go.eIDAS

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Contribution for ETSI ESI#85

Barcelona, February 4th-6th 2025

Towards the common Certificate Policy for Wallet-Relying Party Access Certificates

Dr. Detlef Hühnlein

EUDI Wallet-Relying Parties

(Art. 5b of (EU) No. 910/2014)

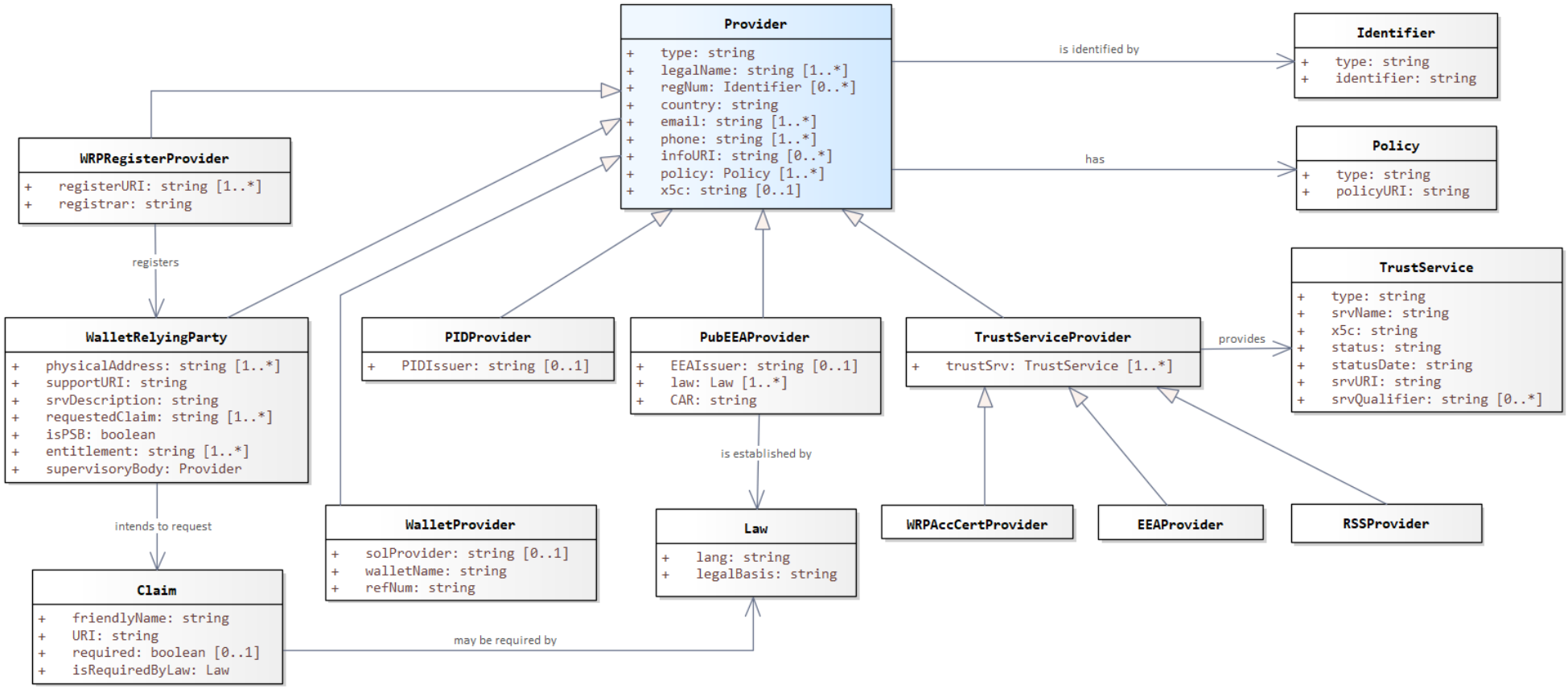
- (1) Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.
- (2) The registration process shall be **cost-effective** and **proportionate-to-risk**. The relying party shall provide at least:
  . (a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes:
    (i) the Member State in which the relying party is established; and
    (ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record;
  (b) the contact details of the relying party;
  (c) the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.
- (3) Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).
- (4) Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.
- (5) Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing
- (6) Relying parties registered in accordance with this Article shall inform Member States without delay about any changes to the information provided in the registration pursuant to paragraph 2.
- (7) Member States shall provide a **common mechanism for allowing the identification and authentication of relying parties**, as referred to in Article 5a(5), point (c).
- (8) Where **relying parties** intend to rely upon European Digital Identity Wallets, they shall **identify themselves to the user.**
- (9) Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.
- (10) Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction

