The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2023

Volume 24, Pages 83-88

IConTech 2023: International Conference on Technology

S/MIME Certificate Test Suite

Yagmur Fidaner
Gazi University

Aysun Coskun
Gazi University

Tamer Ergun
Cloudpeer

Abstract: In today's world, email usage has become a necessity. Emails, with a large user base, serve various functions not only for personal purposes but also for facilitating communication between teams in the business world and acting as a point of contact for organizations with their customers. Emails that have infiltrated our lives are also at the center of data breaches, leaks, and malicious attacks. To ensure email security, it is possible to send digitally signed and encrypted emails using the public key infrastructure-based S/MIME certificates. The existing standards for S/MIME certificates were deemed insufficient, and in 2023, for the first time, the Certificate Authority/Browser (CA/B) Forum, consisting of Certificate Authorities (CA) and application software providers and recognized as an international authority, published the S/MIME Baseline Requirements (BR) document. While compliance with the Baseline Requirements document published by the CA/B Forum ensures reliability through conformity checks for SSL certificates used in web security, this audit was considered insufficient. To monitor and audit SSL certificates, the Certificate Transparency project was introduced, aiming to provide an open structure to safeguard the certificate issuance process. However, in reliable S/MIME certificates, the control mechanism is limited to BR audits. The study establishes a comprehensive S/MIME certificate public key infrastructure that allows analyzing email applications; behaviors in the face of certificates that do not comply with the BR during the certificate validation phase. Additionally, the study aims to develop a user application that enables end-users to test the security and compliance of certificates with the BR.

Keywords: S/mime, Email, Public key infrastructure, Certificate, Security

Introduction

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a protocol that ensures secure sending and receiving of electronic messages (Schaad, 2019). S/MIME employs digital signatures for authentication, non-repudiation and message integrity, while encryption ensures data confidentiality. These capabilities are derived from public key infrastructure (Schaad et al., 2019). Using certificates in X.509 format (ITU, 2019), cryptographic key pairs are digitally associated with email addresses. Certification Authorities (CAs) are responsible for certificate generation, issuance, revocation, and management. The CA/B Forum, a voluntary international organization comprising certificate authorities, email service providers, web browser providers, and third-party application software vendors, has been established (CA/ Browser Forum, 2023). In 2020, the CA/B Forum formed a working group to define rules for the production of reliable S/MIME certificates, leading to the publication of the Baseline Requirements (BR) in 2023. CAs must comply with BR to produce internationally recognized trustworthy S/MIME certificates (CA/Browser Forum, 2023).

The Certificate Transparency (CT) project, initially developed for SSL certificates, aims to maintain the integrity of the certificate issuance process by providing an open framework for monitoring and auditing SSL certificates (Laurie et al., 2021). A study revealed 907,000 SSL certificates were issued without compliance to the CA/B Forum's Baseline Requirements, using data from CT logs (Scheitle & Gasser, 2018). Despite the expectation that CAs produce certificates following a specific template, the number of SSL certificates in use that do not align with public key infrastructure and BR requirements is significant. Literature suggests the creation of a test suite to evaluate web browsers' behavior towards certificates not conforming to the SSL Baseline Requirements (Simsek et al., 2022). The Baseline Requirements document considered in the study is specific to SSL certificates, and the test suite was tailored to SSL certificates.

Unlike SSL certificates, there is no third-party framework for monitoring and auditing generated S/MIME certificates; the control mechanism is limited to the certifying authorities and email applications. It is crucial not only for CAs to produce certificates using appropriate templates but also for email applications to authenticate the utilized certificate properly. A study in 2009 focused on the user interfaces of applications supporting S/MIME structure, resulting in a product emphasizing these interfaces (Levi & Guder, 2009). Additionally, research has been conducted on plugins verifying digital signatures in S/MIME and OpenPGP-supported applications (Poddebniak, 2018; Muller, 2019). These studies include attacks on various aspects, one of which is the Cryptographic Message Syntax (CMS) attack utilizing the Encrypted Message Syntax (CMS) standard developed by IETF for cryptographic protection and digital signing and encryption processes (Housley, 2009). Vulnerabilities in handling various CMS structures and secure certificate chain establishment in S/MIME applications were identified and exploited for attack purposes. Our product will preemptively identify and mitigate these vulnerabilities in S/MIME applications' CMS structures.

