Network Working Group
Internet-Draft
Updates: 2510,4210
(if approved)
Intended status: Standards Track
Expires: January 31, 2010

A. Kapoor
R. Tschalaer
Certicom
T. Kause
SSH
M. Peylo
NSN
July 30, 2009

Internet X.509 Public Key Infrastructure -- Transport Protocols for CMP
draft-ietf-pkix-cmp-transport-protocols-06.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 31, 2010.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document describes how to layer Certificate Management Protocols over various transport protocols.

Table of Contents

1. Introduction

Well defined transport mechanisms are required for the Certificate Management Protocol [RFC4210] in order to allow end entities, RAs and CAs to pass PKIMessage sequences between them.

2. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document (in uppercase, as shown) are to be interpreted as described in [RFC2119].

3. TCP-Based Management Protocol

While this section is called TCP-based and the messages are called TCP-Messages, the same protocol can be used over any reliable, connection oriented transport protocol (e.g. SNA, DECnet, etc.). This protocol is suitable for cases where an end entity (or an RA) initiates a transaction and can poll to pick up the results.

The client sends a TCP-Message to the server, and the server responds with another TCP-Message. A response MUST be sent for every request, even if the encapsulated CMP message in the request does not have a corresponding response.

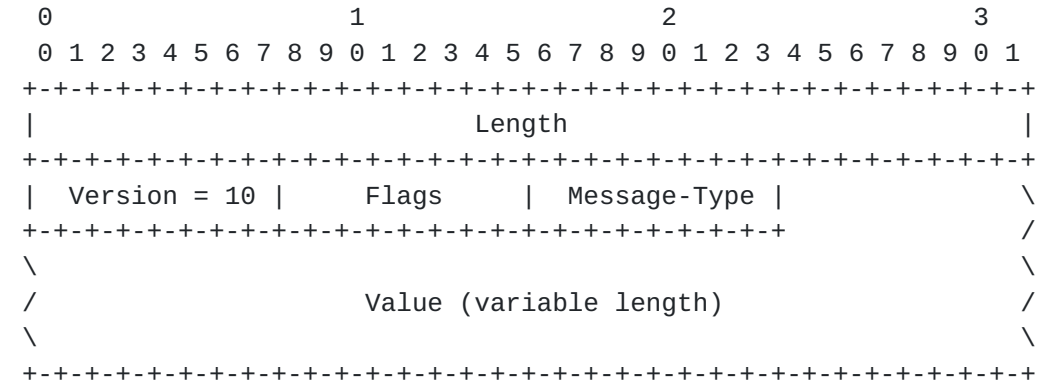
The protocol requires a listener process on an RA or CA which can accept TCP-Messages on a well-defined port (default TCP port number is 829). Typically a client initiates the connection to the server and instantly submits a TCP-Message. The server replies with a TCP-Message containing either a CMP message or a reference number to be used later when polling for the actual CMP response message.

If a polling-reference was supplied, the client SHOULD send a polling request using this polling-reference after waiting for at least the time specified along with the reference number. The server may again reply with a new polling-reference or with the actual CMP message response.

When the final CMP response message has been picked up by the client, no new polling reference is supplied.

3.1. General Form

The format of a TCP-Message is shown below:



Length: 32 bits (unsigned integer)
This field contains the number of remaining octets of the TCP-Message (i.e. number of octets of the Value field plus 3). All bit values in this protocol are specified to be in network byte order.

Version: 8-bits (unsigned integer)
The version of the TCP-Message is 10 in for this document. It MUST be incremented in each future specification modification e.g. changing the Flags field in a way that is not fully backwards compatible.

Flags: 8 bits
TCP-Message specific flags as described in Section 3.3.

Message-Type: 8 bits
A value indicating the type of the TCP-Message.

Value: variable length
Message-type dependent data is stored here. The usage of this field is described along with the respective message-type

3.2. Version

The TCP-Message version is 10 for this document. The number has deliberately been chosen to prevent [RFC2510] compliant applications from treating it as a valid message type. Applications receiving a version less than 10 SHOULD interpret the message as being an [RFC2510] style message.

