資料2－2

eシールに係る組織識別子及び共通証明書ポリシーOIDについて

eシールに係る検討会（第2回）
令和5年10月2日
一般社団法人デジタルトラスト協議会
小田嶋　昭浩

1）組織識別子

組織識別子および識別子プレフィクスについて

組織識別子の必要性

✓ eシールの定義※1：eシールは「**電子文書等の発行元の組織等を示す**目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み」。

eシール用**電子証明書へ「組織等を一意に識別可能な番号」を格納することが必要**
（商号などでは同一名称もあり一意に識別することが難しい）。

✓ 一意に識別可能な番号は、既存の番号体系の中に複数候補が存在※2しているため、eシール用電子証明書に**格納された番号が、どの番号体系なのか判別可能なプレフィクスが必要**。（当該プレフィクスは電子証明書を発行する認証局が異なっても共通で使用できなければならない。）

組織識別子に関して決定すべき項目

① eシール用電子証明書へ格納する**「組織等を一意に識別可能な」既存番号体系**として何を使用するか。
② 各々の組織識別子に使用する**識別子プレフィクスの仕様**はどうするか。
③ 識別子プレフィクスの**管理方法（追加・削除・公表等）等**をどうするか。

※１：総務省「eシールに係る指針」より引用

※２：法人番号、適格請求書発行事業者登録番号、その他民間企業コードを想定（次頁以降で候補を提示）

組織識別子および識別子プレフィクスについて

eシールに使用する組織識別子案

【凡例】　◎：全てに付番（悉皆性）　○：基本的には付番可　－：付番対象外

- ✓ ①国際的に決まったプレフィクスを使用した組織識別子と②日本独自のプレフィクスを設けて使用する組織識別子を使用して、日本における組織等を網羅的に一意に識別可能とする。
- ✓ ①には法人番号と個人事業主も採番可能な番号、②にはEDINETコードとTDB企業コード、標準企業コード等が候補としてあげられる。
- ✓ 個人事業主等も採番可能な番号については、実在性確認の方法も含めて別途検討が必要。

			①国際的に決まったプレフィクスを使用する組織識別子案		②日本独自のプレフィクスを設けて使用する組織識別子案						LEI ※5
			法人番号	個人事業主等も採番可能な番号	企業コード等						
					会社法人等番号※2	EDINETコード	TDB企業コード	標準企業コード	TSR企業コード	D-U-N-S® Number	
			公的機関が管理する番号体系				民間が管理する番号体系				
識別子プレフィクス案			NTRJP※1	VATJP	CO:JP	ED:JP※3	TD:JP	JI:JP	※3※4	※3※4	
組織識別子記載例			NTRJP-1234567890123		CO:JP-1234567890123	ED:JP-E12345	TD:JP-123456789	JI:JP-123456	※3※4	※4※4	
eシール用電子証明書を発行する対象	組織・団体等	法人	◎		◎	○	○	○	○	○	○
		権利能力なき社団・財団	○		－	○	○	○	○	○	－
		その他任意の団体	－		－	○	○	○	○	○	－
		個人事業主	－		－	○	○	○	○	○	○
		その他の個人	－		－	○	－	－	－	－	－

※1：政府機関や地方自治体は「GOVJP」を使用可能だが、採用番号体系は法人番号を使用するか要確認。
※2：法人番号に包含されるため不要か要確認。
※3：国際利用される企業等コードであるため「XG」を使用することが可能。
※4：TSRコードはDUNS Numberと連携した番号体系であり、日本独自のプレフィクス設定は不要か要確認。
※5：LEIは組織識別子ではなく、別の国際標準の証明書拡張により記載可能。

組織識別子および識別子プレフィクスについて

国際的に決まったプレフィクスに使用する番号体系案

✓ 国際的に決まったプレフィクスであるNTRJPに使用する既存番号体系は下記を考慮して**「法人番号」**とすることが考えられる。
① 省庁含め、広範囲に付番されている
② 誰でも容易に検索可能なウェブサイト及びAPIが具備されており、認証局や検証者にとって利便性が高い
③ 番号法に則り自由に活用可能　等
✓ VATJPについては、個人事業主の実在性確認の方法等の検討含めて、使用する番号を検討する必要がある。