This study will analyze email application certificate verification mechanisms, referencing the Baseline Requirements document, which encompasses RFC 5280 and X.509 standards and additional requirements. An S/MIME certificate test public key infrastructure, the S/MIME Test Suite, has been established. The S/MIME Test Suite consists of PKI components, each representing a scenario with a single BR requirement violation. This enables the analysis of email application behavior concerning the specific violation.

Method

In the study, a certificate hierarchy has been established to be used in the conducted tests. Within the certificate hierarchy, root certificates, sub-root certificates, and end-user certificates have been generated in the X.509 ASN.1 structure. Certificate Revocation Lists (CRLs) have been utilized to ensure the revocation status checks of the generated certificates. An example certificate hierarchy model is illustrated below:

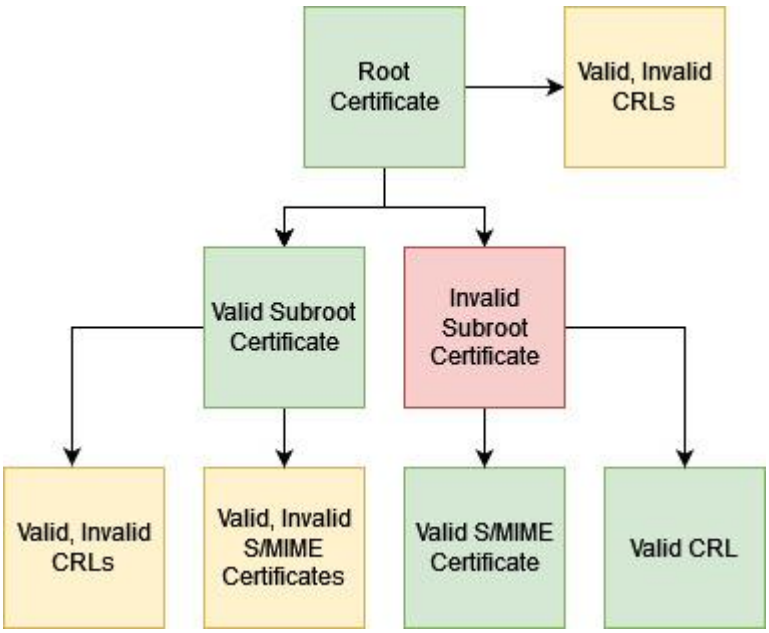

Figure 1. S/MIME certificate hierarchy model

The certificate hierarchy progresses from a valid root certificate that complies with BR requirements. Scenarios will be tested using different sub-root and end-user certificates generated by this root. Signing and encryption operations on emails will be performed using both invalid and valid S/MIME certificates. The behaviors of email applications in response to these scenarios will be analyzed.

Certificate Validation and Scenario Generation

Requirements related to the validation of S/MIME certificate profiles in BR have been shared, which should not be overlooked during the certificate verification phase. Based on BR 1.0.0 version, the following requirements have been identified and added to the test scenarios for verification.

Certificate Version Control

X.509 certificates in Version 1 and Version 2 formats were found lacking in certain aspects, necessitating additional information within the certificates. Therefore, the Version 3 certificate format, which includes Version 2, was introduced (Cooper, et al., 2008). BR-compliant certificates must be in X.509 format and Version 3, as specified in BR Section 7.1.1 (Yee, 2013). To ensure compliance, Version 2 S/MIME certificates were generated.

Certificate Algorithm and Key Control

According to BR Section 6.1.5, certificates must be signed starting from root certificates using RSA and ECDSA key pairs. RSA key pairs should be at least 2048 bits in size. For ECDSA, NIST P-256, NIST P-384, NIST P-521 elliptic curves, and *curve25519* and *curve448* elliptic curve algorithms in EdDSA are accepted. BR Section 7.1.3 provides detailed object identifiers (OIDs) for algorithms. Certificates with algorithms and OIDs not specified in the accepted algorithms were generated to conduct the checks.

Certificate Validity Period Control

Certificates generated must have a maximum validity period of 825 days for Strict and Multipurpose certificates and 1185 days for Legacy certificates, as per BR Section 6.3.2. Certificates exceeding the allowed validity period were generated for verification.

Certificate Content and Extension Checks

BR Section 7.1.2 specifies the required format for certificate content and extensions, termed as the application of RFC 6818. RFC 6818 updates RFC 5280, presenting profiles for X.509 public key infrastructure certificates and CRLs. Certificates not adhering to these specifications were generated for analysis.

