Identity Assurance

with OpenID Connect

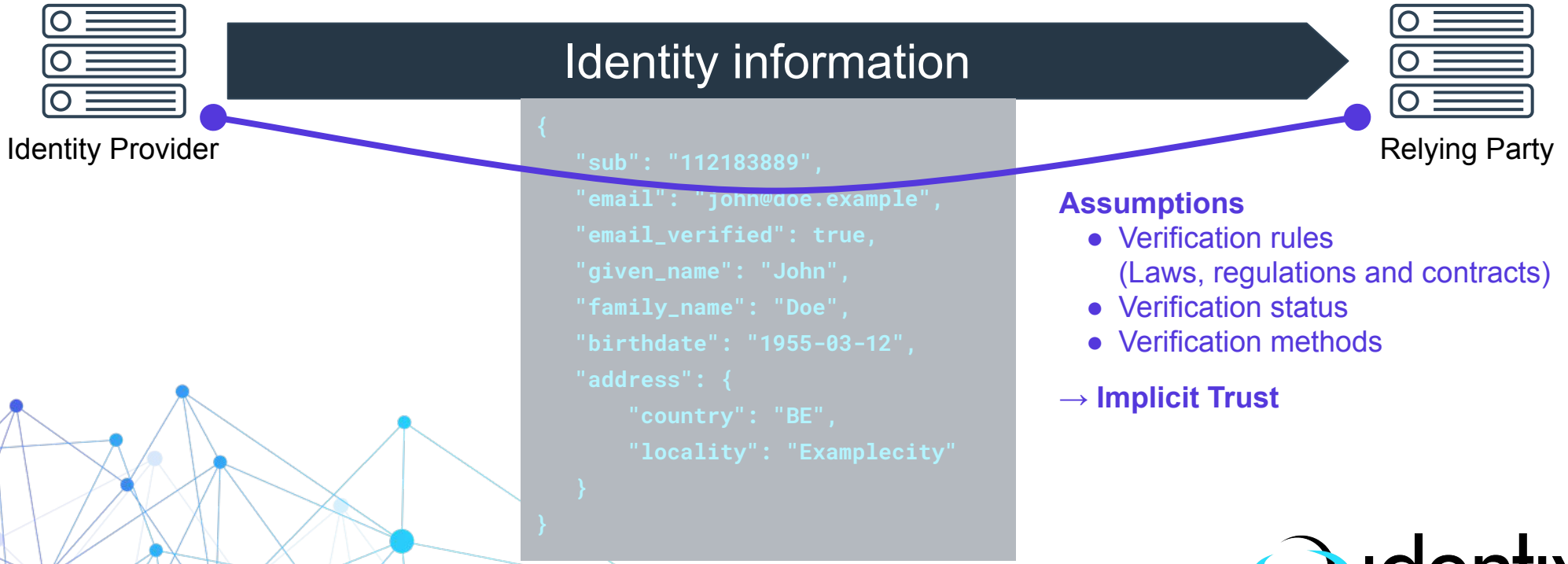
Dr. Daniel Fett

identiverse® 2020

What is this about?

identiverse® 2020

OpenID



Assumptions

- Verification rules
  (Laws, regulations and contracts)
- Verification status
- Verification methods

