Standardized Connectivity Management Objects
EAP Parameters

For use with OMA Device Management

Approved Version 1.0 – 24 Oct 2008

Open Mobile Alliance

OMA-DDS-DM_ConnMO_EAP-V1_0-20081024-A

Contents

Figures

Tables

1. Scope

This document defines EAP specific parameters that are used together with the standardized connectivity management object [CONNMO] in order to have a complete standardized EAP management object for WLANand other bearers in the OMA DM management tree.

While this EAP object is optional for any OMA DM implementation, their widespread use will simplify the management of basic EAP parameters in mobile devices.

The object is defined using the OMA DM Device Description Framework [DMTND]. The object has standardized points of extension to permit implementation-specific parameters to accompany the standardized parameters. This added flexibility is intended to encourage the use of the standardized object while not unnecessarily restricting individual vendor innovations.

2. References

[CONNMO] *Standardized Connectivity Management Objects, Version 1.0*
OMA-DDS-DM-ConnMO-V1.0, URL:http://www.openmobilealliance.org

[DMTND] *Device Management Tree and Description, Version 1.2*, Open Mobile Alliance™, OMA-TS-DM-DMTND-V1_2, URL:http://www.openmobilealliance.org

[RFC2119] *RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, S. Bradner, March 1997,* URL:http://www.ietf.org/rfc/rfc2119.txt

2.1 Normative Authorities of References

Various parameters specified in the management objects defined in this document rely on an authority outside the scope of this specification to supply the set of acceptable values and value formats. In such references to external authority, only the directly cited material is referenced, not the entire external specification. The following authorities of reference are cited in this document:

[802.1X] IEEE Standard 802.1x-2001, IEEE, URL: http://www.ieee.org

[IANA-EAPTYPE] Extensible Authentication Protocol (EAP) Registry,
URL: *http://www.iana.org/assignments/eap-numbers*

[WPA] Wi-Fi Protected Access (WPA) Version 3.1. Wi-Fi Alliance, August 2004,
URL: http://www.wi-fi.org/

[RFC2634] *RFC 2634, Enhanced Security Services for S/MIME*, The Internet Society, June 1999, URL: ftp://ftp.rfc-editor.org/in-notes/rfc2634.txt

[RFC2716] *RFC 2716, PPP EAP TLS Authentication Protocol,*
The Internet Society, 1999, URL: ftp://ftp.rfc-editor.org/in-notes/rfc2716.txt

[RFC3280] *RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, The Internet Society, 2002, URL: ftp://ftp.rfc-editor.org/in-notes/rfc3280.txt

[RFC3748] *RFC 3748, Extensible Authentication Protocol (EAP)*,
The Internet Society, 2004, URL: ftp://ftp.rfc-editor.org/in-notes/rfc3748.txt

[RFC4187] *RFC4187, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),* The Internet Society, January 2006, URL: ftp://ftp.rfc-editor.org/in-notes/rfc4187.txt

[RFC4282] *RFC 4282, The Network Access Identifier*, Dec 2005, URL: ftp://ftp.rfc-editor.org/in-notes/rfc4282.txt

[RFC4387] *RFC 4387, Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP*, The Internet Society, Feb 2006, URL: ftp://ftp.rfc-editor.org/in-notes/rfc4387.txt

[WLAN] IEEE Standard 802.11-2007, URL: http://www.ieee.org/

2.2 Informative References

None

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.

3.2 Definitions

See the DM Tree and Description [DMTND] document for definitions of terms related to the management tree.

3.3 Abbreviations

EAP	Extensible Authentication Protocol
IETF	Internet Engineering Task Force
MS	Mobile Station
NAI	Network Access Identifier
OMA	Open Mobile Alliance
WLAN	Wireless Local Area Network

4. Introduction

Usually over time network protocols grow and are replaced as the market cycle plays out. Connectivity Management Object [CONNMO] is structured in such a way as to be resilient to the addition of new bearer and proxy types without requiring wholesale replacement of the object definitions. In this way, the common structure survives into future versions of the management objects thus easing the burden of transition from old bearer types to new.

This document specifies generic EAP management object, which also allows for vendor specific extensions.

