IGTF
Interoperable Global Trust Federation
AP | EU | TAG

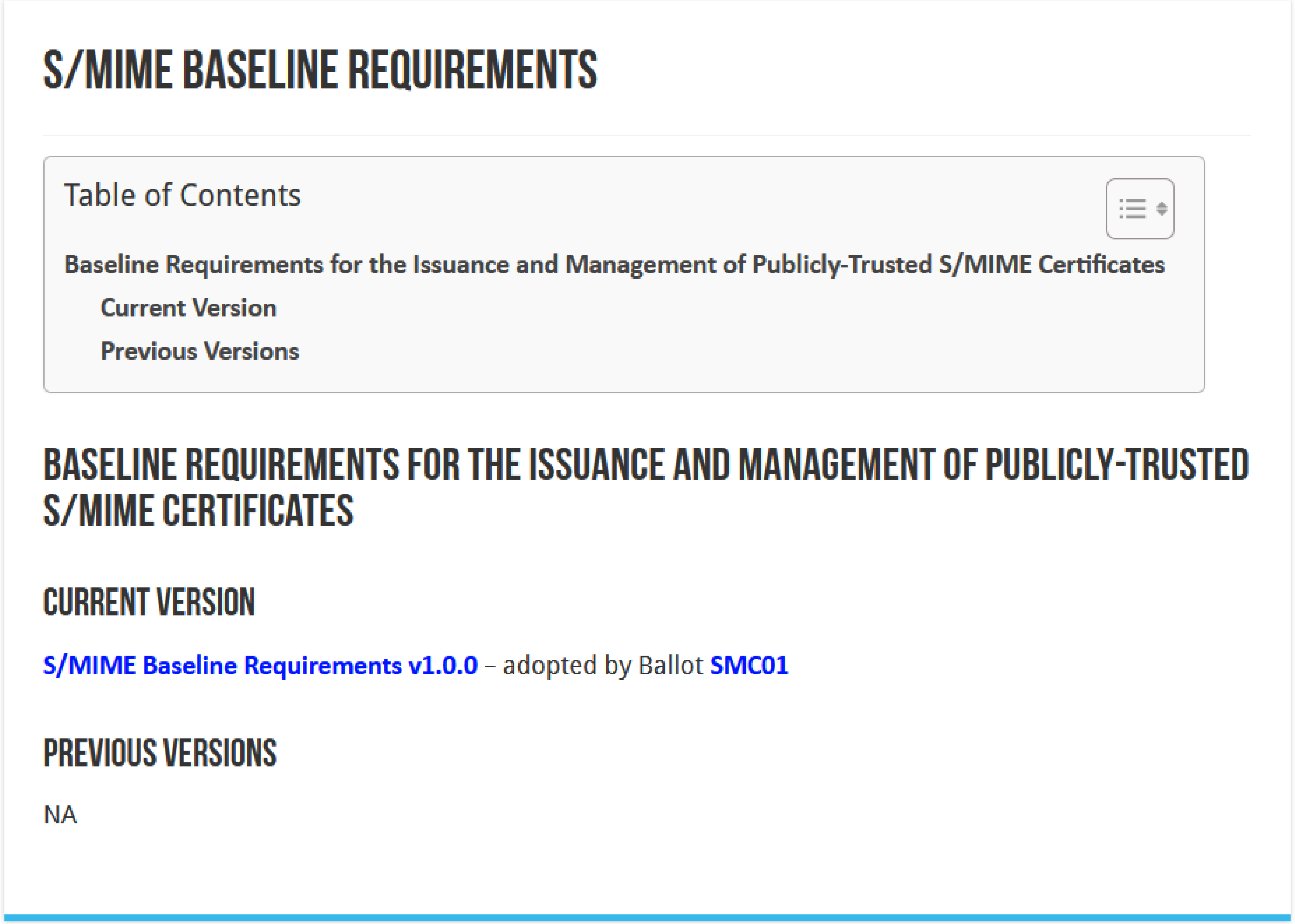
eugridpma

S/MIME and authentication with the SMIME WG BRs

February 2023

David Groep
Nikhef
Maastricht University

CA/BROWSER Forum



S/MIME BASELINE REQUIREMENTS

Table of Contents

BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED S/MIME CERTIFICATES

CURRENT VERSION

S/MIME Baseline Requirements v1.0.0 – adopted by Ballot SMC01

PREVIOUS VERSIONS

NA

Public Trust S/MIME (personal) is getting regulated

- It was basically a ‘free-for-all’, as long as the email address worked
- most ‘useful use’ for the general public signing was in bespoke certificates types (Adobe) or in Qualified Certificates (EC regulated)

- until now, the IGTF personal requirements were much stricter than ‘public’ email signing, in that we did insist on a reasonable name and a ‘sponsor’ (organization) that was validated
- Now CA/BF is putting requirements on S/MIME for the first time

