OMA SEC-CERT Management Objects (MO)

Approved Version 1.0 – 02 Sep 2008

Open Mobile Alliance

OMA-DDS-SEC_CERT_MO-V1_0-20080902-A

Contents

Figures

1. Scope

This data specification defines Management Objects (MO) required for the management of security properties in the context of the SEC_CF enabler. The structure and the machanisms to use Management Objects (MO) are defined in OMA Device Management Enabler [DM]. This specification does not detail how these MOs are created or transported to the devices but rather defines the contents and the purpose of the MOs.

This specification intends to specify all the necessary management objects required for the operation of the SEC_CF v1.0 enabler and does not intent to specify all the security related MOs that may be defined in other existing OMA enablers. This specification will be updated as required following the new versions of SEC_CF Enabler specifications.

2. References

2.1 Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[DM] "OMA Device Managemet Enabler ", Version 1.2, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[DMBOOT] "OMA Device Management Bootstrap, Version 1.2". Open Mobile Alliance™. OMA-TS-DM_Bootstrap-V1_2. URL:http://www.openmobilealliance.org

[DMTNDS] "OMA Device Management Tree and Description Serialization Specification, Version 1.2". Open Mobile Alliance. OMA-TS-DM_TNDS-V1_2. URL:http://www.openmobilealliance.org

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL:http://www.ietf.org/rfc/rfc4234.txt

[TLS] "Transport Layer Security (TLS) Version 1.0", IETF RFC 2246, Jan 1999

URL: http://www.ietf.org/rfc/rfc2246.txt

[WAP-219-TLS] "WAP TLS Profile and Tunneling Specification ",WAP Forum ™, WAP-219-TLS-20010411-a, URL: http://www.openmobilealliance.org

[RFC2817] "Upgrading to TLS Within HTTP/1.1," rfc 2817, R. Khare, S. Lawrence, May 2000.

URL: http://www.ietf.org/rfc/rfc2817.txt

[RFC3280] "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," rfc 2459, R. Housley, W. Ford, W. Polk, D. Solo, April 2002. URL: http://www.ietf.org/rfc/rfc3280.txt

[CertProf] "Certificate and CRL Profiles", Open Mobile Alliance™. OMA-Security-CertProf-V1_1-20040615-C. URL: http://www.openmobilealliance.org/release_program/wpki_v10.html

[OCSP] "Online Certificate Status Protocol Mobile Profile", OMA-WAP-OCSP_MP-V1_0-20070403-A, URL: http://www.openmobilealliance.org

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, URL:http://www.openmobilealliance.org/

[SEC_CF AD] "Common Security Functions Architecture", OMA-AD-SEC_CF-V1_0,

URL: http://www.openmobilealliance.org

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

3.3 Abbreviations

OMA	Open Mobile Alliance
TLS	Transport Layer Security
SEC_CF	Security Common Functions
CA	Certificate Authority
OCSP	Online Certificate Status Protocol
DM	Device Management

4. Introduction

OMA Device Management [DM] enabler defines a protocol (as well as a data format) that allows the provisioning of Management Objects [MO] to devices that support the enabler. Device Management enabler is generally implemented using a DM Server that stores the MOs to be transferred to a device management client using the DM protocol. Additionally, the devices can be first initialized (bootstrapped) in 3 different ways: at the factory, with a smartcard or via a DM server.

MOs can contain various types of information (e.g. configuration data, account information, white lists, etc) that can be used by the device depending on the functionality required by the OMA enabler that is implemented by the device.

In the case of SEC_CF enabler, MOs contain security related parameters required for the operation of SEC_CF enabler by the device.

5. Justification

Digital certificate is widely used as the identity of customers in the network environment for user authentication, digital signature, key agreement, etc.

The Certificate MO provides a standardized set of management objects for maintaining certificates in the mobile terminal. It allows an external entity, e.g. a CA, to add a new certificate, to update/replace a certificate, and to delete a certificate in the mobile terminal via DM enabler.

6. OMA SEC-CERT Management Object (MO)

6.1 Introduction to Management Objects

Management objects are the entities that can be manipulated by management actions carried over the OMA DM protocol. A management object can be as small as an integer or large and complex like a background picture, screen saver, or security certificate. The OMA DM protocol is neutral about the contents, or values, of the management objects and treats the node values as opaque data.

6.1.1 Definition and description of management objects

OMA DM management objects are defined using the OMA DM Device Description Framework [DMTND], or DDF. The use of this description framework produces detailed information about the device in question. However, due to the high level of detail in these descriptions, they are sometimes hard for humans to digest and it can be a time consuming task to get an overview of a particular object's structure.

