OMA TLS Profile

Approved Version 1.1 – 31 Jul 2012

Open Mobile Alliance

OMA-TS-TLS_Profile-V1_1-20120731-A

Contents

1. SCOPE ... 4
2. REFERENCES ... 5
2.1 NORMATIVE REFERENCES ... 5
2.2 INFORMATIVE REFERENCES ... 6
3. TERMINOLOGY AND CONVENTIONS ... 7
3.1 CONVENTIONS ... 7
3.2 DEFINITIONS ... 7
3.3 ABBREVIATIONS ... 7
4. INTRODUCTION ... 8
4.1 VERSION 1.0 ... 8
4.2 VERSION 1.1 ... 8
5. OMA TLS PROFILE ... 9
5.1 SUPPORTED VERSIONS ... 9
5.2 SUPPORTED CIPHER SUITES FOR TLS ... 9
5.3 SUPPORTED CIPHER SUITES FOR PSK-TLS ... 9
5.4 SESSION RESUMPTION ... 10
5.5 SERVER AUTHENTICATION ... 10
5.6 CLIENT AUTHENTICATION ... 10
5.7 TLS TUNNELING ... 10
5.8 TLS EXTENSIONS FOR WIRELESS NETWORKS ... 10
5.9 PROFILING DTLS TO SUPPORT OMA ENABLERS OVER UDP ... 11
APPENDIX A. CHANGE HISTORY (INFORMATIVE) ... 12
A.1 APPROVED VERSION 1.0 HISTORY ... 12
APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) ... 13
B.1 SCR FOR TLS CLIENT ... 13
B.2 SCR FOR TLS SERVER ... 13

1. Scope

This specification defines an OMA profile of TLS related specifications specified in IETF, [RFC2246], [RFC4346], [RFC4279], [RFC4366], [RFC3268], [RFC4347], [RFC5246], [RFC4785][RFC5487]. The TLS related specifications are often used in OMA Enabler Specifications and the current TLS specifications include several optional features for the enabler specifications to choose from. Existence of several versions and options in the TLS related specifications may lead to interoperability problems in some implementations of TLS in OMA Enablers. In addition, requiring implementations of some options in the TLS protocol for OMA enablers can increase the level of security compared to only implementing the mandatory features in the TLS related specifications. OMA Workgroups developing enabler specifications are recommended to use the OMA Profile of TLS.

.

