ACE
Internet-Draft
Intended status: Standards Track
Expires: January 14, 2021

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

July 13, 2020

CoAP Transport for CMPV2
draft-msahni-ace-cmpv2-coap-transport-00

Abstract

This document specifies how to use Constrained Application Protocol (CoAP) as a Transport Medium for the Certificate management protocol version 2 (CMPv2) and Lightweight CMP Profile [Lightweight-CMP-Profile] which is a subset of CMPv2 defined for Constrained devices. The CMPv2 defines the interaction between various PKI entities for the purpose of certificate creation and management. The CoAP is a HTTP like client-server protocol used by various constrained devices in the IoT and industrial scenarios. Constrained devices are devices that have low memory or CPU or power constraints and avoid the use of complex protocols like TCP to save resources.

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 January 14, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
1.1. Terminology 3
2. CoAP Transport For CMPv2 3
2.1. Discovery of CMP Entities 3
2.2. CoAP URI Format 3
2.3. CoAP Request Format 4
2.4. CoAP Content-Format 4
2.5. Announcement PKIMessage 4
2.6. CoAP Block Wise Transfer Mode 4
2.7. Multicast CoAP 4
3. Using CoAP over DTLS 5
4. Proxy support 5
4.1. CoAP to HTTP Proxy 5
4.2. CoAPs to HTTPs Proxy 5
5. Security Considerations 5
6. IANA Considerations 6
7. Acknowledgments 6
8. References 6
8.1. Normative References 6
8.2. Informative References 7
8.3. URL References 7
Authors' Addresses 7

1. Introduction

The CMPv2 is used by the entities in PKI for the generation and management of the certificates. One of the requirements of CMPv2 [RFC4210] is to be usable over a variety of transport mechanisms. The CMP is designed to be independent of the transport protocol being used and has mechanisms to take care of transactions, error reporting and encryption of messages where ever required. The CoAP defined in [RFC7252], [RFC7959] and [RFC8323] is a client-server protocol, like HTTP, that is designed to be used by constrained devices over constrained networks (low power lossy 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 as a transport medium for the CMPv2 and Lightweight CMP Profile [Lightweight-CMP-Profile]. This document, in general, follows the HTTP transport specifications for CMPv2 defined in

[RFC6712] and specifies the additional requirements for CoAP transport. 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 being used for the CMPv2 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 CMPv2

CMPv2 transaction consists of passing PKIMesssage [RFC4210] between the PKI End Entities (EEs), Registration Authorities (RAs), and Certification Authorities (CAs). If the EEs are constrained devices then they will prefer, as a client, the use of CoAP instead of HTTP as a transport medium, while the RAs and CAs, in general, are not constrained and can support both CoAP and HTTP Client and Server implementation. This section specifes how to use CoAP as transport mechanism for CMPv2 or Lightweight CMP Profile [Lightweight-CMP-Profile].

2.1. Discovery of CMP Entities

The information about the URIs of CA and RA that is required by EEs can be either configured out of band on EEs or the EEs can use the service discovery mechanism described in section 7 of [RFC7252] to find them. The EE, RA SHOULD support service discovery as described

in section 7 of [RFC7252]. An EE MUST verify the configured Root CA certificate against the Root CA certificate of the discovered entity to make sure it is talking to correct endpoint.

2.2. CoAP URI Format

The CoAP URI MUST follow the guidelines defined in section 3.6 of [RFC6712] for CMPv2 protocol. Implementations supporting the Lightweight CMP Profile [Lightweight-CMP-Profile] MUST follow the guidelines specified for HTTP transport defined in section 7.1 of Lightweight CMP Profile [Lightweight-CMP-Profile]. The URI's for

CoAP resources should start with coap:// instead of http:// and coaps:// instead of https://

2.3. CoAP Request Format

The CMPv2 PKIMessage MUST be DER encoded and sent as the body of the CoAP POST request. 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.