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-SMIMEBR-1.0.0.pdf

Different ‘profiles’ and validations

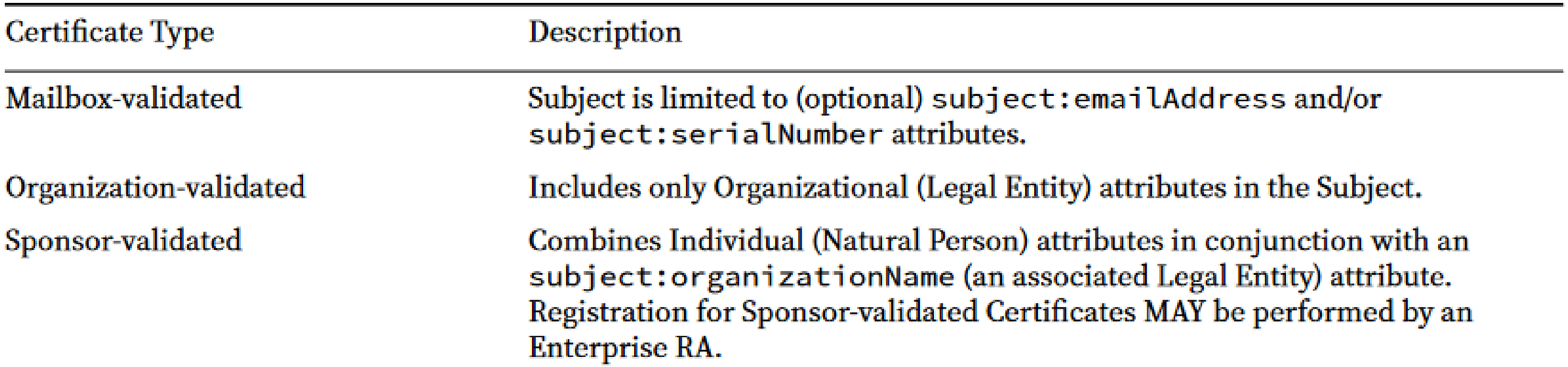
- **Strict**
  - 825-days (2yr), limited RDN attributes allowed
  - intended only for S/MIME
- **Multi-purpose**
  - 825 days (2yr), slightly more eKUs allowed
  - crossover use cases between document signing and secure erossover use cases between document signing and secure emailmail
- **Legacy**
  - 1185 days (3yr)
  - transitional profile (likely to be phased out in the end)
  - bit more freedom in subject, but not much more than MP

- **mailbox-validated**
  - just the rfc822name (only!)
- **organization-validated**
  - includes only Organizational (Legal Entity) attributes in the Subject
- **sponsor-validated**
  - Combines Individual (Natural Person) attributes and organizationName (associated Legal Entity) attribute
- **individual-validated**
  - Includes only Individual (Natural Person) attributes in the Subject

Sponsor validated

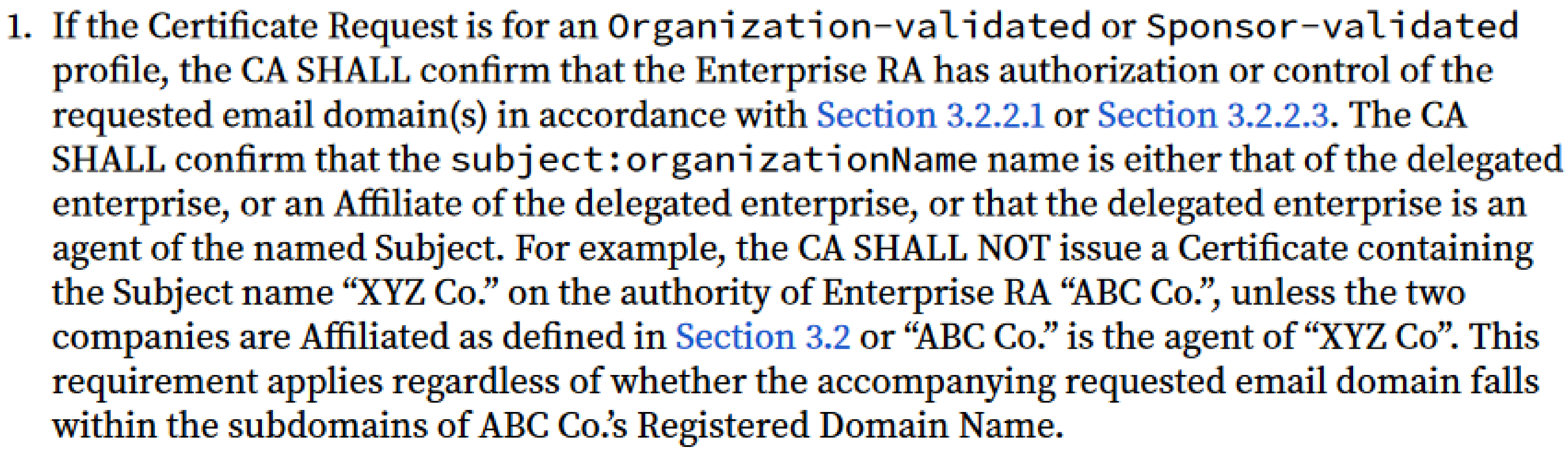
Sponsor-validated:

Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the subject:organizationName is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization.

