BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2025
http://excel.fit.vutbr.cz

S/MIME Email Security in Roundcube

Zdeněk Dobeš*

Abstract

S/MIME is a technology that utilizes digital certificates to provide end-to-end security to e-mail communication via digital signature and encryption. This work presents a Roundcube plugin for a faculty e-mail client to enable students, academic staff and faculty employees to achieve confidentiality, integrity, authenticity and non-repudiation of their messages.

Plugin offers a server-based solution that performs digital signature and encryption directly into the MIME message as well as verifies the signature and decrypts the message. It focuses on keeping digital certificates validated before each use and securely stores them in the hierarchical certificate store. The current implementation successfully secures both text and attachments and accurately restores and displays verified data.

*xdobes21@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

With the rise of AI technologies that enable users to easily generate scam messages and impersonate others, the need for trusted and secured messages is much critical than ever. The Plugin S/LIME offers solution by securing e-mail messages through standard S/MIME 4.0 [1] using cryptographic message syntax (CMS) [2] which is based on cryptographic standard PKCS#7. To ensure credibility of the users S/MIME uses digital certificates issued and managed by centralized certificate authorities.

The current solution for Roundcube users represents plugin Enigma, that provides security through standard OpenPGP [3]. The biggest disadvantage of OpenPGP lies in its trust model that is called 'Web of Trust'. The credibility of OpenPGP keys relies on mutual trust built upon signing each others public keys or certificates with their own private keys [4]. Each user then should spend time validating the keys and considering the proper risks based on key references which can easily become unsustainable. On the other hand the advantage of the OpenPGP is definitely the price. Every user can start using their key pairs immediately after they've been generated. S/MIME requires certificate authorities to manage their certificates which commonly comes with a charge.

S/LIME enables users to sign and encrypt messages to ensure its safety during transition. Even though most of the SMTP communication is secured by SSL these days, it is not a rule and it doesn't provide certainty to the user that his message won't be read or modified along the way. S/LIME can make the messages encrypted through combination of symmetrical and asymmetrical encryption and ensures its non-modifiability with asymmetrical encryption and hash functions.

S/LIME is designed for a default Roundcube skin Elastic but also supports historically popular skin Larry, that is still widely used by many users. The UI elements are based on Roundcube elements so it matches the aesthetics of the client.

2. Storing Certificates

The plugin stores certificates in the hierarchical structure based on hash values of the last N bits to optimize performance and provide scalability. Each user has its own folder where are his certificate and private key stored in PKCS#12 secured files. Files are protected by the hash of his password so even though database is leaked, the certificates remain secure. There can be found stored also previous PKCS#12 files of the user so he can easily decrypt and view older messages encrypted by expired certificates. There are also stored public certificates of the other users which are necessary for encrypting operation to other users. Every file do not only contain a digital certificate

but also its certificate path so the certificates can be anytime validated to remain credible.

3. Certificate Verification

The plugin focuses on ensuring that all composed messages are signed or encrypted with valid certificates therefore every certificate is validated before each use. In case of an error during composing a message users are notified about its nature and are forbidden to finish the operation. When importing their certificates, users are also notified about the error, but not stopped because they of potential importing of expired certificate that was once valid and that are required to view old messages. On the other hand importing public certificates is purely strict because it is all about working with real time data.

4. Digital Signature and Message Encryption

To ensure integrity, authenticity and non-repudation of data S/MIME offers securing messages through digital signature. User at first calculates hash of the message and encrypts it with its own private key. If recipient calculates hash of the message and decrypts the value of the attached hash, he ensures that message was not modified. Plugin makes this possible thanks to CMS data type SignedData, that holds information such as signature, used signature algorithm and time of signing. This Data type is then directly integrated into e-mail MIME structure and is sent in the message.

To ensure confidentiality and also partially integrity S/MIME offers securing data through encryption. Firstly the key for a symmetrical encryption is generated and data are secured with it. Then the key is encrypted through asymmetrical encryption provided beforehand by the recipient of the message. The content of the message is encapsulated into either CMS data type EnvelopedData or AuthEnvelopedData based on used algorithm.

5. Distributing Certificates

Because encrypting data is not possible without sender owning a certificate of its recipient, plugin offers a way of distributing certificates directly through messages. The message accompanied by a digital certificate does also contain its certificate path so sender is able to validate the received certificate. S/LIME enables to import these attached certificates simply by clicking the import button above the message when its detected.

6. Plugin Customizability

Plugin offers multiple ways of adjusting behavior to satisfy every user. Plugin enables users to automatize both signing and encrypting in every message and also automatize the process of obtaining certificates by importing every automatically importing every received certificate. For more experienced users the plugin offers advanced option such as selecting a specific symmetrical algorithm to be used for an encryption.

7. Conclusions

S/LIME provides server based solution for securing data via standard S/MIME 4.0 by signing and encrypting their data. To ensure the credibility of the users S/MIME integrates digital certificates into its standard.

If you're looking for a way to secure your sent data in Roundcube feel free to use the new plugin S/LIME!

Acknowledgements

I would like to thank my supervisor Ing. Jaroslav Dytrych, Ph.D for for his wise guidance, consultations, reviews and allaround support. Especially when I'm disturbing his peace during weekends.

References

[1] Jim Schaad, Blake C. Ramsdell, and Sean Turner. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. RFC 8551, April 2019.

[2] Russ Housley. Cryptographic Message Syntax (CMS). RFC 5652, September 2009.

[3] Paul Wouters, Daniel Huigens, Justus Winter, and Niibe Yutaka. OpenPGP. RFC 9580, July 2024.

[4] Jörg Schwenk. *Guide to internet cryptography security protocols and real-world attack implications*. Information security and cryptography. Springer, Cham, 2022.