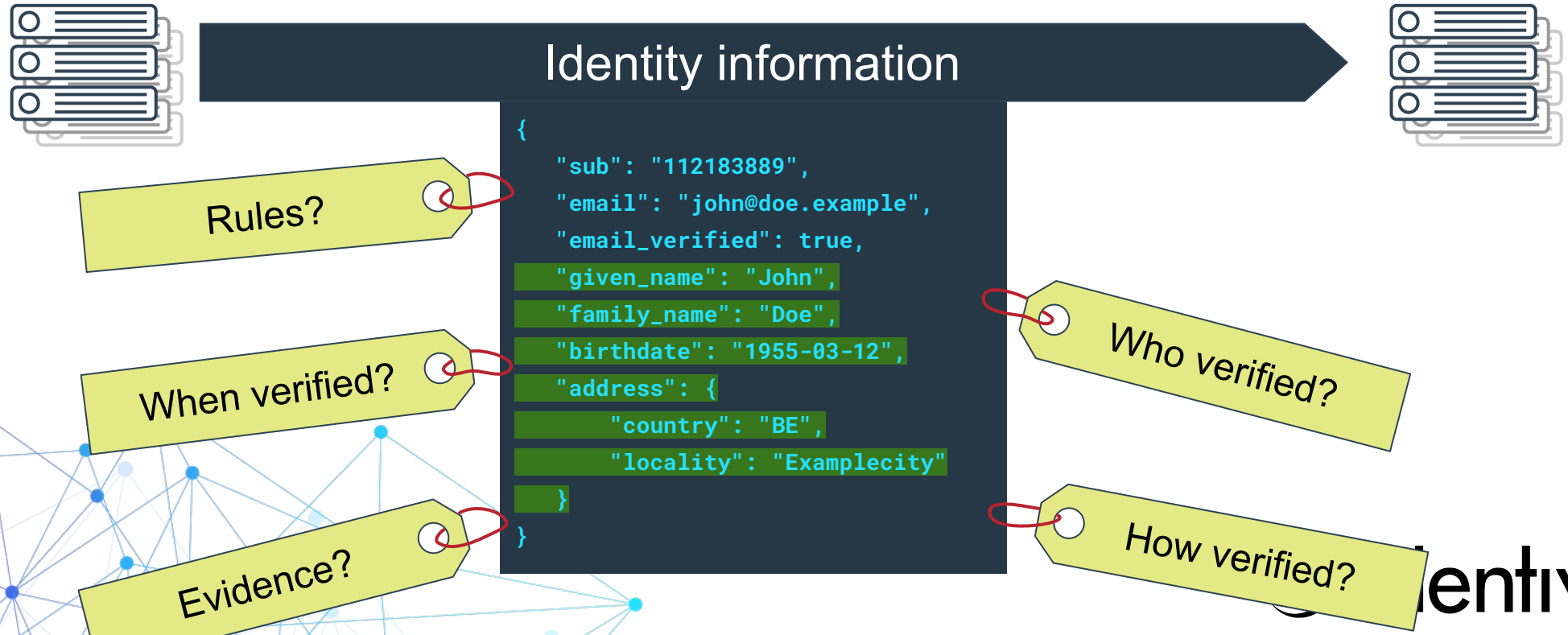
→ **Implicit Trust**

Dr. Daniel Fett

identiverse® 2020

OpenID

- eGovernment
- Anti Money Laundering
- Telecommunications
- Health Data
- Fraud Prevention
- Risk Mitigation



OpenID Connect for Identity Assurance

- Under development at the OpenID Foundation
- Representation for verified claims and verification information
- Enables
  - mapping between regulatory and legal contexts
  - dispute resolution
  - auditing

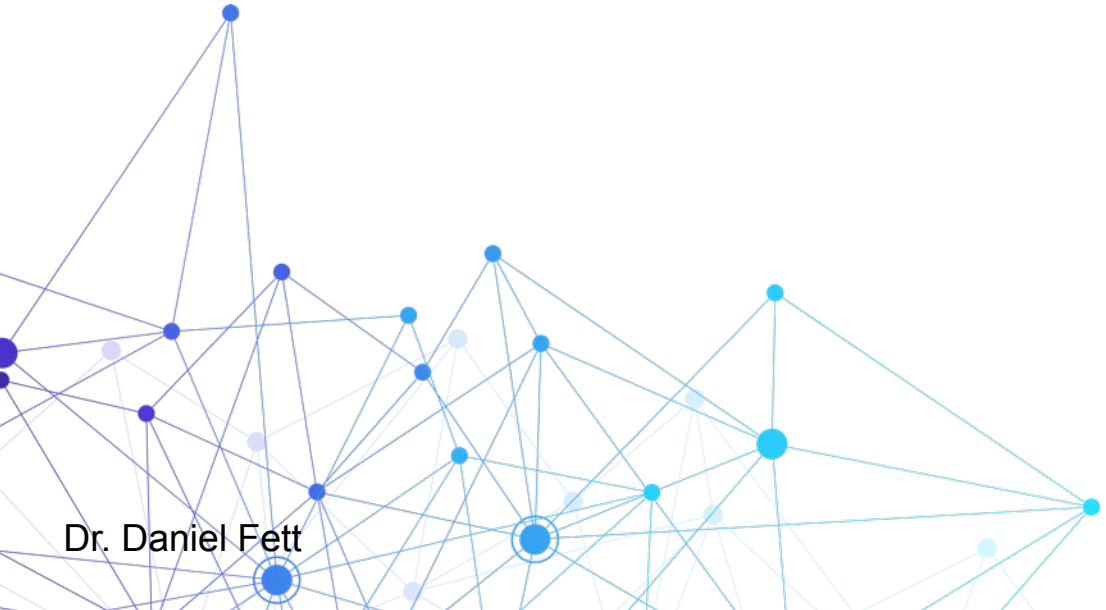
Dr. Daniel Fett

Main Concepts

identiverse® 2020

Concept 1: Explicitness

- Explicit Attestation of
  - Trust Framework the IDP complies with
  - Time of verification
  - Verifying party
  - Evidence used in the process
  - Verification method: how the evidence was verified