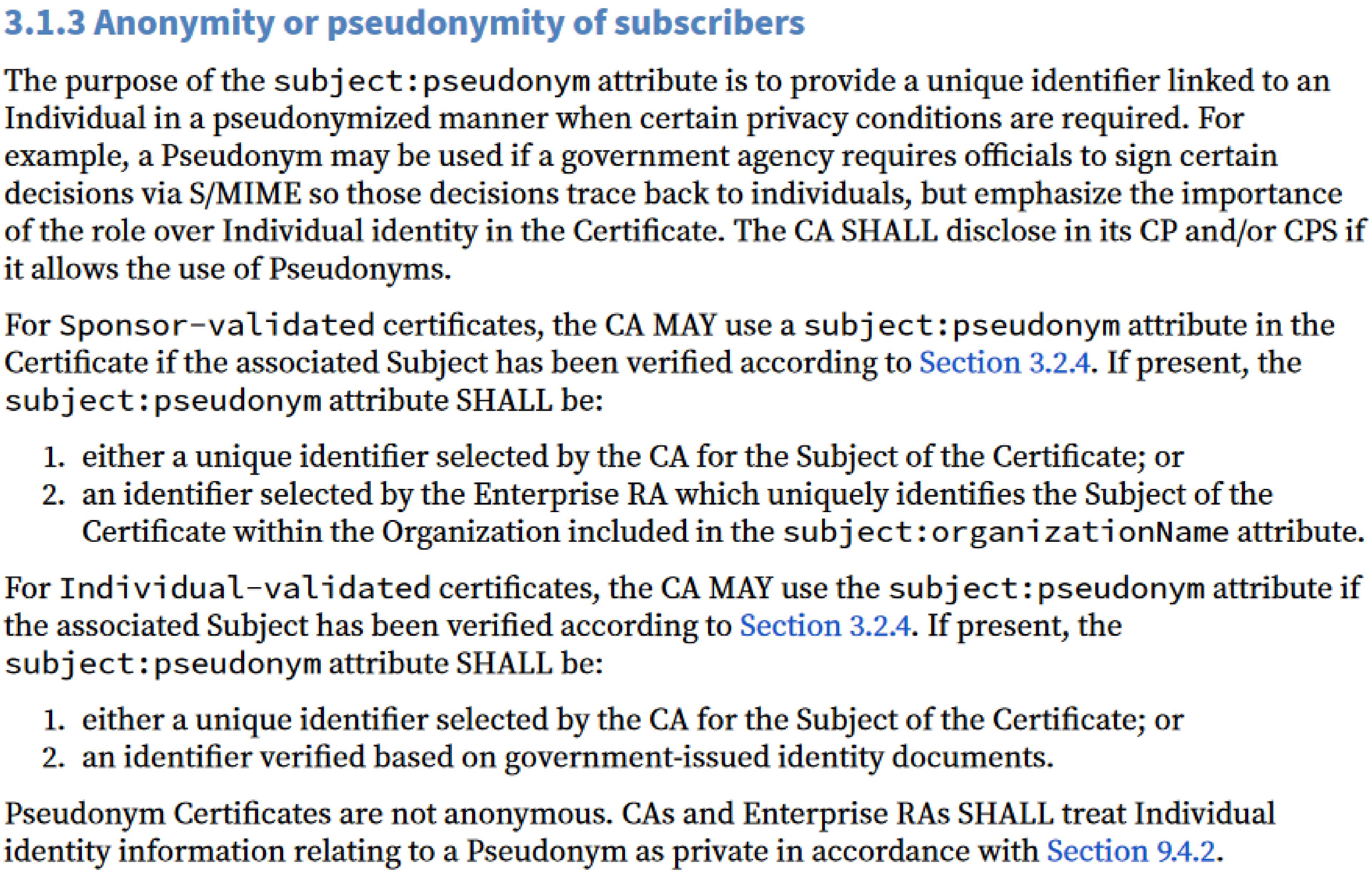


Certificate Type	Description
Mailbox-validated	Subject is limited to (optional) `subject:emailAddress` and/or `subject:serialNumber` attributes.
Organization-validated	Includes only Organizational (Legal Entity) attributes in the Subject.
Sponsor-validated	Combines Individual (Natural Person) attributes in conjunction with an `subject:organizationName` (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA.

