3GPP TSG SA WG3 Security – S3#24 **S3-020366**

14 - 17 May 2002

Helsinki, Finland

Source: **SSH Communications Security Corp.**

Title: **CMP and CMC Comparison**

Document for: **Discussion**

Agenda Item: **7.20**

1. Introduction

Certificate life cycle management refers to operations and online interactions between PKI entities that are needed for enrolling certificates, updating end entity (EE) private keys before certificate expiration, certification authority (CA) key rollover, and requesting revocation online. The PKI initialisation of an end entity requires always some manual intervention for establishing trust with the CA. This intervention might include for example typing in a pre-shared key, which was distributed by the CA out-of-band to the EE administrator. On the other hand, updating the private key and enrolling a new certificate can be made fully automatic online operations. Deploying a PKI where network elements can perform these operations and communicate with the CA requires a standard, which specifies both transport protocol and message syntaxes for certificate lifecycle management.

Currently there are two different technologies available for certificate life cycle management

1. Certificate Management Protocol version 2 (CMPv2) [2]
2. Certificate Management Messages over CMS (CMC) [3].

This contribution introduces comparison criteria for the technologies, compares the technologies and proposes a preferred technology to be adopted in 3GPP networks.

2. Comparison Criteria

This chapter introduces the comparison criteria of the technologies in an alphabetical order.

Available products

Lists the products that are available of the technologies.

Deployment status

Defines the current status of the technology deployment.

Complexity

Defines the technology complexity in a high level.

Features

Lists the essential features that differ between technologies. The features that are similar in both technologies are not listed.

Interoperability status

Describes the current status of interoperability, number of interoperability testings held etc.

Organization support

The organisation support defines the status at the other organisations and forums that are considering the selection of CMPv2 or CMC.

Reference implementations

Lists the reference implementations available of the technologies.

Standardization status

Describes the level of standardization (standard frozen, work ongoing, new version under standardization etc.).

3. Protocol Comparison

Criterion	CMP	CMC
Available products & companies with technology support.	1. RSA Keon CA 2. SSH Certifier 3. Entrust Authority 4. Baltimore Unicert 5. Utimaco Safeguard PKI 6. OpenSSL (partial support) Companies with interoperable CMPv2 code include Baltimore, Certicom, Cryptlib, Cylink, Entegrity, Entrust, IBM, RSA Security, SSH and TC TrustCenter. [5]	1. MS CA server in .NET 2. Verising it its managed PKI service No available products from CA vendors.
Complexity	CMP introduce its own message syntax so existing implementations of other cryptographic message syntaxes cannot be re-used.	The fact that CMC utilizes common message syntaxes can bring 5-10% savings in code size if the implementation already supports CMS (PKCS#7) and PKCS#10.
Deployment status	Deployment of several years.	Few supporting products in 2002.

Features	CMPv2 offers a mechamism to transfer root CA certificate to the end entity, so that certificate can be trusted without out-of-band finger print check (shared secret issued by the CA is being used to achieve this).	The basic functionality is similar to CMP except that CA certificates cannot be authenticated with pre-shared key similarly to CMP.
Interoperability status	PKI Forum in co-operation with ICSA has conducted an interoperability testing in 2001. [5]	None.
Organization support	CMPv2 is the preferred life cycle management mechanism of 1. PKI Forum 2. NIST 3. EEMA The PKI Challenge project of EEMA supports full implementation of CMPv2 for implementing end entity enrolment, sub-ordination and cross-certification functions. [6]	PKI Challenge project of EEMA supports in addition to CMPv2 also a 'simple version' of CMC which utilizes PKCS#10 as a certification request. However, it can only be used for first time enrolment, not for complete certificate lifecycle management. [6]
Reference implementations	1. NIST 2. OpenSSL (partial implementation)	None.
Standardization status	CMPv1 received the RFC status in 1999. CMPv2 is currently at the final draft phase (draft-ietf-pkix-rfc2510bis-06) and is expected soon to receive the RFC status.	CMC received the RFC status in 2000. That specification has been updated later, and the latest Internet Draft is draft-ietf-pkix-2797-bis-01.

3. Proposal

The basic functionality, certificate lifecycle management for PKI entities is being provided by both CMP and CMC. There are small functional differences such as the ability of CMP to transfer directly trusted root CA certificates to the end entities, but the functionality alone cannot be used as a basis for the decision of choosing between these protocols. The strongest argument of CMC against CMP is the fact that existing CMS code can be re-used to enable faster implementation and more efficient code. However, CMS does not specify messages nor protocol for lifecycle management and therefore the savings are rather limited (estimated 5-10% saving in code size).

The biggest differences between CMP and CMC are in the areas of maturity level, interoperability and deployment status. CMP is widely supported by most of the PKI/CA products today and an extensive industry-wide interoperability testing has been conducted to enable interoperability in multi-vendor PKI environment. Since this kind of testing effort has not been conducted with CMC due to lack of implementations, it would likely take several more years for CMC to reach the stability and interoperability status that CMP has today. The support of Microsoft for CMC will potentially introduce CMC-enabled Windows applications in the future. However, in one-vendor environment (Microsoft CA) the interoperability requirements are not as critical as in multi-operator network infrastructure.

It is suggested that SA3 will take CMPv2 as a working assumption for certificate lifecycle management for NDS/AF work.

Reference

[1] C. Adams & S. Farrell, “RFC2510: Certificate Management Protocols”, March 1999

[2] C. Adams & S. Farrell, “Internet draft: Certificate Management Protocols”, December 2001 < draft-ietf-pkix-rfc2510bis-06.txt >

[3] Manyfolks, “RFC 2797: Certificate Management Messages over CMS”, April 2000

[4] The ProjectDPLOY Archives, March – June 2002
< http://postal.trusecure.com/pipermail/projectdploy/ >

[5] PKI Forum, “PKI Forum Advances Interoperability of Certificate Lifecycle Management“, January 2001
< http://www.pkiforum.org/news/2001/CMP_FINAL3.htm >

[6] EEMA, PKI Challenge Project, July 2002
< https://www.eema.org/pki-challenge/ >

[7] R. Moskowitz, „Prologue to a Protocol?“, June 1999
< http://www.networkcomputing.com/1012/1012colmoskowitz.html >

[8] NIST, “ Minimum Interoperability Specification for PKI Components, Version 2 - Second DRAFT“, August 2000
< http://csrc.nist.gov/pki/documents/MISPC2_public3_20000831.pdf >