OMA IPsec Profile

Approved Version 1.1 – 31 Jul 2012

Open Mobile Alliance

OMA-TS-IPSec_Profile-V1_1-20120731-A

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at http://www.openmobilealliance.org/ipr.html. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR’S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

Contents

Figures

1. Scope

The set of IPsec protocols include two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP). The IPsec AH provides connectionless integrity, data origin authentication, and an optional anti-replay service. The IPsec ESP also provides connectionless integrity, data origin authentication, an anti-replay service as well as confidentiality. In order to make implementation more simply and to avoid interoperability problems in some implementations of IPsec in OMA Enablers, it's suggested profiling only IPsec ESP to secure OMA enablers.

This specification is to profile IPsec ESP related specifications [RFC 2401] [RFC 2406] [RFC 4301][RFC 4303][RFC 4305] to provide data origin authentication, an anti-replay service, data integrity and encryption for OMA enablers operating over the protocol IP, especially for those OMA enablers operating over the protocol UDP.

Note: the old RFCs related to IPsec (e.g., [RFC 2406][RFC 2401]) are not recommended for new implementations.

2. References

2.1 Normative References

[3GPP TS 33.203] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services", URL:http://www.3GPP.org/

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

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

[RFC2401] "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson. November 1998**,** obsoleted by RFC4301, URL:http://www.ietf.org/rfc/rfc2401.txt

[RFC2404] "The Use of HMAC-SHA-1-96 within ESP and AH", C. Madson, R. Glenn. November 1998, Obsoleted by RFC4305, URL:http://www.ietf.org/rfc/rfc2404.txt

[RFC2406] "IP Encapsulating Security Payload (ESP)", S. Kent, R. Atkinson. November 1998., Obsoleted by RFC4303, RFC4305, URL:http://www.ietf.org/rfc/rfc2406.txt

[RFC2409] "The Internet Key Exchange (IKE)", D. Harkins, D. Carrel. November 1998., obsoleted by RFC4306,URL:http://www.ietf.org/rfc/rfc2409.txt

[RFC2410] "The NULL Encryption Algorithm and Its Use With IPsec", R. Glenn, S. Kent. November 1998., URL:http://www.ietf.org/rfc/rfc2410.txt

[RFC2451] "The ESP CBC-Mode Cipher Algorithms", R. Pereira, R. Adams. November 1998., URL:http://www.ietf.org/rfc/rfc2451.txt

[RFC3566] "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", S. Frankel, H. Herbert. September 2003., URL:http://www.ietf.org/rfc/rfc3566.txt

[RFC3602] "The AES-CBC Cipher Algorithm and Its Use with IPsec", S. Frankel, R. Glenn, S. Kelly. September 2003., URL:http://www.ietf.org/rfc/rfc3602.txt

[RFC4301] "Security Architecture for the Internet Protocol", S. Kent, K. Seo. December 2005., URL:http://www.ietf.org/rfc/rfc4301.txt

[RFC4303] "IP Encapsulating Security Payload (ESP)", S. Kent. December 2005., URL:http://www.ietf.org/rfc/rfc4303.txt

[RFC4305] "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", D. Eastlake 3rd. December 2005., obsoleted by 4835, URL:http://www.ietf.org/rfc/rfc4305.txt

[RFC4306] "Internet Key Exchange (IKEv2) Protocol", C. Kaufman, Ed.. December 2005., URL:http://www.ietf.org/rfc/rfc4306.txt

[RFC4835] "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", V. Manral, April 2007, URL:http://www.ietf.org/rfc/rfc4835.txt

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, 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/

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

AES	Advanced Encryption Standard
AH	Authentication Header
AKA	Authentication and Key Agreement
CBC	Cipher Block Chaining
DES	Data Encryption Standard
ESP	Encapsulating Security Payload
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hyperlink Text Transfer Protocol
IKE	Internet Key Exchange
IPsec	IP Security
MAC	Message Authentication Code
MD5	Message Digest 5 (a message digest algorithm with output 128 bits)
OMA	Open Mobile Alliance
SA	Security Association
SHA-1	Secure Hash Algorithm (a message digest algorithm with output 160 bits)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

