OIX OPEN IDENTITY EXCHANGE

Data Standards for Digital ID Interoperability

August 2023 | Version 1.1

Produced by: Nick Mothershaw, OIX Chief Identity Strategist

Table of Contents

1 EXECUTIVE SUMMARY 3
2 THE NEED FOR DATA STANDARDS 4
3 CONTENT DATA VS PROTOCOLS 5
4 STANDARDS AND GOVERNANCE FOR CONTENT DATA 5
5 TYPES OF CONTENT DATA 6
6 WHO SETS DATA STANDARDS TODAY 8
7 HIGH LEVEL ANALYSIS OF EXISTING STANDARDS FOR CORE ID INFORMATION 9
8 OVERARCHING STANDARDS RECOMMENDATIONS 10
8.1 TRUST FRAMEWORK STANDARDS – POLICY COMMUNICATION 10
8.2 PER-CLAIM LEVEL OF TRUST 10
8.3 CLAIM PERIOD OF VALIDITY STANDARD 10
8.4 CLAIM CONTEXT TYPE STANDARD 11
9 CORE ID CLAIMS 12
9.1 NAME 12
9.2 ADDRESS 14
9.3 DATE OF BIRTH 17
9.4 NATIONALITY 18
9.5 CONTACT PHONES 19
9.6 CONTACT EMAILS 20
9.7 PERSONAL IDENTIFIERS 21
10 ID EVIDENCE 24
10.1 GENERAL REQUIREMENTS AROUND RECORDING EVIDENCE 24
10.2 ID DOCUMENTS 25
10.3 ELECTRONIC RECORDS 28
10.4 VOUCH 29
11 ID PROOFING 31
11.1 PROOFING STANDARDS 31
11.2 DATA USED TO DESCRIBE AND RECORD WHAT PROOFING CHECK TOOK PLACE. 32
12 ID ASSURANCE 36
13 COMMON CONTENT DATA, DIFFERENT PROTOCOL ENVELOPES 39
14 SUMMARY OF RECOMMENDATIONS 40
15 ACTION PLAN 41

1 Executive Summary

This document explores the need for data standards to enable interoperability of Digital IDs both in federations within an ID ecosystem, and across ID ecosystems. In this paper we focus on the data contained in a credential: the claims, evidence, proofing, and ID assurance, as opposed to the meta-data about the credential i.e., how it is securely transmitted and traced from one party to another.

We start by exploring the need for data standards at the ‘content data’ level:

- core claims about in individual.
- common evidence types and associated proofing techniques.
- communicating identity assurance.

In the production of this paper, we took a conscious scope decision to not try and cover standards for broader eligibility data, such as education, health, or employment information; standards for this type of information are required but should be defined by specialists in those use case areas.

There are many bodies who already provide part of the standards required to achieve interoperability such as ISO, ICAO, OIDF and W3C, but none of these cover the whole picture. Our analysis finds that there is a mixed bag of standards for the core claims about an individual and the associated evidence. In addition, the new OIDC for Identity Assurance standard covers standards for communicating proofing techniques and assurance levels, but does not set the standards as to how those processes are done; this is currently left to local ID Assurance Policies defined by each trust framework.

The paper goes into a great level of detail on how standards might be implemented from the data item level upwards. It reveals a layered requirement: there are many granular standards for individual data items of evidence, but as we work up to the whole data package, the parts need consistently assembling into a whole.

Throughout the paper we make a series of recommendations as to how data should be standardised, and by whom, to enable interoperability. A final summary of our recommendations can be found be found towards the end of the paper **here.** The key recommendations are:

- **A single protocol independent data standard is created** that allows core ID information to be communicated consistently regardless of the protocol (e.g., OIDC, Verifiable Credentials) used to securely exchange it. This should be based on the OIDC for Identity Assurance standard.
- Existing ISO and ICAO standards should be used for core ID Claims as far as possible.
- A per claim level of trust and period of validity construct should be considered.
- Where evidence specific standards exist for evidence types, they should be used for those pieces of evidence (e.g., passports, driving licenses.)
- **Standards are required for proofing techniques** that will enable different trust frameworks to assemble sets of proofed credentials as part of their individual assurance policies. Key proofing standards required are: Document Scanning (with different light options), Document OCR, Image Capture Liveness, Biometric Matching.

OIX’s next step will be to influence standards setters to adopt and progress the recommendations of this paper.

2 The need for Data Standards

If relying parties are to embrace the use of Digital ID, it must be as easy as possible for them to consume. The relying party might want to accept credentials from different sources. If the relying party must deal with data in different formats depending on who credential issuer is then that will be a barrier to adoption. It will mean the relying party has to assess, and possibly code differently, for the same types of credentials from different issuers.

This problem can manifest in various scenarios:

- Where there is a federation of ID providers, who are issuing verified core ID information such as name, address and supporting evidence.
- Where they are multiple issuers of the same type of credential (e.g., digitized passport, covid vaccine certificate, education certificate).
- Where credentials are used across international boundaries to prove who a user is in a new country. This applies in particular to “golden ticket” credentials that are used internationally: Passports, Driving Licences, Bank Accounts, Telco Account and National ID Cards.

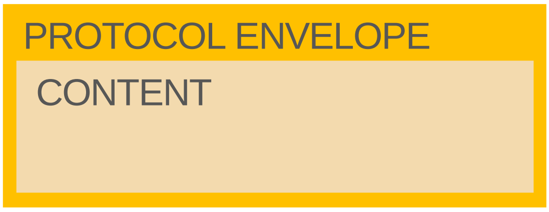
Whilst there are ways to allow the issuers of credentials to describe the format of the data they are providing (e.g., JSON-LD, JSPN-JWT, credential Schemas) if these are not agreed across different issuers of the same type of credential this pushes the problem of interpretation, translation and data normalisation to the relying party.

Common agreed data standards will mean less work for relying parties when adopting digital ID. They will also mean less risk of:

- Error – as data does not need be translated.
- Security breach – as third-party translation services are not required.
- Data over exposure – data Minimisation can be achieved when required.

3 Content Data Vs Protocols

This paper focusses on standards for the data and metadata that describes the **content** of the credential itself rather than the protocol envelope that carries the data:



Example of content data are:

- **Claims** about an individual: Name, Address, DoB, Age, Covid Status. Claims might be verified or un-verified (self-attested).
- **Evidence** supporting verified claims (metadata about the core content data)
- Levels of **Assurance**, and the **Proofing** approaches taken to show how they have been achieved

as opposed to data about the credentials such as:

- Who issued it
- Who can read it
- Terms of Use
- Delegated Authority
- Other Policy Metadata applicable to the credential.

In DIDCOMM this content data would be in the body, in a Verifiable Credential it would be in the credential_subject or evidence elements, in OIDC for Identity Assurance IDA it would be within the verified_claims element.

Content data items are independent of protocols, and so must be standardised in terms of name, format and meaning and be consistent across protocols.

4 Standards and Governance for Content Data

A consistent governance approach for content data is required. This can be applied at two levels, often both:

- At a trust framework level, when a framework permits multiple issuers of the same type of credential.
- Globally for key content items to allow global framework interoperability.

This document explores which content data items should be standardised and makes recommendations as to where standards governance needs to be owned. This is generally at global level, with trust frameworks adopting and extending global standards as required.

Recommendations made in this document appear in boxes formatted as follows. Not all rows in the table apply to all types of recommendation. Optional rows may be omitted:

Item	The data items or areas in question
Global Recommendation	Should a global standard be created?

Candidate Global Owner	If a global standard is recommended, who should own and govern this standard?
Trust Framework Recommendation	How should trust frameworks address the standardization need?
Relying Party Approach (Optional)	How should relying parties address the standardization need?
Recommendation on handling types (Optional)	If the data item has different types (e.g., current and previous addresses, types of nationality) how should these be handled?
Recommendation on periods of validity (Optional)	If the data item has periods of validity (e.g., start and end dates) how should these be handled?