Response

```
"verification": {
    "trust_framework": "de_aml",
    "time": "2012-04-23T18:25Z",
    "verification_process": "f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
    "evidence": [
        {
            "type": "id_document",
            "method": "pipp",
            "verifier": {
                "organization": "Deutsche Post",
                "txn": "1aa05779-0775-470f-a5c4-9f1f5e56cf06"
            },
            "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"
            }
        }
    ]
},
```

German Anti-Money Laundering Law

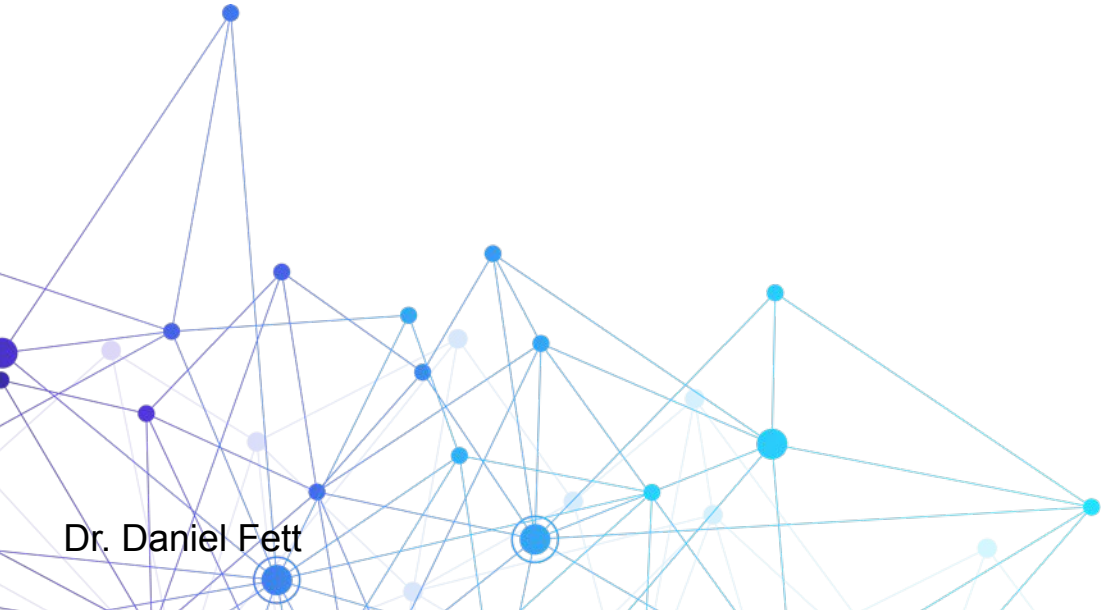
Physical In-Person Proofing

External verifier on behalf of the IDP

Proofing via ID Card

Concept 2: Clarity

- Clear distinction between claims with and without attestation
- Can be used together with existing OpenID Connect Claims
- Separate data structure for verification data