5. Justification

This Reference Release includes several Management Object definitions for use, in conjunction with the OMA Device Management Enabler, to manage data network connectivity settings for mobile terminals over common bearer and proxy types.

5.1 Standardized Connectivity Management

Providing a standardized set of management objects for configuration of data network connectivity through the OMA Device Management system will improve the usability and customer experience of mobile terminals that rely upon data services. As proposed, the management object definitions may be used in conjunction with OMA Device Management Candidate and Approved Enabler Releases over a variety of transports including: HTTP, HTTPS, OBEX over IrDA, OBEX over Bluetooth, and various forms of Smart Card.

5.2 Application-Neutral

Producing these management object definitions in an application-neutral fashion, we avoid reinvention of solutions to the same set of problems for each of new application that requires data connectivity. This reduces the connectivity parameters that an application must define to a simple reference node, ConRef (Connectivity Reference).

5.3 Bearer-Neutral

By presenting the specifications in two parts, a bearer-neutral part and bearer-specific bindings, we reinforce the OMA principle of network neutrality while providing specificity where needed but without bias for or against any particular network type.

6. EAP Specific Management Object

6.1 Introduction

A general introduction of the connectivity management object is given in the connectivity management object document [CONNMO] as well as the needed compliance rules. This document specifies the EAP specific subtree in order to enable EAP specific parameter manipulation.

6.2 Graphical Representation (Informative)

The following figure provides the structure of EAP specific parameter sub-tree.