識別子プレフィクスの管理方法等の提案

✓ eシール用電子証明書へ格納する組織識別子として、認定に係るeシールは必ず公的機関の番号体系を使用※1し、それ以外のeシールは民間企業コードも使用可能とすべき。

✓ 組織識別子として使用する既存番号体系、及び、識別子プレフィクスについては、認定制度運用開始後も追加、削除等が発生する可能性がある。したがって、認定制度においても追加登録方法や削除、公表方法が明確化される必要がある。
⇒　eシール用電子証明書に使用する既存番号やプレフィクス等の管理は総務省に実施頂きたい。

✓ 組織識別子が不正使用されないよう、制度設計・運用において配慮する必要がある。

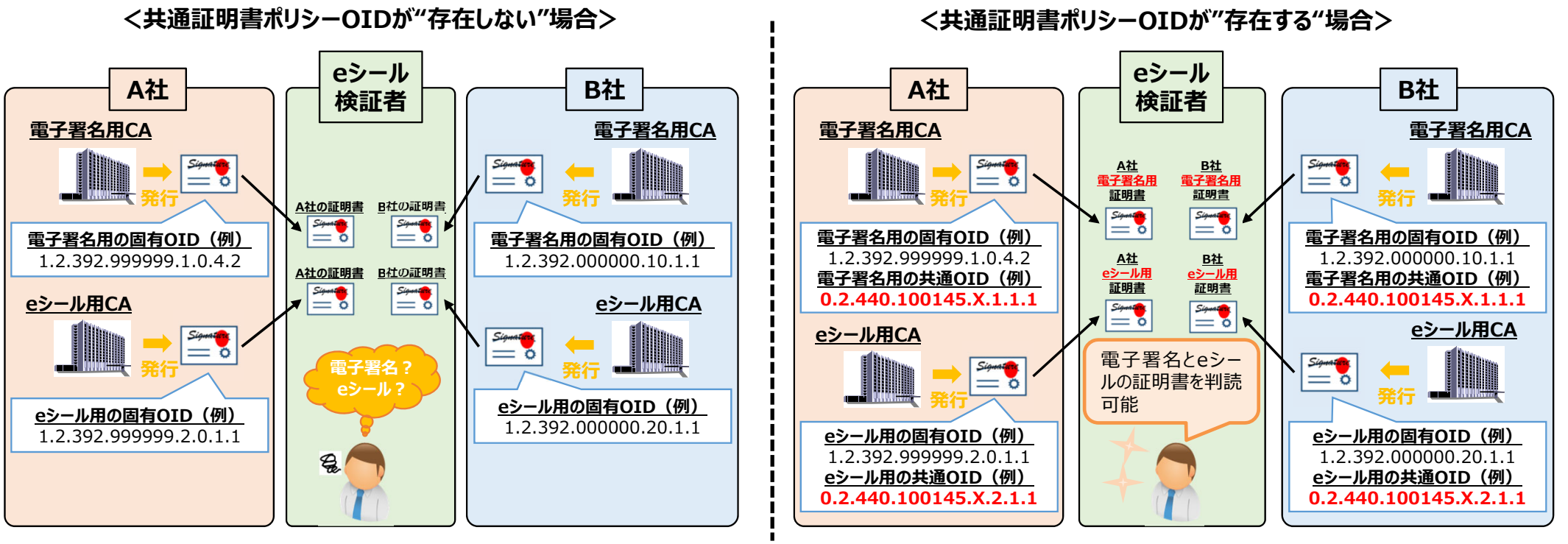
※1：電子証明書の任意の拡張領域には、民間コード記載も可能とする。

２）共通証明書ポリシーOID

共通証明書ポリシーOIDについて

eシール用共通証明書ポリシーOIDの必要性

- ✓ 異なる認証局においても、「eシール」用電子証明書であることが、電子証明書の記載事項から機械判読できる共通な仕様が必要。
- ✓ eシール用電子証明書は活用観点から「レベル」を想定しているが、eシール用電子証明書を受領した**検証側が当該証明書のレベルを記載事項で機械判読できる共通な仕様**が必要である。



