Internet Engineering Task Force (IETF)
Request for Comments: 9811
Obsoletes: 6712, 9480
Category: Standards Track
ISSN: 2070-1721

H. Brockhaus
D. von Oheimb
Siemens
M. Ounsworth
J. Gray
Entrust

July 2025

Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)

Abstract

This document describes how to layer the Certificate Management Protocol (CMP) over HTTP.

It includes the updates to RFC 6712 specified in Section 3 of RFC 9480; these updates introduce CMP URIs using a well-known prefix. It obsoletes RFC 6712; and, together with RFC 9810, it also obsoletes RFC 9480.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9811.

Table of Contents

1. Introduction

The Certificate Management Protocol (CMP) [RFC9810] requires a well-defined transfer mechanism to enable End Entities (EEs), Registration Authorities (RAs), and Certification Authorities (CAs) to pass PKIMessage structures between them.

The first version of the CMP specification [RFC2510] included a brief description of a simple transfer protocol layer on top of TCP. Its features were simple transfer-level error handling and a mechanism to poll for outstanding PKI messages. Additionally, it was mentioned that PKI messages could also be conveyed using file-, email-, and HTTP-based transfer, but those were not specified in detail.

Since the second version of the CMP specification [RFC4210] incorporated its own polling mechanism, the need for a transfer protocol providing this functionality vanished. The remaining features CMP requires from its transfer protocols are connection and error handling.

CMP can benefit from utilizing reliable transport, as it requires connection and error handling from the transfer protocol. All these features are covered by HTTP. Additionally, delayed delivery of CMP response messages may be handled at transfer level, regardless of the message contents. Since [RFC9480] extends the polling mechanism specified in the second version of CMP [RFC4210] to cover all types of PKI management transactions, delays detected at application level may also be handled within CMP, using pollReq and pollRep messages.

The usage of HTTP (e.g., HTTP/1.1 as specified in [RFC9110] and [RFC9112]) for transferring CMP messages exclusively uses the POST method for requests, effectively tunneling CMP over HTTP. While this is generally considered bad practice (see RFC 9205 [BCP56] for best current practice on building protocols with HTTP) and should not be emulated, there are good reasons to do so for transferring CMP. HTTP is used as it is generally easy to implement and it is able to traverse network borders utilizing ubiquitous proxies. Most importantly, HTTP is already commonly used in existing CMP implementations. Other HTTP request methods, such as GET, are not used because PKI management operations can only be triggered using CMP's PKI messages, which need to be transferred using a POST request.

With its status codes, HTTP provides needed error reporting capabilities. General problems on the server side, as well as those directly caused by the respective request, can be reported to the client.

As CMP implements a transaction identification (transactionID), identifying transactions spanning over more than just a single request/response pair, the statelessness of HTTP is not blocking its usage as the transfer protocol for CMP messages.

1.1. Changes Made by RFC 9480

CMP Updates [RFC9480] updated Section 3.6 of [RFC6712], supporting

the PKI management operations specified in the Lightweight CMP Profile [RFC9483], in the following areas:

* Introduced the HTTP URI path prefix '/.well-known/cmp'.

* Added options for extending the URI structure with further segments and defined a new protocol registry group to that aim.

1.2. Changes Made by This Document

This document obsoletes [RFC6712]. It includes the changes specified in Section 3 of [RFC9480], as described in Section 1.1 of this document. Additionally, it adds the following changes:

* Removed the requirement to support HTTP/1.0 [RFC1945] in accordance with Section 4.1 of RFC 9205 [BCP56].

* Implementations MUST forward CMP messages when an HTTP error status code occurs; see Section 3.1.

* Removed Section 3.8 of [RFC6712] as it contains information redundant with current HTTP specification.