2. References

2.1 Normative References

[3GPP TS 33.102]	"3G Security; Security architecture", 3GPP TS 33.102, URL: http://www.3gpp.org/
[3GPP TS 33.203]	"3G security; Access security for IP-based services", 3GPP TS 33.203, URL: http://www.3gpp.org/
[3GPP TS 33.310]	"Network Domain Security (NDS); Authentication Framework (AF)", 3GPP TS 33.310, URL: http://www.3gpp.org/
[CertProf]	"Certificate and CRL Profiles", Open Mobile Alliance™, OMA-Security-CertProf-V1_1, URL: http://www.openmobilealliance.org/
[RFC768]	"User Datagram Protocol", IETF RFC 768, J. Postel, August 1980, URL: http://www.ietf.org/rfc/rfc768.txt
[RFC793]	"Transmission Control Protocol", IETF RFC 793, J. Postel, September 1981, URL: http://www.ietf.org/rfc/rfc793.txt
[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt
[RFC2234]	"Augmented BNF for Syntax Specifications: ABNF", IETF RFC 2234, D. Crocker, Ed., P. Overell. November 1997, URL: http://www.ietf.org/rfc/rfc2234.txt
[RFC2246]	"Transport Layer Security (TLS) Version 1.0", T. Dierks, E. Rescorla, IETF RFC 2246, Jan 1999, obsoleted by RFC4346, URL: http://www.ietf.org/rfc/rfc2246.txt
[RFC2459]	"Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 2459, R. Housley, W. Ford, W. Polk, D. Solo, January 1999, obsoleted by RFC3280, URL: http://www.ietf.org/rfc/rfc2459.txt
[RFC2616]	"Hypertext Transfer Protocol -- HTTP/1.1", IETF RFC 2616, R. Fielding, J. Gettys, et al, June 1999, URL:http://www.ietf.org/rfc/rfc2616.txt
[RFC2817]	"Upgrading to TLS Within HTTP/1.1," IETF RFC 2817, R. Khare, S. Lawrence, May 2000, URL: http://www.ietf.org/rfc/rfc2817.txt
[RFC3268]	"Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", IETF RFC 3268, June 2002, URL: http://www.ietf.org/rfc/rfc3268.txt
[RFC3280]	"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", R. Housley, W. Polk, W. Ford, D. Solo, April 2002, obsoleted by RFC5280, URL: http://www.ietf.org/rfc/rfc3280.txt
[RFC4279]	"Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", IETF RFC 4279, P. Eronen, et al, December 2005, URL: http://www.ietf.org/rfc/rfc4279.txt
[RFC4346]	"Transport Layer Security (TLS) Version 1.1", T. Dierks, E. Rescorla, IETF RFC 4346, April 2006, obsoleted by RFC5246, URL: http://www.ietf.org/rfc/rfc4346.txt
[RFC4347]	"Datagram Transport Layer Security", E. Rescorla, N. Modadugu, IETF RFC 4347, April 2006, URL: http://www.ietf.org/rfc/rfc4347.txt
[RFC4366]	"Transport Layer Security (TLS) Extensions", S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, T. Wright, IETF RFC 4366, April 2006, obsoleted by RFC5246, URL: http://www.ietf.org/rfc/rfc4366.txt
[RFC4785]	"Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", IETF RFC4785, January 2007, URL: http://www.ietf.org/rfc/rfc4785.txt
[RFC5246]	"Transport Layer Security (TLS) Protocol Version 1.2", IETF RFC 5246, August 2008, URL: http://www.ietf.org/rfc/rfc5246.txt
[RFC 5280]	"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, May 2008, URL: http://www.ietf.org/rfc/rfc5280.txt
[RFC5487]	"Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", IETF RFC5487, March 2009, URL: http://www.ietf.org/rfc/rfc5487.txt

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

[SEC_CERT_MO] "OMA SEC_CF Device Management (DM) Management Objects ", Open Mobile Alliance™, OMA-DDS-SEC_CERT_MO-V1_0,URL: http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_8, URL:http://www.openmobilealliance.org/

[OCSP_MP] "Online Certificate Status Protocol Mobile Profile", Version 1.0, Open Mobile Alliance™, OMA-WAP-OCSP_MP-V1_0, URL: http://www.openmobilealliance.org

[SEC_CF AD] "Security Common Functions Architecture", Version 1.1, Open Mobile Alliance™, OMA-AD-SEC_CF-V1_1, 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.

3.2 Definitions

None

3.3 Abbreviations

DDF	Data Description Format
DM	Device Management
DTLS	Datagram Transport Layer Security
MO	Management Object
OCSP_MP	OMA Online Certificate Status Protocol Mobile Profile
OMA	Open Mobile Alliance
PSK-TLS	Pre-Shared Key TLS
SEC_CF	Security Common Function
TLS	Transport Layer Security
UDP	User Datagram Protocol

4. Introduction

TLS (Transport Layer Security) related specifications [RFC2246], [RFC4346], [RFC4279], [RFC4366], [RFC3268], [RFC4347], [RFC5246], [RFC4785][RFC5487] among others, provide a secure and reliable transport mechanism between two communicating parties. It provides confidentiality and integrity protection for the transport used. It can also provide unilateral or mutual authentication depending on the implementations. TLS works in a client-server model, where the initiator is called the Client and the responder is called the Server. In most cases, a TLS client can authenticate a TLS server using a public key certificate. Mutual authentication is also possible using public key certificates or shared secrets (using PSK-TLS RFC4279).