Validation requirements



1. If the Certificate Request is for an `Organization-validated` or `Sponsor-validated` profile, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.1 or Section 3.2.2.3. The CA SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are Affiliated as defined in Section 3.2 or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.'s Registered Domain Name.



3.1.3 Anonymity or pseudonymity of subscribers

The purpose of the `subject:pseudonym` attribute is to provide a unique identifier linked to an Individual in a pseudonymized manner when certain privacy conditions are required. For example, a Pseudonym may be used if a government agency requires officials to sign certain decisions via S/MIME so those decisions trace back to individuals, but emphasize the importance of the role over Individual identity in the Certificate. The CA SHALL disclose in its CP and/or CPS if it allows the use of Pseudonyms.

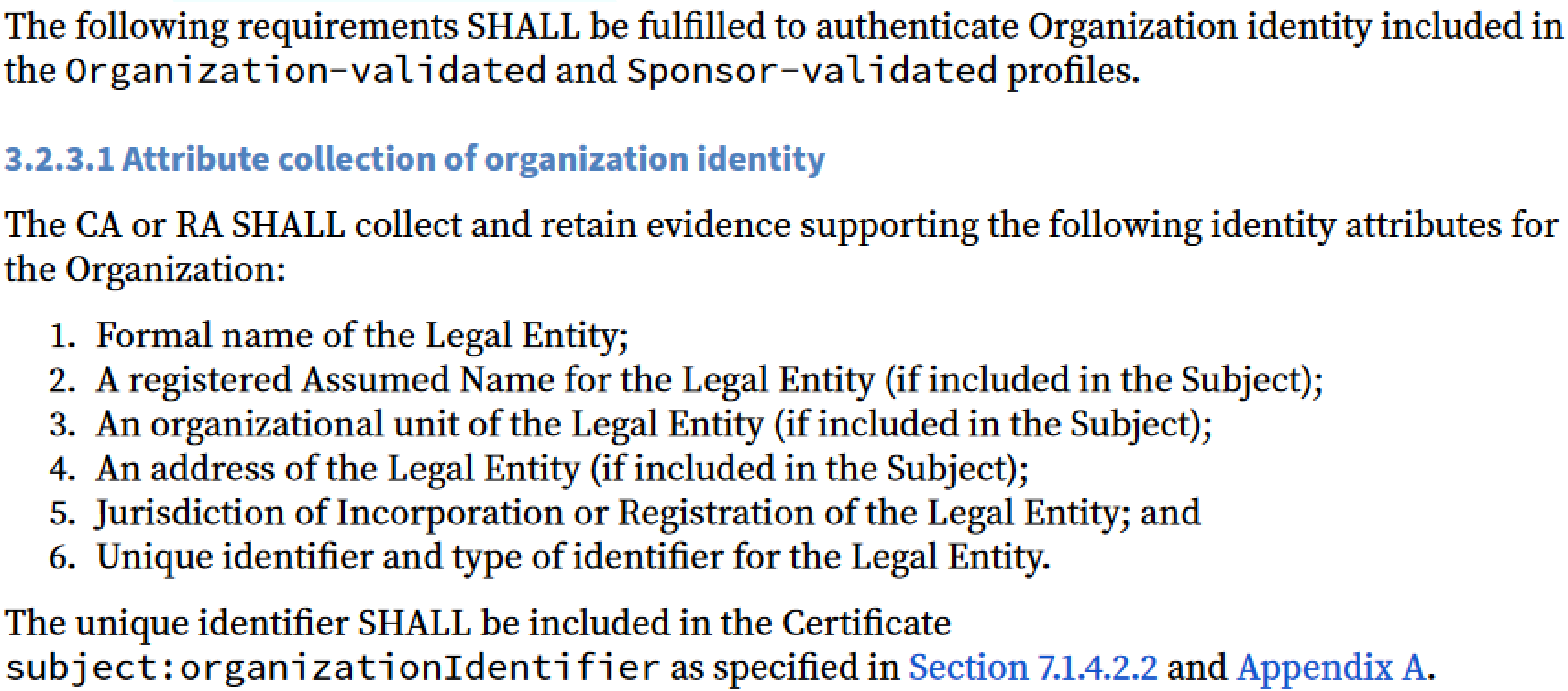
For `Sponsor-validated` certificates, the CA MAY use a `subject:pseudonym` attribute in the Certificate if the associated Subject has been verified according to Section 3.2.4. If present, the `subject:pseudonym` attribute SHALL be:

1. either a unique identifier selected by the CA for the Subject of the Certificate; or
2. an identifier selected by the Enterprise RA which uniquely identifies the Subject of the Certificate within the Organization included in the `subject:organizationName` attribute.