Response

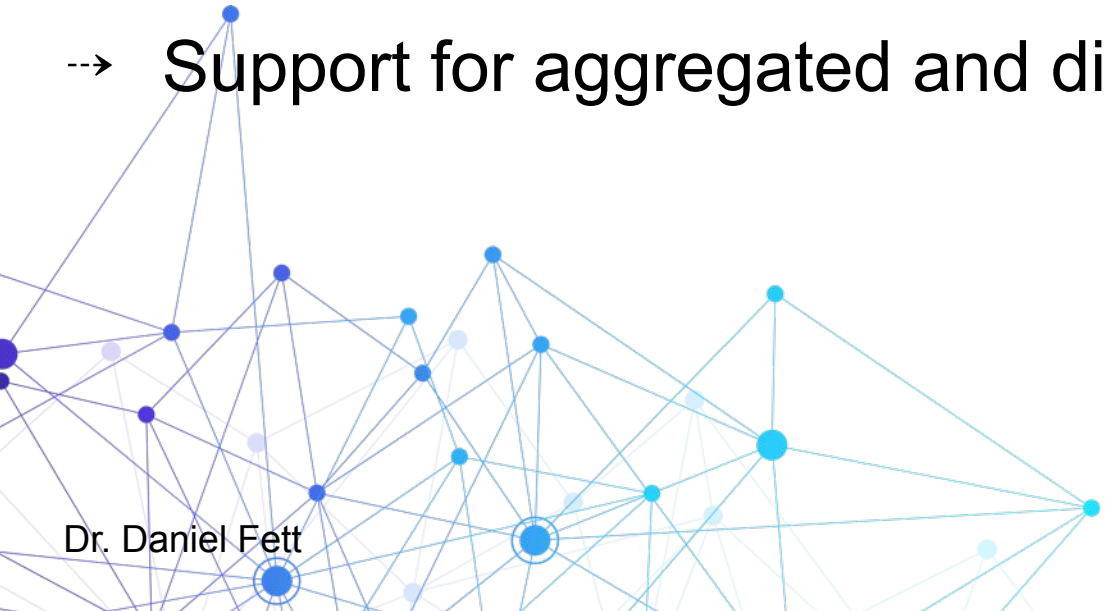
```
{
    "sub": "24400320",
    "email": "janedoe@example.com",
    "preferred_username": "j.doe",
    "picture": "http://example.com/janedoe/me.jpg",
    "verified_claims": {
        "verification": {
            "trust_framework": "de_aml",
            "time": "2012-04-23T18:25Z",
            "verification_process": "f24c6f4ec597",
            "evidence": ...
        },
        "claims": {
            "given_name": "Max",
            "family_name": "Meier",
            "birthdate": "1956-01-28"
        }
    }
}
```

Standard OpenID Connect Claims

Verified Claims data structure

Concept 3: Versatility

- Representation suitable for various channels
  - ID Token
  - Userinfo-Endpoint
  - Access Tokens
  - Token Introspection Responses
- Support for verified data sets with different metadata
- Support for aggregated and distributed claims



Response


```
{
   "sub": "24400320",
   "email": "janedoe@example.com",
   "preferred_username": "j.doe",
   "picture": "http://example.com/janedoe/me.jpg",
   "verified_claims": [
       {
           "verification": {
               "trust_framework": "eidas_ial_substantial"
           },
           "claims": {
               "given_name": "Max",
               "family_name": "Meier",
               "birthdate": "1956-01-28",
           }
       },
       {
           "verification": {
               "trust_framework": "de_aml"
           },
           "claims": {
               "address": {
                   "locality": "Maxstadt",
                   "postal_code": "12344",
                   "country": "DE",
                   "street_address": "An der Sandd&#252;ne 22"
               }
           }
       }
   ]
}
```


First set of verified Claims

Second set of verified Claims

Response


```
{
   "iss": "https://self-issued.me",
   "sub": "248289761001",
   "preferred_username": "superman445",
   "_claim_names": {
       "verified_claims": [
           "src1",
           "src2"
       ]
   },
   "_claim_sources": {
       "src1": {
           "JWT": "eyJhbGciOiJSUzI1NiIsImtpZCI6IkpXVC59.eyJpc3MiOiJodHRw
     ovL3NlcnZlci5vdGhlcm9wLmNvbSIsInN1YiI6ImU4MTQ4NjAzLTg5MzQtNDI0N
     SO4MjViLWMxMDhiOGI2YjkONSIsInZlcmlmaWVkX2NsYWltcyI6eyJ2ZXJpZmlj
     YXRpb24iOnsidHJ1c3RfZnJhbWV3b3JrIjoiaWFsX2V4YW1wbGVfZ29sZCJ9LCJ
     jbGFpbXMiOnsiZ2l2ZW5fbmFtZSI6Ik1heCIsImZhbWlseV9uYW1lIjoiTWVpZX
     IiLCJiaXJ0aGRhdGUiOiIxOTU2LTAxLTI4In19fQ.FArlPUtUVn95HCExePlWJQ
     6ctVfVpQyeSbe3xkH9MH1QJjnk5GVbBW0qe1b7R3lE-8iVv__0mhRTUI5lcFhLj
     oGjDS8zgWSarVsEEjwBK7WD3r9cEw6ZAhfEkhHL9eqAaED2rhhDbHD5dZWXkJCu
     XIcn65g6rryiBanxlXK0ZmcK4fD9HV9MFduk0LRG_p4yocMaFvVkqawat5NV9QQ
     3ij7UBr3G7A4FojcKEkoJKScdGoozir8m5XD83Sn45_79nCcgWSnCX2QTukL8Ny
     wIItu_K48cjHiAGXXSzydDm_ccGCe0sY-Ai2-iFFuQo2PtfuK2SqPPmAZJxEFrF
     oLY4g"
       },
       "src2": {
           "endpoint": "https://op.mymno.com/claim_source",
           "access_token": "ksj3n283dkeafb76cdef"
       }
   }
}
```