Definitions
(Art. 2 of (EU) 2024/2980)

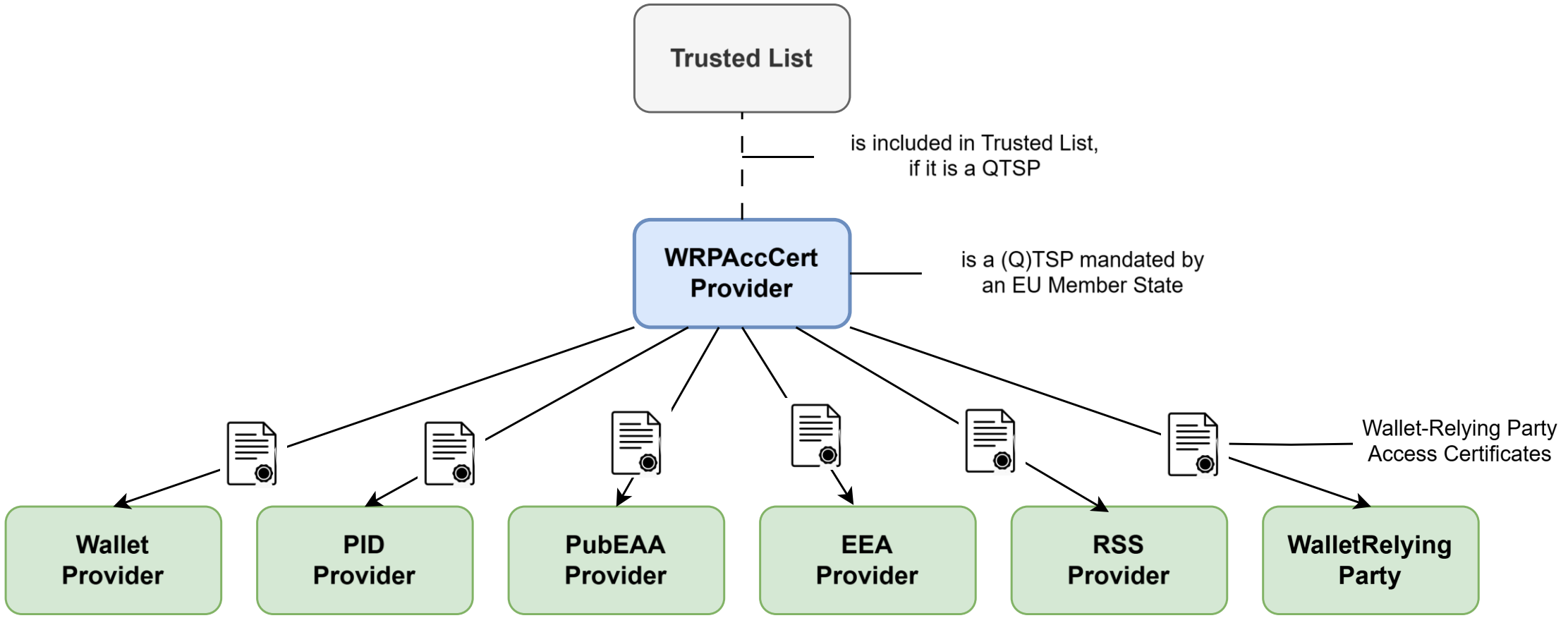
- (1) '**wallet provider**' means a natural or legal person who provides wallet solutions;
- (2) '**provider of person identification data**' means a natural or legal person responsible for issuing and revoking the person identification data and ensuring that the person identification data of a user is cryptographically bound to a wallet unit;
- (3) '**wallet-relying party**' means a relying party that intends to rely upon wallet units for the provision of public or private services by means of digital interaction;
- (4) '**register of wallet-relying parties**' means an electronic register used by a Member State to make information on wallet-relying parties registered in that Member State publicly available as set out in Article 5b(5) of Regulation (EU) No 910/2014;
- (5) '**registrar of wallet-relying parties**' means the body responsible for establishing and maintaining the list of registered wallet-relying parties established in their territory who has been designated by a Member State;
- […]
- (13) '**provider of wallet-relying party access certificates**' means a natural or legal person mandated by a Member State to issue relying party access certificates to wallet-relying parties registered in that Member State;
- (14) '**wallet-relying party access certificate**' means a certificate for electronic seals or signatures authenticating and validating the wallet-relying party issued by a provider of wallet-relying party access certificates.

