Title: **CMPv2 profile for 3GPP subscriber certificate enrollment**

Source: **SSH Communications Security**

Document for: **Discussion/Decision**

Agenda item: **7.9 (Support for subscriber certificates)**

Contact: Ville Salmensuu, SSH Communications Security
Tel. +358 20 500 7496
ville.salmensuu@ssh.com

1. Introduction

In the SA#28 meeting, Tdoc S3-030239 [1] argued for the use of CMPv2 [2] as the Protocol B for subscriber certificate enrolment instead of PKCS#10-over-HTTP. Further work on the CMPv2 approach was agreed on, SSH promising a lightweight profile of CMPv2 for use as the Protocol B.

2. Discussion

The basis for the profile is [2], with the following features explicitly supported or not supported.

UE and CA shall support:

- initial registration/certification
    - basic authenticated scheme (B4)
- certificate request
- PKCS#10
- Implicit Confirm (3.1.1.1) - reduces number of round-trips to one
- CA shall send its self-signed certificate as the first Certificate in the "caPubs" field of the Certification Response message (3.3.4) (but probably the CA certificate is already installed in the UE)

UE and CA are not required to support:

- CRMF
- key update (not End-Entity nor CA)
- revocation request
- cross certification request
- polling
- key recovery
- announcements

ReferenceNumber and the shared secret are generated from AKA.

If centralized key generation in the server side is required, CRMF shall be supported by both the CA and the UE. CMPv2 specifies CRMF use for sending empty key pairs in the certificate request, while PKCS#10 does not.

Normally a user generates at least one key pair locally and uses that to get a certificate from a CA, according to profile B4. Key pairs for additional certificates from one CA can be generated centrally (according to profile B4 if one is enough, or B5 if more are needed).

If we have to support centralized key generation before requesting any other certificates, we have to deviate from the draft profile B4 as follows:

If a) "centralized SIGNATURE key generation" or b) "centralized ENCRYPTION key generation WITHOUT the associated local SIGNATURE key generation" are required, in addition crm[0] as defined by the draft shall not be present in the certificate request (this is deviating from the draft), but crm[1] shall be present, thus becoming crm[0] if needed. Notably the public key bits shall not be included.

4. Proposal

It is proposed that CMPv2 with profile above is selected as the recommended or the only protocol B. For the next SA3 meeting, a pseudo-CR stating such selection should be created.

5. References

[1] Tdoc S3-030239, Notes for the use of CMPv2 as the Protocol B

[2] IETF Draft draft-ietf-pkix-rfc2510bis-08.txt: “Internet X.509 Public Key Infrastructure Certificate Management Protocol”
http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc2510bis-08.txt