In order to make it easier to quickly get an overview of how a management object is organized and its intended use, a simplified graphical notation in the shape of a block diagram is used in this document. Even though the notation is graphical, it still uses some printable characters, e.g. to denote the number of occurrences of a node. These are mainly borrowed from the syntax of DTDs for XML. The characters and their meaning are defined in the following table.

Character	Meaning
+	one or many occurrences
*	zero or more occurrences
?	zero or one occurrences

If none of these characters is used, the default occurrence is exactly once.

There is one more feature of the DDF that needs to have a corresponding graphical notation, the un-named block. These are blocks that act as placeholders in the description and are instantiated with information when the nodes are used at run-time. Un-named blocks in the description are represented by a lower case character in italics, e.g. *x*.

Each block in the graphical notation corresponds to a described node, and the text is the name of the node. If a block contains an *x,* it means that the name is not known in the description and that it will be assigned at run-time. The names of all ancestral nodes are used to construct the URI for each node in the management object. It is not possible to see the actual parameters, or data, stored in the nodes by looking at the graphical notation of a management object.

For a further introduction to this graphical notation, please refer to [DMStdObj].

6.2 SEC-CERT Management Object

6.2.1 Introduction

If SEC_CF MOs are provisioned together with other management object(s) during the bootstrap, then [DMTNDS] and [DMBOOT] MUST be used.

The SEC_CF Management Objects are compatible with OMA DM [DM] protocol version 1.2 or any later compatible version.

Management Object Identifier for the SEC_CF Certificate (SEC-CERT) Management Object SHALL be:
urn:oma:mo:oma-sec-cert:1.0

6.2.2 Figure of the Certificate MO

The following figure shows the structure of the certificate management object.

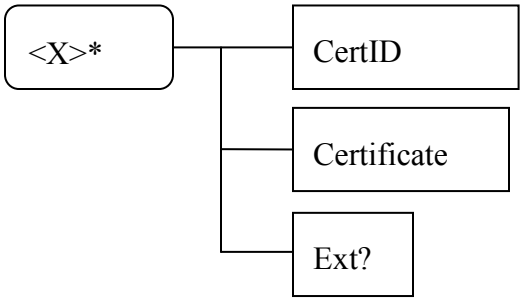

Figure 1: Structure of the SEC-CERT MO.

6.2.3 Node Description

This section provides a description of the elements of the Certificate MO.

1. …/<X>

This interior node acts as a placeholder for each set of certificate information. The name of this node will be assigned when it is created. The purpose of this interior node is to group together the parameters of a single certificate object. The ancestor elements of this node define the position in the management tree of the proxy object. But the structure of the DM tree and hence positions in the tree of management objects is out of scope of this specification.

- Occurrence: ZeroOrMore
- Format: Node
- Access Types: Get
- Values: N/A

2. <X>/ CertID

This leaf node specifies the identifier of the Certificate and it is mandatory. The identifier can be equal to the "Certificate serial number" field in the Certificate but it is not mandatory.

- Occurrence: One
- Format: Chr
- AccessType: Get
- Values: the identifier of the Certificate

3. <X>/Certificate

This leaf node contains the actual binary Certificate. This node is the logical storage position of the certificate and the physical storage depends on the implementation which is out of scope of this specification.

- Occurrence: One
- Format: Bin
- Access Types: Get
- Values: the Certificate

4. <X>/Ext

This is a node for supporting possible extensions.

- Occurrence: ZeroOrOne
- Format: Node
- Access Types: Get
- Values: N/A

7. Operational Considerations

7.1 Conformance aspect

SEC-CERT MO is normatively dependent on the DM 1.2 specifications. However, this normative dependency should not be seen as restricting this MO definition only to DM clients implementing that version of the DM enabler.

For example, a management authority may exchange SEC-CERT MO data-files using means not specifically defined in the DM 1.2 enabler.

7.2 Security aspect

The SEC-CERT MO can be used to maintain root certificates and non-root certificates. As to the root certificates, the DM enabler should take measurement to assure the integrity of them both during their transfer from DM Server to DM Client and when stored in the terminal. As to the non-root certificates, it is not required that special mechanism be used because their intergrity is assured by the signature made by the CA.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
Approved Versions OMA-DDS-SEC_CERT_MO-V1_0	02 Sep 2008	Status changed to Approved by TP OMA-TP-2008-0321-INP_SEC_CF_V1_0_ERP_for_Final_Approval