For `Individual-validated` certificates, the CA MAY use the `subject:pseudonym` attribute if the associated Subject has been verified according to Section 3.2.4. If present, the `subject:pseudonym` attribute SHALL be:

1. either a unique identifier selected by the CA for the Subject of the Certificate; or
2. an identifier verified based on government-issued identity documents.

Pseudonym Certificates are not anonymous. CAs and Enterprise RAs SHALL treat Individual identity information relating to a Pseudonym as private in accordance with Section 9.4.2.



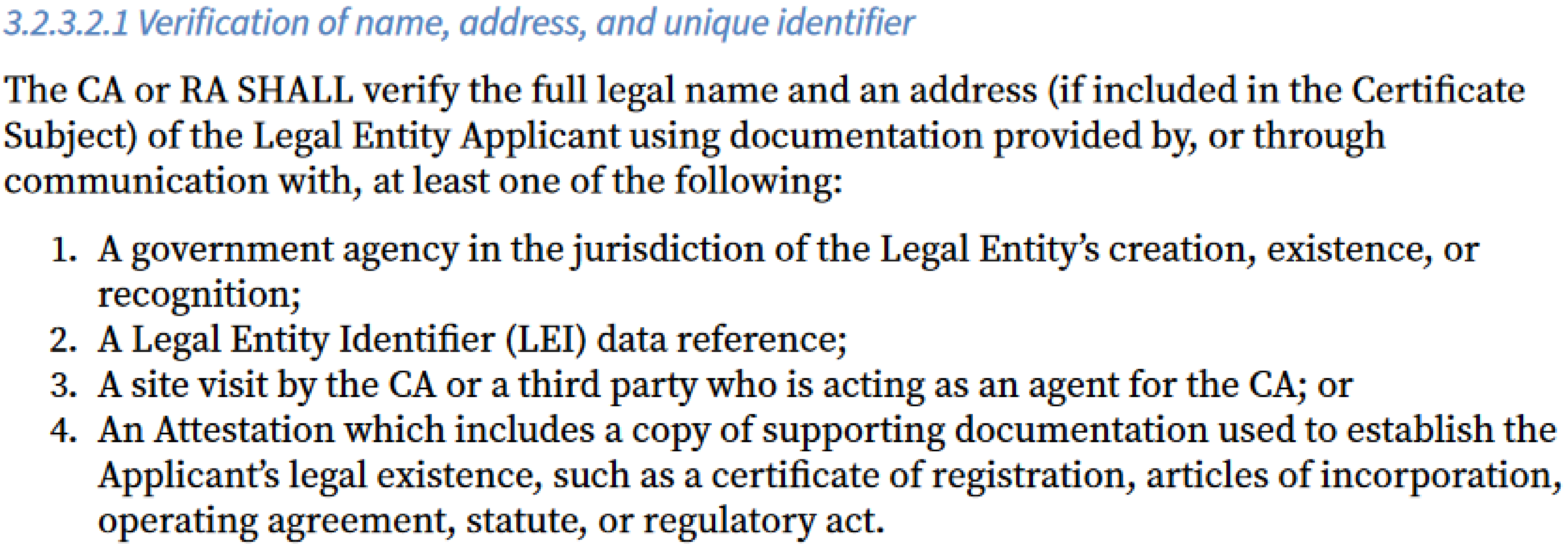
The following requirements SHALL be fulfilled to authenticate Organization identity included in the `Organization-validated` and `Sponsor-validated` profiles.

3.2.3.1 Attribute collection of organization identity

The CA or RA SHALL collect and retain evidence supporting the following identity attributes for the Organization:

1. Formal name of the Legal Entity;
2. A registered Assumed Name for the Legal Entity (if included in the Subject);
3. An organizational unit of the Legal Entity (if included in the Subject);
4. An address of the Legal Entity (if included in the Subject);
5. Jurisdiction of Incorporation or Registration of the Legal Entity; and
6. Unique identifier and type of identifier for the Legal Entity.

