

# NEW S/MIME

## Standard changes and

# FAQ's

Frequently Asked Questions - Upcoming S/MIME standard changes effective September 1, 2023

### What is this about?

The CA/Browser Forum, a consortium of certification authorities and web browsers, has recently drafted and approved the Baseline Requirements for the issuance of Publicly Trusted S/MIME certificates of which Sectigo as a trusted certification authority must comply with by September 1, 2023.

To reinforce the security of email encryption and digital signatures, with stronger encryption algorithms, secure key lengths, and reliable certificate validation procedures.

### Why is this happening?

### What are the key changes?

The CA/Browser Forum have defined new validation methods relevant to our Sectigo Certificate Manager (SCM) customers:

- **Organization Validation** – Validate organization and email address in the certificate with government registered name.
- **Sponsor Validation** – Validate organization, email address and person name in the certificate with government registered name.
- Customers, during or prior to issuance of certificates, will have to trigger the validation in SCM.
- Shortened the lifetime of certificates from 3 years down to 1 & 2 years.

- ❑ **Aug 19, 2023:** SCM 23.8 release, supporting the new S/MIME certificates.
- ❑ **Aug 28, 2023 (9:00 AM UTC):** The current S/MIME certificates will be blocked from being issued or renewed
- ❑ Existing certificates will continue to work until their expiry

### What key dates should you be aware of?

## What do you need to do?

As an SCM customer you have two options to ensure you comply with the new industry standards (either option A or option B):

### A

#### Between now and Aug 28, 2023

- ✓ Issue or renew your existing SMIME certificates

### B

#### Only an option after Aug 19, 2023

Perform the following to start using the NEW SMIME certificates:

1. Validate/Revalidate Organizations following the instructions in SCM.
2. Create new certificate profiles based on the two new certificate templates.

The templates names are:

- ❑ **Public S/MIME Organization Validation Multipurpose** – *If you want email and organization information in the certificate*
- ❑ **Public S/MIME Sponsored Validation Multipurpose** – *If you want email, employee name and organization information in the certificate*

3. Replace the certificate profiles with the new ones in the enrollment endpoints

4. Issue the (new) SMIME certificates [Detailed instructions can be viewed here.](#)

## We are here to help

We understand that the adoption of new standards may require effort and coordination within your organization. If you encounter any challenges or require assistance during the transition, do not hesitate to reach your account manager ([24/7 support team](#)). We appreciate your attention to this matter and thank you for being a valued customer.

To learn more about this upcoming change, view our FAQ page:

[Click here for more FAQ](#)