SECTIGO®

FAQ's

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

Q1: What is happening with the S/MIME standards on September 1, 2023?

Starting from September 1, 2023, there will be a change in the Secure/Multipurpose Internet Mail Extensions (S/MIME) standards. These changes are driven by the CA/Browser (CA/B) Forum and aim to enhance the security and trustworthiness of email communication.

Q2: Why are the S/MIME standards being implemented?

The S/MIME standards are being implemented to ensure strong encryption algorithms, adequate key lengths, and reliable certificate validation procedures. These standards will contribute to a more secure email communication ecosystem.

Q3: Why is Sectigo implementing an earlier cut-off date vs. September 1, 2023?

The process of obtaining a validated S/MIME certificate has and will continue to require key steps. Therefore, to offer new Baseline Requirements (BR) compliant S/MIME certificates, Sectigo will enforce earlier cut-off dates for each S/MIME validation task involved.

Q4: Who else is implementing and reinforcing this change?

All CAs that offer S/MIME certificates will need to ensure that their systems and offerings are updated to be compliant with the new standards.

Q5: How does this change impact my existing S/MIME certificates?

Existing S/MIME certificates will not be impacted and can still be used until they expire. Any renewals or replacements issued after the deadline will need to adhere to the new standards.

Q6: Will Sectigo's S/MIME certificates offering differ going forward?

Yes, as of August 14, 2023, Sectigo will no longer be offering 3-year S/MIME certificates. S/MIME certificates with 1 or 2-year validity period will still be offered through our online store, adhering to new standards.

Q7: Will this impact pricing for Sectigo's S/MIME certificates?

Prices are subject to change at any time. Please see our online store for current prices.

Q8: What actions do I need to take as an S/MIME customer?

Due to the more stringent validation required in the updated standards, you should start planning ASAP and allow sufficient time to generate new S/MIME certificates for your organization and any new employees onboard. Plan and renew your existing S/MIME certificates based on the below cut-off dates:

- **Purchase:** August 14, 2023 is the last day to purchase or renew your S/MIME certificates under existing standards.
- **Order Submission:** For S/MIME certificates that have been purchased or renewed under existing standards, August 21, 2023 is the last day for order submission.
- **Validation:** Any orders not validated by August 28, 2023 will be canceled and refunded through store credits.

You can seek help from the Sectigo support team 24/7 if you encounter any challenges during the transition.

SECTIGO®

FAQ's

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

Q9: What happens if I miss any of the Sectigo cut-off dates?

Your S/MIME orders will be canceled. A Sectigo store credit will be refunded for the same value purchased. New S/MIME certificates that are compliant with the updated standards will be available in-store for future purchases.

Q10: How will these changes benefit my organization?

The CA/Browser Forum intends for the new S/MIME Baseline Requirements to ensure a uniformly high degree of security and trustworthiness for S/MIME certificates, just as the Baseline Requirements do for SSL and Code Signing certificates. As these are universal requirements that all public CAs must follow, ongoing use of S/MIME certificates requires adherence to these new standards.

Q11: What happens if I don't update my S/MIME configuration?

Most environments will be able simply to use BR-compliant S/MIME certificates without impact. If your systems use certificates in an atypical way, with pinning, for example, that could result in service outages. To ensure maximum compatibility and uptime, you should look for and remove custom requirements that are beyond the expectations for commonplace S/MIME certificates.

Q12: Can I continue using my existing S/MIME certificates after September 1st,

To comply with the new S/MIME standards, generating new S/MIME certificates that adhere to the updated requirements is recommended. While you may still be able to use existing certificates, replacing them with new certificates is advisable to benefit from the enhanced security features.

Q13: What support is available if I need assistance during the transition?

If you require any assistance or encounter challenges during the transition to the new S/MIME standards, our Sectigo support team is available to help 24/7.

Q14: Will these changes affect my email recipients who are using different email clients?

These changes are not expected to impact email clients. However, we recommend testing the compatibility of the new S/MIME certificates with other existing applications for your email recipients.

Q15: How do these changes contribute to overall email security?

The updated S/MIME standards, with stronger encryption algorithms, improved key lengths, and enhanced certificate validation procedures, enhance the security and trustworthiness of email communication. By adopting these changes, the integrity, confidentiality, and authenticity of your email communications will be strengthened, ensuring a higher level of overall email security.

Q16: Where can I find more information about the upcoming S/MIME standard changes?

For more information and further details about the upcoming S/MIME standard changes, you are invited to watch Sectigo New S/MIME Baseline Requirements Webinar or read about the official baseline requirements document here.