OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Protocol Independent Standards for Data Interoperability

Nick Mothershaw
Chief Identity Strategist

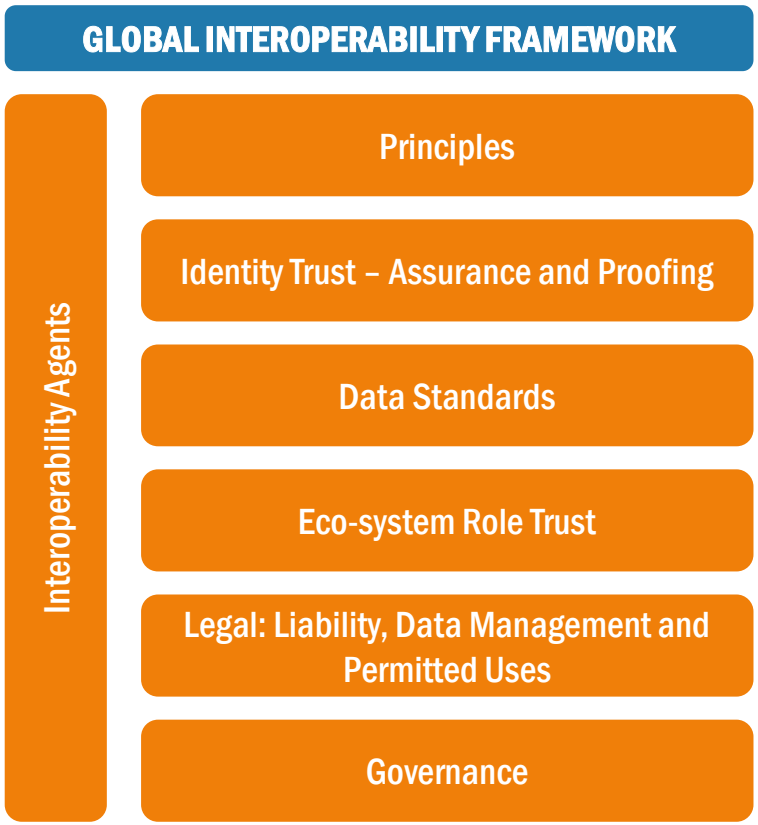
OIX Architecture Interoperability Working Group

Exploring two questions:

- Can we define a common Data Schema for ”Core ID Information?
- Can it work for both Verifiable Credentials and OIDC for ID Assurance?

Working Group members include:
Barclays, Deloitte, Lexis Nexis, Microsoft, NatWest, Sopra Steria, Consult Hyperian, Digtal Identity Net, Hooyu, ID Crowd, YOTI, UK government.

GAIN - Global Interoperability Framework



The output of this working group will feed into the work OIX is doing in Trust Frameworks as part of the GAIN initiative

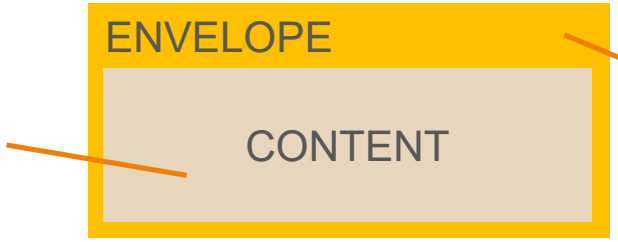
OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Common Data Schema

Common Data Schema

- **Can we define a common Data Schema for ”Core ID Information?**



- Can it work for both Verifiable Credentials and OIDC for ID Assurance?

Claims and Evidence:

- Consistent naming: e.g. first name, last name, address fields, DoB, etc.
- Consistent typology: e.g. types, method for proofing
- Consistent communication **of metadata**
- Consistent communication **of levels of assurance**

What is “Core ID Information”

IN SCOPE

	Claims	Evidence	Proofing	Assurance
CORE ID INFORMATION	Core ID Claims • Name • Address • DoB • Nationalities • Contact Details • Personal Identifiers	ID Documents • Passport • National ID • Driving License Electronic Records • CRA Check • Bank Account • 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
ELIGIBILITY	Eligibility Claims • Right to Work • Right to Rent • Driving Permissions • Travel VISA • Education Records • COVID Safe • Right to Vote • Bank Account Transactions (Open Banking)	ID Documents • Passport • National ID • Driving License Electronic Records • COVID Test • COVID Vaccine • CRA Check • Bank Account • Electoral Roll • Right to Work / Reside lists		•

Standards for “Core ID Information”, in the context of ID Ecosystems

Naming: a mixed bag of standards!