4. Introduction

IPsec offers security services such as authentication, data integrity and encryption for both the higher layer protocols (e.g., TCP, UDP and HTTP) and applications (e.g., web browser). This specification is to profile IPsec related specifications (e.g., IPsec ESP) [RFC 2406] [RFC 2401] to provide data original authentication, data integrity and encryption for OMA enablers operating over the protocol IP, especially for those OMA enablers operating over the protocol UDP.

4.1 Version 1.1

This specification is to profile IPsec related specifications to provide data original authentication, data integrity and encryption for OMA enablers operating over the protocol IP, especially for those OMA enablers operating over the protocol UDP.

5. OMA IPsec Profile

OMA IPsec Profile is based on IPsec related specifications (e.g., IPsec ESP) [RFC 2406][RFC 2401][RFC 4301][RFC 4303][RFC 4305]. All OMA IPsec Profile compliant implementations MUST also conform to IPsec related specifications. This specification profiles IPsec related specifications to provide data original authentication, data integrity and encryption for OMA enablers operating over the protocol IP, especially for those OMA enablers operating over the protocol UDP.

Note: the old RFCs related to IPsec (e.g., [RFC 2406][RFC 2401]) are not recommended for new implementations.

5.1 Profile of IPsec ESP

5.1.1 Confidentiality

The confidentiality protection for OMA enablers at the IP level SHALL be provided by profiling IPsec ESP either according to [RFC 4303][RFC 4305] or [RFC 2406], however [RFC 4303] [RFC 4305] support is recommended. If [RFC 4303] [RFC 4305] is not supported, [RFC 2406] shall be supported.

- The encryption key is the same for the two pairs of simultaneously established SAs. The encryption key can be derived from the key pre-configured or established as a result of AKA [3GPP TS 33.203] or IKE [RFC 2409][RFC 4306].

The encryption algorithms SHALL comply with the following rules.

- The encryption algorithm is NULL encryption algorithm as specified in [RFC 2410], or DES EDE3 CBC as specified in [RFC 2451] or AES CBC with 128 bit key as specified in [RFC 3602].
- The Client SHALL support one of above three encryption algorithms.
- The Server SHALL support above three encryption algorithms.

5.1.2 Integrity

The integrity protection for OMA enablers at the IP level SHALL be provided by profiling IPsec ESP either according to [RFC 4303] [RFC 4305] or [RFC 2406], however [RFC 4303] [RFC 4305] support is recommended. If [RFC 4303] [RFC 4305] is not supported, [RFC 2406] shall be supported.

- The integrity key is the same for the two pairs of simultaneously established SAs. The integrity key can be derived from the key pre-configured or established as a result of AKA [3GPP TS 33.203] or IKE [RFC 2409][RFC 4306].

If [RFC 4303] [RFC 4305] is supported, the integrity algorithms SHALL comply with the following rules.

- The integrity algorithm is NULL integrity algorithm as specified in [RFC 2410], HMAC-SHA1-96 as specified in [RFC 2404] or AES-XCBC-MAC-96 as specified in [RFC 3566].
- The Client SHALL support one of above three integrity algorithms.
- The Server SHALL support above three integrity algorithms.

If [RFC 4303] [RFC 4305] is not supported, [RFC 2406] shall be supported and the integrity algorithms SHALL comply with the following rules.

- The integrity algorithm is NULL integrity algorithms as specified in [RFC 2410], HMAC-MD5-96 as specified in [RFC 2403] or HMAC-SHA1-96 as specified in [RFC 2404].
- The Client SHALL support one of above two integrity algorithms.
- The Server SHALL support both above integrity algorithms.

Note 1: Known weaknesses of SHA-1 should not affect the use of SHA-1 with HMAC.

