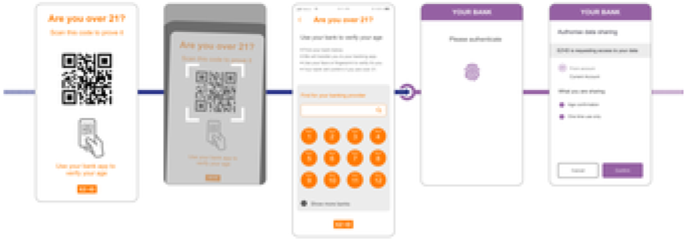
```
{
 "iss": "https://server.example.com",
 "sub": "13300320",
 "aud": "RP-client-id-j4BhdRkqh9",
 "nonce": "n-1P6_rqA2Mm",
 "exp": 1311281970,
 "iat": 1311280970,
 "auth_time": 1311280969,
 "acr": "urn:mace:incommon:iap:silver",
  "verified_claims":{
   "verification":{
     "trust_framework":"UK_ECA_Example",
     "time":"2021-01-02T18:25Z"
   },
   "claims":{
     "name":"John Doe",
     "address":{
      "locality":"Norwich",
      "postal_code":"NR1 3QP",
      "country":"GBR",
      "street_address":"31-33 St. Stephens Street"
     }
   }
  }
}
```

Customer Experience Guidelines (CEGs)

The following wireframes and prototypes, unlike other examples in the OBIE CEGs, are not not intended to be prescriptive but rather to:

1. Act as a catalyst to help implementers (ASPSPs and Relying Parties) identify actual use cases
2. Help ensure the specification contains standardised data elements/claims which supports these use cases
3. Provide guidance for implementers in delivering consistent messaging and the right level of friction (e.g. not introducing unnecessary steps in the authentication flow)

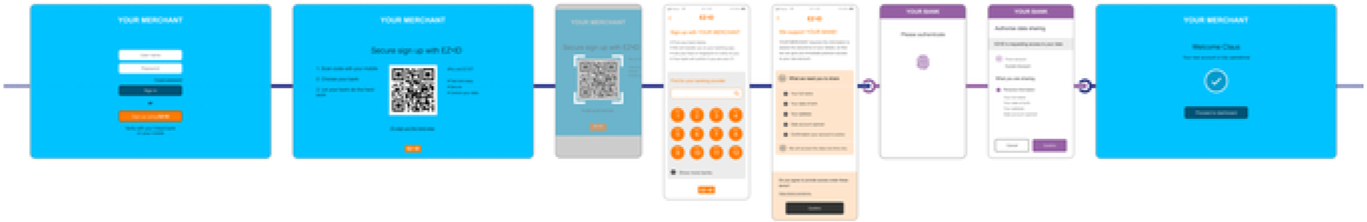
Example 1: Age verification



In our first demo of innovative use cases for bank verified ID, the customer shares the minimum information which is necessary to verify their age via their ASPSP. A venue or merchant that requires age verification presents a QR code. The user scans the code to link to their mobile banking app, via search / menu of available providers. In this scenario the venue does not need the actual age or data of birth, the need only a binary response from the ASPSP that the customer is indeed over 21, for example.

View prototype

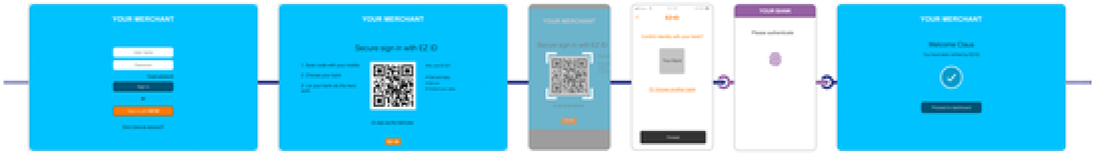
Example 2: Onboarding for a service



Onboarding journeys present the primary friction for users of online services and mobile apps. With the need for good anti-fraud measures onboarding can even become asynchronous while a human verifies uploaded documentation. Here the bank provides information to optimise sign-up, and good assurance of identity via their own login protocols, eg. biometric.

View prototype

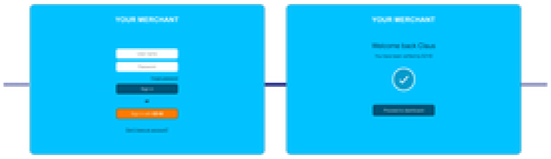
Example 3: Secure login via QR code



In a non-cookied state, the ID provider uses registered bank account to offer a secure login journey. Embedded QR code instructions trigger an app-to-app redirect to the PSU's mobile banking app.

View prototype

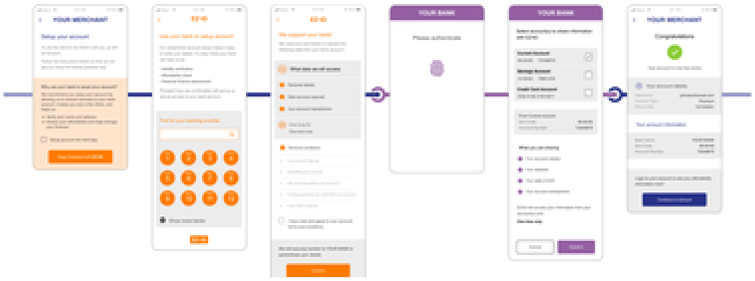
Example 4: Persistent login



Similar to Google suite, our third party ID provider is maintaining a persistent logged-in state, so access is frictionless.