2. Conventions Used in This Document

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. HTTP-Based Protocol

For direct interaction between two entities, where a reliable transport protocol like TCP [RFC9293] is available, HTTP [RFC9110] SHOULD be utilized for conveying CMP messages. This specification requires using the POST method (Section 3.1) and the "Content-Type" header field (Section 3.2), which are available since HTTP/1.0 [RFC1945].

Note: In some situations, CMP requires multiple request/response pairs to perform a PKI management operation. Their affiliation with a PKI management operation is indicated by a transaction identifier in the CMP message header (see transactionID described in Section 5.1.1 of [RFC9810]). For details on how to transfer multiple requests, see Section 4.11 of RFC 9205 [BCP56].

3.1. General Form

A DER-encoded [ITU.X690.2021] PKIMessage (Section 5.1 of [RFC9810]) MUST be sent as the content of an HTTP POST request. If this HTTP request is successful, the server returns the CMP response in the content of the HTTP response. The HTTP response status code in this case MUST be 200 (OK); other Successful 2xx status codes MUST NOT be used for this purpose. HTTP responses to pushed CMP announcement messages described in Section 3.5 utilize the status codes 201 and 202 to identify whether the received information was processed.

While Redirection 3xx status codes MAY be supported by implementations, clients should only be enabled to automatically follow them after careful consideration of possible security implications. As described in Section 5, the 301 (Moved Permanently) status code could be misused for permanent denial of service.

All applicable Client Error 4xx or Server Error 5xx status codes MAY be used to inform the client about errors. Whenever a client

receives an HTTP response with a status code in the 2xx, 4xx, or 5xx ranges, it MUST support handling response message content containing a CMP response PKIMessage.

3.2. Media Type

The Internet media type "application/pkixcmp" MUST be set in the HTTP "Content-Type" header field when conveying a PKIMessage.

3.3. Communication Workflow

In CMP, most communication is initiated by the EEs where every CMP request triggers a CMP response message from the CA or RA.

The CMP announcement messages described in Section 3.5 are an exception. Their creation may be triggered by certain events or done on a regular basis by a CA. The recipient of the announcement only replies with an HTTP status code acknowledging the receipt or indicating an error, but not with a CMP response.

If the receipt of an HTTP request is not confirmed by receiving an HTTP response, it MUST be assumed that the transferred CMP message was not successfully delivered to its destination.

3.4. HTTP Request-URI

Each CMP server on a PKI management entity supporting HTTP or HTTPS transfer MUST support the use of the path prefix '/.well-known/' as defined in [RFC8615] and the registered name 'cmp' to ease interworking in a multi-vendor environment.

CMP clients have to be configured with sufficient information to form the CMP server URI. This is at least the authority portion of the URI, e.g., 'www.example.com:80', or the full operation path segment of the PKI management entity. Additionally, path segments MAY be added after the registered application name as part of the full operation path to provide further distinction. The path segment 'p' followed by an arbitraryLabel <name> could, for example, support the differentiation of specific CAs or certificate profiles. Further path segments, e.g., as specified in the Lightweight CMP Profile [RFC9483], could indicate PKI management operations using an operationLabel <operation>. The following list shows examples of valid full CMP URIs:

* http://www.example.com/.well-known/cmp

* http://www.example.com/.well-known/cmp/<operation>

* http://www.example.com/.well-known/cmp/p/<name>

* http://www.example.com/.well-known/cmp/p/<name>/<operation>

Note that https can also be used instead of http; see item 5 in the Security Considerations (Section 5).

3.5. Pushing of Announcements

A CMP server may create event-triggered announcements or generate them on a regular basis. It MAY utilize HTTP transfer to convey them to a suitable recipient. In this use case, the CMP server acts as an HTTP client, and the recipient needs to utilize an HTTP server. As no request messages are specified for those announcements, they can only be pushed to the recipient.

If an EE wants to poll for a potential CA Key Update Announcement or the current Certificate Revocation List (CRL), a PKI Information

Request using a general message as described in Appendix D.5 of [RFC9810] can be used.