3.2.1. Version Negotiation

If a client knows the protocol version(s) supported by the server (e.g. from a previous TCP-Message exchange or via some out-of-band means) then it SHOULD send a TCP-Message with the highest version supported both by it and the server. If a client does not know what version(s) the server supports then it SHOULD send a TCP-Message using the highest version it supports.

If a server receives a TCP-Message version that it supports, then it MUST reply with a TCP-Message of the same version. If the version received is higher than what the server supports, it MUST send back a VersionNotSupported errorMsgRep containing the highest version it supports, see Section 3.4.6.

3.2.2. Detection and Interoperation with RFC2510 Conformant Implementations

Servers wishing to interoperate with clients conforming to [RFC2510] can do so by treating any received message with a version less than 10 as an [RFC2510] message and responding in that format. Servers not wishing to support [RFC2510] messages MUST respond with a [RFC2510] errorMsgRep.

If a client receives a [RFC2510] errorMsgRep (message-type 06) message, it MAY automatically resend the same request on the same connection, falling back to the [RFC2510] format; if the received message is not an errorMsgRep, it MUST terminate the connection. It MAY then retry the communication falling back completely to the [RFC2510] format.

Naturally, a client MUST abort the connection attempt if the server does not support any of the client's supported versions. It SHOULD retry the version negotiation after a delay to check if the server was updated.

3.3. Flags

The LSB of the Flags field is used to indicate a connection close; all other bits in the Flags octet MUST be ignored by receivers, and MUST be set to zero by senders.

3.3.1. Connection Close Flag

By default connections are kept open after the receipt of a response. Either party (client or server) MAY set the connection close bit at any time. If the connection close bit is set on a request, then the server MUST set the bit in the response and close the connection after sending the response. If the bit is set on a response from the server, the client MUST NOT send any further requests on that connection. Applications MAY decide to close an idle connection (one on which no response is outstanding) after some time-out. Because of the problem where a client sends a request and the server closes the connection while the request is still in flight, clients SHOULD automatically retry a request for which no part of the response could be read due to a connection close or reset.

If the connection is kept open, it MUST only be used for subsequent request/response transactions started by the client - the server MUST NOT use it to send requests to the client. Different transactions may be freely interwoven on the same connection. E.g. a CR/CP need not immediately be followed by the Confirm, but may be followed by any other request from a different transaction.

3.4. Message-Types

Message-Types 0-127 are reserved and are to be issued under IANA auspices. Message-types 128-255 are reserved for application use.

The Message-Types currently defined are:

ID Value	Message Name
'00'H	pkiReq
'01'H	pollRep
'02'H	pollReq
'03'H	finRep
'05'H	pkiRep
'06'H	errorMsgRep

If a server receives an unknown message-type, it MUST reply with an InvalidMessageType errorMsgRep. If a client receives an unknown message-type, it MUST abort the current CMP transaction and terminate the connection.

The different TCP-Message-types are discussed in the following sections:

3.4.1. pkiReq

A pkiReq message conveys a PKIMessage from a client to a server. The Value field of this TCP-Message contains a DER-encoded PKIMessage.

The type of PKIMessages that can be carried by pkiReq TCP-Messages are (in the order they are defined in [RFC4210]):

[0] Initialization Request
[2] Certification Request
[4] PKCS-10 Request
[6] pop Response
[7] Key Update Request
[9] Key Recovery Request
[11] Revocation Request
[13] Cross-Certification Request
[15] CA Key Update Announcement
[16] Certificate Announcement
[17] Revocation Announcement
[18] CRL Announcement
[20] Nested Message
[21] General Message
[23] Error Message

[24] Certificate Confirmation
[25] Polling Request

3.4.2. pkiRep

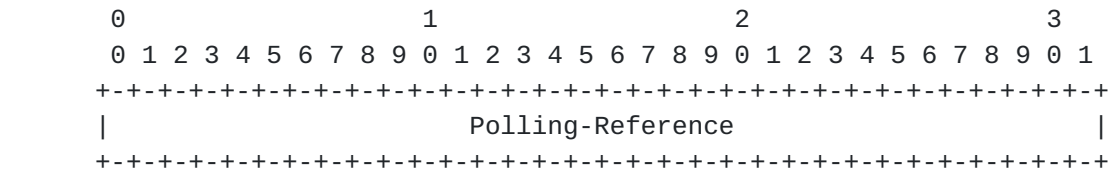
TCP-Messages of this type are used to send a response to the requestor. The Value field of the pkiRep contains a DER encoded PKIMessage.