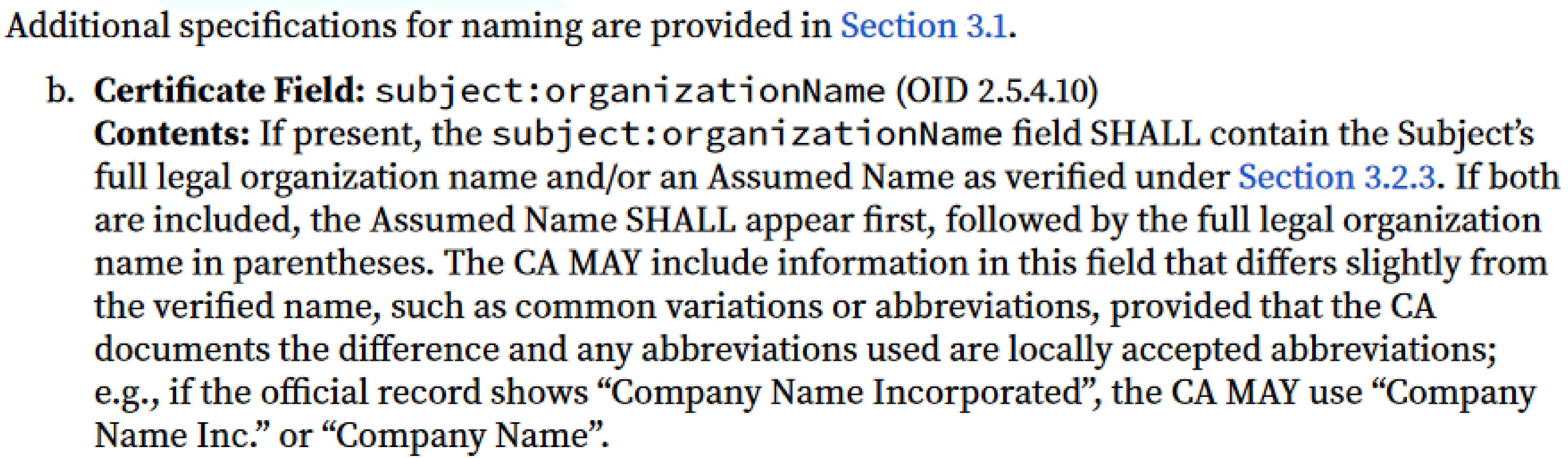
The unique identifier SHALL be included in the Certificate `subject:organizationIdentifier` as specified in Section 7.1.4.2.2 and Appendix A.



3.2.3.2.1 Verification of name, address, and unique identifier

The CA or RA SHALL verify the full legal name and an address (if included in the Certificate Subject) of the Legal Entity Applicant using documentation provided by, or through communication with, at least one of the following:

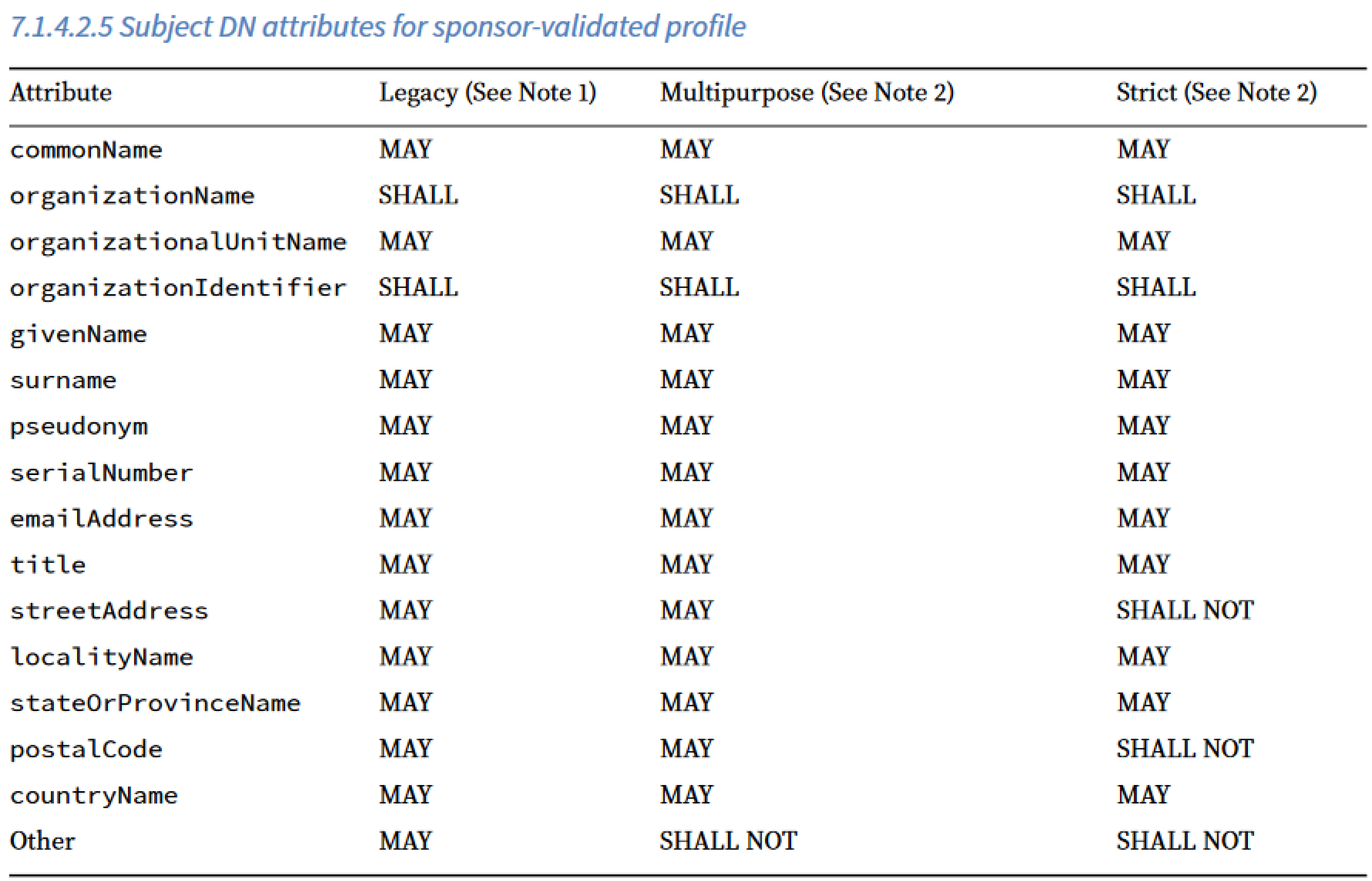
1. A government agency in the jurisdiction of the Legal Entity's creation, existence, or recognition;
2. A Legal Entity Identifier (LEI) data reference;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation which includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act.