TLS can be used to secure other protocols that run above the transport layer such as HTTP [RFC2616]. Current TLS related specifications work for both TCP [RFC793] and UDP [RFC768].

This specification aims to provide a common implementation of the TLS related specifications that can be used by all the OMA Enablers including the Security Common Functions specifications [SEC_CF AD]. The intention is to create a secure and interoperable TLS implementation that can be re-used without the need to define the requirements for TLS implementations separately in each OMA Enabler specifications.

Developers of OMA Enablers who wish to use TLS related specifications as a transport layer security mechanism is recommended to use this specification to define the requirements for their TLS implementations. Alternatively, developers can refer to the common security functions specifications which in turn include this specification.

This specification also defines how TLS tunnelling [RFC2817] via HTTP proxies is profiled for OMA Enablers.

4.1 Version 1.0

OMA TLS Profile v1.0 can be used to secure OMA Enablers which operate over a reliable transport protocol such as TCP.

4.2 Version 1.1

OMA TLS Profile v1.1 is to extend TLS Profile v1.0 to make it work for OMA Enablers which operate over either a reliable transport protocol such as TCP or an unreliable transport protocol such as UDP. This profile also sets conformance requirements aligned to IETF thus simplifying interoperability. Legacy support and backward compatibility have been considered.

5. OMA TLS Profile

OMA TLS Profile is based on the TLS related specifications TLS1.0 [RFC2246], TLS1.1 [RFC4346], TLS1.2 [RFC5246], PSK-TLS [RFC4279], [RFC4785], [RFC5487], TLS Extensions [RFC4366], AES-TLS [RFC3268], DTLS [RFC4347] among others.

5.1 Supported versions

The following versions are supported by this profile as follows:

- TLS 1.1 [RFC4346] MUST be supported
- TLS 1.0 [RFC2246] SHOULD be supported in those cases when interworking with legacy OMA enablers supporting only TLS 1.0 is needed. The fallback mechanism to the TLS 1.0 protocol version is described in [RFC4346] and [RFC5246].
- TLS 1.2 [RFC5246] SHOULD be supported
- PSK-TLS [RFC4279] MAY be supported

All OMA TLS Profile compliant implementations MUST also conform to TLS related specifications.

This specification profiles a particular implementation of TLS 1.1 and other relevant specifications that can be used with TLS 1.1 such as PSK-TLS and DTLS. PSK-TLS implementations must conform to PSK-TLS [RFC4279] specifications. DTLS [RFC4347] implementations must conform to DTLS specification.

Normative text included in this section MUST be considered as additions to the existing baseline TLS and related specifications. All terminology used in this specification MUST be taken in the context of TLS 1.1 and related specifications.

5.2 Supported Cipher Suites for TLS

TLS compliant OMA enablers MUST support the mandatory cipher suite of the corresponding TLS specification. The following ciphersuite SHALL be additionally supported due to its widely deployed status in the market:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

OMA enablers that need *additional* cipher suites for application-specific purposes MAY require those in their specifications, based on the set of ciphersuites defined in [RFC5246]. Ciphersuites with RC4 SHOULD NOT be used.

Note that this set has been chosen because it contains ciphersuites with state-of-the art strength, and does not contain those ciphersuites from earlier TLS versions that have been deprecated or discouraged in later TLS versions.

Note that OMA enablers to be deployed in 3GPP networks have to consider the TLS conformance requirements defined in [TS 33.310].

5.3 Supported Cipher Suites for PSK-TLS

If PSK-TLS is supported then the following cipher suite in [RFC4279] below MUST be supported:

- TLS_PSK_WITH_AES_128_CBC_SHA

The pre-shared keys may be generated from the result of GBA procedures [OMA-TS-GBA_Profile], or UMTS AKA procedures [3GPP TS 33.102], or IMS AKA procedures [3GPP TS 33.203], or other proprietary solutions.

OMA enablers that need *additional* cipher suites for application-specific purposes MAY require those in their specifications, based on the set of ciphersuites defined in [RFC5246]. Ciphersuites with RC4 SHOULD NOT be used.

