Network Working Group
Request for Comments: 5273
Category: Standards Track

J. Schaad
Soaring Hawk Consulting
M. Myers
TraceRoute Security, Inc.

June 2008

Certificate Management over CMS (CMC): Transport Protocols

Status of This Memo

Abstract

This document defines a number of transport mechanisms that are used to move CMC (Certificate Management over CMS (Cryptographic Message Syntax)) 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 (defined in [CMC-STRUCT]). 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 [MUST].

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, Full PKI Request or Full PKI 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
Simple PKI Request	.p10
Full PKI Request	.crq
Simple PKI Response	.p7c
Full PKI Response	.crp

File PKI Request/Response Identification

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 [SMIMEV3]. When using a mail-based protocol, MIME wrapping between the layers of CMS wrapping is optional. Note that this is different from the standard S/MIME (Secure MIME) message.

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-Request". 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" extension MUST be specified as part of the content-type or content-disposition statement.

Item	MIME Type	File Extension	SMIME Type
Simple PKI Request	application/pkcs10	.p10	N/A
Full PKI Request	application/pkcs7-mime	.p7m	CMC-request
Simple PKI Response	application/pkcs7-mime	.p7c	certs-only
Full PKI Response	application/pkcs7-mime	.p7m	CMC-response

Table 1: MIME PKI Request/Response Identification

4. HTTP/HTTPS-Based Protocol

This section describes the conventions for use of HTTP [HTTP] as a transport layer. In most circumstances, the use of HTTP over TLS [TLS] provides any necessary content protection from eavesdroppers.

In order for CMC clients and servers using HTTP to interoperate, the following rules apply.

Clients MUST use the POST method to submit their requests.

Servers MUST use the 200 response code for successful responses.

Clients MAY attempt to send HTTP requests using TLS 1.0 [TLS] or later, although servers are not required to support TLS.

Servers MUST NOT assume client support for any type of HTTP authentication such as cookies, Basic authentication, or Digest authentication.

Clients and servers are expected to follow the other rules and restrictions in [HTTP]. Note that some of those rules are for HTTP methods other than POST; clearly, only the rules that apply to POST are relevant for this specification.

4.1. PKI Request

A PKI Request using the POST method is constructed as follows:

The Content-Type header MUST have the appropriate value from Table 1.

The body of the message is the binary value of the encoding of the PKI Request.

4.2. PKI Response

An HTTP-based PKI Response is composed of the appropriate HTTP headers, followed by the binary value of the BER (Basic Encoding Rules) encoding of either a Simple or Full PKI Response.

The Content-Type header MUST have the appropriate value from Table 1.

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 client closes a connection after receiving a response, or it issues another request to the server using the same connection. Reusing one connection for multiple successive requests, instead of opening multiple connections that are only used for a single request, is RECOMMENDED for performance and resource conservation reasons. A server MAY close a connection after it has been idle for some period of time; this timeout would typically be several minutes long.

There is no specific port that is to be used when doing TCP-based transport. Only the Private Ports 49152-65535 may be used in this manner (without registration). The ports in the range of 1-49151 SHOULD NOT be used. The port to be used is configured out of band.

6. 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 Certification Authority (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 6.6 of [CMC-STRUCT]. Developers of state-constrained PKI clients are strongly encouraged to incorporate the use of these attributes.

Initiation of a secure communications channel between an end-entity and a CA or Registration Authority (RA) -- and, similarly, between an RA and another RA or CA -- necessarily requires an out-of-band trust initiation mechanism. For example, a secure channel may be constructed between the end-entity and the CA via IPsec [IPsec] or

TLS [TLS]. Many such schemes exist, and the choice of any particular scheme for trust initiation is outside the scope of this document. Implementers of this protocol are strongly encouraged to consider generally accepted principles of secure key management when integrating this capability within an overall security architecture.

In some instances, no prior out-of-band trust will have been initiated prior to use of this protocol. This can occur when the protocol itself is being used to download onto the system the set of trust anchors to be used for these protocols. In these instances, the Enveloped Data content type (Section 3.2.1.3.3 in [CMC-STRUCT]) must be used to provide the same shrouding that TLS would have provided.

7. Acknowledgments

The authors and the PKIX Working Group are grateful for the participation of Xiaoyi Liu and Jeff Weinstein in helping to author the original versions of this document.

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.

8. References

8.1. Normative References

[CMC-STRUCT] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, June 2008.

[HTTP] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[IPsec] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

[SMIMEV3] Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

8.2. Informative References

[TLS] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

Authors' Addresses

Jim Schaad
Soaring Hawk Consulting
PO Box 675
Gold Bar, WA 98251

Phone: (425) 785-1031
EMail: jimsch@nwlink.com

Michael Myers
TraceRoute Security, Inc.

EMail: mmyers@fastq.com

Full Copyright Statement

Intellectual Property