The type of PKIMessages that can be carried by such pkiRep messages are (in the order they are defined in [RFC4210]):

[1] Initialization Response
[3] Certification Response
[5] pop Challenge
[8] Key Update Response
[10] Key Recovery Response
[12] Revocation Response
[14] Cross-Certificate Response
[19] Confirmation
[22] General Response
[23] Error Message
[26] Polling Response

3.4.3. pollReq

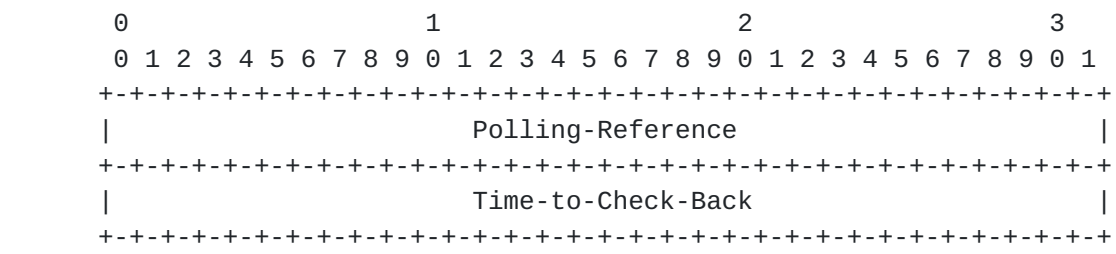
A pollReq is used by a client to check the status of a pending TCP-Message. The Value portion of a pollReq contains:



Polling-Reference: 32 bits (unsigned integer)
This polling-reference MUST be the one returned via the respective pollRep TCP-Message.

3.4.4. pollRep

A pollRep is sent by the server to the client as response in case there is no PKIMessage ready yet. The Value portion of the pollRep looks as follows:

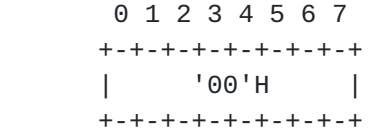


Polling-Reference: 32 bits (unsigned integer)
A unique 32-bit number identifying the transaction.

Time-to-Check-Back: 32 bits (unsigned integer)
The time in seconds indicating the minimum interval after which the client SHOULD check the status again. The duration for which the server keeps the polling-reference unique is left to the implementation.

3.4.5. finRep

A finRep is sent by the server whenever no other response applies, such as after receiving a CMP pkiConf. The Value portion of the finRep SHALL contain:



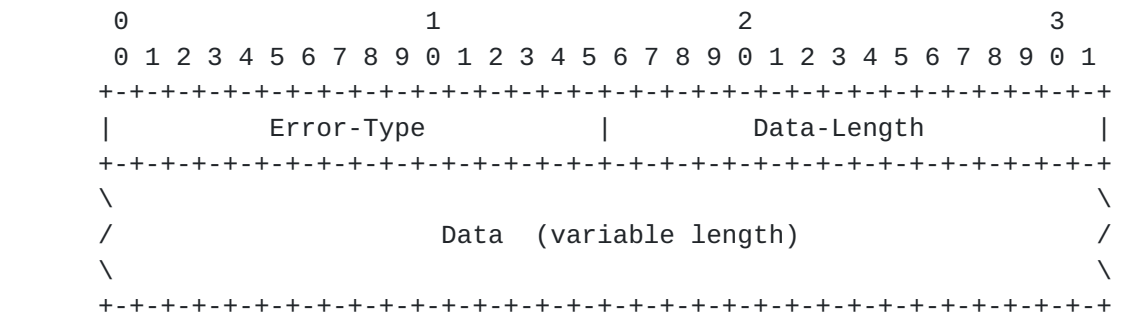
'00'H: 8 bits
All bits set to zero.