5 Types of Content Data

OIX has categorized content data for Digital ID into the following types:

ID Claims	Evidence	ID Proofing	ID Assurance
Core ID Claims • Names • Addresses • DoB • Nationalities • Contact Phones • Contact Emails • Personal Identifiers	ID Documents • National ID • Passport • Driving License Electronic Records • Bank Account • CRA Check • Electoral Roll • Fraud Check • Mortality Vouches • Via Digital ID • Face to Face	Validation Methods: • Face to Face • Scanning • API Call using self declared data Verification Methods: • KBVs • OTCs • Selfie Cross Matches • Face to Face Activity Methods • Electronic Activity Evidence • Vouched Activity ID Fraud Methods: • Known Fraud • Risk Signal	• Trust Framework • Assurance Level • Assurance Policy • Assurance Procedure • Assurance Elements and Scores: ○ Strength / Validation ○ Activity ○ ID Fraud ○ Verification • Mapping Elements Scores back to Evidence

This paper focusses on data standards and governance for the following four areas, in the following order:

1. Core ID Claims
2. ID Evidence
3. ID Proofing
4. ID Assurance Information

Our analysis focuses on the data items for natural persons rather than legal entities.

From a Relying Party point of view, it is most important that data elements are in a standard format when presented to them. So, one approach to standardisation is for Identity Providers (e.g., a wallet provider) to apply it at point of presentation. However, this may affect the integrity of originally issued credentials and require the IdP to issue a new credential, so ideally standardization is applied by original credential issuers.

For the purposes of our analyses, we have only considered phone and email forms of contact details.

Different use cases will ask for different sets of claims and evidence to be presented as a subset of this information. This could be as simple as: a) an Age and a Photo, b) Name, Address, DoB and an LoA, or c) it could be a full record of the evidence and proofing process.

Other Claims, such as the below eligibility and certification claims, are not within the scope of this document in order to limit the scope of this analysis, but they will also need standardising:

- Right to Work
- Right to Rent
- Driving Permissions
- Travel VISA
- Education Records
- COVID Vaccine
- COVID Test
- Bank Account Transactions (Open Banking).

It should be noted that some forms of ID Evidence are also often a form of Eligibility information. For example, a Driving Licence is often used as a form of ID but its primary purpose is to convey entitlement to drive.

Governance for Eligibility information is required but is not considered within the scope of this paper. For example, the COVID pandemic has shown the need for standardisation around the communication of personal covid status information. In this case and some standardisation has been suggested by the WHO, whilst a separate standard has been implemented across the EU.

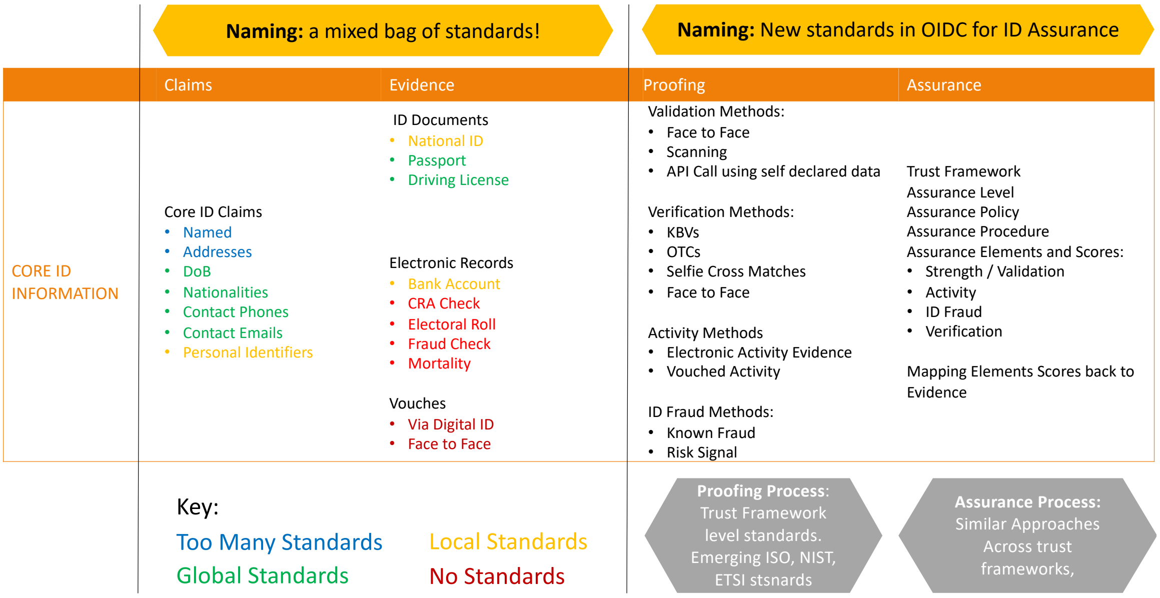
6 Who sets data standards today

OIX has assessed the following bodies who set a standard today, and where applicable the credentials they define standards for:

Body	Full name of Body	Claim / Credential	Core ID fields Covered	ID Document Specific Fields Covered	ID Proofing / ID Assurance fields covered
IANA	Internet Assigned Numbers Authority		Name, DoB, Address	-	-
ICAO	International Civil Aviation Organization	Passport	Name, DoB, Nationality	Issue Date, Expiry Date.	-
EU	European Union	ID Cards	Refers to ICAO 9303 Part 5.	-	-
ISO	International Organisation for Standardization	Mobile Driving Licence	Name, DoB	Issue Date, Expiry Date.	-
ISO	International Organisation for Standardization	Dates	Any date / time	-	-
ISO	International Organisation for Standardization	Address ISO 19160	Address	-	-
ITU	International Telecommunication Union	Telephone Numbers ITU-T E164.	Telephone Numbers	-	-
W3C	World Wide Web Consortium	Do not make recommendations for data content standards. Refer to schema.org as a depository for issuer-based claim definitions that RPs can use to interpret data.			
OIDF	Open Identity Foundation	None	Generally registers core ID standardization to IANA.	Naming of core evidence field in OIDC4IDA.	Publishes permitted values in these areas in a wiki
ETSI	European Telecommunications Standards Institute	Do not make recommendations for data	-	-	Proofing Standard for eIDAS

7 High Level Analysis of Existing Standards for Core ID Information

OIX's analysis has determined that there is an inconsistent mixed of standards in existence today across the scope of the data items are considering. The following graphic summarises our findings:



Naming: a mixed bag of standards!

Naming: New standards in OIDC for ID Assurance

	Claims	Evidence	Proofing	Assurance
CORE ID INFORMATION	Core ID Claims • Named • Addresses • DoB • Nationalities • Contact Phones • Contact Emails • Personal Identifiers	ID Documents • National ID • Passport • Driving License Electronic Records • Bank Account • CRA Check • Electoral Roll • Fraud Check • Mortality Vouches • Via Digital ID • Face to Face	Validation Methods: • Face to Face • Scanning • API Call using self declared data Verification Methods: • KBVs • OTCs • Selfie Cross Matches • Face to Face Activity Methods • Electronic Activity Evidence • Vouched Activity ID Fraud Methods: • Known Fraud • Risk Signal	Trust Framework Assurance Level Assurance Policy Assurance Procedure Assurance Elements and Scores: • Strength / Validation • Activity • ID Fraud • Verification Mapping Elements Scores back to Evidence

Key:

Too Many Standards

Local Standards

Global Standards

No Standards

Proofing Process: Trust Framework level standards. Emerging ISO, NIST, ETSI stsnards

Assurance Process: Similar Approaches Across trust frameworks,

The standards landscape divides broadly into areas in the context of **element naming**, typology and permitted values:

- Claims and Evidence element have a real "mixed bag" of standards. Many items do not have standards set at all, whilst at the other end, for items such as name and address, there are (too many) standards to choose from. However, for some items – Date of Birth, Nationalities, Contact Details – there existing global standards that should be adopted in the context of Digital ID. Items such a Personal Identifiers and Bank Accounts (via Online Banking) have local country or region-based standards in place.
- For Proofing and Assurance elements, a new standard has been defined at the OIDF: OIDC for Identity Assurance.