Providers are Wallet-Relying Parties

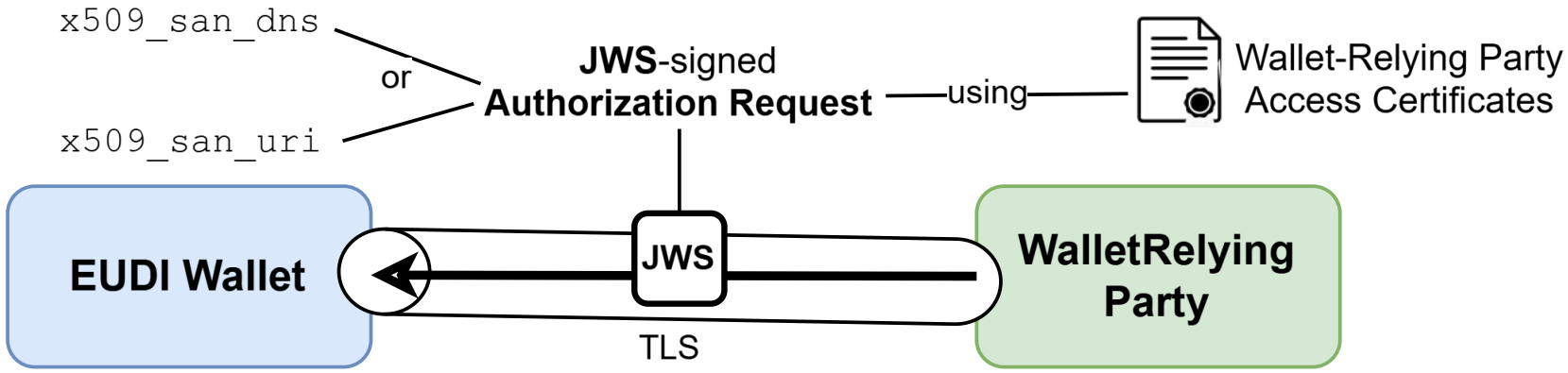
Name: EUDI-Providers
Package: EUDI-Framework
Version: Draft for Discussion at ESI#85
Author: Dr. Detlef Hühnlein



The Wallet-Relying Party Access Certificate PKI



Wallet-Relying Party Authentication



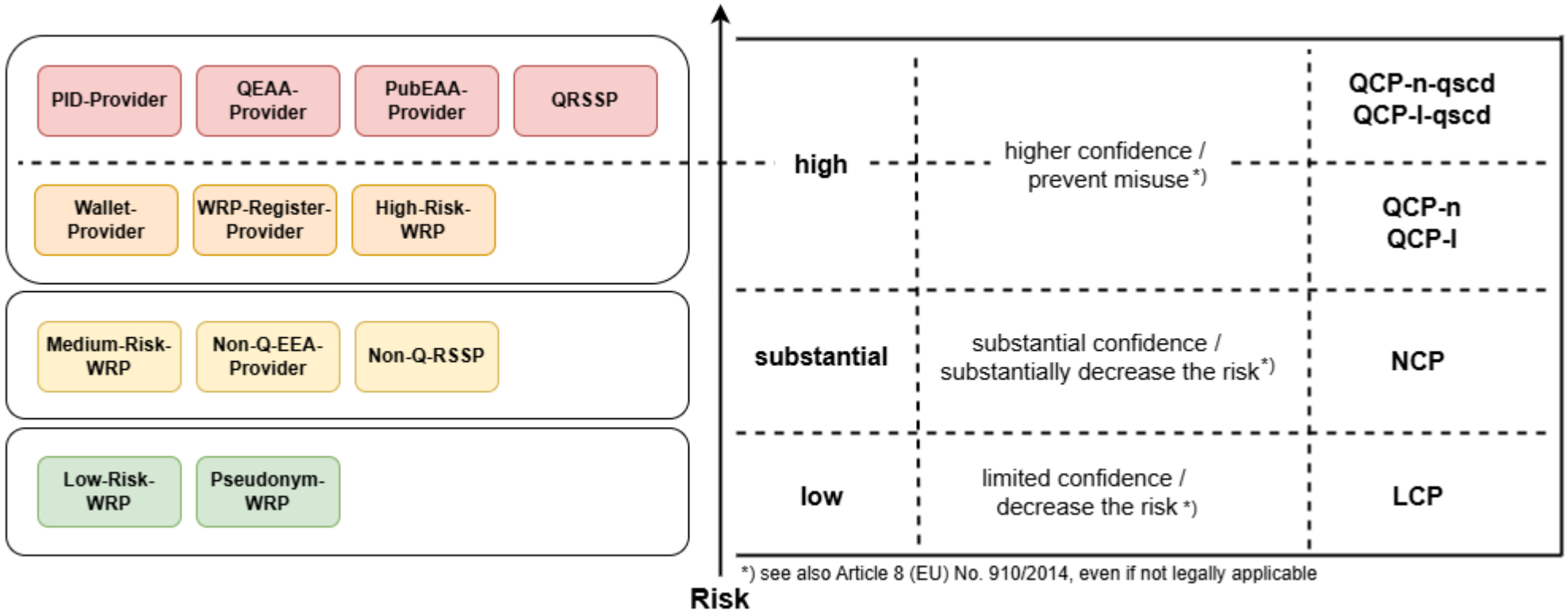
https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