Naming: New standards in OIDC for ID Assurancev

	Claims	Evidence	Proofing	Assurance
CORE ID INFORMATION	Core ID Claims • Name • Address • DoB • Nationalities • Contact Details • 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, ESTC stsnards

Assurance Process: Similar Approaches Across trust frameworks,

Name

Any Standards?	Recommendation	Users can have more than one?	Example Types	Recommendation on Types	Has Periods of Validity?	Recommendation on Periods of Validity
ICAO for passport. ISO for mDL.	A **Global** Extensible structured name schema is defined.	Yes	Current Previous Professional	**Global** values are set for Types. Collisions are not allowed. Trust Frameworks may define their own values.	Yes	**Global** standard of From and To dates is adopted by all Trust Frameworks

Titles and Salutations may be excluded from any Global standards and be left to Trust Frameworks. Where these form part of a legal name, translation into global standard should be implemented by trust frameworks.

Address

Any Standards?	Recommendation	Users can have more than one?	Example Types	Recommendation on Types	Has Periods of Validity?	Recommendation on Periods of Validity
Many ISO19160-6 defines global standards for address presentation.	**Trust Frameworks define which locally available standard is adopted for address format** to meet highest possible address quality for that locale. Interoperability through ISO19160-6 is being explored further by the working group.	Yes	Home Second Home Correspondence	**Global** values are set for Types?	Yes	**Global** standard of From and To dates is adopted by all Trust Frameworks

Date of Birth

Any Standards?	Recommendation	Users can have more than one?	Example Types	Recommendation on Types	Has Periods of Validity?	Recommendation on Periods of Validity
	Calendar Date at place of birth is used.	No		Not required	No	

Nationalities

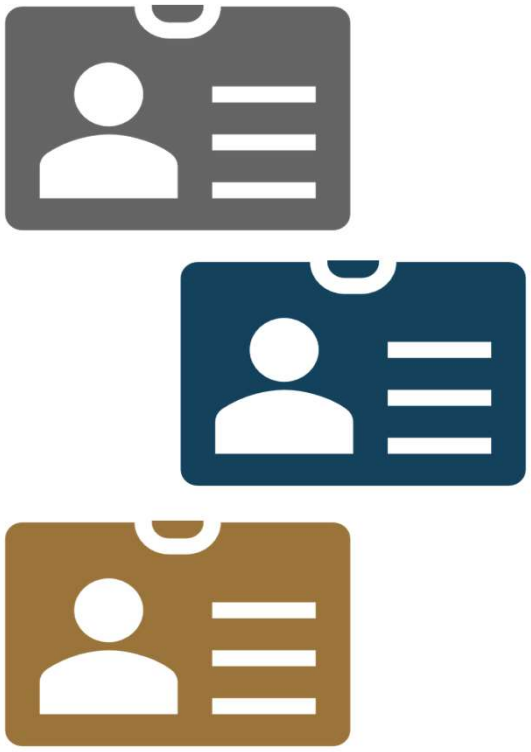
Any Standards?	Recommendation	Users can have more than one?	Example Types	Recommendation on Types	Has Periods of Validity?	Recommendation on Periods of Validity
ICAO ISO	**ICAO standard is used** as passports are the primary cross border from of identification.	Yes		**ICAO standard codes are adopted**	Yes - Sometimes	**Frameworks** may choose to adopt From / To dates

Personal Identifiers

Any Standards?	Recommendation	Users can have more than one?	Example Types	Recommendation on Types	Has Periods of Validity?	Recommendation on Periods of Validity
Personal Identifiers	Various, usually from issuer on the number	**Global** approach to use Type-Value pairs. (e.g. SSN:1234567890)	Yes	National ID # SSN NINO	**Frameworks** define **Types.** I**ssuers** define **Value** formats.	Yes – sometimes