Proofing processes are often defined by individual trust frameworks, for example they will define:

- how documents must be checked face to face or scanned
- how selfies must be captured
- the tolerances for biometric selfie cross matches

Proofing processes are not consistent across trust frameworks yet. For global interoperability of credentials, consistent referenceable proofing standards will be vital.

Equally Assurance policies and procedures are trust framework specific. This is likely to remain the case as one of the core purposes of a trust framework is to define the value of specific credential evidence in the context of that trust framework. OIX's work on global interoperability is analysing whether the Assurance Policies of different trust frameworks can be described in a standard way.

8 Overarching Standards Recommendations

Please note that this document does not cover UNICODE concerns.

The following overarching standards recommendations are made:

8.1 Trust Framework Standards – Policy Communication

Item	Trust Framework Standards – Open Policy Communication
Global Recommendation	An Open Policy Metadata Framework is defined that allows trust frameworks to publish which standards they have adopted.
Candidate Global Owner	OIX is currently undertaking an analysis of what such a Policy Metadata Framework might look like which may lead to a candidate owner.
Trust Framework Recommendation	Trust Frameworks publish a resource (at a URI) that can be systemically accessed (e.g., machine readable) using an Open Policy Metadata Framework to describe the frameworks implementation of standards (e.g., mapping to global name and address schemas, personal identifiers it publishes, it's assurance policy model).
Relying Party Approach	Relying parties can use the same Open Policy Metadata Framework to describe their policy requirements.

8.2 Per-Claim level of trust

Item	Per-Claim level of trust
Global Recommendation	All claims have "unverified" / "verified" meta-data. For some frameworks a claim level of assurance is applied (e.g., this name has been verified to LoA3, whereas this address is only verified to LoA2).
Candidate Global Owner	OIDF as Part of Global Protocol Independent Data Standard. This is already. Supported in OIDC, however could be refined to be made less verbose.
Trust Framework Recommendation	Trust Frameworks choose whether to adopt field level verification and whether field level LoAs are applied.

8.3 Claim Period of Validity Standard

Item	Claim Period of Validity Standard

Global Recommendation	Many claims have a period of validity. For example, a person can change their name, address, phone number and emails addresses over time. They can also have more than one of these. A global standard for expressing the period of validity of a claim is recommended
Candidate Global Owner	OIDF as Part of Global Protocol Independent Data Standard
Trust Framework Recommendation	Adopt global standard

8.4 Claim Context Type Standard

Item	Claim Context Type Standard
Global Recommendation	Many claims have context types, allowing the user to add a context for the claim. For example, a person can have a current and previous name or address. They could also have business and personal email addresses or phone numbers. A global standard for expressing context types for claims should is recommended. Some core “starter” claim context types permitted values might be specified at a global level, whilst others may be more appropriate at a trust framework level.
Candidate Global Owner	OIDF as Part of Global Protocol Independent Data Standard
Trust Framework Recommendation	Adopt global standard for expressing types. Choose whether to adopt globally defined permitted values and / or extend.

9 Core ID Claims

By Core ID claims, OIX means the fundamental personal information that allows an individual to be:

- Uniquely identified
- Contacted

Again, Core ID claims can sometimes be eligibility information as well. For example, age can be derived from date of birth, or nationality might make a person eligible for certain government services.

To determine how Core ID Claims might best be standardised and governed, we have grouped them as below:

- Names
- Addresses
- DoB
- Nationalities
- Contact Phones
- Contact Emails
- Personal Identifiers

Standardisation for each group is considered in the following sub-sections:

9.1 Name

9.1.1 How does the data field break down?

Name breaks down into the parts of a person’s name. This is often handled by breaking storage of the name down into 2 or 3 parts:

2 parts – Forenames, Last Name
3 parts – First Name, Middle Names, Last Name.

There are also titles, salutations, surname prefixes and postfixes to be considered.

9.1.2 Terms Used

There is inconsistency in terms used for names. For example:

- ICAO on the face of passports uses – Surname / Nom and Given Names / Prenoms
- ICAO data standard uses – Surname and Given Name, where Given Name includes second names and title.
- ISO mDL standard uses – family_name and given_names
- IANA used by OIDC – family_name and given_name. IANA also supports middle_name

9.1.3 Types, Lengths and Permitted Values

Whilst most names are alphabetic in nature, from a data type point of view they are often defined as alphanumeric. For example, both ICAO and ISO mDL use alphanumeric.

Lengths vary. ICAO passenger exchange format allows for 64 characters in a name field.

There are no restrictions on permitted values.

Titles, such as Mr, Mrs, Lord, Doctor, do have permitted values.

9.1.4 Can the person have more than one of these?

Yes. People change their names over time. They may also operate separate names simultaneously, for example for professional purposes Vs private purposes.

Support for multiple names, of different context types with periods of validity should be considered. A list of permitted values for types of names is required.

9.1.5 Standards Recommendations for Name

See Section 4.1 in https://openid.net/specs/openid-connect-4-identity-assurance-1_0-12.html for current OIDC definitions.

Item	Name
Global Recommendation	Global Standardization is not recommended. Names are too local in nature, and there are local standards and conventions that need to be catered for. To allow interoperability, as structured ”global name schema” should be defined that: • Supports multiple standards • Points to the local / sector / organizational standard used for a particular name • Shows how the elements of the local / sector standard map to a set of generic interoperability profiles for specific user cases e.g., travel (e.g., ICAO), finance, social media. • Support periods of validity. • Can this be based around the two key fields of: first_name, family_name? • Needs to consider encoding (e.g., Unicode). Consideration needs to be given to: • Different names in non-roman character sets. • Lengths definitions for names – the longest name in the world is 747 characters! • Simplified names for everyday use.

Candidate Global Owner	ISO
Trust Framework Recommendation	Trust frameworks define a standard for names within their ecosystem. This is mapped to the “global name schema” by the framework
Relying Party Approach	Relying parties ask for name using the local trust framework convention. This may include asking for simplified or concatenated names.
Recommendation on handling types	Trust Frameworks may define permitted context types. Relying parties define types as part of their request to the user. The user then maps the names they have stored in their ID to the required context types. E.g., This is my current name, this is my previous name. User may also indicate their preferred name.
Recommendation on periods of validity	Trust frameworks adopt global convention for periods of validity, which can be mapped to the “global name schema”

9.2 Address

9.2.1 How does the data field break down?

Address breaks down into several fields.

How postal addresses are structured varies country by country, with some countries having tighter definitions than others.

Typically, there is some form of **postal code** that identifies an area or a cluster of buildings.

Street numbers are also commonly used, as are **apartment or unit numbers** when a building contains multiple dwellings or businesses. As are **street names** and **building names**.

The major **town/city** that a street is in might form part of the address. As might a governmental region, such as a **county** or **state**.

When sending international correspondence, a **country** will also be used.

Japan for example uses as postal code, prefecture, city/town, sub-area. Sub-area breaks down to: **subarea name**, **subarea number**, block number, building number.

The terms highlighted in bold above are used as generic field names in the table below.

Examples of different Address breakdowns for different countries are shown below:

Generic Field Names	UK Address	US Address	German Address	Japanese Address
Apartment / unit number		315		1
Building name	Sandstone Cottage	Jacksons House		

Block				2
Street number	45	1335	9	
Street name	Long Road	41st Street	Rontgenstr	
Sub Area number				5
Sub Area name				Ginza
Town/city	Carnforth	Townville	MAXDORF	Chuo Ward
County/Area	Cumbria			
Prefecture				Tokyo
State		TX		
Postal Code	CM45 6YT	43345	67133	170-3293
Country	UK	USA	Deutschland	Japan

Addresses also often refer to a Geo location. Some addresses may also have a unique property reference[1].

9.2.2 Terms Used

The is considerable inconsistency in terms used to describe the elements of an address.