Multiple verified Claims sets

Aggregated Claim


```
{
  "iss": "https://otherop.com",
  "sub": "e814864108b8b6b45...",
  "verified_claims": {
     "verification": {
       "trust_framework": "example"
     },
     "claims": {
       "given_name": "Max",
       "family_name": "Meier",
       "birthdate": "1956-01-28"
     }
  }
}
```

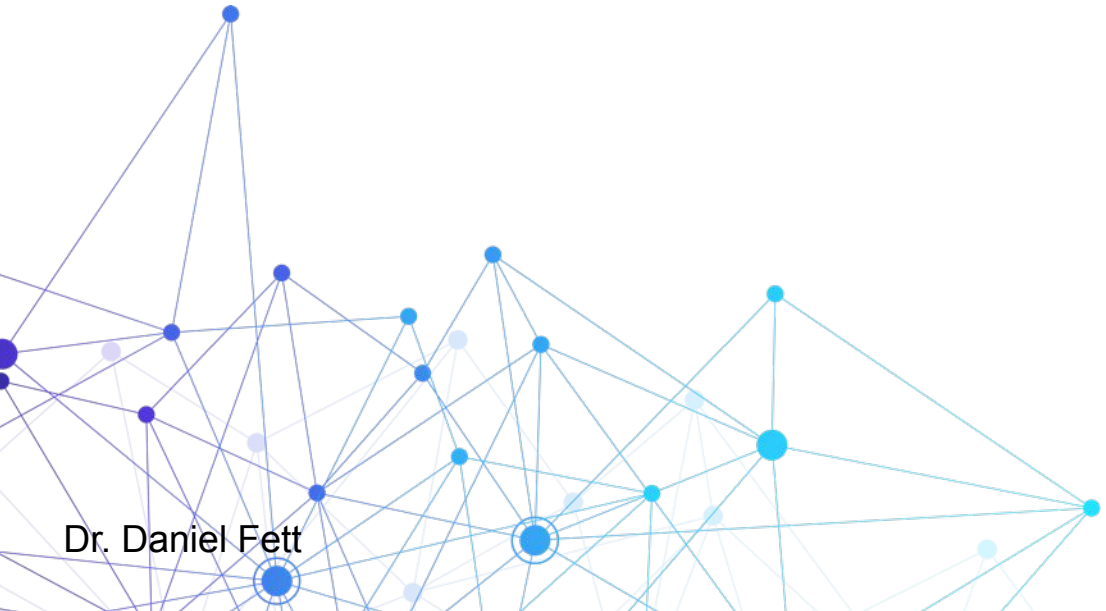

Distributed Claim

Requesting Identity Information

Dr. Daniel Fett

Concept 4: Preservation of Privacy

- Relying party can express fine-grained data requests
- Asks for individual Claims and verification data elements
- Purpose of request can be conveyed
  (per transaction or individual claim)



Request

```
{
   "userinfo": {
       "verified_claims": {
           "verification": {
               "trust_framework": {
                   "value": "eidas_ial_substantial"
               },
               "time": null,
               "evidence": [
                   {
                       "type": {
                           "value": "id_document"
                       },
                       "method": null,
                       "document": {
                           "type": null
                       }
                   }
               ]
           },
           "claims": {
               "given_name": null,
               "family_name": null,
               "birthdate": null
           }
       }
   }
}
```

Required trust framework

Evidence type: ID document

Requested Claims

What else?