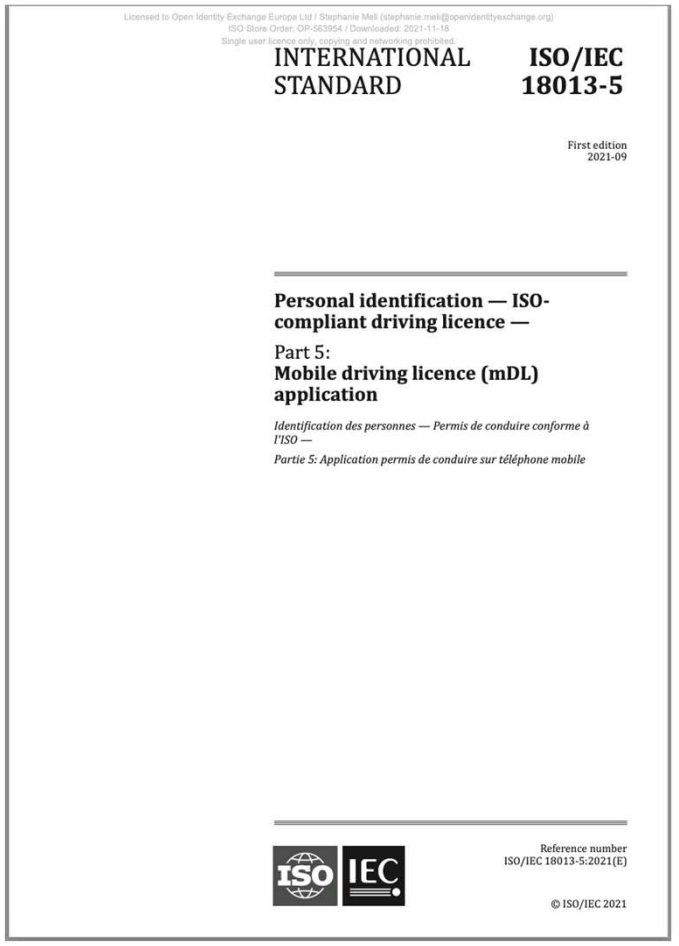
Evidence – ID Documents

National ID Card – Local Standards



Passport – ICAO Standard

Driving License – ISO mDL Standard



INTERNATIONAL STANDARD

ISO/IEC 18013-5

First edition
2021-09

Personal identification — ISO-compliant driving licence —

Part 5:
Mobile driving licence (mDL) application

Identification des personnes — Permis de conduire conforme à l'ISO —

Partie 5: Application permis de conduire sur téléphone mobile

Reference number
ISO/IEC 18013-5:2021(E)

Evidence – Electronic Evidence and Vouches

Electronic Records
- CRA Check
- Bank Account
- Electoral Roll
- Fraud Check
- Mortality
- etc.

Field
type
positive_negative
result
source
personal_number
created_at
date_of_expiry
date_last_updated

Vouches
- Via Digital ID
- Face to Face

Field
type
positive_negative
voucher_declaration
occupation
organisation
reference_number
voucher_given_name
voucher_family_name
voucher_birth_date
voucher_address
date_of_issuance
date_of_expiry
vouch_document_image
vouchee_photo

Recommendation:

New **Global** Standards / Registry should be set for:
- Field naming (see tables)
- Record and Vouch type values

Proofing

Proofing Type	check_method	Proofing Process Standard
Direct Issue	direct_issued	
Validation	Face to Face – Manual	
	Scan – Crypto	Local
	Scan – with Specialist Scanner	Local
	Scan – Natutral Light	Some emerging standards
	QR Code Read	
	API Call	
Verification	Selfie Cross Matches – Person	Global Border Standards
	Selfie Cross Matches - Machine	Some liveness and FP/PN rate standards
	One Time Codes (OTC)	
	Knowledge Based Verification (KBV)	
	Face to Face	
Activity	Face to Face Activity Evidence	
	Electronic Activity Evidence - API	
	Vouched Activity	
ID Fraud	Any ID Fraud Check	

Recommendation:
New **Global** Standards/ Registry should be set for:

- Check Method **values**

OIX Global Interoperability working group is exploring proofing process standards. Can these be globalized?