Many terms could be regarded as equivalent, such as County/Area and Prefecture, but in practise both can be used in some addresses.

There is general consistency in the use of Postal Codes. However, these map to very different areas. For some countries Postal Codes map 1:1 or n:1 to a town/city, making the town/city redundant (e.g., the UK).

9.2.3 Types, Lengths and Permitted Values

Most address fields are alphanumeric.

Building and street numbers usually need to support an ‘nnA’ so are likely to be implemented as alphanumeric.

Postal codes often have defined types, lengths and are often able to be validated in that respect. Whilst there may be a theoretical set of permitted values for postal codes, these may only be able to be validated with commercial address quality management tools.

9.2.4 Can the person have more than one of these?

Yes - people move over time. They may also operate separate simultaneous addresses, for example for professional purposes Vs private purposes, as well as have addresses for second properties.

Support for multiple addresses, of different context types with periods of validity should be supported. A list of permitted values for types of address should be considered.

[1] https://www.geoplace.co.uk/addresses-streets/location-data/the-uprn

9.2.5 Standards Recommendations for Address

Item	Address
Any Standards?	Many. ISO19160-6 defines global standards for address presentation.
Global Recommendation	Global Standardization is not recommended. Addresses are too local in nature. Standardization would affect address quality. Structured “global address schema” is defined that: • Supports multiple standards • Points to the local / sector / organizational standard used for a particular address. • Shows how the elements of the local / sector / organization standard map to a set of generic interoperability profiles for specific user cases e.g., travel (e.g., ICAO), finance, retail. • Needs to consider encoding (e.g., Unicode).
Candidate Global Owner	ISO19160-6 is marked as Deleted. However, it could be used as a start point for a standard that specifies a set of data models suitable for machine encoding of address information, called the “Address Interchange Object” (“AXO”) models, and the usage of them. Specifically, this document provides: • data models for digital storage and interchange of address profiles conforming to ISO 19160-1; • data models for digital storage and interchange of addresses conforming to a specific address profile; • data models for entry and display templates for entering and displaying addresses conforming to the profile and encoding rules above; and • the management and operations of a register of address profiles conforming to this document.
Trust Framework Recommendation	Trust frameworks define a standard for address within their ecosystem. This is mapped to the “global address schema” by the framework
Relying Party Approach	RP should ask for an address in the format defined by its applicable trust framework. Address may be presented as a concatenated field for many use cases, with the rules for concatenation being defined by that use case. Often the relying party is only interested in the person’s current address.
Recommendation on handling types	Trust Frameworks may define permitted context types. User would map an address they have in their ID to an RPs request for address of a certain context type, at point of presentation. User may also indicate their primary address.
Recommendation on periods of validity	Trust frameworks adopt global convention for periods of validity, which can be mapped to the “global address schema”

9.3 Date of Birth

9.3.1 How does the data field break down?

This is a single field.

If an age is to be derived from a date of birth this is a separate credential and should be treated as such. See section below on presentation.

9.3.2 Terms Used

Usually called Date of Birth. Abbreviated to DoB.

9.3.3 Types, Lengths and Permitted Values

Date or Date Time

9.3.4 Can the person have more than one of these?

No. It cannot change over time.

9.3.5 Standards Recommendations for Date of Birth

Item	Date of Birth
Any Standards?	ISO-8601
Global Recommendation	A global standard for date of birth is recommended using ISO-8601. Gregorian Calendar date is recommended.
Candidate Global Owner	ISO
Trust Framework Recommendation	Trust frameworks define a standard for date of birth within their ecosystem aligned to the global standard.
Relying Party Approach	RP should ask for a date of birth in the format defined by its applicable trust framework. Often the relying party is only interested in the person age, or that they are within a certain age bracket. In which case a data minimisation approach should be applied. It may also be important to know whether the age assessment is definitive or is based on an estimation.

9.4 Nationality

9.4.1 How does the data field break down?

This is a single field.

9.4.2 Terms Used

Usually called Nationality

9.4.3 Types, Lengths and Permitted Values

Use ICAO references?

9.4.4 Can the person have more than one of these?

Yes, a person can multiple nationalities. This can be valid from and to a specific time. For example, many UK nationals claims dual nationality elsewhere in Europe where possible as a result of Brexit.

A valid from and to date should be implemented.

9.4.5 Standards Recommendations for Nationality

Item	Nationalities
Any Standards?	ICAO Doc 9303, ISO-3166 Country Codes
Global Recommendation	As ICAO Doc 9303 standard addresses global travel and includes other countries that not on the ISO list, ICAO standards should be adopted as a global standard for Digital ID. These should include provision for periods of validity.
Candidate Global Owner	ICAO
Trust Framework Recommendation	Trust frameworks adopt ICAO standards for nationalities
Relying Party Approach	Relying party asks for nationalities using ICAO standards
Recommendation on handling types	ICAO types are adopted by all trust frameworks
Recommendation on periods of validity	Trust frameworks adopt global convention for periods of validity, which can be mapped to the global standard

9.5 Contact Phones

9.5.1 How does the data field break down?

The field is consistently recorded and presented on a global basis as country code and number.

9.5.2 Terms Used

There is general consistency in terms used.

9.5.3 Types, Lengths and Permitted Values

Phone numbers are numeric, but are prefixed by a + to indicate the international dialling code.

There are permitted values for the international and regional code part of a phone number. Although validation is not possible.

9.5.4 Can the person have more than one of these?

Yes. People habitually have multiple phone numbers.

Phone numbers break down into different types:

- Personal Landline
- Personal Mobile
- Work Landline
- Work Mobile

Support for multiple phone numbers, of different context types with periods of validity should be considered.

9.5.5 Standards Recommendations for Contact Phones

The following recommendation is made

Item	Phone
Any Standards?	ITU-T E164. Global standard of +nnnnnnnnnnn
Global Recommendation	Align with global standard
Candidate Global Owner	ITU
Trust Framework Recommendation	Align with global standard

Relying Party Approach	Relying party asks for phone in the global standard. Often the relying party is only interested in the person's current phone number, or a phone number of a particular type. A preferred contact number is potentially required so the user can indicate which one should be used. This may vary by circumstance.
Recommendation on handling types	Trust Frameworks may define permitted context types. User would map a phone they have in their ID to an RPs request for phone of a certain type (e.g. 'home phone'), at point of presentation. User may also indicate their primary or preferred phone.
Recommendation on periods of validity	Trust frameworks adopt global convention for periods of validity, which can be mapped to the global standard

9.6 Contact Emails

9.6.1 How does the data field break down?

The field is consistently recorded and presented on a global basis as local_identifier@domain.

9.6.2 Terms Used

There is general consistency in terms used.

9.6.3 Types, Lengths and Permitted Values

Emails are alphanumeric and are subject for formatting rules regarding containing a @.

No permitted values are defined for email addresses. It is not possible to validate them, other than that they are in the correct format, and possibly for a valid domain.

Maximum length is 254 characters.

9.6.4 Can the person have more than one of these?

Yes. People habitually have multiple emails.

Email addresses break down into different types:

- Personal – often several
- Work – often several

Support for multiple phone numbers and email addresses, of different context types with periods of validity should be supported.