Note 2: Due to known security vulnerabilities, the use of MD5 is deprecated. Existing implementations MAY still use it, but it is recommended to use stronger methods such as HMAC-SHA1-96, AES-XCBC-MAC-96 instead

5.1.3 Flow of IPsec ESP SA set-up

The following Figure xx is an overview of the flow of IPsec ESP SA set-up.

Note: How to establish security associations before setting up IPsec ESP SA is out of scope. The key used to protect IPsec ESP SA set-up may be pre-configured or established as a result of AKA [3GPP TS 33.203] or IKE [RFC 2409][RFC 4306].

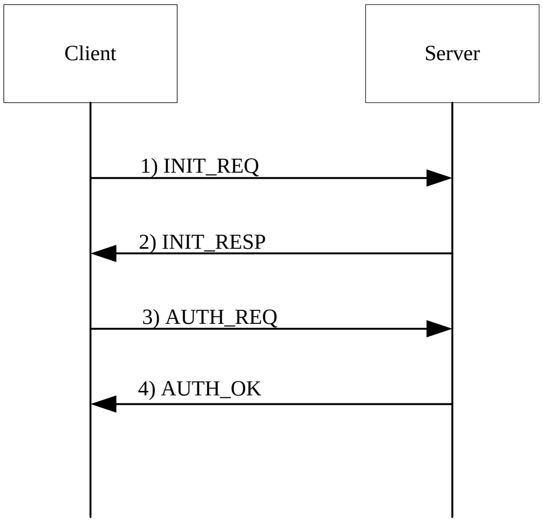

Figure 1: Flow of IPsec ESP SA set-up

Above Figure 1 is outlined as below:

1) The Client sends INIT_REQ message towards the Server to start the procedures of the security mode set-up.

2) After receiving message INIT_REQ, the Server temporarily stores the parameters received in this message together with the Client IP address from the source IP address of the IP packet header, the Client identifier.

   The Server shall define the SPIs such that they are unique and different from any SPIs as received from the Client.

   In order to determine the integrity and encryption algorithm the Server proceeds as follows: the Server has a list of integrity and encryption algorithms it supports, ordered by priority. The Server selects the first algorithm combination on its own list which is also supported by the Client. If the Client did not include any confidentiality algorithm in INIT_REQ message then the Server shall either select the NULL encryption algorithm or abort the procedure, according to its policy on confidentiality.

   The Server then establishes two new pairs of SAs in the local security association database.

   The Server calculates the Server Response from the key used to protect IPsec ESP SA set-up. It’s assumed the Server can get the key used to protect IPsec ESP SA set-up.

   The Server sends message INIT_RESP to the Client.

3) After receiving message INIT_RESP, the Client checks if the Server Response is correct, and determines the integrity and encryption algorithms as follows: the Client selects the first integrity and encryption algorithm combination on the list received from the Server in message INIT_RESP which is also supported by the Client. If the Server did not include any confidentiality algorithm in message INIT_RESP then the Client shall select the NULL encryption algorithm.

The Client then proceeds to establish two new pairs of SAs in the local SAD.

The Client generates the Client Response from the key used to protect IPsec ESP SA set-up. It's assumed the Client can get the key used to protect IPsec ESP SA set-up

The Client sends message AUTH_REQ to the Client.

4) After receiving message AUTH_REQ from the Client, the Server shall check if the Client Response is correct, and also checks whether the integrity and encryption algorithms list received in message AUTH_REQ is identical with the corresponding parameters sent in message INIT_RESP. It further checks whether other parameters (e.g., IP address, port number) received in message AUTH_REQ are identical with those received in message INIT_REQ. If these checks are not successful the registration procedure is aborted.

The Server finally sends message AUTH_OK to the Client.

