Internet Engineering Task Force (IETF)
Request for Comments: 9482
Category: Standards Track
ISSN: 2070-1721

M. Sahni, Ed.
S. Tripathi, Ed.
Palo Alto Networks

November 2023

Constrained Application Protocol (CoAP) Transfer for the Certificate Management Protocol

Abstract

This document specifies the use of the 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 Internet of Things space.

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/rfc9482.

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 CMP 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 CMP version 2 [RFC4210], CMP version 3 [RFC9480] (designated as CMP in this document), and the Lightweight CMP Profile [RFC9483]. In general, this document follows the HTTP transfer for CMP specifications defined in [RFC6712] and specifies the requirements for using CoAP as a transfer mechanism for CMP.

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

1.1. Requirements Language

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. In general, the RAs and CAs 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 CMP.

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, for example, as specified in Lightweight CMP Profile [RFC9483], 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/<profileLabel>
coap://www.example.com/.well-known/cmp/p/<profileLabel>/<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 port numbers MUST be assumed for the "coap:" and "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 RA or 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 Constrained RESTful Environments (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 MUST send each CoAP request marked as a Confirmable message [RFC7252]. If the CoAP request is successful, then the CMP RA or CA MUST return a Success 2.xx response code; otherwise, the CMP RA or CA MUST return an appropriate Client Error 4.xx or Server Error 5.xx response code. A CMP RA or CA may choose to send a piggybacked response [RFC7252] to the client, or it MAY send a separate response [RFC7252] in case it takes some time for the RA or CA to process the CMP transaction.

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

2.4. CoAP Block-Wise Transfer Mode

A CMP PKIMessage consists of a header, body, protection, and extraCerts structure, 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 an RA or EEs and a CA and if the server supports, then 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 triggered by an event or periodically for the other PKI entities. Here is the list of CMP announcement messages prefixed by their respective ASN.1 identifier (see Section 5.1.2 of [RFC4210]):

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

An EE MAY use the 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 announcement messages, then it MUST send an appropriate Success 2.xx response code; otherwise, it MUST send an appropriate Client Error 4.xx or Server Error 5.xx response code. If for some reason the 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. Upon receiving a Success 2.xx response without the Observe Option [RFC7641], after some time, a client MAY try to register again for announcements from the CMP server. Since a server can remove the EE from the list of observers for announcement messages, an EE SHOULD periodically reregister itself for announcement messages.

Alternatively, an EE MAY periodically poll for the current status of the CA via the "PKI Information Request" message; see Section 6.5 of [RFC4210]. If supported, EEs MAY also use "support messages" defined

in Section 4.3 of Lightweight CMP Profile [RFC9483] to get information about the CA status. 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 the 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 the 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 preconfigured servers. It is out of scope of this document to specify 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 the "coaps://" scheme for routing CoAP requests.

4. Security Considerations

* If PKIProtection is used, the PKIHeader and PKIBody of the CMP are cryptographically protected against malicious modifications. As such, UDP can be used without compromising the security of the CMP. Security considerations for CoAP are defined in [RFC7252].
* The CMP does not provide confidentiality of the CMP payloads. If confidentiality is desired, CoAP over DTLS [RFC9147] SHOULD be used to provide confidentiality for the CMP payloads; although, it cannot conceal that the CMP is used within the DTLS layer.
* Section 9.1 of [RFC7252] defines how to use DTLS [RFC9147] for securing CoAP. DTLS [RFC9147] associations SHOULD be kept alive and reused where possible to amortize on the additional overhead of DTLS on constrained devices.
* An EE might not witness all of the announcement messages when using the CoAP Observe Option [RFC7641], since the Observe Option is a "best-effort" approach and the server might lose its state for subscribers to its announcement messages. The EEs may use an alternate method described in Section 2.6 to obtain time critical changes, such as Certificate Revocation List (CRL) [RFC5280] updates.
* Implementations SHOULD use the available datagram size and avoid

sending small datagrams containing partial CMP PKIMessage data in order to reduce memory usage for packet buffering.

* A CoAP-to-HTTP proxy can also protect the PKI entities by handling UDP and CoAP messages. The 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, proper role-based access control should be in place. The proxy can be deployed at the edge of the "end entities" network or in front of an RA and CA to protect them. However, the proxy 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

IANA has registered "application/pkixcmp" (ID 259) in the "CoAP Content-Formats" registry <https://www.iana.org/assignments/core-parameters> to transfer CMP transactions over CoAP.

Type name: application
Subtype name: pkixcmp
Reference: RFC 9482 [RFC4210]

IANA has also registered a new path segment "ann" in the "CMP Well-Known URI Path Segments" registry <https://www.iana.org/assignments/cmp> for the EEs to register themselves for the announcement messages.

Path Segment: ann
Description: The path to send a GET request with the CoAP Observe Option to register for CMP announcement messages.
Reference: RFC 9482

IANA has added this document as a reference for the "cmp" entry in the "Well-Known URIs" registry <https://www.iana.org/assignments/well-known-uris>.

IANA has also added this document as a reference for the "p" entry in the "CMP Well-Known URI Path Segments" registry <https://www.iana.org/assignments/cmp/>.

6. References

6.1. 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>.

[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>.

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

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

6.2. 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>.

[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>.

[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>.

Acknowledgements

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.

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