PKIX Working Group
Internet Draft
Document: draft-ietf-pkix-cmc-trans-01.txt
March 2002
Expires: September 2002

J. Schaad
Soaring Hawk Consulting
M.Myers
TraceRoute Security
X.Liu
Cisco
J. Weinstein

CMC Transport

Status of this Memo

Copyright Notice

Abstract

This document defines a number of transport mechanisms that are used to move [CMC] messages. The transport mechanisms described in this document are: HTTP, file, mail and TCP.

1. Overview

This document defines a number of transport methods that are used to move [CMC] messages. The transport mechanisms described in this document are: HTTP, file, mail and TCP.

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].

2. File based protocol

Enrollment messages and responses may be transferred between clients and servers using file system-based mechanisms, such as when enrollment is performed for an off-line client. When files are used to transport binary, BER-encoded Full Enrollment Request and Response messages. There MUST be only one instance of a request or response message in a single file. The following file type extensions SHOULD be used:

Message Type	File Extension
Full PKI Request	.crq
Full PKI Response	.crp

3. Mail based protocol

MIME wrapping is defined for those environments that are MIME native.

The basic mime wrapping in this section is taken from [SMIMEV2] and [SMIMEV3]. Simple enrollment requests are encoded using the "application/pkcs10" content type. A file name MUST be included either in a content type or a content disposition statement. The extension for the file MUST be ".p10".

Simple enrollment response messages MUST be encoded as content-type "application/pkcs7-mime". An smime-type parameter MUST be on the content-type statement with a value of "certs-only." A file name with the ".p7c" extension MUST be specified as part of the content-type or content-disposition statement.

Full enrollment request messages MUST be encoded as content-type "application/pkcs7-mime". The smime-type parameter MUST be included with a value of "CMC-enroll". A file name with the ".p7m" extension MUST be specified as part of the content-type or content-disposition statement.

Full enrollment response messages MUST be encoded as content-type "application/pkcs7-mime". The smime-type parameter MUST be included with a value of "CMC-response." A file name with the ".p7m" extensions MUST be specified as part of the content-type or content-disposition statement.

MIME TYPE	File Extension	SMIME-TYPE
application/pkcs10 (simple PKI request)	.p10	N/A
application/pkcs7-mime (full PKI request)	.p7m	CMC-request
application/pkcs7-mime (simple PKI response)	.p7c	certs-only
application/pkcs7-mime (full PKI response)	.p7m	CMC-response

4. HTTP/HTTPS based protocol

HTTP messages are wrapped with by a mime object as specified above.

5. TCP based protocol

When CMC messages are sent over a TCP-Based connection, no wrapping is required of the message. Messages are sent in their binary encoded form.

The connection is closed by the server after generating a response for the client. (All CMC request messages from client to server generate a response message.) If a second set of messages from the client to the server is required to complete the transaction, the client generates a new TCP-Based connection for this purpose, it cannot reuse an existing one.

Out of band setup can be used to keep a TCP-Based connection open for more than one message pair. A situation where this can occur is an RA talking to a CA over a specially setup TCP connection.

6 Socket-Based Transport

When enrollment messages and responses are sent over sockets, no wrapping is required. Messages MUST be sent in their binary, BER-encoded form.

7. Security Considerations

Mechanisms for thwarting replay attacks may be required in particular implementations of this protocol depending on the operational environment. In cases where the CA maintains significant state information, replay attacks may be detectable without the inclusion of the optional nonce mechanisms. Implementers of this

protocol need to carefully consider environmental conditions before choosing whether or not to implement the senderNonce and recipientNonce attributes described in section 5.6. Developers of state-constrained PKI clients are strongly encouraged to incorporate the use of these attributes.

8. Acknowledgments

The authors would like to thank Brian LaMacchia for his work in developing and writing up many of the concepts presented in this document. The authors would also like to thank Alex Deacon and Barb Fox for their contributions.

9. References

[CMC] J. Schaad, M. Myers, X. Liu, J. Weinstein, ôBASEö, <base>.

[CMS] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[CRMF] Myers, M., Adams, C., Solo, D. and D. Kemp, "Internet X.509 Certificate Request Message Format", RFC 2511, March 1999.

[DH] B. Kaliski, "PKCS 3: Diffie-Hellman Key Agreement v1.4"

[DH-POP] H. Prafullchandra, J. Schaad, "Diffie-Hellman Proof-of-Possession Algorithms", Work in Progress.

[HMAC] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[PKCS1] Kaliski, B., "PKCS #1: RSA Encryption, Version 1.5", RFC 2313, March 1998.

[PKCS7] Kaliski, B., "PKCS #7: Cryptographic Message Syntax v1.5", RFC 2315, October 1997.

[PKCS8] RSA Laboratories, "PKCS#8: Private-Key Information Syntax Standard, Version 1.2", November 1, 1993.

[PKCS10] Kaliski, B., "PKCS #10: Certification Request Syntax v1.5", RFC 2314, October 1997.

[PKIXCERT] Housley, R., Ford, W., Polk, W. and D. Solo "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

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

[SMIMEV2] Dusse, S., Hoffman, P., Ramsdell, B., Lundblade, L. and L. Repka, "S/MIME Version 2 Message Specification", RFC 2311, March 1998.

[SMIMEV3] Ramsdell, B., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

[X942] Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999.

10. Authors' Addresses

Jim Schaad
Soaring Hawk Consulting

EMail: jimsch@exmsft.com

Michael Myers
TraceRoute Security, Inc.

EMail: myers@coastside.net

Xiaoyi Liu
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134

Phone: (480) 526-7430
EMail: xliu@cisco.com

Jeff Weinstein

EMail: jsw@meer.net

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.