Note that this set has been chosen because it contains ciphersuites with state-of-the art strength, and does not contain those ciphersuites from earlier TLS versions that have been deprecated or discouraged in later TLS versions.

5.4 Session Resumption

The client and the server MUST support the session resumption as defined in TLS. The longer session life (e.g., 12 hours) SHOULD be used. The guidelines on the session resumption as documented in TLS SHOULD be respected.

5.5 Server Authentication

The client and server MUST support server authentication using TLS. The client MUST support processing of X.509 server certificates as detailed in "WAP Certificate and CRL Profile" [CertProf]. The client implementations MUST conform to the guidelines for server identity as documented in [RFC 2818] (Section 3.1).

Furthermore, the client SHOULD use the guidelines for handling X.509 server certificates including the unknown attributes and extensions as described in "WAP Certificate and CRL Profiles Specification" [CertProf].

The server SHOULD use the WAP profiled X.509 server certificate [CertProf], and MAY use the X.509 server certificate [RFC2459].

Please note that if PSK-TLS is supported, then mutual authentication between the client and the server can be achieved using shared keys.

5.6 Client Authentication

The server SHOULD support client authentication. If client authentication is supported, the server MUST support the client certificates in the form of the WAP profiled X.509 client certificate [CertProf] and the X.509 client certificate [RFC2459]. The server MUST also include the RSA certificate type (i.e., `rsa_sign`) in the certificate request [RFC4346] for client certificates, and support verification of the RSA client certificate and signature.

The client MAY support client authentication. If the client authentication is supported, the client MUST support use of the WAP profiled X.509 client certificate and SHOULD support use of the X.509 certificate [RFC2459]. The client MUST support RSA client certificate and signature. CA should issue the WAP profiled X.509 client certificates [CertProf].

Please note that if PSK-TLS is supported, then mutual authentication between the client and the server is achieved using shared keys if the shared key is only shared by the two end points.

5.7 TLS Tunneling

A HTTP proxy [RFC 2616] MAY be used between a client and a server using the TLS protocol. In order to maintain the end to end security at the transport layer while using a proxy, TLS tunneling MUST be used between the client and the origin server. The client MUST support TLS tunneling if it supports the HTTP proxy functionality. To establish a TLS tunnel, the client MUST use HTTP CONNECT method as defined in [RFC2817].

Furthermore, the client MUST only establish the tunnel over a raw TCP connection, not an "upgraded" connection per [RFC2817]. The HTTP proxy server should support the HTTP CONNECT method in the manner as defined in [RFC 2817].

It SHOULD be noted that a chain of HTTP proxy servers, including proxy servers that do not support HTTP CONNECT method, may be involved for a desired TLS tunnel, the client SHOULD not assume that a TLS tunnel can always be successfully established. The client MUST abort the attempt to establish a TLS tunnel if a non-successful response for an HTTP CONNECT request is received.

5.8 TLS Extensions for Wireless Networks

In wireless environment, these may be many constraints, including bandwidth limitations, computational power limitations, memory limitations, and battery life limitations. Wireless environments often suffer from such above constraints not commonly present in wired environments. Therefore, TLS may not work as effectively in wireless environment as in wireline environment. Fortunately, TLS extensions [RFC4366] are designed to enable TLS to operate as effectively as possible in wireless environments.

[RFC4366] provides both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms.

General extension mechanisms for the TLS handshake client hello and server hello messages:

- In extended client hello message, the new field "client_hello_extension_list" contains a list of extensions.
- In server hello message, the new field "server_hello_extension_list" contains a list of extensions.