共通証明書ポリシーOIDについて

共通証明書ポリシーOIDに関して決定すべき項目

① **トラストサービス全体でOID体系**を設定するか、**eシール単独でOID体系**を設定するか。
② **共通証明書ポリシーOIDの番号体系**はどうするか。
③ **共通証明書ポリシーOIDの管理方法（追加・削除・公表等）等**をどうするか。

共通証明書ポリシーOID案

✓ 国際相互承認を見据えて、トラストサービス関連で１つのOID体系を設定すべき。
✓ 今後OIDを設定する各種トラストサービスはOID体系を一つの山（OIDアーク）に纏めたい。
✓ レベルを設けるeシールは自動識別できるように、各々に共通の証明書ポリシーOIDを付与したい。

【日本のトラストサービスのOID体系案】
0.2.440.100145. 総務省
0.2.440.100145.X. トラストサービス関連のOID群
↑ 現在使用されていない番号を使用する
0.2.440.100145.X.1. 電子署名用証明書ポリシー群
※番号体系は要検討

少なくともeシール用の番号体系は必要

0.2.440.100145.X.2. eシール用証明書ポリシー群
0.2.440.100145.X.2.1. 認定に係るローカル/リモートeシールで使用する証明書ポリシー群
0.2.440.100145.X.2.1.1 認定に係るローカルeシールで使用する証明書ポリシー
0.2.440.100145.X.2.1.2 認定に係るリモートeシールで使用する証明書ポリシー
0.2.440.100145.X.2.2. 認定以外のローカル/リモートeシールで使用する証明書ポリシー群
0.2.440.100145.X.2.2.1 認定以外のローカルeシールで使用する証明書ポリシー
0.2.440.100145.X.2.2.2 認定以外のリモートeシールで使用する証明書ポリシー

【参考】（EU eIDASにおける共通の証明書ポリシ 具体例）

0.4.0.194112　ETSI適格証明書ポリシ
0.4.0.194112.1　ETSI適格証明書ポリシ識別子
0.4.0.194112.1.0　自然人用適格証明書ポリシ（=EU適格署名用ポリシ）
0.4.0.194112.1.1　法人用適格証明書ポリシ（=EU適格eシール用ポリシ）
0.4.0.194112.1.2　QSCDを用いた自然人用適格証明書ポリシ（=EU適格署名用ポリシ）
0.4.0.194112.1.3　QSCDを用いた法人用適格証明書ポリシ（=EU適格eシール用ポリシ）
0.4.0.194112.1.4　EU適格ウェブサーバー用証明書ポリシ

共通証明書ポリシーOIDについて

共通証明書ポリシーOIDの管理方法等の提案

- ✓ eシール用電子証明書へ格納する共通証明書ポリシーOIDとして、認定eシールは指定の共通証明書ポリシーOIDを使用することを要件とし、それ以外のeシールは指定の共通証明書ポリシーOIDを使用することが望ましいとする。

- ✓ トラストサービス関連で１つのOIDを設定する場合、トラストサービス用OIDを管理する省庁を決定していただく必要がある。

⇒ OIDのレベル4を管理は総務省にて実施中。

⇒ レベル5（トラストサービス群を示す）とレベル6（トラストサービス種別を示す）は総務省で実施、レベル7以下は各々のトラストサービス所管省庁で管理する方針は可能か。