9.6.5 Standards Recommendations for Contact Details

Item	Email

Any Standards?	Global standard of aaaa@bbbb.xxx
Global Recommendation	Align with global standard
Candidate Global Owner	**Internet Engineering Task Force and the Internet Society**. Together, they set standards for the usage of the Internet at large. RFC 5322 concerns itself with electronic mail, or email (source).
Trust Framework Recommendation	Align with global standard
Relying Party Approach	Relying party asks for email in the global standard, with a type of that is relevant.
Recommendation on handling types	Trust Frameworks may define permitted context types. User would map an email they have in their ID to an RPs request for email of a certain type (e.g., 'Work Email'), at point of presentation. User may also indicate their primary email.
Recommendation on periods of validity	Trust frameworks adopt global convention for periods of validity, which can be mapped to the global standard

9.7 Personal Identifiers

9.7.1 How does the data field break down?

The format of the field varies by personal identifier. Some are entirely numeric, many are alphanumeric. Some examples are:

Country	Personal Identifier Term	Format	Example
United States	Social Security Number (SSN)	NNN-NN-NNNN	778-62-8144
United Kingdom	National Insurance Number (NINO)	AANNNNNNA	AB123456A
Sweden	Social Security Number (SSN)	NNNNNN-NNNN	19901027-5312
Singapore	National Identification Number (NRIC)	ANNNNNNNA	S7788888H

Some personal identifiers contain meaningful information. For example, the Swedish SSN starts with the persons date of birth. The second 2 digits in Singapore's NRIC indicate the persons birth year. However, many personal identifiers are deliberately meaningless to ensure no other personally identifiable information can be inferred from the number alone.

9.7.2 Terms Used

As can be seen from, the table above the terms used to describe personal identifiers also vary from implementation to implementation.

9.7.3 Types, Lengths and Permitted Values

These also vary for each personal identifier. There are often published validation routines for personal identifiers. Many persona identifiers also incorporate check digits.

9.7.4 Can the person have more than one of these?

Yes - people many have many personal identifiers. Some countries issue a national personal identifier that is consistently used across the identity ecosystem to uniquely identify a person. Many countries do not issue national ID numbers and instead the user is known by many different numbers associated with different use cases e.g., tax, benefits, health, driving, travel.

9.7.5 Standards Recommendations for Personal Identifiers

Item	Personal Identifiers
Any Standards?	Various, usually from issuer of the identifier
Global Recommendation	A global “personal identifier schema” approach is defined that supports Trust Framework, Issuer, Type and Value. The following examples show how this might work: NIST>DSS>SSN>NNN-NN-NNNN BankID>SwedenGov>SSN>NNNNNN-NNNN UKTF>DWP>NINO>AA999999A UKTF>NHSE>NHS#>NNNNNNNNNNN SingaporeGTA>>NRIC>ANNNNNNNS Passports and driving license claims should also be formatted in this manner. The schema should also support periods of validity. Issuers, or trust frameworks on their behalf, should publish format guides and check tools as resources.
Candidate Global Owner	**ISO is a candidate owner for a new standard for Personal Identifiers.** *There is NATIONAL PERSONAL IDENTIFIERS: ISO 24366, but this defines a new format for an NPI on the context of financial services and then goes on to define a standard for core identity claims: name, address, DoB, phone numbers, types for addresses, phone numbers, emails*
Trust Framework Recommendation	Trust frameworks adopt the global schema approach. Trust Frameworks define and publish the issuers of personal identifiers and their types within their framework.

Relying Party Approach	Relying Parties may ask the user for an identifier of a specific framework>issuer>type. Or they may ask for a suitable unique identifier and the IdP will allow the user to choose the appropriate one.
Recommendation on handling types	Trust Frameworks define and publish the types within their framework.
Recommendation on periods of validity	Trust frameworks adopt global convention for periods of validity, which can be mapped to the global standard

10 ID Evidence

This analysis breaks ID evidence down into 3 categories that should be applicable within any trust framework. Several of these categories have been taken from the OIDC ID Assurance standard.

ID Documents such as:

- National IDs
- Passports
- Driving Licenses

Electronic Records such as:

- CRA Checks
- Bank Accounts
- Electoral Roll
- Selfie Verification

Vouches, covering:

- Via Digital ID
- Face to Face

In this section we look in more detail at the data contents of each category and consider how these might be standardised.

10.1 General requirements around recording evidence

It is important to know who the party was that checked the ID evidence. This could be a third party who checks the users physical ID document and issues a digitised credential. Also – the time / date at which they checked it.

A unique reference number should be generated to allow the check to be traced.

The following fields are recommended for all evidence types:

Field	Type	Permitted Values	Who defines permitted Values?
evidence_checker	An	Yes	Trust Framework
evidence_check_datetime	date		
evidence_period_of_validity	An		
evidence_check_txn_ref	An		

Recommendations in this area are:

Item	Standard evidence data items
Any Standards?	OIDC for IDA
Global Recommendation	IDA element of OIDC is evolved to be a protocol independent standard for the communication of evidence and assurance information. A key thing to note is that many trust frameworks will support multiple forms of the same ID Evidence being used, so

	when planning to communicate these repeating groups should be allowed for.
Candidate Global Owner	Leverage OIDC for IDA electronic records schema. OIDF to review the standards data items recommendations above.
Trust Framework Recommendation	Trust frameworks adopt OIDC for IDA schema approach.
Relying Party Approach	Relying Parties may ask the user for an identifier of a specific framework>issuer>type. Or they may ask for a suitable unique identifier and the IdP will allow the user to choose the appropriate one.
Recommendation on handling types	Trust Frameworks define and publish the permitted values for evidence_checker within their frameworks. These values could be pointers to trust framework certified agents such as those certified to undertake document scan and selfie checks, or to access authoritative sources.
Recommendation on periods of validity	Trust frameworks adopt global convention for periods of validity, which can be mapped to the global standard. This could be linked to verification date.

10.2 ID Documents

10.2.1 National IDs

By National IDs we mean those that are issued specifically for the purpose of citizen ID verification. We do not mean entitlement documents such a driving licences and passports that are sometimes used as a proxy for a national ID.

Most national IDs are plastic cards, usually with a photo of the individual so that the person can be identified in a face-to-face interaction. Some national IDs include other machine-readable biometric information, such as fingerprints.

National IDs are generally designed for domestic use.

There is no international standard for national IDs.

The EU has a standard for ID Cards – 2019/1157. This refers to ICAO 9303 Part 5 for standards for data elements included on Identity Cards.

Due to the wide variety of national IDs, it's not possible to come up with a standard set of fields.

Recommendations in this area are:

Item	National IDs

Any Standards?	The EU has a standard for ID Cards – 2019/1157. This refers to ICAO 9303 Part 5 for standards for data elements included on Identity Cards.
Global Recommendation	ICAO 9303 Part 5 for standards for data elements included on Identity Cards should be used to National IDs
Candidate Global Owner	ICAO
Trust Framework Recommendation	Align with global standard
Relying Party Approach	Relying party asks for passport data in ICAO format.

10.2.2 Passports

Passports are designed to prove eligibility for travel. They are issued for a fixed time, which is usually many years.

They are designed to show the person is a citizen of a particular country, not that they reside in that country or indeed where they reside. As a result, they do not generally contain the person's address.

International standards for passports are clearly and comprehensively defined by ICAO 9303. This includes:

- Standards for printed documents
- Standards for data stored on biometric chips

A passport will contain the following information:

Field	**Synonyms**	**Permitted Values**	**Who Defines format?**	**Who defines permitted Values?**	**On Biometric Chip?**	**Mandatory**
Country Code	Code du Pays	Yes	ICAO	ICAO	Y	Yes
Passport Number	No de Passport Document Number		ICAO		Y	Yes
Primary Identifier	Surname Nom		ICAO		Y	Yes
Secondary Identifier	Given Names Prenoms	To be discussed	ICAO	TBD	Y	Yes
Nationality		Yes, but with opt out.	ICAO	ICAO	Y	Yes
Date of Birth		Yes, DD MMM YY Can be XX(X) if	ICAO	ICAO	Y	Yes

		partial or unknown				
Sex		F, M, X	ICAO	ICAO	Y	Yes
Place of Birth						No
Personal No	No Personnel					No
Date of Issue						Yes
Date of Expiry					Y	Yes
Issuing Authority						???
Holders IDentification Features	Signature, fingerprint					No
Holders Picture					Y	Yes

Recommendations for standards for this item are:

Item	Passport
Any Standards?	ICAO 9303
Global Recommendation	The ICAO standard for Logical Data Structure from 9303 should be used. Future Digital Travel Credentials will use this.
Candidate Global Owner	ICAO
Trust Framework Recommendation	Align with global standard
Relying Party Approach	Relying party asks for passport data in ICAO format.

