

# Sectigo S/Mime Guidelines

August 2023

# CA/Browser Forum S/MIME Baseline Requirements

## CA/B Forum Baseline Requirements

<https://cabforum.org/smime-br>

## ETSI Standard

[https://www.etsi.org/deliver/etsi\\_en/319400\\_319499/31941201/01.04.04\\_60/en\\_31941201v010404p.pdf](https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.04.04_60/en_31941201v010404p.pdf)

[https://www.etsi.org/deliver/etsi\\_ts/119400\\_119499/119495/01.05.01\\_60/ts\\_119495v010501p.pdf](https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.05.01_60/ts_119495v010501p.pdf)

## Brief Change Description

Effective September 1, 2023, the issuance and management of Publicly-Trusted S/MIME Certificates will become subject to compliance with the CA/B Forum Baseline Requirements.

## What is a “S/MIME Certificate”?

- In laymen’s terms, an S/MIME Certificate is identified by the existence of an Extended Key Usage (EKU) for id-kp-emailProtection (OID: 1.3.6.1.5.5.7.3.4).

# New S/Mime Requirements

## Summary:

- Per the CA/B Forum, effective **September 1, 2023**, all organizations who wish to use S/MIME certificates must be validated with a Registration QGIS (Reg QGIS)
  - Along with the Reg QGIS, organization identifiers will be used to help classify each organization type
- If a Reg QGIS cannot be found directly from the State/Province/Country's registration agency, you may need to find government acts, statutes, acts or decrees that established the organization.
  - If this is for a US College or University, per Compliance 'you cannot use "accredited" type sites from the US Federal Government. It needs to be something from the state '

# Things To Keep In Mind for SCM Accounts

- If an organization does not need S/Mime Certificates, the OV Anchor will remain active until it expires or until someone clicks the “**Re-Validate**” button in the SCM account
  - When either of these events happen, the SCM account will need to be re-validated under the new S/Mime guidelines
  - While the SCM account is in re-validation, customers will not be able to issue OV certificates until the master template for the new information is complete.
- If the customer wishes to use a “**DBA Name**”, it must be validated according to the CA/Forum guidelines and **MUST** be included with the organization’s legal entity name.
  - It will be written like the EV naming convention: **DBA (Legal Entity Name)**
- **Account names cannot exceed 64 characters**. If it does, the agent must work with the customer on a proper name update. This means any abbreviations used must be a recognized legal abbreviation in that country. The customer must also approve the name change. If in doubt, please consult with a Manager.

# Validation : General Overview

	<b>Domain Validation</b>	<b>Organization Validation</b> (including organizationIdentifier attribute)	<b>Individual Validation</b>
<b>Mailbox S/MIME</b>	Required	N/A	N/A
<b>Organization S/MIME</b>	Required	Required	N/A
<b>Sponsored S/MIME</b>	Required	Required	Required

# Subject Fields

	Mailbox*	Organization	Sponsored
<u>emailAddress</u> (E)	✓	✓	✓
<u>commonName</u> (CN)	✗	✓ <i>Organization Name</i>	✓ <i>Personal Name</i>
<u>organizationIdentifier</u>	✗	✓	✓
<u>OrganizationName</u> (O)	✗	✓	✓
<u>StateorProvince</u>	✗	✓	✓
<u>countryName</u> (C)	✗	✓	✓
Title	✗	✗	✓
Name (G)	✗	✗	✓
Surname (SN)	✗	✗	✓

(\* ) Includes both multipurpose and strict.

- New S/MIME Certificate Attributes:
  - organizationIdentifier
  - givenName
  - surname
  - title (allowed by CPS but will not be included in the certificates)
- Multiple email addresses allowed in **SAN:RFC822Name**
- If **subject:CommonName** is included in the certificate, it must be identical to one of the email addresses in SAN:RFC822Name
- Requirements for **subject:Locality(L)** and **subject:StateorProvince(S)** are the same for publicly-trusted SSL and S/MIME certificates
- The **subject:OrganizationIdentifier** is the same as for eIDAS certificates with only the following differences:
  - Exception (!) : PSD identity type should not be used for S/MIME.
  - Note1 (!) : GOV and INT may not be used for eIDAS.
  - Note2 (!) : For NTR identity type, there is one more format option for S/MIME certificates containing state name (which is not acceptable for eIDAS).