x509_san_dns / x509_san_uri

- `x509_san_dns`: When the Client Identifier Scheme is `x509_san_dns`, the Client Identifier MUST be a DNS name and match a `dNSName` Subject Alternative Name (SAN) [RFC5280] entry in the leaf certificate passed with the request. The request MUST be signed with the private key corresponding to the public key in the leaf X.509 certificate of the certificate chain added to the request in the `x5c` JOSE header [RFC7515] of the signed request object. The Wallet MUST validate the signature and the trust chain of the X.509 certificate. All Verifier metadata other than the public key MUST be obtained from the `client_metadata` parameter. If the Wallet can establish trust in the Client Identifier authenticated through the certificate, e.g. because the Client Identifier is contained in a list of trusted Client Identifiers, it may allow the client to freely choose the `redirect_uri` value. If not, the FQDN of the `redirect_uri` value MUST match the Client Identifier without the prefix `x509_san_dns:`. Example Client Identifier: `x509_san_dns:client.example.org`.
- `x509_san_uri`: When the Client Identifier Scheme is `x509_san_uri`, the Client Identifier MUST be a URI and match a `uniformResourceIdentifier` Subject Alternative Name (SAN) [RFC5280] entry in the leaf certificate passed with the request. The request MUST be signed with the private key corresponding to the public key in the leaf X.509 certificate of the certificate chain added to the request in the `x5c` JOSE header [RFC7515] of the signed request object. The Wallet MUST validate the signature and the trust chain of the X.509 certificate. All Verifier metadata other than the public key MUST be obtained from the `client_metadata` parameter. If the Wallet can establish trust in the Client Identifier authenticated through the certificate, e.g., because the Client Identifier is contained in a list of trusted Client Identifiers, it may allow the client to freely choose the `redirect_uri` value. If not, the `redirect_uri` value MUST match the Client Identifier without the prefix `x509_san_uri:`. Example Client Identifier: `x509_san_uri:https://client.example.org/cb`.

https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-client-identifier-scheme-an

Towards a common Certificate Policy, which is *proportionate-to-risk*



ETSI EN 319 411-2

ETSI EN 319 411-1

Example: QcPSB for PubEEA

```
QcPSB ::= SEQUENCE {
    country PrintableString (SIZE (2))
         (CONSTRAINED BY { -- ISO 3166 alpha-2 codes only -- }),
        -- this field shall contain the alpha-2 country code of the legislation framework of public sector body
        -- in the case of EU legislation use the "EU" country-code.
    actingOnBehalfOf ::= GeneralNames OPTIONAL,
       -- this field shall be present, if and only if the certificate acts on behalf an authentic source
    legalName UTF8String,
       -- this field is for the unique identification of authentic source
    laws Laws
}
```

with

```
Laws ::= SEQUENCE SIZE (1..MAX) OF Law
Law ::= SEQUENCE {
    lang PrintableString (SIZE(2)), --ISO 639-1 language code
      -- the language (code) of the legislation description
    legalBasis UTF8String
     -- the legislation name in the language set,
     -- at minimum the english (en) translation of the legistlation's name shall be included
}
```

NOTE: The attribute `actingOnBehalfOf` has been inspired both by the somewhat similar `issuedOnBehalfOf` certificate extension defined in clause 17.5.2.6 of X.509 [REF-X509] and the `Procuration` attribute defined in Table 29a of ISIS-MTT [REF-ISIS-MTT].

[REF-509] https://www.itu.int/rec/T-REC-X.509-201910-I/en
[REF-ISIS-MTT] https://www.teletrust.de/fileadmin/files/ISIS-MTT_Core_Specification_v1.1.pdf

Thank you very much for your kind attention!

Are there any open questions?

Contact