Assurance Process

Trust Framework	Assurance Level	Assurance Policy	Assurance Procedure	Assurance Elements and Scores
eIDAS	Low Substantial High	ETSI TS 119 461 V1.1.1		Validation>8.2.3+8.2.4>Passport Verification>8.4.4>Selfie
NIST	IAL1 IAL2 IAL3			
UK	Low Medium High Very High	GPG45	M2B	Validation>3:3>Passport Validation>3:2>Driving Licence Activity>3>CRA Verification>3>Selfie
DIACC	1 2 3			
TDIF	Basic – IL1 Basic – IL1+ Standard – IL2 Standard –IL2+ Strong – IL3 Very String – IL4			
SingPass	Claim level assurance: '1' - Government-Originated '2' - User provided '3' - Field is Not Applicable to Person '4' - Verified by SingPass			

Recommendation:

- New **Global** Standards should be set for **describing** the Assurance Process **based on the OIDF OIDC for ID Assurance**

Further work on Trust Framework assurance level interoperability will be undertaken by OIX Global Interoperability Working Group

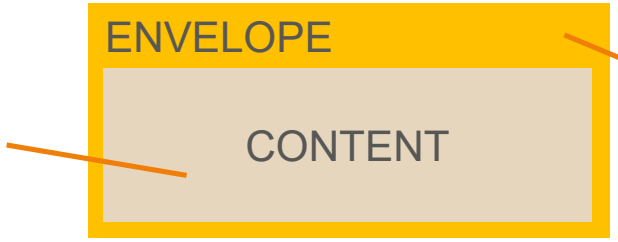
OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Working Across Protocols

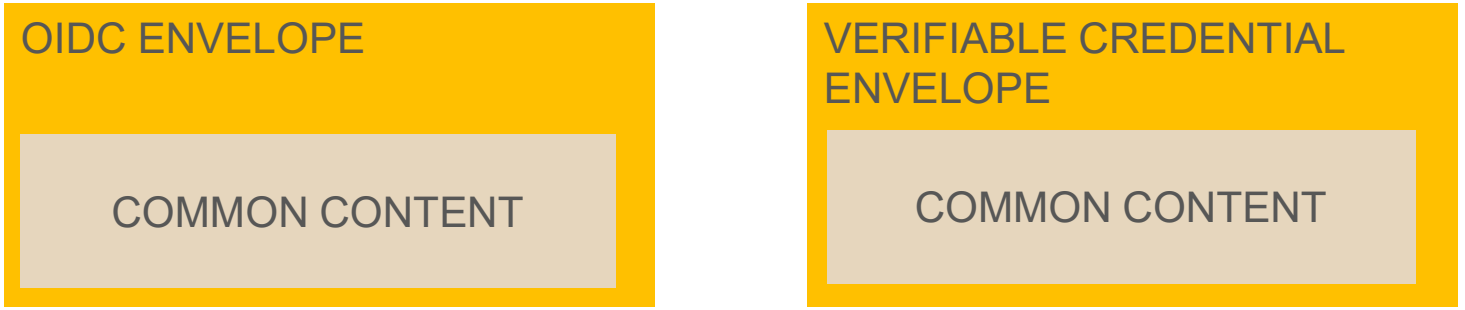
Common content for different protocols

- Can we define a common Data Schema for ”Core ID Information?