identiverse® 2020

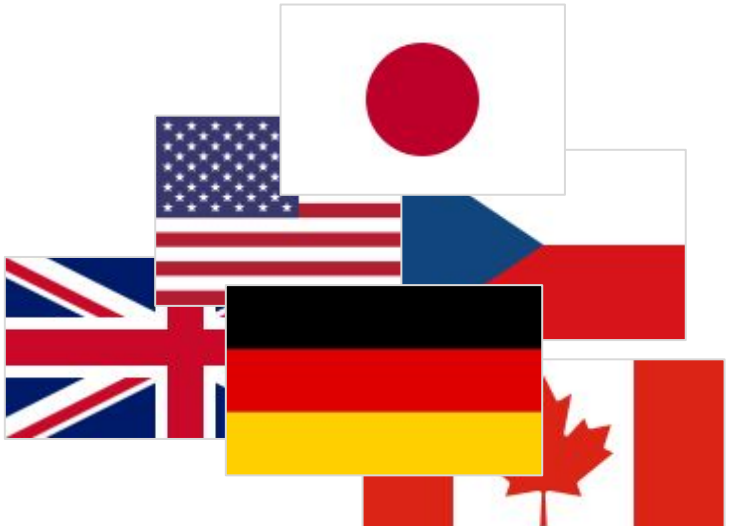
International Standard

- Identifiers for…

Trust Frameworks	Identity Documents	Verification Methods
eIDAS & NIST 800-63A	ID Card & Passport	Physical In-Person Proofing
Japanese & German AML	Driver's License	Supervised remote In-Person Proofing
…	…	…

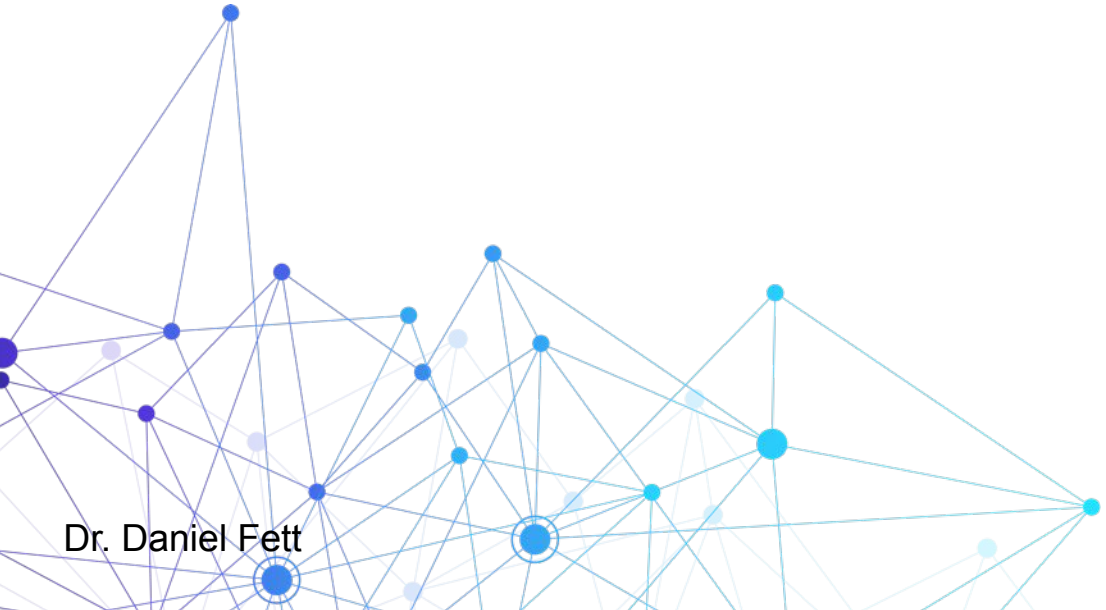
Full list: https://bitbucket.org/openid/ekyc-ida/wiki/identifiers

- Extensible
- Contributions welcome!