View prototype

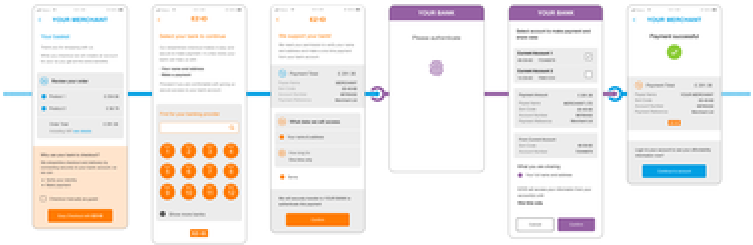
Example 5: Account sign-up with AIS



In this example, the merchant streamlines account onboarding and identity verification via a third party facility, including an AIS service for checking affordability. This reduces the need for manual user input and asynchronous verifications, including email and identification documents.

View prototype

Example 6: eCommerce checkout with PIS



Here the third party assurance provider streamlines a standard checkout, to reduce user friction and fraud, using a PISP to make the payment.

View prototype

Implementation considerations/risks

This ECA Standard does not include any Operational Guidelines, such as those included with the OBIE Standard.

In developing this ECA Standard, the authors have identified a number of risks which implementers should take into account, together with mitigating actions which can or should be considered.

These are documented here: Risk log

The ECA standard does not constitute legal advice. While certain aspects have been designed to relevant regulatory provisions and best practice, they are not a complete list of the regulatory or legal obligations that apply to ASPPSs and/or relying parties. Although intended to be consistent with regulations and laws, in the event of any conflict with such regulations and laws, those regulations and laws will take priority. ASPSPs and relying parties solely responsible for their own compliance with all regulations and laws that apply to them, including without limitation, PSRs, PSD2, GDPR and consumer protection laws. ASPSPs and Relying Parties that choose to implement the ECA Standard will need to assess for themselves their own risks and regulatory obligations prior to doing so.

Appendix 1: ECA Intellectual Property Rights Policy

This Extended Customer Attributes (“**ECA**”) Intellectual Property Rights Policy (“**IPR Policy**”) defines the intellectual property rights and obligations of Contributors (as defined below) in relation to Contributions (as defined below) proposed to Open Banking Limited (“**OBL**”) for the creation of Specifications.

1. <u>**Definitions**</u>
   a. “**Contributions**” mean any of the following, to the extent provided by a Contributor in connection with a Specification: (a) communications to or through a particular mailing list; (b) other communications provided at a face-to-face or video call working group meeting (without subsequent and timely objection by the putative Contributor); or (c) any other communications offered in any online collaboration tools selected by the applicable working group (e.g., Atlassian and other web-based collaboration platforms).
   b. “**Contributor**” means, with regard to a particular working group, any person (individual, entity, or otherwise) who has joined such working group by requesting access or otherwise provided Contributions to OBL in connection with a Specification.
   c. **“Specification**” means the draft and final versions and contents of API specifications including associated documentation and guidelines that have been deemed as such by the relevant working group.
   d. **“Implementation”** means a product (e.g., but without limitation, hardware, software, or firmware) or service that consists of (or makes use of) a Specification or any Contributions.
   e. **“Implementer”** means a person or other entity that creates, distributes, or offers a product or service that contains or makes use of a Specification.
   f. **“IntellectualPropertyRights”**means patents, rights to inventions, copyright and related rights, moral rights, trade marks, business names and domain names, rights in get-up, goodwill and the right to sue for passing off, rights in designs, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how) and all otherintellectualpropertyrights, in each case whether registered or unregistered and including all applications and rights to apply

for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

2. **General**
   a. By making any Contribution to a Specification, Contributors agree to be bound by this IPR Policy. A Contributor may withdraw from a working group at any time and agrees to be bound by the terms of this IPR Policy in relation to any Contributions made prior to withdrawal.

   b. No Contributor will incorporate any third party materials into any Contribution, unless it has all the rights and licenses necessary from such third party to submit such Contribution in accordance with the terms and conditions of this IPR Policy.

3. **Confidentiality**
   a. All Contributions, and other materials shared with OBL in connection with Specifications will be considered non-confidential information, regardless of any markings to the contrary included thereon or related thereto.

4. **Intellectual Property Rights**
   a. To the extent that a Contribution is or may be subject to Intellectual Property Rights, the Contributor hereby grants a perpetual, irrevocable (except in case of breach of this license), non-exclusive, royalty-free, worldwide license in such Intellectual Property Rights to OBL, to other Contributors, and to Implementers, to reproduce, prepare derivative works from, distribute, perform, and display the Contribution and derivative works thereof for the of development and Implementation of Specifications.

   b. Contributor represents that Contributions comprised of written submissions submitted by such a Contributor to OBL comply with any attribution requirements relating to third party content.

   c. Subject to each Contributor's rights in individual Contributions, the Intellectual Property Rights in any Specifications will be the property of OBL and published open source under the Open Licence defined at https://www.openbanking.org.uk/open-licence/. Each Contributor will execute and deliver such instruments and take such other actions as and when OBL may reasonably request to perfect or protect its Intellectual Property Rights in the Specifications to enable it to publish them open source.

   d. Each Contributor hereby irrevocably promises not to assert any claim against any other entity (whether OBL, a Contributor, an Implementer or otherwise) for making, using, selling, offering for sale, importing, or distributing any Implementation or offering any product or service to the extent it contains or uses a Specification and/or any Contributions.