- ✓ eシールについては、認定制度運用開始後も追加、削除等が発生する可能性がある。認定制度においても追加登録方法や削除、公表方法が明確化される必要がある。

- ✓ 共通証明書ポリシーOIDが不正使用されないよう、制度設計・運用において配慮する必要がある。

＜参考資料＞

＜参考＞オブジェクト識別子と組織識別子①概要

- 組織識別子(organizationIdentifier)とは
  - EU eIDAS、CABF S/MIME基本要求で用いられる組織を一意に識別するための値。
  - 各国の法人番号NTR、付加価値税番号VAT、金融向けにLEI・PSDなどの接頭辞がある。
  - EUの適格証明書では証明書の識別名の属性タイプとしてorganizationIdentifierを設定しなければならず、値のフォーマットはETSIのセマンティックID、CABF S/MIME基本要求として定められている。
  - 例えば、総務省の法人番号を用いた場合、値はNTRJP-2000012020001となる。
- オブジェクト識別子(OID:objectIdentifier)とは
  - 通信プロトコルの様々な用途で用いられるグローバルで一意な識別番号で、整数の並びによって表現される。用途の例は以下の通り。
    - (国際)標準化された(通信プロトコルで使われる)データの型を表す識別子
      - データフォーマット、暗号アルゴリズム等の識別子
      - 証明書や署名フォーマットの識別名属性タイプ、拡張タイプ、属性タイプなど
        - 証明書識別名で使われる属性タイプ(国C、組織名O、組織識別子(下記)、一般名CNなども)OIDで表される。
    - 会社等の組織が自社の製品、サービスで使用される通信データの型、値など
      - 必要な組織は「組織OID」を登録する。
      - 日本では組織OIDは総務省かJIPDECで登録できる。
      - 組織が使用する証明書ポリシOID、タイムスタンプポリシOIDなど
      - オンラインで通信機器やサービスの状態を参照、設定するSNMPプロトコル等

＜参考＞オブジェクト識別子と組織識別子②OIDの体系

- OIDは数値の並びになっているが1、2番目には規則がある。

1番目	2番目
0 - 通信系の標準化機関 ITU-T	0 – 勧告(recommendation) 1 – 課題(question) 2 – 管理組織(administration) 3 – ネットワークオペレーター(network operator)
1 - 製品系の標準化機関 ISO	0 – 標準(standard) 1 – 登録機関(registration-authority) 2 – 加盟団体(member-body) 3 – 身元が明らかな組織(identified-organization)
2 - ITU-TとISO/IECの合同標準	