Additional specifications for naming are provided in Section 3.1.

b. **Certificate Field:** `subject:organizationName` (OID 2.5.4.10)
   Contents: If present, the `subject:organizationName` field SHALL contain the Subject's full legal organization name and/or an Assumed Name as verified under Section 3.2.3. If both are included, the Assumed Name SHALL appear first, followed by the full legal organization name in parentheses. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".

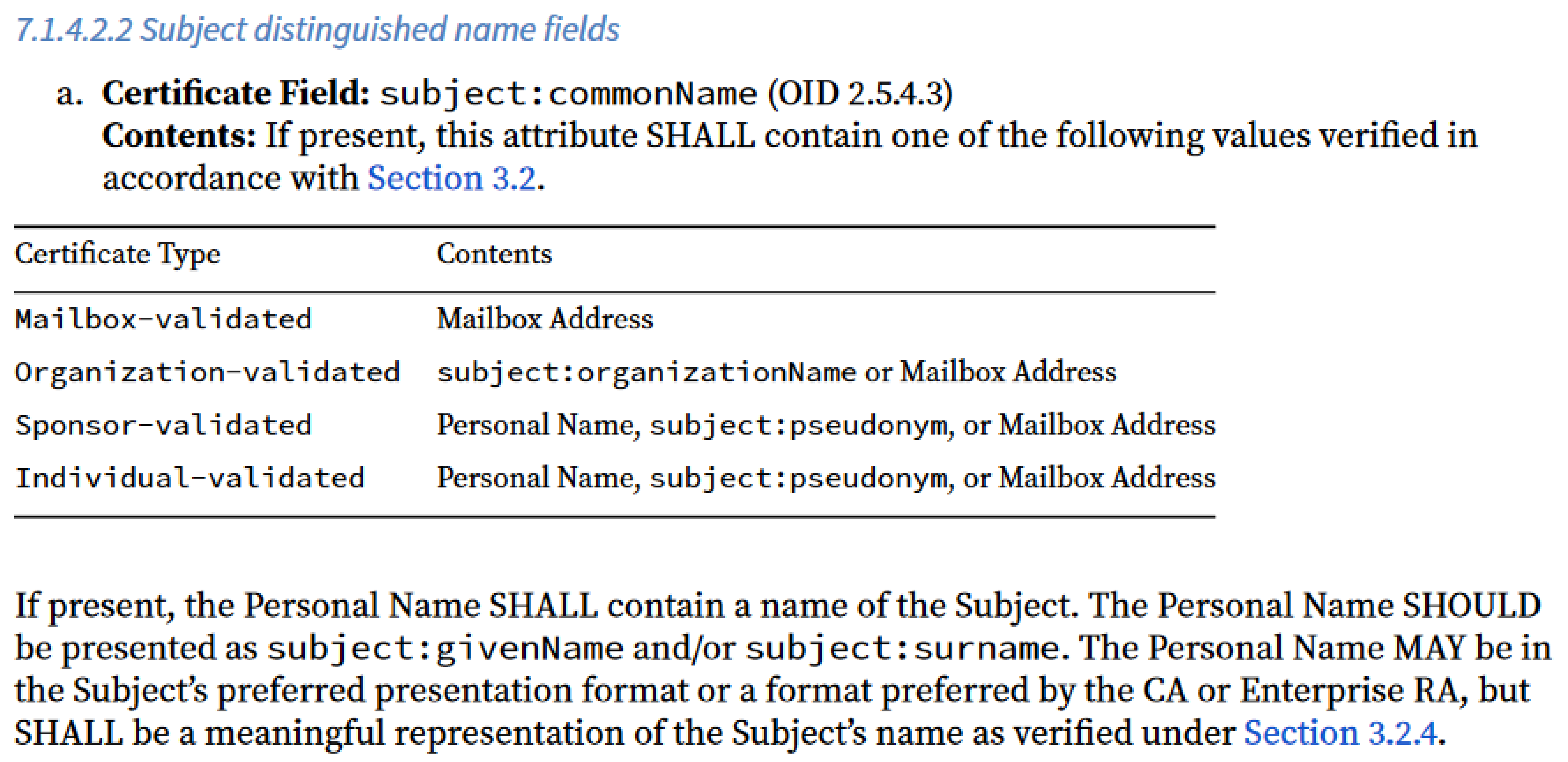
Some challenges – the name format



7.1.4.2.5 Subject DN attributes for sponsor-validated profile

Attribute	Legacy (See Note 1)	Multipurpose (See Note 2)	Strict (See Note 2)
commonName	MAY	MAY	MAY
organizationName	SHALL	SHALL	SHALL
organizationalUnitName	MAY	MAY	MAY
organizationIdentifier	SHALL	SHALL	SHALL
givenName	MAY	MAY	MAY
surname	MAY	MAY	MAY
pseudonym	MAY	MAY	MAY
serialNumber	MAY	MAY	MAY
emailAddress	MAY	MAY	MAY
title	MAY	MAY	MAY
streetAddress	MAY	MAY	SHALL NOT
localityName	MAY	MAY	MAY
stateOrProvinceName	MAY	MAY	MAY
postalCode	MAY	MAY	SHALL NOT
countryName	MAY	MAY	MAY
Other	MAY	SHALL NOT	SHALL NOT

commonName



7.1.4.2.2 Subject distinguished name fields

a. **Certificate Field:** `subject:commonName` (OID 2.5.4.3)
Contents: If present, this attribute SHALL contain one of the following values verified in accordance with Section 3.2.

Certificate Type	Contents
`Mailbox-validated`	Mailbox Address
`Organization-validated`	`subject:organizationName` or Mailbox Address
`Sponsor-validated`	Personal Name, `subject:pseudonym`, or Mailbox Address
`Individual-validated`	Personal Name, `subject:pseudonym`, or Mailbox Address

If present, the Personal Name SHALL contain a name of the Subject. The Personal Name SHOULD be presented as `subject:givenName` and/or `subject:surname`. The Personal Name MAY be in the Subject's preferred presentation format or a format preferred by the CA or Enterprise RA, but SHALL be a meaningful representation of the Subject's name as verified under Section 3.2.4.

Where does that leave us?