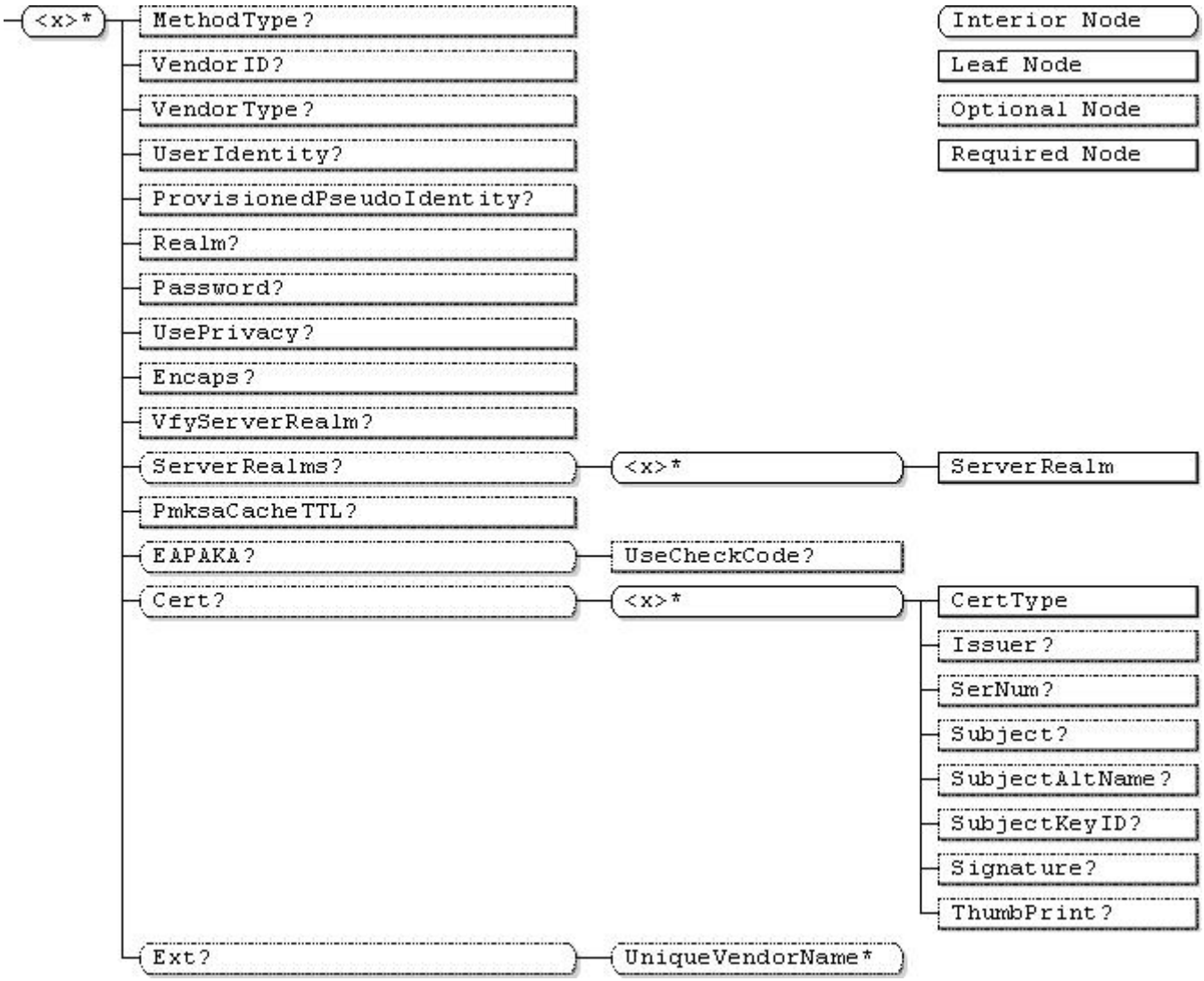

Figure 1. EAP MO

6.3 Node Descriptions

<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node distinguishes different EAP methods. Not all security methods use all of these settings. There can be multiple sets of EAP settings. The priority of the various EAP methods is implementation-specific. Management Object Identifier for the EAP MO MUST be: "urn:oma:mo:oma-connmo-eap:1.0".

MethodType

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

The EAP Type [WPA] specifies the EAP method type of the actual method. The integer value space for EAP method types is defined in [RFC3748] and represents both standard and extended type spaces. The value of this node represents the Method Type field [RFC3748] §5.7. The specific allocated values are registered with IANA [IANA-EAPTYPE]. Values used here MUST be from the IANA registry.

An alternate way to specify the used method is to use VendorID and VendorType leaf nodes. Either MethodType or VendorID & VendorType must be present in the EAP node.

VendorID

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

The EAP Vendor ID specifies the SMI Network Management Private Enterprise Code of the Vendor of the actual method. The integer value space for EAP Vendor ID is defined in [RFC3748] §5.7. The specific allocated values are registered with IANA [IANA-EAPTYPE]. Values used here MUST be from the IANA registry.

An alternate way to specify the used method is to use MethodType leaf node. Either MethodType or VendorID & VendorType must be present in the EAP node.

VendorType

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

The EAP Vendor Type specifies the vendor specific method type. The integer value space for EAP Vendor Type and selected pre-assigned values are defined in [RFC3748] §5.7.

UserIdentity

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The UserIdentity parameter specifies the user's identity [RFC3748]. If this is not specified then the type itself decides what is sent as the user identity. For example, a terminal authenticating using EAP-TLS might use the user identity from the user's certificate. As a further example, some implementations might choose to ask the user directly during authentication. The format of the parameter is UTF-8 and maximum length 255 bytes [RFC4282].

ProvisionedPseudoIdentity

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The value of this leaf node specifies the starting pseudo identity value for use by identity privacy mechanisms employed by some EAP method types. This value is meaningful only for some EAP method types and is meaningful only if UsePrivacy is TRUE.

Realm

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

The Realm parameter specifies the override realm that is sent, for example, in the EAP Identity/Response packet [RFC3748]. The complete identity response is of the form: "*UserIdentity-value@Realm-value*" [RFC4282].

Password

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	No Get

Password is the password that is used in EAP Authentication. The format of the parameter is UTF-8 and maximum length 255 bytes [RFC4282].

UsePrivacy

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

This leaf node exists in order to inform the device of the policy about the identity privacy. The meaning of this leaf node is different for each EAP method because each EAP method has its own identity privacy mechanism. If the value is TRUE, the identity hiding mechanisms of the specified EAP method are active; if FALSE or if the node is omitted, identity hiding mechanisms are not active or are not supported.

Encaps

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

Certain EAP methods can run other methods encapsulated in a secure tunnel. The Encaps parameter specifies for which encapsulating EAP method the settings in this set are associated. The value is a run-time URI to the EAP method parameter set of the encapsulating method. The Encaps value must point to an EAP method parameter set defined in the same EAP MO to which the Encaps node belong.

