Continuing the Work on the CMP Transport Draft

Version 1.0

Martin Peylo
NSN Research / Security Technologies

Slides Overview

How Am I Involved?

The Need For CMP Transport Specification

CMP Transport Specification Background

Official pkix-WG CMPtrans draft versions

Unofficial CMPtrans draft versions

Other and Prior Authors’ Status

What CMPtrans Should Contain

How Am I Involved?

Main developer of open source CMP patch for OpenSSL

- Current focus on client-side, thus important target is to be compatible with existing server-side Implementations (e.g. cryptlib, Insta Certifier, EJBCA)
  - Had to cope with oddities in server-side implementations and discussed those in-depth with the authors
- Short-term goal to provide all functionality needed for client-side of 3GPP TS 33.310
- Long-term goal to have all CMP features implemented and accessible via API
- https://sourceforge.net/projects/cmpforopenssl/

Created Wireshark CMPv2 dissector

- Including TCP-Messaging dissector
- Had to cope with problems in existing implementations

The Need For CMP Transport Specification

Implementers need guidance how to profile the HTTP usage when transporting CMP.

Upcoming need e.g. through 3GPP TS 33.310:

- Transport of CMPv2 messages […] shall be done using HTTP-based protocol as specified in draft-ietf-pkix-cmp-transport-protocols. [not formally referenced as it is a draft]

CMP Transport Specification Background

RFC 2510 (March 1999, obsoleted) ”ietf-version2”/”cmp1999”

- Includes ”Direct TCP-Based Management Protocol”
- Registers MIME media type ”application/pkixcmp”
  - Transport via HTTP and E-mail mentioned but not specified in detail

RFC 4210 (September 2005) ”cmp2000”

- “A new polling mechanism is introduced, deprecating the old polling method at the CMP transport level. The CMP transport protocol issues are handled in a separate document [CMPtrans], thus the Transports section is removed.”
  - **But**, CMPtrans ”was allowed to die in 2004 by the authors”

→ ”cmp2000” transport is not specified at all

→ No need for old polling method (reason for ”TCP-Messaging”) anymore as cmp2000 includes this now

Official pkix-WG CMPtrans draft versions

http://tools.ietf.org/html/draft-ietf-pkix-cmp-transport-protocols

00/01: June 22, 2000

- Continuation of the Transport Protocols from RFC 2510, focussing on ”TCP-Message” protocoll
- HTTP transport defined to contain CMP with ”TCP-Message” header, MIME-type ”application/x-pkixcmp”

02: October 23, 2000

- MIME-type changed to ”application/x-pkixcmp-poll”

03/04: November 24, 2000 – minor changes

05: February 9, 2004

- MIME-type changed to ”application/pkixcmp”

Unofficial CMPtrans draft versions

http://tools.ietf.org/html/draft-ietf-pkix-cmp-transport-protocols

Resulting from discussions between Implementors

06: July 30, 2009

- HTTP transport now for PKIMessages (plain CMP) without the TCP-Message header
- General beautification

07: October 26, 2009

- HTTP-based transport SHOULD be preferred, ”TCP-based transport” OPTIONAL and deprecated
- HTTP transport described in more detail

08: April 27, 2009 – minor changes

09: July 09, 2010

- Ideas how Announcements can be polled by clients via HTTP

Other and Prior Authors' Status

Tomi Kause

- Will also spend some time on this
- Supplied the xml source used for draft version 5

Ronald Tschalär and Amit Kapoor

- "will not be able to participate as an author"
- "no time or desire to participate any further"

→ remove names from the author's list and move them to Acknowledgements with their approval

What CMPtrans Should Contain

- Explicit deprecating the useless and TCP-Messaging
  - But keeping the description as it has been implemented to some extend
- Profiling the HTTP use
  - HTTP Versions to use
  - General Form
  - Media Type
  - HTTP Request-URI
  - Communication Workflow
  - Persistent Connections
  - How to handle Announcements
    - Pushing/Polloing
- Mentioning other possible transport protocols
  - Desire to use those seems not to be existing

Questions

Thank You
Kiitos
Danke
धन्यवाद
谢谢
Grazie
Köszönöm