Contents

1. SCOPE .............................................................................................................................................................................4

2. REFERENCES .................................................................................................................................................................5
   2.1 NORMATIVE REFERENCES ........................................................................................................................................5
   2.2 INFORMATIVE REFERENCES ..................................................................................................................................5

3. TERMINOLOGY AND CONVENTIONS ..........................................................................................................................6
   3.1 CONVENTIONS .........................................................................................................................................................6
   3.2 DEFINITIONS ...........................................................................................................................................................6
   3.3 ABBREVIATIONS ......................................................................................................................................................6

4. INTRODUCTION ..............................................................................................................................................................7
   4.1 VERSION 1.1 ..............................................................................................................................................................7

5. OMA IPSEC PROFILE ...................................................................................................................................................8
   5.1 PROFILE OF IPsec ESP .............................................................................................................................................8
      5.1.1 Confidentiality ................................................................................................................................................9
      5.1.2 Integrity ...........................................................................................................................................................8
      5.1.3 Flow of IPsec ESP SA set-up ...........................................................................................................................9

APPENDIX A. CHANGE HISTORY (INFORMATIVE) ........................................................................................................11
   A.1 APPROVED VERSION HISTORY ............................................................................................................................11
   A.2 DRAFT VERSION 1.1 HISTORY ..............................................................................................................................11

APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) .............................................................12
   B.1 SCR FOR IPSEC CLIENT .........................................................................................................................................12
   B.2 SCR FOR IPSEC SERVER .....................................................................................................................................12

Figures

Figure 1: Flow of IPsec ESP SA set-up ..............................................................................................................................9
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


2.2 Informative References

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULDN’T”, “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.

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

- 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 2404] 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].

![Flow of IPsec ESP SA set-up](image)

**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

A.1 Approved Version History

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>No prior version—or- No previous version within OMA</td>
</tr>
</tbody>
</table>

A.2 Draft Version 1.1 History

<table>
<thead>
<tr>
<th>Document Identifier</th>
<th>Date</th>
<th>Sections</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft Versions</td>
<td>25 Dec 2009</td>
<td>All</td>
<td>Incorporates input to committee: OMA-ARC-SEC-2009-0086R01-INP_Baseline_of_SEC_CF1.1_TS_Development</td>
</tr>
<tr>
<td>OMA-TS-IPSec_Profile-V1_1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>15 Apr 2010</td>
<td>4</td>
<td>OMA-ARC-SEC-2010-0032R01-CR_SEC_CF1.1_TS_IPSec_Profile_Introduction</td>
</tr>
<tr>
<td></td>
<td>30 Apr 2010</td>
<td>1, 5</td>
<td>OMA-ARC-SEC-2010-0033R02-CR_SEC_CF1.1_TS_IPSec_Profile_IPSEC_ESP OMA-ARC-SEC-2010-0037R02-CR_SEC_CF1.1_TS_IPSec_Profile_Scope</td>
</tr>
<tr>
<td></td>
<td>01 Sep 2010</td>
<td>All</td>
<td>OMA-ARC-SEC-2010-0073-CR_Minor_Fixes_IPsec_Profile OMA-ARC-SEC-2010-0077-CR_IPsec_Profile_Abbreviations</td>
</tr>
<tr>
<td></td>
<td>03 Oct 2010</td>
<td>All</td>
<td>OMA-ARC-SEC-2010-0095R01-CR_IPsec_Profile_ESP_</td>
</tr>
<tr>
<td></td>
<td>04 Oct 2010</td>
<td>All</td>
<td>Editorial fixes: 2010 copyright Removed empty rows in tables Fixed History table Added Figures in Contents</td>
</tr>
<tr>
<td></td>
<td>29 Oct 2010</td>
<td>5.1.3</td>
<td>Incorporates the input: OMA-ARC-SEC-2010-0108-CR_CONR_SEC_CF1.1_TS_IPSec_Profile_E001</td>
</tr>
<tr>
<td>Candidate Version</td>
<td>30 Nov 2010</td>
<td>All</td>
<td>Status changed by TP: OMA-TP-2010-0472-INP_SEC_CF_V1_1_ERP_for_Candidate_Approval</td>
</tr>
</tbody>
</table>
### Appendix B. Static Conformance Requirements (Normative)

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

#### B.1 SCR for IPsec Client

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

#### B.2 SCR for IPsec Server

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