TSG-SA WG3 #28 **S3-030239**
Berlin, Germany, 6th–9th May 2003 **Agenda Item: 7.9**

Title:	**Notes for the use of CMPv2 as the subscriber certificate enrollment protocol (Protocol B)**
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

Tdoc S3-030073 (Protocol B: Subscriber Certificate Enrollment based on Bootstrapping) compares various certificate enrollment mechanisms. Some of the arguments for the preferred mechanism (PKCS#10 over HTTP) and against CMPv2 are debatable, and this document points out those, hoping for a reconsideration of CMPv2.

2. Discussion

2.1. Reuse of existing protocols

The PKCS#10-on-HTTP approach offers the minimum specification and development effort to achieve the PKI bootstrapping functionality as the protocol A draft already mandates the presence of all the building blocks required by this approach. It is debatable, though, whether this is in line with the requirement of using existing specifications as much as possible, or whether it actually means the genesis of yet another certificate life cycle management protocol.

If we observe the requirements of introducing the UE (mobile phone) as a client to full-blooded large-scale PKI systems, it is obvious that sooner or later it will be desirable to offer certificate life cycle management mechanisms (automatic UE cert renewal, CA cert renewal, UE initiated revocations etc.) for certificates associated with UE based private keys.

CMPv2 [1] is widely supported and interoperable [2], even though it has not yet passed to a draft standard status in IETF. CMPv1 is an RFC, but is not interoperable.

2.2. Delays in certificate enrollment

The requirement for CAs to instantly issue the certificates may be justified in the initial PKI bootstrapping scenario, but will limit the applicability of the certificate enrollment mechanism for some real life use cases. Delays in enrollment will occur both for technical reasons (a remote CA box is down/unreachable) and for certification policy reasons (certificates for some critical purpose must be issued manually). These delays will require a polling mechanism in the enrollment protocol.

2.3. Implications of not doing revocation checks

The document ignores certificate revocation status checks based on the assumption that all certificates which must be validated by the UE have a short validity period (hours/days). This approach:

- Prohibits integration with existing PKI systems which rely on revocation checks.
- Has implications on the scalability of the PKI: the CAs will end up performing more private key operations if all the certificates to be validated by the UE must be short-lived and thus reissued often, as opposed to periodically signing a revocation list.
- May suffice for initial small-scale deployments, but still it is recommandable to explicitly state something about the revocation check mechanisms (CRL/LDAP, CRL/HTTP, OCSP, DPD/DPV) that may be implemented now (and thus probably must be implemented by future versions of the standard).

CMPv2 specification supports certificate revocation requests, which can be used by the subscriber or the service provider to terminate the service.

2.4. "Heaviness" of CMPv2

CMPv2 is deemed "maybe too heavy for UE when it is used just for certificate enrollment and CA certificate delivery". The increase in client side complexity would be rather marginal, especially if only the initial enrollment functionality is required by the first version of the specification. This would be a bargain price for the room of growth offered by the full CMPv2 protocol specification.

2.5. CA certificate delivery

Whether or not CMPV2 specifies exactly how the CA certificate delivery is done is debatable. The extraCerts attribute is clearly intended for that purpose, and picking the top certificate even from a randomly ordered set of certificates is a trivial task for the client. The only valid problem in that solution is that extraCerts is an optional attribute in CA responses. Relying on this feature imposes a new strict requirement to the CA's CMPV2 server. In principle this is a problem. In practice this feature is so convenient for any PKI bootstrapping scenario that very probably the CMPV2 server implementations either already support or will support it in the future anyhow.

If major PKI vendors do not already support this, it is suggested that 3GPP construct a CMPV2 profile that mandates the transmission of the CA certificate as the first certificate within extraCerts.

2.6. Ready interface to CA products

Out-of-the-box CA's are widely capable of receiving CMPv2 requests over HTTP or TCP. The interface to receive a plain PKCS#10 request (as required by PKCS#10-over-HTTP) is not standardized, and often is a web interface, which is not suitable for the required level of automatic operation.

2.7. "Multiple messages"

PKCS#10-over-HTTP approach requires 4 messages total.

CMPv2 enrollment (profile B5, with certificate confirmations) requires 4 messages total. There does not seem to be a difference in the number of messages.

Additionally, the certificate confirmations provide a chance for the UE to not approve a certificate that did not match its request.

3. Conclusions

Despite the apparent “cons” of the full CMPv2 as defined, an appropriate profiling of CMPv2 for 3GPP use can provide the advantages of a light-weight enrollment protocol with room for growth and easy integration to existing PKI systems.

4. Proposal

It is proposed to re-evaluate the use of CMPv2 as the Protocol B.

5. References

[1] IETF Draft draft-ietf-pkix-rfc2510bis-08.txt: “Internet X.509 Public Key Infrastructure Certificate Management Protocol”
[2] CMPV2 Interop Project: http://www.ietf.org/proceedings/00dec/slides/PKIX-4/