Lightweight industrial CMP profile

draft-brockhaus-lamps-industrial-cmp-profile-00

Hendrik Brockhaus, Steffen Fries, David von Oheimb

IETF 104 – LAMPS Working Group

Complex, but used in industry for over 10 years

- CMP V2 (RFC4210) and CRMF V2 (RFC4211) were released in 2005
- HTTP transfer for CMP (RFC6712) was published in 2012

- CMP was implemented by various PKI products in the past 20 years, especially between RA and CA
- CMP was profiled for certificate management in
  - 4G and 5G mobile backbone network since 2006
  - ETCS (European Train Control System) for on-board and track-side equipment since 2015

Very feature rich – profiling needed

- Feature rich protocols like CMP support many use cases like
  - Self-contained messages; use unprotected transport, including piggybacking and out-of-band
  - Support end-to-end security and complex trust relationships, e.g., to support central authorization
  - Various protection mechanisms, like signature and password based
  - Confidentiality for transport of centrally generated keys
  - Out-of-band transport using very small poll-messages
  - In-band confirmation to ensure reliable certificate management
  - Supports root CA update, endpoint configuration, etc.
  - Easily extendable to post quantum cryptography using the same structures as X.509
  - …
- Implementing all specified features of CMP and CRMF is not needed and far to complex
- Profiling reduces the complexity to the functionality needed and ensures interoperable implementation

Industrial certificate management use cases are bound to the device lifecycle

- Initial enrollment in an operational environment
- Update
- Revocation
- Delivery of new CA certificate chains
- Update of root CA certificate
- Configuration for certificate management
- Installation of new trust anchor, e.g., transport of RFC 8366 vouchers
- Confirmation and error messages

Real-life industrial requirements

- 4G and 5G mobile network use case from 3GPP TS 33.310 using CMP
- ETCS (European Train Control System) use case from UNISIG Subset-137 using CMP
- Power distribution substation use case from IEC 62351 Part 9 using SCEP or EST
- E-car charging use case using CMP via OCPP
- Offline trackside and interlocking systems
- IT-equipment on rolling stock
- Building automation during construction time
- Central authorization of certificate request

⇒ Fully automated, reliable, and self-contained certificate management protocol needed

Details of the use case can be found in the BAK.

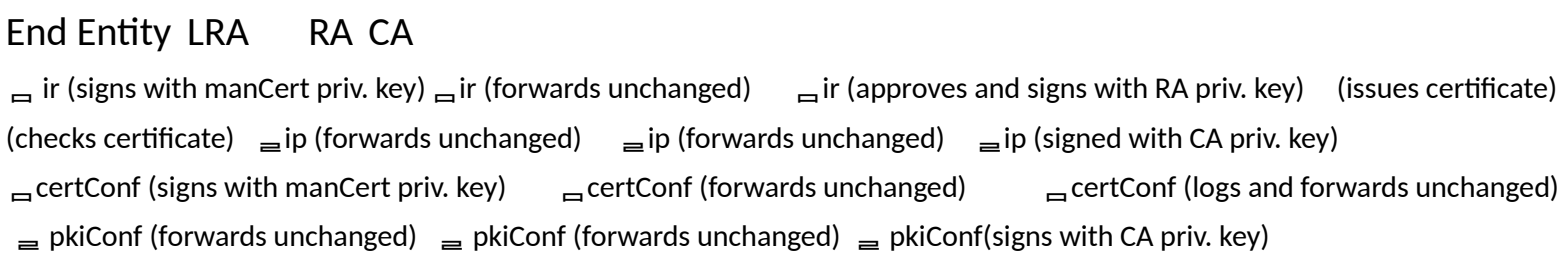
Profiling not only needed for end points

- Today’s certificate management standards focus on the end entity
- In industrial installations also PKI infrastructure components are needed, like LRA and RA as part of or interacting with, e.g.
  - Engineering tool
  - Management tool
  - Asset inventory
  - Monitoring system
  - Network access control
- To support different vendors, the LRA – RA – CA communication should also be standardized

CMP needs to be tailored for industrial use

- CMP V2 defines feature-rich protocol mainly intended for management of human user certificates
- 4G/5G and ETCS standardization developed profiles for very limited industrial use cases

- We propose to specify a set of lightweight message flows to address industrial use cases, e.g.
  - end entity signs the certificate request using its manufacturer provided certificate;
  - local RA receives and forwards certificate requests without changing end entity signature;
  - central RA checks certificate requests and proved approval with RA signature to CA;
  - CA processes certificate requests signed by RA, issues requested certificate and signs the response message;
  - response messages and proceeding confirmation messages are forwarded unchanged by LRA and RA



- Is the WG interested in this work?

CMP messages according to RFC 4210
ir: initialization request, requests a certificate from a new PKI; ip: initialization response, certConf: certificate confirmation; pkiConf: confirmation response
manCert: manufacturer provided certificate, also called IDevID

Backup

Real-life industrial requirements

- 4G and 5G mobile network use case from 3GPP TS 33.310 using CMP
  - Initial enrollment protected with manCert* signature
  - Update protected with old opCert* signature
  - Confirmation of successful enrollment and update
- ETCS (European Train Control System) use case from UNISIG Subset-137 using CMP
  - Initial enrollment protected with pre-shared secret
  - Update protected with old opCert* signature
  - Confirmation of successful enrollment and update
- Power distribution substation use case from IEC 62351 Part 9 using SCEP or EST
  - Initial enrollment protected with manCert* signature or optional TLS-Client authentication
  - Update protected with old opCert* signature or TLS-Client authentication
  - Currently a local CA is needed, in future central control center will do this via a proxy terminating TLS security
- E-car charging use case using CMP via OCPP
  - Initial enrollment and update with confirmation; protected with signature
  - Only OCPP communication allowed, no second protocol for certificate management, CMP messages will be piggybacked in OCPP container messages
- Offline track side and interlocking systems
  - Initial enrollment and update protected with signature
  - Revocation from end entity as well as from local RA
  - File-based message transport from local RA to central RA by technician; polling at local RA by end entity
- IT-equipment on rolling stock
  - Needs asynchronous certificate management due to lack of connectivity to the service partner under way
- Building automation during construction time
  - Needs asynchronous certificate management due to lack of online connectivity during construction time, e.g. because the building automation is commissioned, configured and tested floor by floor without central infrastructure available
- Central authorization of certificate request
  - If certificate management is part of the service business, the certificate request will be checked and authorized centrally at the service partner side; therefore the data origin authentication of the requesting entity needs to survive the complete transfer
  - State-of-the-art PKI operation is a central requirement for secure industrial control systems (IEC 62443); In many cases it will not be possible to operate a PKI on such security level locally

Fully automated, reliable, and self-contained certificate management protocol needed

* manCert: manufacturer provided certificate, also called IDevID; opCert: operational certificate, also called LDevID