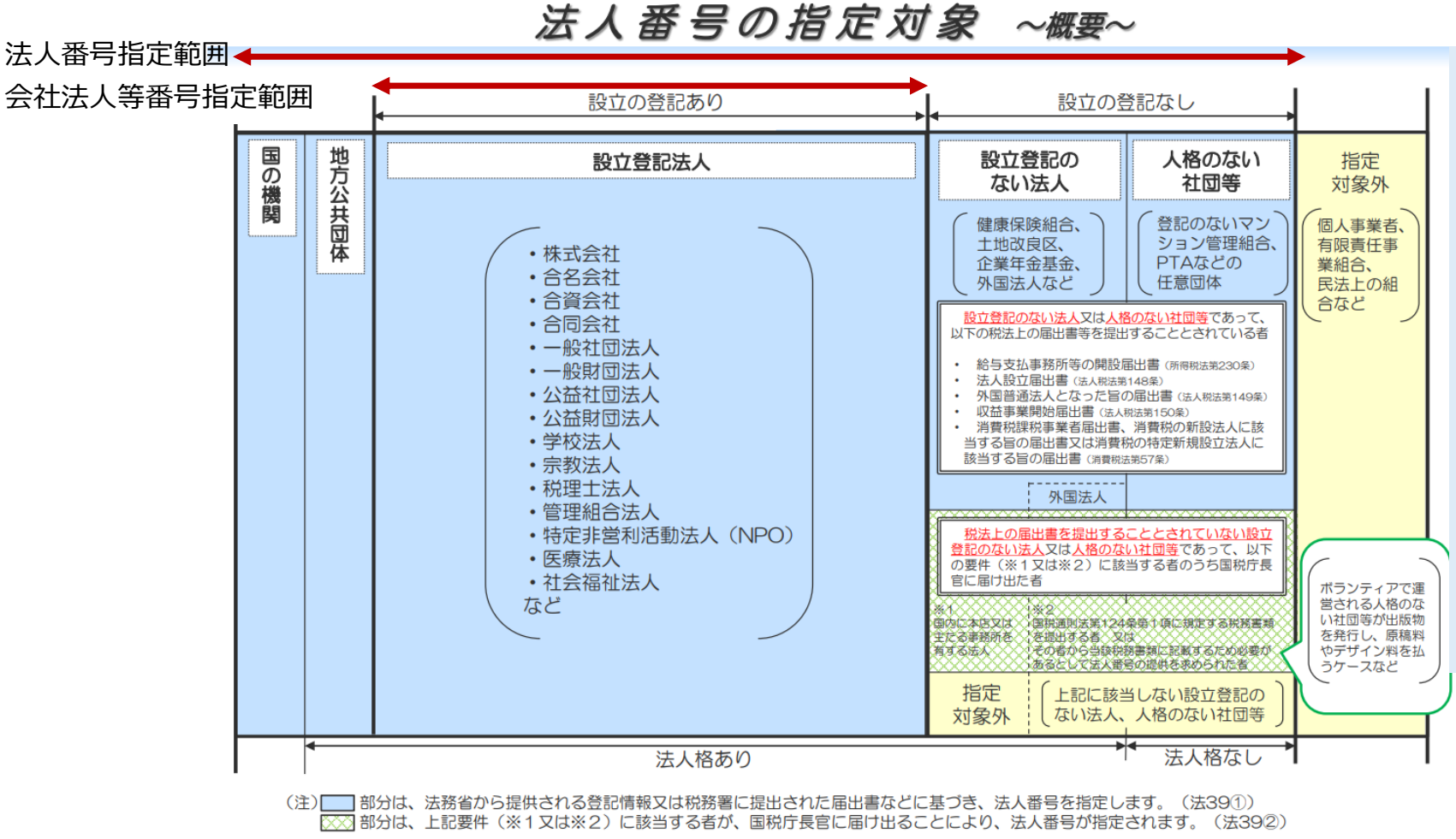
- 例えばSHA256ハッシュアルゴリズムのOIDは「2.16.840.1.101.3.4.2.1」である。
- 数値の並びの体系は「joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)」となっている。

＜参考＞発番機関登録

登録規格	UN/EDIFACT 3055	ISO/IEC 6523-2	ISO/IEC 15459-2
運営機関	国際連合（UN）	国際標準化機構（ISO）	国際標準化機構（ISO）
概要	・電子商取引などデータ通信における授受の当事者を識別するための企業コードに関する規格	・電子商取引などデータ通信における授受の当事者を識別するための企業コードに関する規格	・輸送資材、貨物などの物を識別するためのコードの一部で活用される企業コードに関する規格 ・電子タグなどの自動認識メディアの識別子の中で活用
帝国データバンクに付与された発番機関コード	311	0170	VTD

- 発番機関に関する内容をTDBのWebから引用　https://www.tdb.co.jp/lineup/code.html

＜参考＞各番号の指定範囲



NTRJPの設定に関するJDTF内考察

- 会社法人等番号は「設立の登記あり」の範囲（商号登記した個人事業主を含む）
- 法人番号は左表のとおりカバー範囲が広い
- 法人番号はWebAPIが整備済、eシールを発行するCAや、検証する側双方にメリットあり
- 法人番号の趣旨、利活用観点からも有用

- 国税庁法人番号公表サイト「法人番号の指定対象～概要～」から引用

＜参考＞ETSI TS 119 412-1 V1.3.1 (2019-08)

- ETSI TS 119 412-1 V1.3.1 (2019-08)

5.1.4 Legal person semantics identifier

5) Two characters according to local definition within the specified country and name registration authority,identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).

Other initial character sequences are reserved for future amendments of the present document. In case “VAT” legal person identity type reference is used in combination with the “EU” transnational country code, the identifier value should comply with Council Directive 2006/112/EC [i.12], article 215.

