Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 4, 2014

Y. Kadobayashi
NAIST
K. ANDO
BBsec
K. Kasamatsu
S. Kanno
NTT SOFT

March 3, 2014

Use of S/MIME Encryption Function in Enterprises
draft-kadobayashi-smime-secureops-00

Abstract

In this document, we provide a method for enterprises to utilize and operate the use of S/MIME to handle highly confidential information.

Status of This Memo

This Internet-Draft will expire on September 4, 2014.

Copyright Notice

Table of Contents

1. Introduction

Use of the S/MIME encryption function within enterprises allows them to handle highly confidential information such as business critical information. However, use of encryption, decreases the functionality of anti-virus software and creates the need to manage expired digital certificates. In this document, we provide a method for enterprises to utilize and operate the use of S/MIME to handle highly confidential information.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Decrease of anti-virus functionality on the e-mail server

There is an issue where anti-virus software on e-mail servers may not properly function when encrypted e-mails are received. The following issues are also seen when the anti-virus software does not function properly.

2.1. Use of anti-virus function at S/MIME user agent

Using S/MIME at user agent(MUA), it is highly recommended that the S/ MIME decrypted e-mails must be checked by anti-virus function immediately after the decryption.

2.2. Use of S/MIME at the Gateway

Using S/MIME at the Gateway is one way to work around the anti-virus issue. By implementing S/MIME at the Gateway, viruses can be detected at the Gateway. By storing and managing keys of senders at the Gateway, e-mails can be decrypted and scanned for viruses at the Gateway.

3. Decreased monitoring of highly confidential e-mails that are sent and received

Monitoring may decrease when sending highly confidential information, such as business information to a party outside of the organization. This issue differs from the issue where anti-virus functionality decreases, and an organization must consider that e-mails must be monitored when sending the e-mail (immediate monitoring) and e-mail contents must be monitored every so often after the e-mail has been sent (intermittent monitoring).

For immediate monitoring, S/MIME at the Gateway introduced previously (3.1) can be used to maintain confidentiality outside of the organization and monitoring in accordance to organizational policies also becomes possible. For intermittent monitoring, the following methods where keys are managed or decrypted e-mails are managed can be used.

3.1. Method for managing keys

When digital certificates are disposed, e-mails that were encrypted using that certificate cannot be decrypted, so you can choose to manage and maintain such digital certificates. However, the disclosure of a private key for an expired digital certificate contains the same dangers as the disclosure of a private key for a valid digital certificate. Keys can be managed by sharing keys or delegating management of the keys through the implementation of S/ MIME at the Gateway.

3.2. Accessing e-mails that have been decrypted

Since the contents of encrypted e-mails cannot be read if the expired keys are not stored, decrypted e-mails can be stored in plaintext if expired keys are not managed and stored. In this case, you may be saving highly confidential information in plaintext, therefore access to such information must be managed properly.

4. Importance of the management of expired certificates

In order to be able to use encrypted e-mails into the future, you must store expired digital certificates of the senders. Expired digital certificates may be leveraged for impersonation, so storage of these certificates must be done carefully, increasing the burden on the recipient. To handle this issue, you can use the following technological measure in addition to the methods described in 4.1 and 4.2.

4.1. Use of Dual Key Pairs

Key pairs that have expired should be disposed of as quickly as possible, but key pairs for encryption must be stored for an extended period of time for decryption purposes. One can use separate key pairs for encryption and signing. This allows a user to not have to change key pairs for encryption when the certificate has expired.

5. Acknowledgements

TBD.

6. IANA Considerations

This memo includes no request to IANA.

7. Privacy Considerations

TBD.

8. Security Considerations

TBD.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, January 2010.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

Authors’ Addresses

Youki Kadobayashi
Nara Institute of Science and Technology

Email: youki-k@is.aist-nara.ac.jp

Kazunori Ando
BroadBand Security, Inc.

Email: ando@bbsec.co.jp

Kohei Kasamatsu
NTT Software Corporation

Email: kasamatsu.kohei@po.ntts.co.jp

Satoru Kanno
NTT Software Corporation

Email: kanno.satoru@po.ntts.co.jp