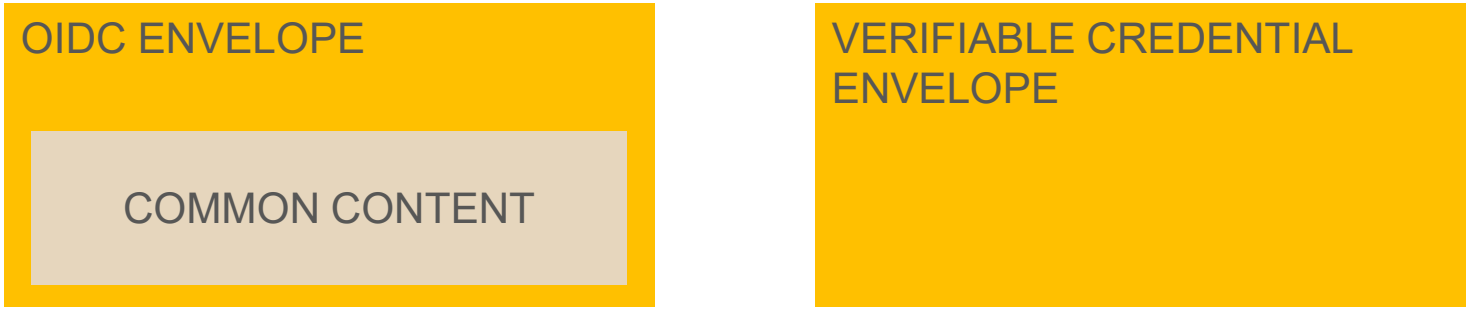


- **Can it work for both Verifiable Credentials and OIDC for ID Assurance?**

Common content for different protocols



Common content for different protocols



OIDC for ID Assurance

COMMON CONTENT


```
{
  "iss": "https://server.example.com",
  "sub": "24400320",
  "aud": "s6BhdRkqt3",
  "nonce": "n-0S6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970,
  "auth_time": 1311280969,
  "acr": "urn:mace:incommon:iap:silver",
  "email": "janedoe@example.com",
  "preferred_username": "j.doe",
  "picture": "http://example.com/janedoe/me.jpg",
  "verified_claims": {
    "verification": {
      "trust_framework": "de_aml",
      "time": "2012-04-23T18:25Z",
      "verification_process": "f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
      "evidence": [
        {
          "type": "document",
          "method": "pipp",
          "time": "2012-04-22T11:30Z",
          "document_details": {
            "type": "idcard",
            "issuer": {
              "name": "Stadt Augsburg",
              "country": "DE"
            },
            "document_number": "53554554",
            "date_of_issuance": "2010-03-23",
            "date_of_expiry": "2020-03-22"
          }
        }
      ]
    },
    "claims": {
      "given_name": "Max",
      "family_name": "Meier",
      "birthdate": "1956-01-28"
    }
  }
}
```