10.2.3 Driving Licenses

Driving licenses are designed to prove eligibility to drive a vehicle. They are issued for a fixed time, which is usually many years.

They are issued at a country level or regionally within a country. The US issues driving licences at a state level for example.

There is a new ISO standard for Mobile Driving Licences (mDLs) - ISO/IEC 18013-5. The term ‘mobile driving licence’ in this context is used to mean an electronic version of the users driving licence that get can hold as a digitized credential. This standard defines the following MANDATORY fields that would be of interest in the ID proofing process:

- family_name
- given_name
- birth_date

- issue_date
- expiry_date
- issuing_country
- issuing_authority
- document_number
- portrait
- un_distinguishing_sign

Note that this ISO standard does not make address a mandatory field, though it is often present on a driving license and is used as proof of address in the ID proofing process.

Recommendations on Driving Licences:

Item	Driving Licenses
Any Standards?	ISO 18013-5
Global Recommendation	Leverage ISO MDL standard for data items on a driving licence.
Candidate Global Owner	ISO
Trust Framework Recommendation	Align with global standard
Relying Party Approach	Relying party asks for Driving License to the global mDL standard.

10.3 Electronic Records

Electronic records come from various sources, such as:

- CRA Checks
- Bank Accounts
- Electoral Roll
- Governement Data Source Checks
- Criminal Records Check
- Disclosure and Barring Checks
- Utility Accounts
- Employment Records (e.g., payslips)
- Social Media Usage
- Electronic Signature of various different types: SES, AES, QES.

This will vary by country. The type of electronic record should be recorded as part of the ID evidence.

The authoritative source used is also key, such as who is the bank, or who holds the electoral role.

Many electronic checks have a ‘result’. This could be a Y/N indicating a match of data, or a score indicating a match confidence.

The amount of time a record has been present on an electronic source is also important, so knowledge of the date a record is created and last updated are recommended.

Some electronic checks look for positive affirmation of the user ID, others look for negative indicators. Examples of negative check electronic records include:

- Mortality
- Sanctions and PEPs
- Fraud databases.

To capture the results of electronic checks the following fields are recommended:

Field	**Permitted Values**	**Who defines permitted Values?**
record_type	Yes	OIDF
positive_negative	Yes – P / N	
result		
authoritative_source	Yes	Trust Framework
authoritative_source_reference		
date_created		ISO8601
date_last_updated		ISO8601

The following recommendations are made for this item:

Item	Electronic Records
Any Standards?	OIDC for IDA
Global Recommendation	Leverage OIDC for IDA electronic records schema. OIDF to review the standards data items recommendations above. OIDF to create a global register of electronic record types to enable interoperability.
Candidate Global Owner	OIDF IANA Registry
Trust Framework Recommendation	Align with OIDF global standard. Define Types for use within their scope.
Relying Party Approach	Relying party asks for electronic record in the trust framework standard.
Recommendation on handling types	Trust Frameworks Define Types for use within their scope.

10.4 Vouch

A vouch is a way for a trusted person to introduce another person they know and trust into the ID ecosystem.

There are several types of Vouch:

- Document Vouch – e.g., Letter
- Digital Vouch
- Digital Vouch with Photo
- In Person

A Digital Vouch with Photo is where the voucher attaches a digital photo of the vouchee to the vouch. The vouch is used in the verification process in the same way as an ID document, with the ID provider cross matching a selfie of the user to the photo attached to the Vouch.

The following fields are recommended to capture the different types of vouch:

Field	**Permitted Values**	**Who defines permitted Values?**	**Document Vouch**	**Digital Vouch**	**Digital Vouch with Photo**
vouch_type	Yes	OIDF?	document	digital	digital_photo
positive_negative	Yes – P / N		Y	Y	Y
voucher_declaration			Y	Y	Y
voucher	Local Decision	Trust Framework	Y	Y	Y
voucher_qualification	Yes	Trust Framework	Y	Y	Y
voucher_txn_reference			Y	Y	Y
vouchee_given_name			Y	Y	Y
vouchee_family_name			Y	Y	Y
vouchee_birth_date			Y	Y	Y
vouchee_address			Y	Y	Y
date_created			Y	Y	Y
vouch_document_image			Y		
vouchee_photo					Y

Recommendations in this area are:

Item	Vouch
Any Standards?	OIDC for IDA
Global Recommendation	Leverage OIDC for vouch schema. OIDF to review the standards data items recommendations above. OIDF to create a global register of vouch types to enable interoperability.
Candidate Global Owner	OIDF
Trust Framework Recommendation	Align with OIDF global standard. Define permitted values for types for use within their scope.
Relying Party Approach	Relying party asks for electronic record in the trust framework standard.
Recommendation on handling types	Trust Frameworks Define Types for use within their scope.

11 ID Proofing

ID proofing breaks down into:

- The direct issue of an ID proof as a Digitized Credential by an authotatative source who verifies they issuing the credential to to genuine user.

- Validation Methods such as:
  - Face to Face
  - Scanning
  - API Call using self declared data
  - Chip Read

- Verification Methods such as:
  - KBVs
  - OTCs
  - Selfie Cross Matches
  - Face to Face
  - Verified Logon

- Activity Methods such as:
  - Electronic Activity Evidence
  - Vouched Activity

- ID Fraud Methods such as:
  - Known Fraud
  - Deceased Check
  - Risk Signal

Pieces of ID evidence can be used for more in more than one proofing method, for example a passport could be used for validation and verification, or an electronic record could be used for both validation and activity.

The results of the proofing processes should be associated with the evidence used.

Sometimes multiple pieces of ID evidence are be used for one proofing process, for example using KBVs from multiple evidence sources.

The possible methods for ID ecosystems should be defined. These are described below as check_methods.

There is a separation of the:

1. Standards used to do the proofing (see 11.1).
2. Data used to describe and record what proofing check took place (see 11.2).

11.1 Proofing Standards

A separate, and key recommendation, is made here around standards used to do the ID Proofing:

Item	ID proofing Standards

Any Standards?	Most trust frameworks set their own standards for ID proofing. However, this means it is difficult to share evidence across frameworks. Whilst there are some emerging standards for ID proofing around liveness checks and acceptable False Positive Rates/False Reject Rates rates on biometric matching, there is much to do this this area in terms of standardisation. Issue of a credential directly from an authoritative source who has taken responsibility for proofing the individual before issuing them the credential is likely to be the most trusted method of credential proofing, and should be recognised as a specific “check_method”. NIST has standards for FAR/FRR which may be used as basis for global standards.
Global Recommendation	OIX and others should influence the creation of testing / accuracy standards for: • Document Scanning (with different light options) • Document OCR • Image Capture Liveness • Biometric Image Matching • Biometric Iris Matching • Biometric Fingerprint Matching • Biometric Vein / Vascular Consideration needs to be given to direct issue of Digital Credentials from a government to its citizens – this a proofing standard in itself OIDC for IDA to be extended to support proofing_standard tag. Global definition of proofing standards permitted values required to enable interoperability.
Candidate Global Owner	ISO may be the best candidate organization to take on the creation of individual standards in this area. For the list of values for proofing_standards - OIDF as an evolution of the OIDC for ID Assurance standard. Global Protocol Independent Data Standard.
Trust Framework Recommendation	Align with global standards once available.
Relying Party Approach	Relying party asks for global standards when available.

11.2 Data used to describe and record what proofing check took place.

11.2.1 Check Method for Directly Issued Digitized Credentials

When an authorative source direcly issues a Digitized Credential to a user they have verified as being the correct user to receive such a credential a single check method can capture this:

		Required data items to describe proofing process

Check Method	ID Evidence Validated and Verified	check_method	proofing_standard	agent
Direct Issue	Directly Issued Digitized Credential	Required	Required	Not required

11.2.2 Validation Check Methods

The process of validation is to ensure the ID evidence is genuine. Validation methods will vary based on the evidence type.