There MUST NOT be two EAP objects with the same value for Encaps.

VfyServerRealm

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

VfyServerRealm [802.1X], if set to TRUE, the realm of the server's certificate is verified. If this is omitted or FALSE server realm is not checked.

ServerRealms

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node contains a list of server realms.

ServerRealms/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node distinguishes the different server realms. There must be exactly one ServerRealm Node for each of these interior nodes.

ServerRealms/<X>/ServerRealm

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

The ServerRealm node defines an allowed realm that the device will accept. The value identifies as much of the domain name that the service provider wishes the MS to verify as part of the DNS name in the server certificate [RFC2716] §3.4.

PmksaCacheTTL

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

PmksaCacheTTL, [WLAN] §5.9.5, specifies the maximum time (as a 16 bit unsigned integer number of minutes) the PMKSA should remain in the client cache before it is assumed stale. This parameter is meaningful only when SEC MODE is WPA2.

EAPAKA

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This node includes EAPAKA [RFC 4187] specific settings.

EAPAKA/UseCheckCode

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

EAPAKA [RFC4187] has a security option of the use of AT_CHECKCODE attribute that can protect EAP/AKA-Identity messages exchanged between the device and the AAA before the keying material is derived.

Cert

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

For those EAP types that use certificates, the required user certificates are specified in this subtree.

Cert/<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node distinguishes different certificates.

Cert/<x>/CertType

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This node specifies the type of certificate. The allowed values are:

CertType	Description
DEVICE	Device certificate. This indicates that authentication is device authentication; other fields in CERT block are not used. [RFC3280]
USER	End entity certificate [RFC3280]. Can be user or device certificate.
CA	CA certificate [RFC3280]

Table 1: CertType

Cert/<x>/Issuer

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

Issuer is the Distinguished Name of the certificate's issuer in human readable UTF-8 form (for example "/C=US/O=Some organization/CN=Some common name"). [RFC3280] §4.1.2.4.

Cert/<x>/SerNum

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This specifies the serial number of the certificate. [RFC3280] §4.1.2.2.

Cert/<x>/Subject

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

Subject specifies the Distinguished Name of the certificate's subject in human readable UTF-8 form (for example, "/C=US/O=Some organization/CN=Some common name"). [RFC3280] §4.1.2.6.

Cert/<x>/SubjectAltName

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

SubjectAltName specifies the NAI included in the subject alt-name field in RFC822 format. [RFC3280] §4.2.1.7.

Cert/<x>/SubjectKeyID

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bin	Get

SubjectKeyID specifies the subject key identifier of a certificate. [RFC3280] §4.2.1.2.

Cert/<x>/Signature

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bin	Get

Signature specifies the digital signature of the certificate.
[RFC3280] §4.1.1.3. The value is encoded as BIT STRING as specified in [RFC3280].

Cert/<x>/ThumbPrint

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bin	Get

ThumbPrint specifies the hash of the certificate as specified in [RFC2634] §5.4.1 and [RFC4387] §2.2. Thumbprint is also known as fingerprint [RFC4387] §2.2 and it is hash function result (e.g. SHA-1as specified in [RFC4387]) of the certificate.

Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This optional interior node designates a branch of the EAP parameters sub-tree into which vendor extensions MAY be added, permanently or dynamically. Ext sub trees, such as this one, are included at various places in the DM connectivity management objects to provide flexible points of extension for implementation-specific parameters. However, vendor extensions MUST NOT be defined outside of one of these `Ext` sub-trees.

Ext/UniqueVendorName

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	node	Get

This interior node is supplied by a vendor to distinguish their extension from those of other vendors. The *UniqueVendorName* SHOULD be a trademark or company name controlled by each vendor to ensure uniqueness. The structure of any sub-tree below a *UniqueVendorName* interior node is implementation-specific.

7. Operational Considerations

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

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

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-DDS-DM_ConnMO_EAP-V1_0-20081024-A	24 Oct 2008	Approved by OMA Technical Plenary: Ref TP#: OMA-TP-2008-0405-INP_ConnMO_V1_0_RRP_for_Notification_and_Final_Approval