2.4. CoAP Content-Format

When transferring CMPv2 PKIMesssage over CoAP the media type application/pkixcmp MUST be used.

2.5. Announcement PKIMessage

When using the CoAP protocol, a PKI entity SHOULD poll for the possible changes via PKI Information request using General Message defined in a PKIMessage for various type of changes like CA key update or to get current CRL to check revocation or using Support messages defined in section 5.4 of Lightweight CMP Profile [Lightweight-CMP-Profile]. This will make use of a CoAP to HTTP proxy transparent to the client.

2.6. CoAP Block Wise Transfer Mode

Since the CMPv2 PKIMesssage consists of a header body and optional

fields a CMPv2 message can be much larger than the MTU of the outgoing interface of the device. In order to avoid IP fragmentation of messages that are exchanged between EEs and RAs or CAs, the Block Wise transfer [RFC7959] mode MUST be used for the CMPv2 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 Proxy opens a connection with the server.

2.7. Multicast CoAP

CMPv2 PKIMessage request messages sent from EEs to RAs or from EEs to CAs over CoAP transport MUST not use a Multicast destination address.

3. Using CoAP over DTLS

When the end to end secrecy is desired for 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. For CMPv2 and Lightweight CMP Profile [Lightweight-CMP-Profile] the clients should follow specifications defined in section 7.1 and section 7.2 of Lightweight CMP Profile [Lightweight-CMP-Profile] for setting up DTLS [RFC6347] connection either using certificates or shared secret. Once a DTLS [RFC6347] connection is established it SHOULD be used for as long as possible to avoid the frequent overhead of using DTLS [RFC6347] connection for constrained devices.

4. Proxy support

The use of a CoAP to HTTP proxy is recommended to avoid significant changes in the implementation of the CAs and RAs. However, if a proxy is in place then Announcements Messages cannot be passed to EEs efficiently. In case a CoAP to HTTP proxy is used for CMP transactions, it SHOULD support service discovery mentioned in section 2.1

4.1. CoAP to HTTP Proxy

If a CoAP to HTTP proxy is used then it MUST be positioned between EEs and RAs or between EEs and CAs when RA is not part of CMP transactions. The use of a CoAP to HTTP proxy between CAs and RAs is not recommended. The implementation of a CoAP to HTTP proxy is specified in Section 10 of [RFC7252]. The CoAP to HTTP proxy will also protect the CAs and RAs from UDP based Denial of Service attacks.

4.2. CoAPs to HTTPs Proxy

A CoAPs to HTTPS proxy (DTLS [RFC6347] transport to TLS [RFC8446] transport proxy) can be used instead of the CoAP to HTTP proxy if the server support HTTPS protocol, however client SHOULD be configured to trust the CA certificate used by proxy to sign the Man in the Middle (MITM) certificate for certificate chain validation [RFC5280].

5. Security Considerations

The CMPv2 protocol itself does not require secure transport and depends upon various mechanisms in the protocol itself to make sure that the transactions are secure. However, the CoAP protocol which uses UDP as layer 4 transport is vulnerable to many issues due to the connectionless characteristics of UDP itself. The Security considerations for CoAP protocol are mentioned in the [RFC7252].

Using a CoAP to HTTP proxy mitigates some of the risks as the requests from the EE's can terminate inside the trusted network and will not require the server to listen on a UDP port making it safe from UDP based address spoofing, Denial of Service, and amplification attacks due to the characteristics of UDP.

6. IANA Considerations

This document requires a new entry to the CoAP Content-Formats Registry code for the content-type application/pkixcmp

7. Acknowledgments

The author 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>.

[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>.

8.2. Informative References

[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>.

8.3. URL References

[Lightweight-CMP-Profile] Brockhaus, H., Fries, S., and D. von Oheimb, "Lightweight CMP Profile", 2020, <https://tools.ietf.org/html/draft-brockhaus-lamps-lightweight-cmp-profile-03>.

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