Basic Constraints Extension Control

Certificates in a certificate chain can generate other certificates. This extension specifies if a certificate is a CA certificate or an end-entity certificate and how deep a certification path may exist. According to BR, root and sub-root certificates must have this extension, with the CA bit set. For end-user certificates, even if this extension exists, the CA bit must not be set. Certificates were generated both without this extension and with this extension set but the CA bit unset for sub-root certificates.

Key Usage Extension Control

This extension indicates the purposes for which the public key can be used. It includes flags for *digitalSignature*, *dataEncipherment*, *keyEncipherment* and *nonRepudiation*. According to BR, root and sub-root certificates must have this extension with the *keyCertSign* and *cRLSign* bits set. Certificates were generated without this extension or with bits set outside those specified in BR.

Extended Key Usage (EKU) Extension Control

For sub-root and end-user certificates other than cross-certificates, this extension must be present and must contain the *id-kp-emailProtection* value. It must not contain *id-kp-codeSigning*, *id-kp-serverAuth*, *id-kp-timeStamping*, or *anyExtendedKeyUsage* values. Certificates were generated both without this extension and with this extension containing undesirable values.

Subject Alternative Name Extension Control

End-user certificates must include this extension. All email addresses found in the subject field must also be in this extension. Certificates were generated that did not comply with this requirement.

Certificate Policies Extension Control

End-user certificates must have policy identifiers as defined in BR Section 7.1.6.1, based on certificate type and usage. Certificates were generated without these specified policy identifiers.

CRL Distribution Points Extension Control

Sub-root and end-user certificates must have this extension, containing at least one URI address of a CA CRL service. Certificates without this extension or with incorrect URI addresses were generated.

Certificate Revocation Checks

Certificates generated using the public key infrastructure can be revoked for specific reasons before their validity period expires. BR-compliant certificates' revocation reasons and periods are detailed in BR Section 4.9.1. Certificate status checks can be done online and offline. CRLs carry information about revoked certificates, generated by the CA, and are published offline after being signed. OCSP allows online certificate revocation checks. In OCSP usage, the certificate status is checked instantly, providing a reliable response to end-users (Santesson et al., 2013). After discussions among authorities in CA/B Forum, OCSP usage is optional in BR (2022-09-29 Minutes of the CA/Browser Forum Teleconference, 2022). This change aims to prevent a potential scenario where OCSP usage might allow a CA to track when and where an S/MIME protected message is opened by the recipient (Digicert, 2023). Additionally, for sub-root and end-user certificates, CRL usage is mandatory for certificate status checks.

CRL Validity Period Control

CRLs for end-users should be updated at least every 7 days, with the difference between *nextUpdate* and *thisUpdate* fields within the CRL not exceeding 10 days, as per BR Section 4.9.7. For sub-root certificates, CRLs should be renewed every 12 months under normal circumstances and within 24 hours if a sub-root certificate is revoked. The difference between *nextUpdate* and *thisUpdate* fields within the CRL should not exceed 12 months. Certificates not meeting these conditions were generated to ensure compliance.

Results and Discussion

As a result, considering BR requirements and potential vulnerabilities, a comprehensive test suite has been designed. The test suite infrastructure consists of 1 root, 4 sub-roots, 8 CRLs, and 19 end-user certificates. Detailed information about the generated certificates for this suite is provided in Table 1.

Conclusion

As a result, emails are frequently used and distributed in nature. The behavior of email applications in the face of non-compliant certificates with BR requirements is crucial for secure email communication.