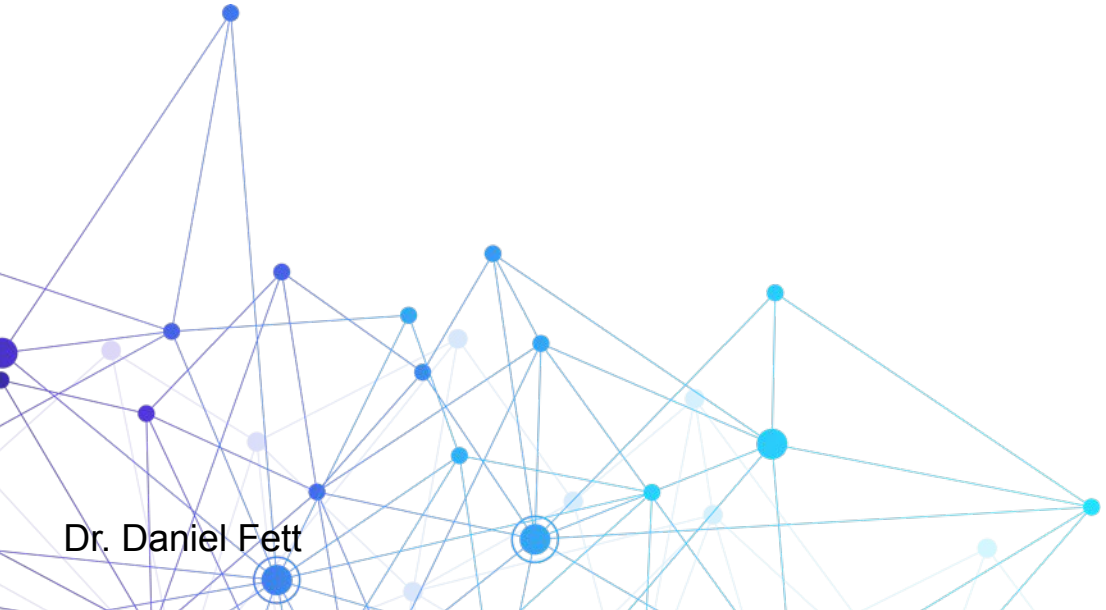
Current Status

- 2nd Implementer's Draft just approved
- Several implementations
  - Connect2ID
  - Authlete
  - id4me
  - yes®



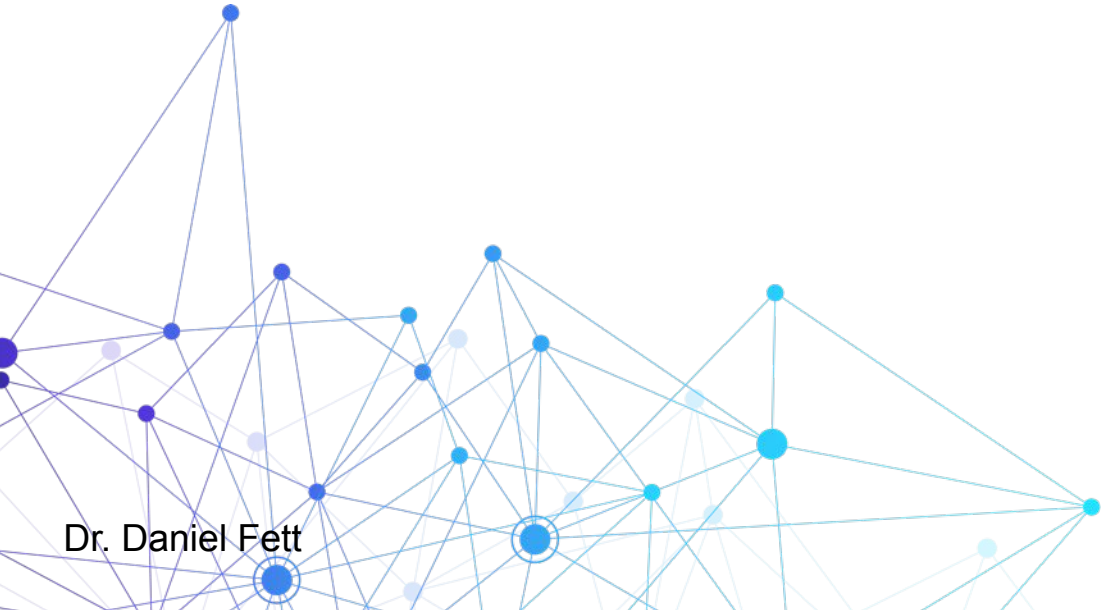
Development

- JSON Schema for Requests and Responses
- Simplified syntax since 2nd Implementer's Draft
- IANA registry entries for new claims (JWT Claims Registry)