3.4.6. errorMsgRep

This TCP-Message is sent when a TCP-Message level protocol error is detected. It is imperative that PKIError messages MUST NOT be sent using this message type. Examples of TCP-Message level errors are:

- Invalid protocol version
- Invalid TCP message-type
- Invalid polling reference number

The Value field of the errorMsgRep TCP-Message MUST contain:



Error-Type: 16 bits A value (format described below) indicating the type of the error.

Data-Length: 16 bits (unsigned integer) Contains the length of the Data field in number of octets. Error messages not conveying additional information MUST set Data-Length to 0.

Data: <data-length> octets
An UTF8 text string for user readable error messages, containing additional information about the error. Note that it does not contain a terminating NULL character at the end. It SHOULD include an [RFC4646] language tag, as described in [RFC2482]

The Error-Type is in the format MMNN where M and N are hex digits (0-F) and MM represents the major category and NN the minor. The major categories defined by this specification are:

ID Value	Major Categories
'01'H	TCP-Message version negotiation
'02'H	client errors
'03'H	server errors

The major categories '80'H-'FF'H are reserved for application use.

The different error-types are discussed in the following sections:

3.4.6.1. VersionNotSupported

The VersionNotSupported errorMsgRep is defined as follows:

Field	Value
Error-Type	'0101'H
Data-Length	1
Data	<version>
UTF8-text String	implementation defined

where <version> is the highest TCP-Message protocol version the server supports.

3.4.6.2. GeneralClientError

The GeneralClientError errorMsgRep is defined as follows:

Field	Value
Error-Type	'0200'H
Data-Length	0
Data	<empty>
UTF8-text String	implementation defined

3.4.6.3. InvalidMessageType

The InvalidMessageType errorMsgRep is defined as follows:

Field	Value
Error-Type	'0201'H
Data-Length	1
Data	<message-type>
UTF8-text String	implementation defined

where <message-type> is the invalid Message-Type ID received by the

server.

3.4.6.4. InvalidPollID

The InvalidPollID errorMsgRep is defined as follows:

Field	Value
Error-Type	'0202'H
Data-Length	4
Data	<polling-reference>
UTF8-text String	implementation defined

where <polling-reference> is the polling-reference received by the server, identifying the transaction.

3.4.6.5. GeneralServerError

The GeneralServerError errorMsgRep is defined as follows:

Field	Value
Error-Type	'0300'H
Data-Length	0
Data	<empty>
UTF8-text String	implementation defined

4. HTTP-Based Protocol

The stateless HTTP MAY be utilized for conveying CMP messages instead of or additionally to the TCP-Messages.

4.1. HTTP Versions

Either HTTP/1.0 as described in [RFC1945] or HTTP/1.1 as in [RFC2616] MAY be used. Naturally, the newer version SHOULD be preferred. Both, server and client implementations MUST be able to interact with counterparts primarily utilizing the different HTTP protocol version.

4.2. General Form

An ASN.1 DER-encoded PKIMessage is sent as the entity-body of an HTTP POST request. If the HTTP request is successful, the server returns the CMP reply in the body of the HTTP response. The response status code in this case MUST be 200; other 2xx codes MUST NOT be used for this purpose.

Note that a server may return any 1xx, 3xx, 4xx, or 5xx code if the HTTP request needs further handling or is otherwise not acceptable.

4.3. MIME Type

The MIME type "application/pkixcmp" MUST be set as in the HTTP header when conveying a PKIMessage.

4.4. HTTP Considerations

In general, CMP messages are not cachable; requests and responses MUST include a "Cache-Control: no-cache" (and, if either side uses HTTP/1.0, a "Pragma: no-cache") to prevent the client from getting cached responses.

Connection management is based on the HTTP provided mechanisms (Connection and Proxy-Connection header fields).

While an implementation MAY make use of all defined features of the HTTP protocol, it SHOULD keep the protocol utilization as simple as possible.

Content codings MAY be applied.

4.5. Compatibility Issues with Legacy Implementations

As this document was subject of multiple changes during the long period of time it was created in, several implementations may exist

using a different approach for HTTP transport.

Thus, legacy implementations might also use an unregistered "application/pkixcmp-poll" MIME type as it was specified in earlier drafts of this document. Here, the entity-body of an HTTP POST request contains a TCP-Message instead of a plain DER-encoded PKIMessage. Effectively, this is conveying PKIMessage over TCP-Message over HTTP.