EXAMPLES: "VATBE-0876866142" and "EI:SE-5567971433".

When a locally defined identity type reference is provided (two characters followed by “:”), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.

Appendix A - Registration schemes

A.1 organizationIdentifier

The following Registration Schemes are recognized as valid under these Requirements for use in the subject:organizationIdentifier attribute described in Section 7.1.4.2.2.

The country code used in the Registration Scheme identifier SHALL match that of the

subject:countryName in the Certificate as specified in Section 7.1.4.2.2.

- NTR: For an identifier allocated by a national or state trade register to the Legal Entity named in the subject:organizationName.
- VAT: For an identifier allocated by the national tax authorities to the Legal Entity named in the subject:organizationName.
- PSD: For a national authorization number allocated to the payment service provider named in the subject:organizationName under Payments Services Directive (EU) 2015/2366.This shall use the extended structure as defined in ETSI TS 119 495, clause 5.2.1.
- LEI: For a Legal Entity Identifier as specified in ISO 17442 for the entity named in the subject:organizationName. The 2 character ISO 3166 country code SHALL be set to 'XG'.

7.1.4.2.2 Subject distinguished name fields

d. Certificate Field: subject:organizationIdentifier (2.5.4.97)

Contents: If present, the subject:organizationIdentifier field SHALL contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme.

The subject:organizationIdentifier SHALL be encoded as a PrintableString or UTF8String.

The Registration Scheme identified in the Certificate SHALL be the result of the verification performed in accordance with Section 3.2.3. The Registration Scheme SHALL be identified using the using the following structure in the presented order:

- 3 character Registration Scheme identifier;
- 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated, or if the scheme is operated globally ISO 3166 code "XG" SHALL be used;
- For the NTR Registration Scheme identifier, where registrations are administrated at the subdivision (state or province) level, a 2 character ISO 3166-2 identifier for the subdivision of the nation in which the Registration Scheme is operated, preceded by plus "+" (0x2B (ASCII), U+002B (UTF-8));
- a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
- Registration Reference allocated in accordance with the identified Registration Scheme.

Note 1: Registration References MAY contain hyphens but Registration Schemes, ISO 3166 country codes, and ISO 3166-2 identifiers do not. Therefore if more than one hyphen appears in the structure, the leftmost hyphen is a separator, and the remaining hyphens are part of the Registration Reference. For example:

- NTRGB-12345678 (NTR scheme, Great Britain, Unique Identifier at Country level is 12345678).
- NTRUS+CA-12345678 (NTR Scheme, United States - California, Unique identifier at State level is 12345678).
- VATDE-123456789 (VAT Scheme, Germany, Unique Identifier at Country Level is 12345678).
- PSDBE-NBB-1234.567.890 (PSD Scheme, Belgium, NCA's identifier is NBB, Unique Identifier assigned by the NCA is 1234.567.890).

Registration Schemes listed in Appendix A are recognized as valid under these Requirements. The CA SHALL:

1. Confirm that the organization represented by the Registration Reference is the same as the organization named in the organizationName field as specified in Section 7.1.4.2.2; and
2. Further verify the Registration Reference matches other information verified in accordance with Section 3.2.3.

Note 2: For the following types of entities that do not have an identifier from the Registration Schemes listed in Appendix A:

- For Government Entities, the CA SHALL enter the Registration Scheme identifier 'GOV' followed by the 2 character ISO 3166 country code for the nation in which the Government Entity is located. If the Government Entity is verified at a subdivision (state or province) level, then a plus "+" (0x2B (ASCII), U+002B (UTF-8)) followed by a 2 character ISO 3166-2 identifier for the subdivision is added.
- For International Organization Entities, the CA SHALL enter the Registration Scheme identifier 'INT' followed by the ISO 3166 code "XG". An International Organization Entity is founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

For example:

- GOVUS (Government Entity, United States)
- GOVUS+CA (Government Entity, United States - California)
- INTXG (International Organization)