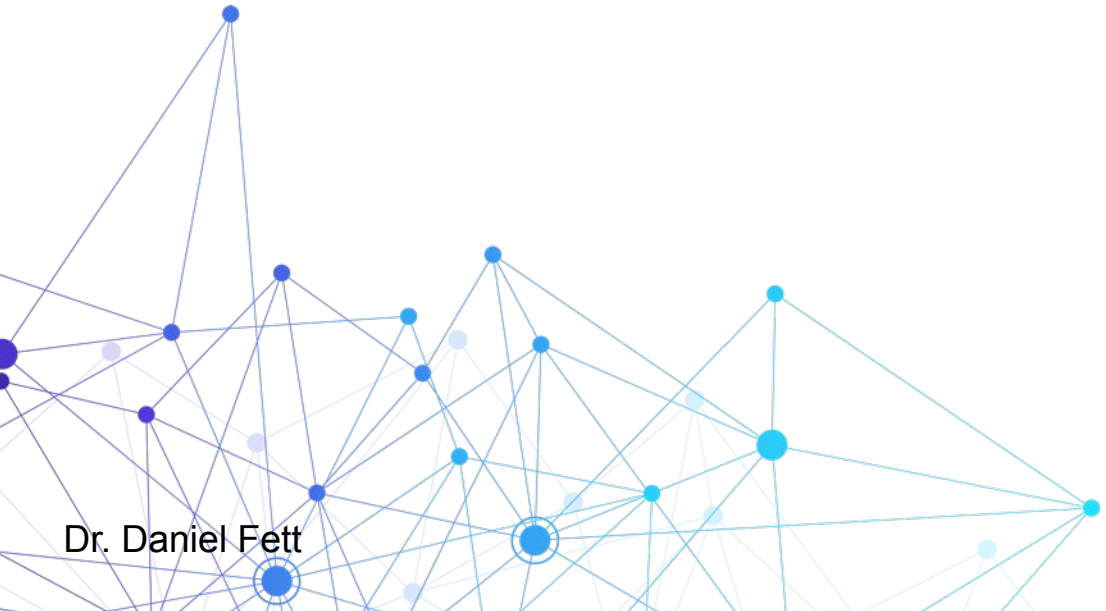
Outlook (1)

- Conformance Tests
- New Claims
  - e.g., age verifications
- Expression Language



Outlook (2)

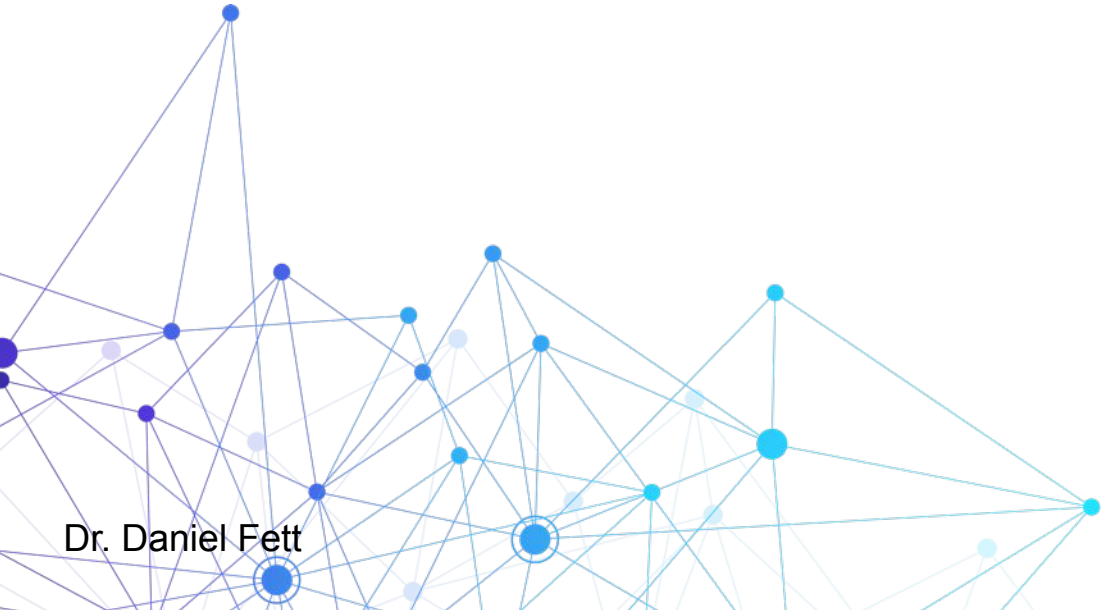
- Work with potential adopters
  - TISA
  - European Commission
  - ETSi
- Support for Legal Entities



Summary

- Versatile representation for verified data and verification metadata
- Explicit, privacy preserving attestation
- Clear query syntax, standardized identifiers

Open development: https://openid.net/wg/ekyc-ida/



Thank you!

Dr. Daniel Fett, yes.com
Twitter: @dfett42
https://yes.com

identiverse® 2020