Workgroup: ACE
Internet-Draft:
draft-ietf-ace-cmpv2-coap-transport-07
Published: 27 January 2023
Intended Status: Standards Track
Expires: 31 July 2023
Authors: M. Sahni, Ed.
Palo Alto Networks
S. Tripathi, Ed.
Palo Alto Networks

CoAP Transfer for the Certificate Management Protocol

Abstract

This document specifies the use of Constrained Application Protocol (CoAP) as a transfer mechanism for the Certificate Management Protocol (CMP). CMP defines the interaction between various PKI entities for the purpose of certificate creation and management. CoAP is an HTTP-like client-server protocol used by various constrained devices in the IoT space.

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 31 July 2023.

Table of Contents

1. Introduction

The Certificate Management Protocol (CMP) [RFC4210] is used by the PKI entities for the generation and management of certificates. One of the requirements of Certificate Management Protocol is to be independent of the transport protocol in use. CMP has mechanisms to take care of required transactions, error reporting and protection of messages.

The Constrained Application Protocol (CoAP) defined in [RFC7252] , [RFC7959] and [RFC8323] is a client-server protocol like HTTP. It is designed to be used by constrained devices over constrained networks. The recommended transport for CoAP is UDP, however [RFC8323] specifies the support of CoAP over TCP, TLS and Websockets.

This document specifies the use of CoAP over UDP as a transport medium for the CMP version 2 [RFC4210] , CMP version 3 [I-D.ietf-lamps-cmp-updates] designated as CMP in this document and Lightweight CMP Profile [I-D.ietf-lamps-lightweight-cmp-profile] . This document, in general, follows the HTTP transfer for CMP specifications defined in [RFC6712] and specifies the requirements for using CoAP as a transfer mechanism for the CMP.

This document also provides guidance on how to use a "CoAP-to-HTTP" proxy to ease adoption of CoAP transfer mechanism by enabling the interconnection with existing PKI entities already providing CMP over HTTP.

1.1. 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.

2. CoAP Transfer Mechanism for CMP

A CMP transaction consists of exchanging PKIMessages [RFC4210] between PKI End Entities (EEs), Registration Authorities (RAs), and Certification Authorities (CAs). If the EEs are constrained devices then they may prefer, as a CMP client, the use of CoAP instead of HTTP as the transfer mechanism. The RAs and CAs, in general, are not constrained and can support both CoAP and HTTP Client and Server implementations. This section specifies how to use CoAP as the transfer mechanism for the Certificate Management Protocol.

2.1. CoAP URI Format

The CoAP URI format is described in section 6 of [RFC7252]. The CoAP endpoints MUST support use of the path prefix "/.well-known/" as defined in [RFC8615] and the registered name "cmp" to help with endpoint discovery and interoperability. Optional path segments MAY be added after the registered application name (i.e. after "/.well-known/cmp") to provide 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 [I-D.ietf-lamps-lightweight-cmp-profile], could indicate PKI management operations using an operationLabel <operation>. A valid full CMP URI can look like this:

```
coap://www.example.com/.well-known/cmp
coap://www.example.com/.well-known/cmp/<operation>
coap://www.example.com/.well-known/cmp/p/<name>
coap://www.example.com/.well-known/cmp/p/<name>/<operation>
```

2.2. Discovery of CMP RA/CA

The EEs can be configured with enough information to form the CMP server URI. The minimum information that can be configured is the scheme i.e. "coap:" or "coaps:" and the authority portion of the URI, e.g. "example.com:5683". If the port number is not specified in the authority, then the default ports numbers MUST be assumed for the "coap:" and the "coaps:" scheme URIs. The default port for coap: scheme URIs is 5683 and the default port for coaps: scheme URIs is 5684 [RFC7252] .

Optionally, in the environments where a Local Registration Authority (LRA) or a Local CA is deployed, EEs can also use the CoAP service discovery mechanism [RFC7252] to discover the URI of the Local RA or CA. The CoAP CMP endpoints supporting service discovery MUST also support resource discovery in the CoRE Link Format as described in

[RFC6690] . The Link MUST include the 'ct' attribute defined in section 7.2.1 of [RFC7252] with the value of "application/pkixcmp" as defined in the CoAP Content-Formats IANA registry.

2.3. CoAP Request Format

The CMP PKIMessages MUST be DER encoded and sent as the body of the CoAP POST request. A CMP client SHOULD send each CoAP requests marked as a Confirmable message Section 2.1 of [RFC7252]. If the CoAP request is successful then the server SHOULD return a "2.05 Content" response code. If the CoAP request is not successful then an appropriate CoAP Client Error 4.xx or a Server Error 5.xx response code MUST be returned. A CMP RA or CA may choose to send a Piggybacked response Section 5.2.1 of [RFC7252], to the client or it MAY send a Separate response Section 5.2.2 of [RFC7252], in case it takes some time for CA RA to process the CMP transaction.