Verifiable Credentials

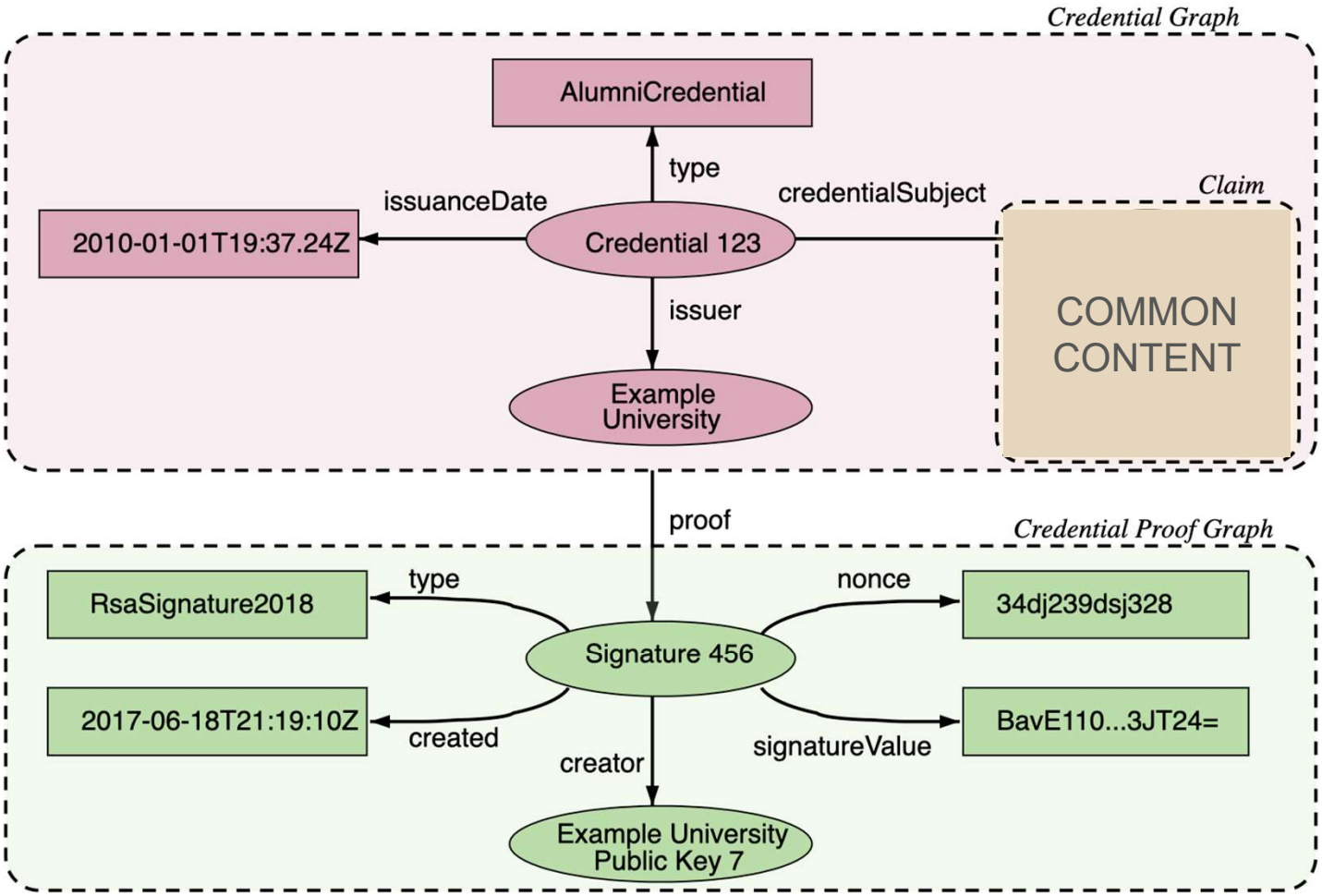


Figure 6 Information graphs associated with a basic verifiable credential.

Verifiable Credential

The Verifiable Credential subject contains the verified_claims object

COMMON CONTENT


```
{
  "NewKey": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://example.edu/credentials/3732",
    "type": [
      "VerifiableCredential",
      "UniversityDegreeCredential"
    ],
    "issuer": {
      "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
      "name": "Example University"
    },
    "issuanceDate": "2010-01-01T19:23:24Z",
    "credentialSubject": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "verified_claims": {
        "verification": {
          "trust_framework": "de_aml",
          "time": "2012-04-23T18:25Z",
          "verification_process": "f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
          "evidence": [
            {
              "type": "id_document",
              "method": "pipp",
              "time": "2012-04-22T11:30Z",
              "document": {
                "type": "idcard",
                "issuer": {
                  "name": "Stadt Augsburg",
                  "country": "DE"
                },
                "number": "53554554",
                "date_of_issuance": "2010-03-23",
                "date_of_expiry": "2020-03-22"
              }
            }
          ]
        },
        "claims": {
          "given_name": "Max",
          "family_name": "Meier",
          "birthdate": "1956-01-28"
        }
      }
    }
  }
}
```

OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Summary

Summary of likely Data Standards Recommendations

We are exploring two questions:

- Can we define a common Data Schema for ”Core ID Information? – YES, we must
  - Global Standards are required for
    - Attribute Naming
    - Names – A global extensible structured name schema is defined
    - Addresses translation. Actual Address standards are local - for data quality purposes
    - Values for types for names, addresses, contact details
    - Values for proofing check methods
    - Common method to describe Assurance Processes
  - Global standards for proofing processes for key proofing check methods will help enable cross trust framework Digital ID interoperability
  - Governance is required for these schema standards at a global level, in liaison with Trust Framework around the world.
- Can it work for both Verifiable Credentials and OIDC for ID Assurance? - YES

OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Thank you!

nick.mothershaw@openidentityexchange.org