When pushing announcement messages, PKIMessage structures MUST be sent as the content of an HTTP POST request.

Suitable recipients for CMP announcements might, for example, be repositories storing the announced information, such as directory services. Those services listen for incoming messages, utilizing the same HTTP Request-URI scheme as defined in Section 3.4.

The following types of PKIMessage are announcements that may be pushed by a CA. The prefixed numbers reflect ASN.1 tags of the PKIBody structure (Section 5.1.2 of [RFC9810]).

[15] CA Key Update Announcement
[16] Certificate Announcement
[17] Revocation Announcement
[18] CRL Announcement

CMP announcement messages do not require any CMP response. However, the recipient MUST acknowledge receipt with an HTTP response having an appropriate status code and empty content. When not receiving such a response, it MUST be assumed that the delivery was not successful. If applicable, the sending side MAY try sending the announcement again after waiting for an appropriate time span.

If the announced issue was successfully stored in a database or was already present, the answer MUST be an HTTP response with a 201 (Created) status code and empty content.

In case the announced information was only accepted for further processing, the status code of the returned HTTP response MAY also be 202 (Accepted). After an appropriate delay, the sender may then try to send the announcement again and may repeat this until it receives a confirmation that it has been successfully processed. The appropriate duration of the delay and the option to increase it between consecutive attempts should be carefully considered.

A receiver MUST answer with a suitable 4xx or 5xx error code when a problem occurs.

4. Implementation Considerations

Implementers should be aware that other implementations might exist that use a different approach for transferring CMP over HTTP. Further, implementations based on earlier documents that led to [RFC6712] might use an unregistered "application/pkixcmp-poll" media type. Conforming implementations MAY handle this type like "application/pkixcmp".

5. Security Considerations

All security considerations in HTTP [RFC9110] apply. The following items need to be considered by implementers and users:

1. There is the risk for denial-of-service attacks through resource consumption by opening many connections to an HTTP server. Therefore, idle connections should be terminated after an appropriate timeout; this may also depend on the available free resources.

2. Without being encapsulated in effective security protocols, such as Transport Layer Security (TLS) [RFC5246] [RFC8446], or without using HTTP digest [RFC9530], there is no integrity protection at the HTTP level. Therefore, information from the HTTP should not

be used to change state of the transaction, regardless of whether any mechanism was used to ensure the authenticity or integrity of HTTP messages (e.g., TLS or HTTP digests).

3. Client users should be aware that storing the target location of an HTTP response with the 301 (Moved Permanently) status code could be exploited by a meddler-in-the-middle attacker trying to block them permanently from contacting the correct server.

4. If no measures to authenticate and protect the HTTP responses to pushed announcement messages are in place, their information regarding the announcement's processing state may not be trusted. In that case, the overall design of the PKI system must not depend on the announcements being reliably received and processed by their destination.

5. CMP provides inbuilt integrity protection and authentication. The information communicated unencrypted in CMP messages does not contain sensitive information endangering the security of the PKI when intercepted. However, it might be possible for an eavesdropper to utilize the available information to gather confidential personal, technical, or business-critical information. The protection of the confidentiality of CMP messages together with an initial authentication of the RA/CA before the first CMP message is transmitted ensures the privacy of the EE requesting certificates. Therefore, users of the HTTP transfer for CMP messages should consider using HTTP over TLS according to [RFC9110] or using virtual private networks created, for example, by utilizing Internet Protocol Security according to [RFC7296].

6. IANA Considerations

IANA has made the following updates:

* the reference for "application/pkixcmp" in the "Media Types" registry <https://www.iana.org/assignments/media-types> refers to this document, instead of [RFC2510].

* the reference for "application/pkixcmp" in the "CoAP Content-Formats" registry <https://www.iana.org/assignments/core-parameters> refers to this document, instead of [RFC4210].

* the reference for "cmp" in the "Well-Known URIs" registry <https://www.iana.org/assignments/well-known-uris/> refers to this document instead of [RFC4210].