Specific extensions in extended TLS handshake client and server hello messages SHOULD include:

- Server Name: It may be desirable for clients to provide this information to facilitate secure connections to servers that host multiple 'virtual' servers at a single underlying network address.
- Maximum Fragment Length Negotiation: It may be desirable for constrained clients to negotiate a smaller maximum fragment length due to memory limitations or bandwidth limitations.
- Client Certificate URLs: It may be desirable for constrained clients to send certificate URLs in place of certificates, so that they do not need to store their certificates and can therefore save memory.
- Trusted CA Indication: Constrained clients that, due to memory limitations, possess only a small number of CA root keys, may wish to indicate to servers which root keys they possess, in order to avoid repeated handshake failures.
- Truncated HMAC: It may be desirable in constrained environments to save bandwidth by truncating the output of the hash function to 80 bits when forming MAC tags.
- Certificate Status Request: Constrained clients may wish to use a certificate-status protocol such as [OCSP] to check the validity of server certificates, in order to avoid transmission of CRLs and therefore save bandwidth on constrained networks. This extension allows for such information to be sent in the TLS handshake, saving roundtrips and resources.

5.9 Profiling DTLS to Support OMA Enablers over UDP

The TLS protocol must run over a reliable transport channel such as TCP. DTLS is based on the TLS protocol and provides equivalent security guarantees to secure unreliable datagram traffic such as UDP.

DTLS implementations in this specification must conform to DTLS specification [RFC4347] in order to secure OMA Enablers over UDP. DTLS compliant OMA enablers MUST follow the corresponding cipher suite conformance requirements for TLS, see section 5.2

Appendix A. Change History (Informative)

A.1 Approved Version 1.0 History

Reference	Date	Description
OMA-TS-TLS-V1_0-20080902-A	02 Sep. 2008	Status changed to Approved by TP OMA-TP-2008-0321-INP_SEC_CF_V1_0_ERP_for_Final_Approval
OMA-TS-TLS_Profile-V1_1-20120731-A	31 Jul 2012	Status changed to Approved by TP Ref TP Doc# OMA-TP-2012-0291-INP_SEC_CF_V1_1_for_Final_Approval

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [SCRRULES].

B.1 SCR for TLS Client

Item	Function	Reference	Requirement
TLS-C-001-C	OMA TLS1.0 implementations conform to [RFC2246]	Section 5.1	For interworking with OMA enablers supporting only TLS 1.0, it is necessary to allow fallback to the TLS 1.0 protocol version as described in [RFC2246] and [RFC5246].
TLS-C-002-M	OMA TLS1.1 implementations conform to [RFC4346]	Section 5.1	
TLS-C-003-O	OMA DTLS implementations conform to [RFC4347]	Section 5.1 Section 5.9	
TLS-C-004-O	OMA PSK-TLS implementations conform to [RFC4279][RFC5487]	Section 5.1 Section 5.3	
TLS-C-005-M	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Section 5.1 Section 5.2	TLS-C-001-C
TLS-C-006-M	TLS_PSK_WITH_AES_128_CBC_SHA	Section 5.3	TLS-C-004-O
TLS-C-007-M	TLS_PSK_WITH_AES_128_CBC_SHA256	Section 5.3	TLS-C-004-O

B.2 SCR for TLS Server

Item	Function	Reference	Requirement
TLS-S-001-C	OMA TLS1.0 implementations conform to [RFC2246]]	Section 5.1	For interworking with OMA enablers supporting only TLS 1.0, it is necessary to allow fallback to the TLS 1.0 protocol version as described in [RFC2246] and [RFC5246].
TLS-S-002-M	OMA TLS1.1 implementations conform to [RFC4346]	Section 5.1	
TLS-S-003-O	OMA DTLS implementations conform to [RFC4347]	Section 5.1 Section 5.9	
TLS-S-004-O	OMA PSK-TLS implementations conform to [RFC4279] [RFC5487]	Section 5.1 Section 5.3	
TLS-S-005-M	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Section 5.1 Section 5.2	TLS-S-001-C
TLS-S-006-M	TLS_RSA_WITH_AES_128_CBC_SHA	Section 5.3	TLS-S-004-O

Item	Function	Reference	Requirement
TLS-S-007-M	TLS_PSK_WITH_AES_128_CBC_SHA256	Section 5.3	TLS-S-004-O