# organizationIdentifier Attribute in S/MIME

## Possible Legal Person Identity Types

- National Trade Register (NTR)
- National Value Added Tax (VAT)
- Global Legal Entity (LEI)
- Government Entity (GOV)
- International Organization (INT)

## Structure Examples

For NTR:                    organizationIdentifier = NTRUS-0768662292  
                                  organizationIdentifier = NTRUS+CA-076866222

For VAT:                    organizationIdentifier = VATBE-0876866142

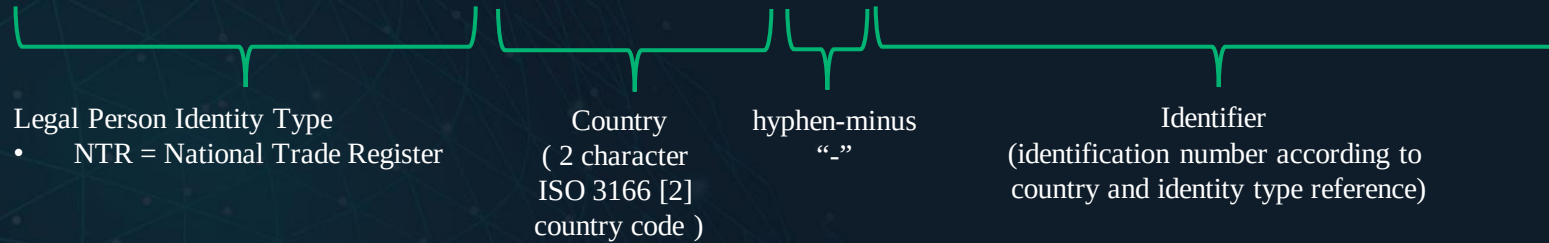
For LEI:                    organizationIdentifier = LEIXG-087685742

For GOV :                   organizationIdentifier = GOVUS  
                                  organizationIdentifier = GOVUS+CA

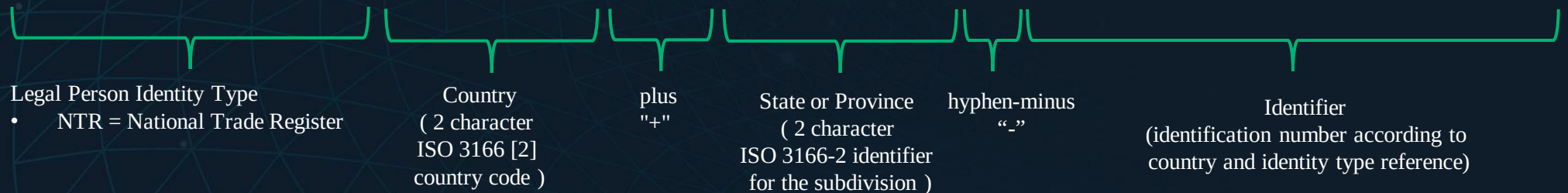
For INT :                    organizationIdentifier = INTXG

# organizationIdentifier Attribute Structure : NTR

(a) NTRUS-542723



(b) NTRUS+CA-542723





# organizationIdentifier Attribute Structure : VAT

# VATBE-0876866142

Legal Person Identity Type

- VAT = National Value Added Tax

Country  
( 2 character  
ISO 3166 [2]  
country code )

hyphen-minus  
“-”

Identifier  
(identification number according to  
country and identity type reference)



# organizationIdentifier Attribute Structure : LEI

# LEIXG-0876866142

Legal Person Identity Type

- LEI = Global Legal Entity

Shall always  
be set to the  
ISO 3166  
code 'XG)

hyphen-minus  
“-”

Identifier  
(identification number according to  
country and identity type reference)

# organizationIdentifier Attribute Structure : GOV

(a)

GOVUS



Legal Person Identity Type

- GOV = Government Entity

Country

( 2 character  
ISO 3166 [2]  
country code )

(b)

GOVUS+CA



Legal Person Identity Type

- GOV = Government Entity

Country

( 2 character  
ISO 3166 [2]  
country code )

a plus  
"+"

State or Province

( 2 character ISO 3166-2  
identifier for the subdivision )

# organizationIdentifier Attribute Structure : INT

# INTXG



Legal Person Identity Type

- INT = International Organization









Shall always be set to  
the ISO 3166 code "XG"

# Key Usage. Extended Key Usage.

## Key Usage

Purpose	Key Type	Key Usage
Signing + Encryption	RSA	<del>digitalSignature</del> , <del>keyEncipherment</del>
	ECC	<del>digitalSignature</del> , <del>keyAgreement</del>

## Extended Key Usage

	Mailbox Multipurpose	Mailbox Strict	Organization Multipurpose	Sponsored Multipurpose
Client Authentication				
Email Protection				

The EKU set should be fixed in a sense that they should not be subject to customer's selection.

# Key Sizes

The following key sizes are supported for S/MIME certificates:

- RSA key pairs: 2048 to 8192 bits.
- ECDSA key pairs: NIST P-256, NIST P-384 elliptic curve.

**Note:** NIST P-521 will not be supported as it is forbidden by <https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/#51-algorithms>

