CoAP Transport for CMPV2
draft-ietf-ace-cmpv2-coap-transport-01

Abstract

This document specifies the use of Constrained Application Protocol (CoAP) as a transport medium 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.

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 encryption 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 [Certificate-Management-Protocol-Updates] and Lightweight CMP Profile [Lightweight-CMP-Profile]. This document, in general, follows the HTTP transport specifications for CMP defined in [RFC6712] and specifies the additional requirements for using CoAP as a transport medium. This document also provides guidance on how to use a "CoAP-to-HTTP" proxy for a better adaptation of CoAP transport without significant changes to the existing PKI entities. Although CoAP transport can be used for communication between Registration Authority (RA) and Certification Authority (CA) or between CAs, the

scope of this document is for communication between End Entity (EE) and RA or EE and CA. This document is applicable only when the CoAP transport is used for the CMP transactions.

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 Transport 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 transport medium, while 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 transport medium 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 path specific to a CA, certificate profile or PKI management operations. A valid full operation path segment can look like this:

```
coap://www.example.com/.well-known/cmp
coap://www.example.com/.well-known/cmp/operationalLabel
coap://www.example.com/.well-known/cmp/profileLabel
coap://www.example.com/.well-known/cmp/profileLabel/operationalLabel
```

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 port 5683 MUST be assumed for the "coap://" scheme and port 5684 MUST be assumed for the "coaps://" scheme. 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's CMP endpoint. The CoAP CMP endpoints supporting service discovery MUST also support resource discovery in the CoRE Link Format as described in [RFC6690].

2.3. CoAP Request Format

The CMP PKIMessages MUST be DER encoded and sent as the body of the CoAP POST request. If the CoAP request is successful then the server MUST 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.

2.4. CoAP Content-Format

When transferring CMP PKIMesssage over CoAP the media type "application/pkixcmp" MUST be used.

2.5. Announcement PKIMessage

When using the CoAP protocol, a PKI EE SHOULD poll for the potential changes via "PKI Information" request using "PKI General Message" defined in the PKIMessage [RFC4210] for various type of changes like CA key update or to get current CRL [RFC5280] to check revocation or using Support messages defined in section 5.4 of Lightweight CMP Profile [Lightweight-CMP-Profile]. This will help constrained devices that are acting as EEs conserve resources by eliminating the need to create an endpoint for receiving notifications from RA or CA. It will also simplify the implementation of CoAP-to-HTTP proxy.

2.6. CoAP Block-Wise Transfer Mode

A CMP PKIMesssage consists of a header, body, protection, and extraCerts structures. These structures may contain many optional and potentially large fields, a CMP message can be much larger than the Maximum Transmission Unit (MTU) of the outgoing interface of the device. In order to avoid IP fragmentation of messages exchanged between EEs and RAs or CAs, the Block-Wise transfer [RFC7959] mode MUST be used for the CMP Transactions over CoAP. If a CoAP-to-HTTP proxy is in the path between EEs and CA or EEs and RA then it MUST receive the entire body from the client before sending the HTTP request to the server. This will avoid unnecessary errors in case the entire content of the PKIMesssage is not received and the proxy opens a connection with the server.

2.7. Multicast CoAP

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

3. Using CoAP over DTLS

Although CMP protocol does not depend upon the underlying transport for protecting the messages but in cases when an end to end secrecy is desired for the CoAP transport, CoAP over DTLS [RFC6347] as a transport medium SHOULD be used. Section 9.1 of [RFC7252] defines how to use DTLS [RFC6347] for securing the CoAP. Once a DTLS [RFC6347] connection is established it SHOULD be used for as long as possible to avoid the frequent overhead of setting up a DTLS [RFC6347] connection for constrained devices.

4. 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 transport, a CoAP-to-HTTP cross protocol proxy can be implemented based on section 10 of [RFC7252]. The CoAP-to-HTTP proxy can be either located closer to the EEs or closer to the RA or CA. In case the proxy is deployed closer to the EEs then it may also 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:

- o Use Uri-Path option to identify a server.
- o Use separate hostnames for each of the configured servers and then use Uri-Host option for routing the CoAP requests.
- o 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.

5. 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 do not carry over to the CMP layer. However the CoAP is vulnerable to many issues due to the connectionless characteristics of UDP itself. The Security considerations for CoAP protocol are mentioned in the [RFC7252].

In order to protect themselves against DDoS attacks, the implementations SHOULD avoid sending or receiving very small packets containing partial CMP PKIMessage data. A CoAP-to-HTTP proxy can also protect the PKI entities from various attacks by enforcing basic checks and validating messages before sending them to PKI entities. Proxy can be deployed at the edge of End Entities" network or in front of an RA and CA to protect them.

6. IANA Considerations

This document requires a new entry to the CoAP Content-Formats Registry code for the content-type "application/pkixcmp" and a new entry in Well-Known URIs for URI Suffix "cmp".

7. 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.

8. References

8.1. 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>.

[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>.

[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>.

[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>.

[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>.

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

8.2. Informative References

[Certificate-Management-Protocol-Updates]
Brockhaus, H. and D. von Oheimb, "Certificate Management Protocol (CMP) Updates", Work in Progress, draft-brockhaus-lamps-cmp-updates-03, 2021, <https://tools.ietf.org/html/draft-brockhaus-lamps-cmp-updates-03>.

[Lightweight-CMP-Profile]
Brockhaus, H., Fries, S., and D. von Oheimb, "Lightweight CMP Profile", Work in Progress, draft-ietf-lamps-lightweight-cmp-profile-05, 2021, <https://tools.ietf.org/html/draft-ietf-lamps-lightweight-cmp-profile-05>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[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>.

Authors' Addresses

Mohit Sahni (editor)
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
US

EMail: msahni@paloaltonetworks.com

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

EMail: stripathi@paloaltonetworks.com