* the reference for "p" in the "CMP Well-Known URI Path Segments" registry <https://www.iana.org/assignments/cmp> refers to this document instead of [RFC9480].

No further action by IANA is necessary for this document or any anticipated updates.

7. References

7.1. Normative References

[ITU.X690.2021]
ITU-T, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, 2021, <https://www.itu.int/rec/T-REC-X.690-202102-I/en>.

[RFC1945] Berners-Lee, T., Fielding, R., and H. Frystyk, "Hypertext

Transfer Protocol -- HTTP/1.0", RFC 1945,
DOI 10.17487/RFC1945, May 1996,
<https://www.rfc-editor.org/info/rfc1945>.

[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/info/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/info/rfc8174>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

[RFC9110] 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/info/rfc9110>.

[RFC9112] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP/1.1", STD 99, RFC 9112, DOI 10.17487/RFC9112, June 2022, <https://www.rfc-editor.org/info/rfc9112>.

[RFC9810] Brockhaus, H., von Oheimb, D., Ounsworth, M., and J. Gray, "Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)", RFC 9810, DOI 10.17487/RFC9810, July 2025, <https://www.rfc-editor.org/info/rfc9810>.

7.2. Informative References

[BCP56] Best Current Practice 56, <https://www.rfc-editor.org/info/bcp56>. At the time of writing, this BCP comprises the following:

Nottingham, M., "Building Protocols with HTTP", BCP 56, RFC 9205, DOI 10.17487/RFC9205, June 2022, <https://www.rfc-editor.org/info/rfc9205>.

[RFC2510] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, DOI 10.17487/RFC2510, March 1999, <https://www.rfc-editor.org/info/rfc2510>.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, DOI 10.17487/RFC4210, September 2005, <https://www.rfc-editor.org/info/rfc4210>.

[RFC5246] 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/info/rfc5246>.

[RFC6712] Kause, T. and M. Peylo, "Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)", RFC 6712, DOI 10.17487/RFC6712, September 2012, <https://www.rfc-editor.org/info/rfc6712>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2

(IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9293] Eddy, W., Ed., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, DOI 10.17487/RFC9293, August 2022, <https://www.rfc-editor.org/info/rfc9293>.

[RFC9480] Brockhaus, H., von Oheimb, D., and J. Gray, "Certificate Management Protocol (CMP) Updates", RFC 9480, DOI 10.17487/RFC9480, November 2023, <https://www.rfc-editor.org/info/rfc9480>.

[RFC9483] Brockhaus, H., von Oheimb, D., and S. Fries, "Lightweight Certificate Management Protocol (CMP) Profile", RFC 9483, DOI 10.17487/RFC9483, November 2023, <https://www.rfc-editor.org/info/rfc9483>.

[RFC9530] Polli, R. and L. Pardue, "Digest Fields", RFC 9530, DOI 10.17487/RFC9530, February 2024, <https://www.rfc-editor.org/info/rfc9530>.

Acknowledgements

The authors wish to thank Tomi Kause and Martin Peylo, the original authors of [RFC6712], for their work.

We also thank all reviewers for their valuable feedback.

Authors' Addresses

Hendrik Brockhaus
Siemens
Werner-von-Siemens-Strasse 1
80333 Munich
Germany
Email: hendrik.brockhaus@siemens.com
URI: https://www.siemens.com

David von Oheimb
Siemens
Werner-von-Siemens-Strasse 1
80333 Munich
Germany
Email: david.von.oheimb@siemens.com
URI: https://www.siemens.com

Mike Ounsworth
Entrust
1187 Park Place
Minneapolis, MN 55379
United States of America
Email: mike.ounsworth@entrust.com
URI: https://www.entrust.com

John Gray
Entrust
1187 Park Place
Minneapolis, MN 55379
United States of America

Email: john.gray@entrust.com
URI: https://www.entrust.com