LAMPS Working Group
Internet-Draft
Obsoletes: 5273, 6402 (if approved)
Intended status: Standards Track
Expires: 29 November 2025

J. Mandel, Ed
AKAYLA, Inc.
S. Turner, Ed
sn3rd

28 May 2025

Certificate Management over CMS (CMC): Transport Protocols
draft-ietf-lamps-rfc5273bis-06

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.

This document obsoletes RFC 5273 and RFC 6402.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-lamps-rfc5273bis/.

Discussion of this document takes place on the WG LAMPS mailing list (mailto:spasm@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/spasm/. Subscribe at https://www.ietf.org/mailman/listinfo/spasm/.

Source for this draft and an issue tracker can be found at https://github.com/seanturner/cmcbis.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 November 2025.

Table of Contents

1. Introduction

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.

This document obsoletes [CMC-TRANSv1] and [CMC-Updates]. This document also incorporates [erratum3593].

2. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Changes Since 5273 and 6402

Merged [CMC-Updates] text.

IANA assigned TCP port 5318 for the use of CMC.

Clarified the file extensions for Full PKI Requests and Responses.

Replaced TLS 1.0 for TLS 1.2 or later, and added that implemetations are required to follow the recommendations in [BCP195].

Addressed [erratum3593].

4. 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. crq and crp stand for Full PKI Request/Response, respectively; for clarity we define file extensions for them. 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

Table 1: File PKI Request/Response Identification

5. Mail-Based Protocol

MIME wrapping is defined for those environments that are MIME native. The basic mime wrapping in this section is taken from [SMIMEV4]. 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 2: MIME PKI Request/Response Identification

6. 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 [HTTP] 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 1.2 [TLS] or later, although servers are not required to support TLS. If TLS is supported by an implementation, then the implementation MUST folow the recommendations in [BCP195].

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.

6.1. PKI Request

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

The Content-Type header MUST have the appropriate value from Table 2.

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

6.2. 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 2.

7. 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.

CMC requires a registered port number to send and receive CMC messages over TCP. The title of this IP Protocol number is "pkix-cmc". The value of this TCP port is 5318.

Prior to [CMC-Updates], CMC did not have a registered port number and used an externally configured port from the Private Port range. Client implementations MAY want to continue to allow for this to occur. Servers SHOULD change to use the new port. It is expected that HTTP will continue to be the primary transport method used by CMC installations.

8. IANA Considerations

IANA has assigned a TCP port number in the Registered Port Number range for the use of CMC.

```
Service name: pkix-cmc
Port Number: 5318
Transport protocol: TCP
Description: PKIX Certificate Management using CMS (CMC)
Reference: RFC 6402
Assignee: iesg@ietf.org
Contact: chair@ietf.org
```

9. 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 of [CMC-STRUCT]) must be used to provide the same shrouding that TLS would have provided.

10. References

10.1. Normative References

[BCP195] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/rfc/rfc9325>.

[CMC-STRUCT] Mandel, J. and S. Turner, "Certificate Management over CMS (CMC)", Work in Progress, Internet-Draft, draft-ietf-lamps-rfc5272bis-06, 28 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-rfc5272bis-06>.

[erratum3593] "RFC 5273 erratum 3593", April 2013, <https://www.rfc-editor.org/errata/eid3593>.

[HTTP] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

[IPsec] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/rfc/rfc4301>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[SMIMEV4] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/rfc/rfc8551>.

10.2. Informative References

[CMC-TRANSv1] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC): Transport Protocols", RFC 5273, DOI 10.17487/RFC5273, June 2008, <https://www.rfc-editor.org/rfc/rfc5273>.

[CMC-Updates]
Schaad, J., "Certificate Management over CMS (CMC) Updates", RFC 6402, DOI 10.17487/RFC6402, November 2011, <https://www.rfc-editor.org/rfc/rfc6402>.

[TLS] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/rfc/rfc5246>.

Acknowledgements

Obviously, the authors of this version of the document would like to thank Jim Schaad and Michael Myers for their work on the previous version of this document.

The acknowledgment from the previous version of this document follows:

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.

Contributors

Jim Schaad
August Cellars

Michael Myers
TraceRoute Security, Inc.

Authors' Addresses

Joseph Mandel
AKAYLA, Inc.
Email: joe@akayla.com

Sean Turner (editor)
sn3rd
Email: sean@sn3rd.com