5. File-Based Protocol

A file containing a PKIMessage MUST contain only the DER encoding of one PKIMessage, there MUST NOT be extraneous header or trailer information in the file.

Such files can be used to transport PKIMessage sequences using e.g. FTP.

6. Mail-Based Protocol

This subsection specifies a means for conveying ASN.1-encoded messages for the protocol exchanges via Internet mail [RFC2821]. A simple MIME object is specified as follows.

```
Content-Type: application/pkixcmp
Content-Transfer-Encoding: base64

<<the ASN.1 DER-encoded PKIX-CMP message, base64-encoded>>
```

This MIME object can be sent and received using common MIME processing engines and provides a simple Internet mail transport for PKIX-CMP messages. Implementations MAY wish to also recognize and use the "application/x-pkixcmp" MIME type (specified in earlier versions of this document) in order to support backward compatibility wherever applicable.

7. Security Considerations

Three aspects need to be considered by server side implementors:

1. There is no security at the TCP and HTTP protocol level (unless tunneled via SSL/TLS) and thus TCP-Messages SHOULD NOT be used to change state of the transaction. Change of state SHOULD be triggered by the signed PKIMessages which are carried within the TCP-Message.

2. If the server is going to be sending messages with sensitive information (not meant for public consumption) in the clear, it is RECOMMENDED that the server sends back the message directly and not use the pollRep.

3. The polling request/response mechanism can be used for all kinds of denial of service attacks. It is RECOMMENDED that a server does not change the polling-reference between polling requests.

8. References

8.1. Normative References

[RFC1945] Berners-Lee, T., Fielding, R., and H. Nielsen, "Hypertext Transfer Protocol -- HTTP/1.0", RFC 1945, May 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2510] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, September 2005.

[RFC4646] Phillips, A. and M. Davis, "Tags for Identifying Languages", BCP 47, RFC 4646, September 2006.

8.2. Informative References

[RFC2482] Whistler, K. and G. Adams, "Language Tagging in Unicode Plain Text", RFC 2482, January 1999.

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

Appendix A. Acknowledgments

The authors gratefully acknowledge the contributions of various members of the IETF PKIX Working Group and the ICSA CA-talk mailing list (a list solely devoted to discussing CMP interoperability efforts).

Appendix B. Registration of the application/pkixcmp Media Type

To: ietf-types@iana.org
Subject: Registration of MIME media type application/pkixcmp

MIME media type name: application

MIME subtype name: pkixcmp

Required parameters: -

Optional parameters: -

Encoding considerations:

Content may contain arbitrary octet values (the ASN.1 DER encoding of a PKIMessage sequence, as defined in the IETF PKIX Working Group specifications). base64 encoding is required for MIME e-mail; no encoding is necessary for HTTP.

Security considerations:

This MIME type may be used to transport Public-Key Infrastructure (PKI) messages between PKI entities. These messages are defined by the IETF PKIX Working Group and are used to establish and maintain an Internet X.509 PKI. There is no requirement for specific security mechanisms to be applied at this level if the PKI messages themselves are protected as defined in the PKIX specifications.

Interoperability considerations: -

Published specification: this document

Applications which use this media type: Applications using certificate management, operational, or ancillary protocols (as defined by the IETF PKIX Working Group) to send PKI message via E-Mail or HTTP.

Additional information:

Magic number (s): -
File extension (s): ".PKI"
Macintosh File Type Code (s): -

Person and email address to contact for further information:
Martin Peylo, martin.peylo@nsn.com

Intended usage: COMMON

Author/Change controller: Martin Peylo

Authors' Addresses

Amit Kapoor
Certicom
25801 Industrial Blvd
Hayward, CA
US

Email: amit@trustpoint.com

Ronald Tschalaer
Certicom
25801 Industrial Blvd
Hayward, CA
US

Email: ronald@trustpoint.com

Tomi Kause
SSH Communications Security Corp.
Fredrikinkatu 42
Helsinki 00100
Finland

Email: toka@ssh.com

Martin Peylo
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Email: martin.peylo@nsn.com