The following table maps validation methods to evidence types:

		Required data items to describe proofing process		
Validation Check Method	**ID Evidence Validated**	**check_method**	**proofing_standard**	**agent**
Face to Face – Manual	ID Document with portrait ID Document Document Vouch	Required Required Required	Required Required Required	Required Required Required
Scan – Cryptographically Read	ID Document with portrait ID Document	Required Required	Required Required	Required (could be self)
Scan – with Specialist Scanner (UV/IV)	ID Document with portrait ID Document	Required Required	Required Required	Required
Scan – natural light	ID Document with portrait ID Document	Required Required	Required Required	Required (could be self)
QR Code Read	Documents	Required	Required	
API Call to Authoritative Source	Various Electronic record sources (e.g., Credit Reference Agency, Bank). Digital Vouch with Photo	Required Required	- -	- -

11.2.3 Verification Check Methods

The process of verification is to ensure the person who is being ID proofed is who they are claiming to be. Are they the genuine individual?

This may be done in many ways. It generally involves the cross check of another a piece of ID Evidence that has already been validated:

		Required data items to describe proofing process		
Verification Check Method	**Other Piece of VALIDATED evidence involved**	**check_method**	**proofing_standard**	**agent**
Selfie Cross Match - Person	ID Document with portrait Vouch with photo	Required Required	Required Required	Required Required
Selfie Cross Match - Machine	ID Document with portrait Vouch with photo	Required Required	Required Required	Optional (e.g. machineID)
One Time Codes (OTC)	Mobile Phone, Bank Account.	Required Required	Required Required	- -
Knowledge Based Verification (KBV)	Various Electronic record sources (e.g., Credit Reference Agency, Bank).	Required	Required	
Face to Face	Qualified person cross check of person to ID Document.	Required	Required	Required

11.2.4 Activity History Check Methods

The process of gathering activity history is to obtain evidence that an identity has existed over time. In face-to-face ID proofing this is typically 'Can you provide x months of statements with name and address'

Identities that have forms of evidence that can be validated but have not evidence of activity in the real or virtual world may well be modified or synthetic identities.

The following table lists Activity History types:

		Required data items to describe proofing process		
Activity History Check Method	**ID Evidence record_type used**	**check_method**	**proofing_standard**	**agent**
Face to Face Activity Evidence	From users statements for: Bank and Credit Accounts Utility Accounts Employment Records (payslips)	Required	Required	Required

Electronic Activity Evidence	The users 'data exhaust', such as: Bank or Credit account history Utilities History Social Media usage	Required	Required	-
Vouched Activity	Part of a Vouch where the Voucher attests to having known the user for a period of time.	Required	Required	Required (Voucher)

Different sources of activity will often be given different credence based on the level of ID proofing required to generate activity within that evidence type. For instance, proof of activity from a bank account is usually afforded more credence than proof of activity from utility bills. Whilst activity evidence from an unverified social media account is given less credence still. So, it is important to know the source the evidence.

11.2.5 ID Fraud Check Methods

The ID Fraud checks look for evidence that indicates there is an ID fraud risk associated with the identity. ID Ecosystems have prescribed very different requirements when it comes to looking for ID fraud.

If an identity provider finds sufficient ID fraud risks they will not allow an account to be used, so the purpose of communicating the results of ID Fraud Checks to relying parties is usually to:

- Show the relying party the IdP is carrying out sufficient checks
- Assure the RP that no ID Fraud risk has been found
- If ID Fraud risk has been found, allow the RP to understand they type of risk. This is most important when the ID is being used as an Access Credential to the RPs account.
- Restrict further access

The following table lists typical ID Fraud checks:

		Required data items to describe proofing process		
ID Fraud Check Method	**Fraud Risk Assessed**	**check_method**	**proofing_standard**	**agent**
Known Fraud	Information about this ID is recorded on a database of	Required	Required	-

	known ID fraud information.			
PEP Check	The person is politically exposed and so at greater risk of fraud	Required	Required	-
Mortality	The Person is deceased and so should not be transacting.	Required	Required	-

11.2.6 Recommendations - Data used to describe and record what proofing check took place

Item	Data used to describe and record what proofing check took place
Any Standards?	OIDC for IDA provides the framework to communicate check methods but it does not define values for this on a global basis.
Global Recommendation	OIDC for IDA is extended to have tags for proofing_standard and agent. To achieve interoperability across trust frameworks the consistent description of check methods and proofing standards will be required. OIX is exploring this as part of its work on Global Interoperability.
Candidate Global Owner	OIX will make recommendations as part of its work on Global Interoperability.
Trust Framework Recommendation	Align with global standards once available.
Relying Party Approach	Relying party asks for global standards when available.

12 ID Assurance

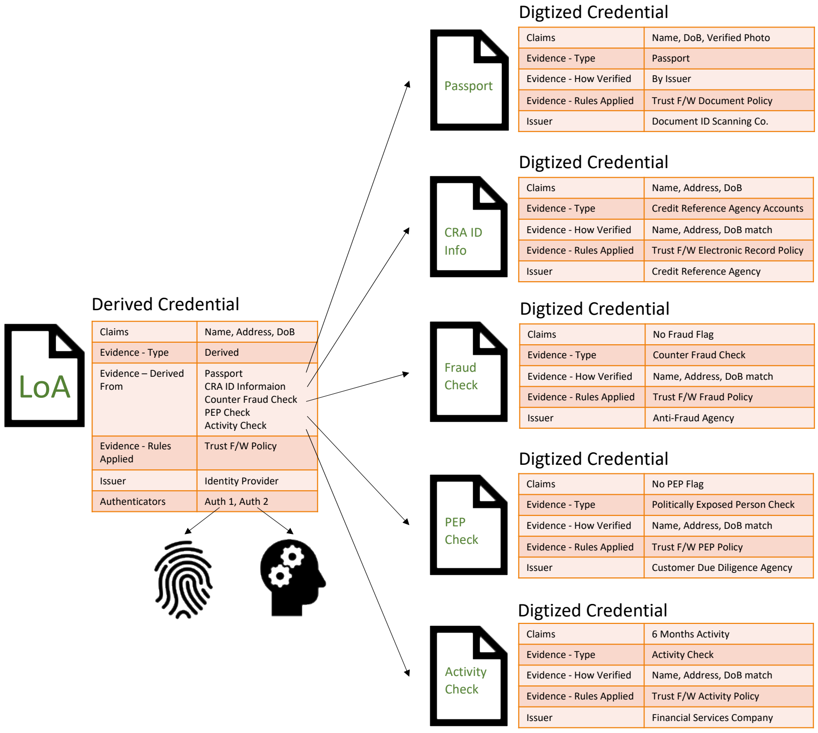
Many trust frameworks define levels of assurance – pre-defined levels of trust that allow the relying party to know how well proofed and authenticated the person presenting credentials is.

Examples of trust frameworks that operate levels of assurance are:

- eIDAS (low, substantial, high)
- NIST (IAL1, IAL2, IAL3)
- UK DIATF (Low, Medium, High)
- Singapore (1, 2, 3, 4).
- Australia (IL1, IL1+, IL2, IL2+, IL3, IL4)

When a level of assurance is derived it may be important to know and record which evidence was used.

The following diagram shows how a Level of Assurance credential might point back to the evidence from which has been derived:



Derived Credential

Claims	Name, Address, DoB
Evidence - Type	Derived
Evidence – Derived From	Passport CRA ID Informaion Counter Fraud Check PEP Check Activity Check
Evidence - Rules Applied	Trust F/W Policy
Issuer	Identity Provider
Authenticators	Auth 1, Auth 2

Digtized Credential

Claims	Name, DoB, Verified Photo
Evidence - Type	Passport
Evidence - How Verified	By Issuer
Evidence - Rules Applied	Trust F/W Document Policy
Issuer	Document ID Scanning Co.