- The ‘Legacy’ profile (still) allowed ‘other’ attributes, so for the moment e.g. DC prefixing would be OK

- However the commonName is regulated, which
  - impacts uniqueness identifiers (like in TCS)
  - does not allow for ‘Robot’s in the commonName
    but these would go to Pseudonym, which is an ill-supported attribute, and anyway inflicts a subjectDN change

- and who knows when the legacy profile will be depricated

However …

… contrary to the host-cert issue, there is no joint-trust needed for email signing and client authentication!

- separating these should always have been done:
  using TCS Personal certs for authentication is bad (since they are not unique), and
  using TCS IGTF MICS client certs for S/MIME email is bad (since it’s 7-bit ASCII only)
- this just formalizes that move beyond restricting keyUsage & eKU

Anticipated moves

- Have the S/MIME personal certs move to sponsor-validated (multi-purpose) BR-compliant certificates
- Move the *client authentication* trust to a ‘private CA’ (non-public trust anchor), retaining *exactly the same subject DNs*, just a different ICA issuerDN
- Add some additional ICAs and non-public Roots to the IGTF distribution and for IGTF RPs the change is minimal and transparent
- Inform relying parties, *also outside of the IGTF*, that client trust will become a specific decision. This is probably good, also for OpenVPN services, web access (.htpasswd), &c. The IGTF RPs are not impacted, others likely will be.

User awareness

- This is a change in communications and documentation

- In request systems, have to clearly distinguish for users *which product to order*. For example:
  - “Personal” == only for EMAIL and NOT for authentication
  - renaming “IGTF MICS Personal” to “Personal Authentication” and explain
  - renaming “IGTF MICS Robot Personal” to “Personal Automated Authentication”?

What to expect in the short term

- Updated CPS for TCS (and likely InCommon Certificate Service?)
- Some new ICAs and a new Root
- deployment in ~ May-June
- no new ‘SMIME-ish’ authentication certs starting from ~ August

Questions?

BUILDING A GLOBAL TRUST FABRIC