After that, the Client can assume the successful completion of the security-mode setup. And the all following data message between the Client and the Server can be protected with integrity and confidentiality. The integrity key and encryption key are the same for the two pairs of simultaneously established SAs and can be derived from the key pre-configured or established as a result of AKA [3GPP TS 33.203] or IKE [RFC 2409][RFC 4306].

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-IPSec_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 IPsec Client

Item	Function	Reference	Requirement
IPsec-C-001-M	OMA IPsec implementations conform to [RFC4303][RFC4305] or [RFC2406]. If [RFC 4303][RFC 4305] is not supported, [RFC 2406] shall be supported.	Section 5.1 Section 5.1.1 Section 5.1.2	
IPsec-C-002-O	The Client SHALL support confidentiality.	Section 5.1.1	IPsec-C-005-O OR IPsec-C-006-O OR IPsec-C-007-O
IPsec-C-003-O	If OMA IPsec implementations conform to [RFC4303][RFC4305], the Client SHALL support integrity.	Section 5.1.2	IPsec-C-008-O OR IPsec-C-009-O OR IPsec-C-010-O
IPsec-C-004-O	If OMA IPsec implementations conform to [RFC2406], the Client SHALL support integrity.	Section 5.1.2	IPsec-C-008-O OR IPsec-C-009-O OR IPsec-C-011-O
IPsec-C-005-O	NULL encryption algorithm as specified in [RFC2410]	Section 5.1.1	
IPsec-C-006-O	Encryption algorithm AES-CBC with 128 bit key as specified in [RFC3602]	Section 5.1.1	
IPsec-C-007-O	Encryption algorithm DES-EDE3-CBC as specified in [RFC2451]	Section 5.1.1	
IPsec-C-008-O	NULL integrity algorithm as specified in [RFC2410]	Section 5.1.2	
IPsec-C-009-O	HMAC-SHA1-96 as specified in [RFC2404]	Section 5.1.2	
IPsec-C-010-O	AES-XCBC-MAC-96 as specified in [RFC3566]	Section 5.1.2	
IPsec-C-011-O	HMAC-MD5-96 as specified in [RFC2403]	Section 5.1.2	

B.2 SCR for IPsec Server

Item	Function	Reference	Requirement
IPsec-S-001-M	OMA IPsec implementations conform to [RFC4303][RFC4305] or [RFC2406]. If [RFC 4303][RFC 4305] is not supported, [RFC 2406] shall be supported.	Section 5.1 Section 5.1.1 Section 5.1.2	
IPsec-S-002-O	If OMA IPsec implementations conform to [RFC4303][RFC4305], the Client SHALL support confidentiality.	Section 5.1.1	IPsec-S-005-O AND IPsec-S-006-O AND IPsec-S-007-O
IPsec-S-003-O	If OMA IPsec implementations conform to [RFC4303][RFC4305], the Client SHALL support integrity.	Section 5.1.2	IPsec-S-008-O AND IPsec-S-009-O AND IPsec-S-010-O
IPsec-S-004-O	If OMA IPsec implementations conform to [RFC2406], the Client SHALL support integrity.	Section 5.1.2	IPsec-S-008-O AND IPsec-S-010-O AND IPsec-S-011-O
IPsec-S-005-O	NULL encryption algorithm as specified in [RFC2410]	Section 5.1.1	
IPsec-S-006-O	Encryption algorithm AES-CBC with 128 bit key as specified in [RFC3602]	Section 5.1.1	
IPsec-S-007-O	Encryption algorithm DES-EDE3-CBC as specified in [RFC2451]	Section 5.1.1	

Item	Function	Reference	Requirement
IPsec-S-008-O	NULL integrity algorithm as specified in [RFC2410]	Section 5.1.2	
IPsec-S-009-O	HMAC-SHA1-96 as specified in [RFC2404]	Section 5.1.2	
IPsec-S-010-O	AES-XCBC-MAC-96 as specified in [RFC3566]	Section 5.1.2	
IPsec-S-011-O	HMAC-MD5-96 as specified in [RFC2403]	Section 5.1.2	