Digtized Credential

Claims	Name, Address, DoB
Evidence - Type	Credit Reference Agency Accounts
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W Electronic Record Policy
Issuer	Credit Reference Agency

Digtized Credential

Claims	No Fraud Flag
Evidence - Type	Counter Fraud Check
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W Fraud Policy
Issuer	Anti-Fraud Agency

Digtized Credential

Claims	No PEP Flag
Evidence - Type	Politically Exposed Person Check
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W PEP Policy
Issuer	Customer Due Diligence Agency

Digtized Credential

Claims	6 Months Activity
Evidence - Type	Activity Check
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W Activity Policy
Issuer	Financial Services Company

It may be that the evidence used needs to be shared with the relying party, or the relying party my simply take the level of assurance achieved “on trust” as a product of the trust framework. In any event, the meaning of the level of assurance needs to be understood by the relying party.

Each trust framework will define its own levels of assurance, leveraging national or supra-national standards where appropriate. It is not expected in the short to medium term that trust frameworks will align on common levels of assurance; each trust framework is designed to reflect the risk conditions and appetite of its implementation domain. Each trust framework’s Assurance Policies will allocate different level of trust to different credentials. What is required is a method to show how a trust framework’s required levels of assurance have been achieved from the credentials used as evidence.

To allow understanding how ID assurance level has been achieved a 6-level structure is supported as part of the OIDC for ID Assurance profile:

- Trust Framework – The Trust Framework defining the level of assurance
- Assurance Level – The level of assurance achieved
- Assurance Process – how the level of assurance was achieved.
- Assurance Policy – which assurance policy was applied,
- Assurance Procedure – which procedure within the assurance policy was followed.

- Assurance Details – which pieces of evidence were used to achieve the level of assurance, along with the score achieved in the assurance policy procedure by each piece of evidence, broken down into assurance elements of Validation, Activity, ID Fraud and Verification.

OIX is undertaking a separate piece of work in its Global Interoperability Working Group that is exploring how several trust frameworks from around the globe can leverage this construct to map how to use credentials proofed to recognised standards to meet their assurance policy. The use of a common terms to describe the proofing processes undertaken – check_methods. – along with commonly recognised standards to which proofing has been undertaken will be vital to the success of this.

Recommendation in this area:

Item	Assurance Policy
Any Standards?	OIDC for IDA provides the framework to communicate how an assurance policy has been met.
Global Recommendation	OIDC for IDA assurance process is used to describe how assurance policies have been achieved. Using the OIDC for IDA assurance process construct to describe how assurance policies have been met will be tested through of OIX Global Interoperability working group. A new assurance policy process description standard may be required, which may be part of the work that comes out of the OIX global interoperability work.
Candidate Global Owner	OIDF
Trust Framework Recommendation	Leverage OIDC for IDA assurance policy construct and possible OIX extension to express assurance levels and how they are achieved.
Relying Party Approach	Leverage OIDC for IDA assurance policy construct and possible OIX extension to express assurance levels and how they are achieved.

13 Common Content Data, Different Protocol Envelopes

At the start of this paper we made it clear that in this work we are focussed on common data content, regardless of the way the data is passed from party to party.

PROTOCOL ENVELOPE
CONTENT

Different protocols for data communication should leverage the same format for data content. This will mean that:

- If protocol translation is required, the data integrity can be assured as it does not need to be transformed as part of the protocol translation.
- As protocols evolve, the data they communicate remains constant. Issuers and Relying Parties may need, or choose, to move to a new protocol, but the data they provide or receive does not change.

In DIDCOMM this content data would be in the body, in a Verifiable Credential it would be in the credential_subject or evidence elements, in OIDC for Identity Assurance IDA it would be within the verified claims element of an id_token or userinfo response.

Recommendation in this area:

Item	Protocol Independent Data Standards
Any Standards?	OIDC for IDA provides a basis for a protocol independent data standard.
Global Recommendation	A protocol Independent Data Standard is created. Protocol creators adopt this Protocol Independent Data Standard. Other recommendations within the paper can be brought together as part of this standard.
Candidate Global Owner	OIDF with an evolution of the OIDC for ID Assurance standard.
Trust Framework Recommendation	Select protocols that support protocol independent data standards
Relying Party Approach	Only choose protocols that support protocol independent data standards.

14 Summary of Recommendations

This paper makes a great many recommendations in the sphere of data standards, which are summarised in the table below:

Item	Recommendation	Recommended Standard
Key Recommendation		
Protocol Independent Data Standard	To bring all the recommendations in this document together into a single new Protocol Independent Data Standard is created. This can be evolved from OIDC4IDA.	New standard evolved from OIDC for Identity Assurance (OIDC4IDA)
General Recommendations		
Trust Framework Policy Communication	An Open Policy Rules Exchange Framework is defined that allows trust frameworks to publish which standards they have adopted.	A new policy description standard is required, which is part of the work global interoperability work at OIX
Per-Claim level of trust	All claims have "unverified" / "verified" meta-data. Claim level of assurance should be supported.	New Standard - Part of Global Protocol Independent Data Standard
Claim Period of Validity and Context Type	Global standard for how these are expressed is created. Global "starter" permitted values are created for some common context types (e.g., Previous Address). Trust frameworks should adopt and extend as required.	New Standard - Part of Global Protocol Independent Data Standard
Core ID Claims		
Name and Address	Local standards represent local convention and ensure local quality; global standardisation to a common format is not recommended. A structured global name and address schema is created to allow cross mapping of local standards.	New ISO Standard for translation from framework to framework.
Date of Birth	ISO-8601 is used	ISO-8601
Nationalities	Adopt ICAO standard	ICAO
Contact Phones an Emails	Existing global standards are used	ITU-T E164, RFC 5322
Personal Identifiers	A new global standard is required. ISO 24366 is completed	ISO 24366
Evidence, Proofing and Assurance		
ID Evidence and ID Assurance data framework	OIDC4IDA evolved into Protocol Independent Data Standard	Evolved Standard
ID Evidence – National IDs	Adopt ICAO standards that are leveraged by the EU for National IDs	ICAO 9303
ID Evidence - Passport	Adopt ICAO standards for Digital Travel Credentials	ICAO 9303
ID Evidence – Driving Licence	Adopt ISO standards for mDL	ISO 18013-5

ID Evidence – Electronic Records and Vouching	Adopt OIDC4IDA	OIDC4IDA
ID Proofing – Proofing Standards	To allow trust frameworks to adopt consistent robust procedures standards for should be created for: • Document Scanning (with different light options) • Document OCR • Image Capture Liveness • Biometric Image Matching • Biometric Iris Matching • Biometric Fingerprint Matching • Biometric Vein / Vascular	ISO should consider new standards in this area.
ID Proofing – Describing the proofing process	OIDC4IDA check methods construct is used. Tags are added for proofing_standard and agent To achieve interoperability across trust frameworks the consistent description of check methods and proofing standards will be required. OIX is exploring this as part of its work on Global Interoperability.	OIDC4IDA New Standard and register for values. Part of Global Protocol Independent Data Standard.
ID Assurance	OIDC for IDA assurance process is used to describe how assurance policies have been achieved along with OIX extension to express assurance levels and how they are achieved.	OIDC4IDA A new policy description standard is required, which is part of the work global interoperability work at OIX.

15 Action Plan

OIX, though it's Data Standards working group, will now take the following actions to drive forward the recommendations in this paper:

1. Validate the need for the Global Protocol Independent Data Standard with Trust Frameworks, OIX members and government stakeholders
2. Determine who should own, create and govern the Global Protocol Independent Data Standard.
3. Influence ISO to:
    a. Create a new structured global name and address schema is created to allow cross mapping of local standards.
    b. A new global standard for communication of personal identifiers is required based on the recommendations in this paper. ISO 24366 is completed
    c. Allow for consistent robust ID Proofing by creating new standards for:
        - Document Scanning (with different light options)
        - Document OCR
        - Image Capture Liveness
        - Biometric Image Matching

- Biometric Iris Matching
- Biometric Fingerprint Matching
- Biometric Vein / Vascular