When transferring CMP PKIMesssage over CoAP the content-format "application/pkixcmp" MUST be used.

2.4. CoAP Block-Wise Transfer Mode

A CMP PKIMesssage consists of a header, body, protection, and extraCerts structures which may contain many optional and potentially large fields. Thus a CMP message can be much larger than the Maximum Transmission Unit (MTU) of the outgoing interface of the device. The EEs and RAs or CAs, MUST use the Block-Wise transfer mode [RFC7959] to transfer such large messages instead of relying on IP fragmentation.

If a CoAP-to-HTTP proxy is in the path between EEs and CA or EEs and RA then, if the server supports, it MUST use the chunked transfer encoding [RFC9112] to send data over the HTTP transport. The proxy MUST try to reduce the number of packets sent by using an optimal chunk length for the HTTP transport.

2.5. Multicast CoAP

CMP PKIMessages sent over CoAP MUST NOT use a Multicast destination address.

2.6. Announcement PKIMessage

A CMP server may publish announcements, that can be event triggered or periodic, for the other PKI entities. Here is the list of CMP announcement messages prefixed by their respective ASN.1 identifier (section 5.1.2 [RFC4210])

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

An EE MAY use CoAP Observe option [RFC7641] to register itself to get any announcement messages from the RA or CA. The EE can send a GET request to the server's URI suffixed by "/ann". For example a path to register for announcement messages may look like this:

coap://www.example.com/.well-known/cmp/ann
coap://www.example.com/.well-known/cmp/p/<profileLabel>/ann

If the server supports CMP Announcements messages, then it SHOULD send appropriate 2.xx success response code, otherwise a 4.xx or 5.xx error response code. If for some reason server cannot add the client to its list of observers for the announcements, it can omit the Observe option [RFC7641] in the response to the client. A client on receiving a 2.xx success response without the Observe option [RFC7641] can try after some time to register again for announcements from the CMP server. Since server can remove the EE from the list of observers for announcement messages, an EE SHOULD periodically re-register itself for announcement messages.

Alternatively, an EE MAY poll for the potential changes via "PKI Information" request using "PKI General Message" choice for the PKIBody of the PKIMessage [RFC4210]. The "PKI Information" request allows the EE to receive information about changes like the CA key update and CRL[RFC5280] updates. If supported, EEs may also use "Support Messages" defined in section 4.3 of the Lightweight CMP Profile [I-D.ietf-lamps-lightweight-cmp-profile] to get information about the changes.

These mechanisms will help constrained devices, that are acting as EEs, to conserve resources by eliminating the need to create an endpoint for receiving notifications from RA or CA. It will also simplify the implementation of a CoAP-to-HTTP proxy.

3. Proxy Support

This section provides guidance on using a CoAP-to-HTTP proxy between EEs and RAs or CAs in order to avoid changes to the existing PKI implementation. Since the CMP payload is same over CoAP and HTTP transfer mechanisms, a CoAP-to-HTTP cross-protocol proxy can be implemented based on section 10 of [RFC7252].

The CoAP-to-HTTP proxy can either be located closer to the EEs or closer to the RA or CA. The proxy MAY support service discovery and resource discovery as described in section 2.2. The CoAP-to-HTTP

proxy MUST function as a reverse proxy, only permitting connections to a limited set of pre-configured servers. It is out of scope of this document on how a reverse proxy can route CoAP client requests to one of the configured servers. Some recommended mechanisms are as follows:

*Use the Uri-Path option to identify a server.

*Use separate hostnames for each of the configured servers and then use the Uri-Host option for routing the CoAP requests.

*Use separate hostnames for each of the configured servers and then use Server Name Indication [RFC8446] in case of "coaps://" scheme for routing CoAP requests.