Table 1. Generated end -user certificates for S/MIME test suite

Certificate name	Certificate information	Expected validation result
SMIME_1	Valid certificate	VALID
SMIME_2	The version information of the certificate is not valid (Version 2)	NOT VALID
SMIME_3	Certificate has expired	NOT VALID
SMIME_4	Certificate has been revoked in CRL	NOT VALID
SMIME_5	Certificate has expired CRL	NOT VALID
SMIME_6	Certificate has incorrect URI address for CRL	NOT VALID
SMIME_7	Certificate has invalid signing algorithm	NOT VALID
SMIME_8	Certificate has no EKU extension	NOT VALID
SMIME_9	Certificate has invalid EKU extension (has no id-kp-emailProtection)	NOT VALID
SMIME_10	Certificate has no SAN extension	NOT VALID
SMIME_11	Certificate has invalid SAN extension	NOT VALID
SMIME_12	Certificate has invalid Key Usage extension (digitalSignature bit not set)	NOT VALID
SMIME_13	Certificate has invalid Basic Constraints extension	NOT VALID
SMIME_14	Certificate has no specified policy identifier	NOT VALID
SMIME_15	Certificate has invalid digital signature	NOT VALID
SMIME_16	The signature of the sub-root certificate is invalid	NOT VALID
SMIME_17	Sub-root certificate has expired	NOT VALID
SMIME_18	Sub-root certificate has been revoked in CRL	NOT VALID
SMIME_19	Root certificate is not trusted	NOT VALID

In this study, potential scenarios have been derived based on BR, and a comprehensive test suite has been designed. In the follow-up study, using the test S/MIME certificates generated in this research, email signing and encryption operations will be conducted to analyze existing email client applications from a security perspective. Additionally, the study aims to develop a user application that allows end users to test the security and compliance of certificates, ensuring compatibility with BR.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Technology (www.icontechno.net) held in Antalya/Turkey on November 16-19, 2023.

References

CA/ Browser Forum. (2022, September 29). Minutes of the CA/Browser Forum teleconference. Retrieved from https://cabforum.org/2022/09/29/2022-09-29-minutes-of-the-ca-browser-forum-teleconference/

CA/ Browser Forum. (2023, August 7). CA/ Browser Forum. Retrieved, from https://cabforum.org/

CA/Browser Forum. (2023). *Baseline requirements for the issuance and management of publicly trusted S/MIME certificates.* Retrieved from https://cabforum.org/wp-content/uploads/CA-Browser-Forum-SMIMEBR-1.0.0.pdf

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, RFC:5280. *Network Working Group*,1-151.

Digicert. (2023, July 8). CA/Browser forum adopts first baseline requirements for S/MIME certificates. Retrieved from https://www.digicert.com/blog/ca-browser-forum-adopts-s-mime-baseline-requirements

Housley, R. (2009). Cryptographic message syntax (CMS) RFC:5652. *Network Working Group.*

ITU. (2019). X.509: Information technology - open systems interconnection - the directory: Public-key and attribute certificate frameworks.

Laurie, B., Messeri, E., & Stradling, R. (2021). Certificate transparency version 2.0 RFC:9162. 1-53. *Internet Engineering Task Force (IETF).*

Levi, A., & Guder, C. (2009). Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach. *Computers & Security*, 105-120.

Muller, J. (2019). {"Johnny}, you are {fired!"}–Spoofing {OpenPGP} and {S/MIME} signatures in emails. *28th USENIX Security Symposium (USENIX Security 19).*

Poddebniak, D. (2018). Efail: Breaking {S/MIME} and {OpenPGP} email encryption using exfiltration channels. *27th USENIX Security Symposium.*

Santesson, S., Myers, M., Ankney, R., & Malpani, A. (2013). X.509 internet public key infrastructure online certificate status protocol - OCSP RFC:6960. *Internet Engineering Task Force (IETF).*

Schaad, J. (2019). Secure/multipurpose internet mail extensions (S/MIME) version 4.0 message specification.

Schaad, J., Cellars, A., & Ramsdell, B. (2019). Secure/multipurpose internet mail extensions (S/MIME) version 4.0 RFC:8550. *Internet Engineering Task Force (IETF).*

Scheitle, Q., & Gasser, O. (2018). The rise of certificate transparency and its implications on the internet ecosystem. *IMC '18: Proceedings of the Internet Measurement Conference.*

Simsek, M. M., Ergun, T., & Temucin, H. (2022). SSL test suite: SSL certificate test public key infrastructure. *30th Signal Processing and Communications Applications Conference (SIU*).

Yee, P. (2013). Updates to the internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. *Internet Engineering Task Force (IETF).*

Author Information

Yagmur Fidaner
Gazi University
Ankara, Turkey
Contact e-mail: *yagmur.fidaner@gazi.edu.tr*

Aysun Coskun
Gazi University
Ankara, Turkey

Tamer Ergun
Cloudpeer
İstanbul, Turkey

To cite this article:

Fidaner, Y., Coskun, A., & Ergun, T. (2023). S/MIME certificate test suite. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 24*, 83-88.