4. Security Considerations

*The CMP protocol depends upon various mechanisms in the protocol itself for making the transactions secure therefore, security issues of CoAP due to using UDP without cryptographic protections for message confidentiality and integrity, do not carry over to the CMP layer. The Security considerations for CoAP are mentioned in the [RFC7252].
*Although the CMP protocol does not depend upon the underlying transfer mechanism for protecting the messages but in cases when confidentiality protection is desired, CoAP over DTLS [RFC9147] MAY be used providing a hop-by-hop security. The use of DTLS can provide confidentiality protection of the CMP-level metadata, however it cannot obscure the fact that CMP is being used in the underlying layer.
*Section 9.1 of [RFC7252] defines how to use DTLS [RFC9147] for securing the CoAP. Once a DTLS [RFC9147] association is established it SHOULD be used for as long as possible to avoid the frequent overhead of setting up a DTLS [RFC9147] association for constrained devices.
*An EE may miss some of the Announcement messages when using CoAP Observe option [RFC7641] since Observe option is a "best-effort" approach and server can lose state about subscribers for announcement messages. The EEs may use alternate method described in section 2.6 to get time critical changes like CRL updates.
*In order to to reduce the risks imposed by DoS attacks, the implementations SHOULD optimally use the available datagram size i.e. avoid small datagrams containing partial CMP PKIMessage data.
*A CoAP-to-HTTP proxy can also protect the PKI entities by handling UDP and CoAP messages. Proxy can mitigate attacks like denial of service attacks, replay attacks and resource-exhaustion attacks by enforcing basic checks like validating that the ASN.1 syntax is compliant to CMP messages and validating the PKIMessage protection before sending them to PKI entities.
*Since the Proxy may have access to the CMP-Level metadata and control over the flow of CMP messages therefore proper role based access control should be in place. Proxy can be deployed at the

edge of the "End Entities" network or in front of an RA and CA to protect them. The proxy however may itself be vulnerable to resource-exhaustion attacks as it's required to buffer the CMP messages received over CoAP transport before sending it to the HTTP endpoint. This can be mitigated by using short timers for discarding the buffered messages and rate limiting clients based on the resource usage.

5. IANA Considerations

This document requires a new entry to the CoAP Content-Formats Registry code for the content-type "application/pkixcmp" for transferring CMP transactions over CoAP from the identifier range 256-9999 reserved for IETF specifications.

Type name: application

Subtype name: pkixcmp

Encoding: Content may contain arbitrary octet values. The octet values are the ASN.1 DER encoding of a PKI message, as defined in the [RFC4210] specifications.

Reference: This document and [RFC4210]

This document also requires a new path segment "ann" in the CMP protocol registry for the EEs to register themselves for the announcement messages.

Path Segment: ann

Description: The path to send a Get request with CoAP Observer Option to register for CMP announcement messages.

Reference: This document.

This document references the cmp, in the Well-Known URIs IANA registry. This document is expected to be published together with [I-D.ietf-lamps-cmp-updates]. Please add a reference of this document to the Well-Known URIs IANA registry for that entry

This document also refers the path segment "p" in the Certificate Management Protocol (CMP) IANA registry. Please add a reference of this document to the Certificate Management Protocol (CMP) for that path segment.

6. Acknowledgments

The authors would like to thank Hendrik Brockhaus, David von Oheimb, and Andreas Kretschmer for their guidance in writing the content of this document and providing valuable feedback.

7. References

7.1. Normative References

[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>.

[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>.

[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>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7959] Bormann, C. and Z. Shelby, Ed., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)", RFC 7959, DOI 10.17487/RFC7959, August 2016, <https://www.rfc-editor.org/info/rfc7959>.

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

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link Format", RFC 6690, DOI 10.17487/RFC6690, August 2012, <https://www.rfc-editor.org/info/rfc6690>.

[RFC7641] Hartke, K., "Observing Resources in the Constrained Application Protocol (CoAP)", RFC 7641, DOI 10.17487/RFC7641, September 2015, <https://www.rfc-editor.org/info/rfc7641>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version

1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/info/rfc9147>.

[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>.

7.2. Informative References

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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>.

[RFC8323] Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., and B. Raymor, Ed., "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets", RFC 8323, DOI 10.17487/RFC8323, February 2018, <https://www.rfc-editor.org/info/rfc8323>.

[I-D.ietf-lamps-cmp-updates] Brockhaus, H., von Oheimb, D., and J. Gray, "Certificate Management Protocol (CMP) Updates", Work in Progress, Internet-Draft, draft-ietf-lamps-cmp-updates-23, 29 June 2022, <https://www.ietf.org/archive/id/draft-ietf-lamps-cmp-updates-23.txt>.

[I-D.ietf-lamps-lightweight-cmp-profile] Brockhaus, H., von Oheimb, D., and S. Fries, "Lightweight Certificate Management Protocol (CMP) Profile", Work in Progress, Internet-Draft, draft-ietf-lamps-lightweight-cmp-profile-13, 8 July 2022, <https://www.ietf.org/archive/id/draft-ietf-lamps-lightweight-cmp-profile-13.txt>.

Authors' Addresses

Mohit Sahni (editor)
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
United States of America

Email: msahni@paloaltonetworks.com

Saurabh Tripathi (editor)
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054

United States of America

Email: stripathi@paloaltonetworks.com