Diameter IKEv2: Support for Interaction between IKEv2 Server and Diameter Server
draft-cakulev-ikev2-psk-diameter-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 3, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

Internet Key Exchange is a component of IPsec used for performing mutual authentication as well as establishing and maintaining security associations (SAs) between two parties such as a user and a network entity. Internet Key Exchange v2 (IKEv2) protocol allows several different mechanisms for authenticating a user, namely the Extensible Authentication Protocol, certificates, and pre-shared secrets. To authenticate and/or authorize the user, the network element such as the Access Gateway may need to dynamically bootstrap a security association based on interaction with the Diameter server. This document specifies the interaction between the Access Gateway and Diameter server for the IKEv2 based on pre-shared secrets.

Table of Contents

1. Introduction ................................................. 4
2. Requirements notation ....................................... 5
3. Application Identifier ...................................... 6
4. Protocol Description ....................................... 7
  4.1. Support for IKEv2 and Pre-Shared Secrets .......... 7
  4.2. Session Management ..................................... 7
    4.2.1. Session-Termination-Request/Answer ............. 8
    4.2.2. AbortSession-Request/Answer .................... 8
5. Command Codes for Diameter IKEv2 with PSK ............... 9
  5.1. IKEv2-PSK-Request (IKEPSKR) Command .............. 9
  5.2. IKEv2-PSK-Answer (IKEPSKA) Command ............. 10
6. Attribute Value Pair Definitions .......................... 11
  6.1. The Master-Security-Association ................... 11
    6.1.1. Key .......................................... 11
    6.1.2. MSA-Lifetime .................................. 11
    6.1.3. MSA-SPI ....................................... 11
  6.2. Session-Key-Nonces ................................... 11
    6.2.1. Ni ........................................... 12
    6.2.2. Nr .......................................... 12
7. AVP Occurrence Tables .................................... 13
8. AVP Flag Rules ........................................... 14
9. IANA Considerations ....................................... 15
  9.1. Command Codes ........................................ 15
  9.2. AVP Codes .......................................... 15
  9.3. Application Identifier ............................... 15
10. Security Considerations .................................. 16
11. References ................................................ 18
  11.1. Normative References ............................... 18
  11.2. Informative References ............................. 18
Authors’ Addresses ........................................... 19
1. Introduction

[RFC4306] defines IKEv2 as a protocol that performs mutual authentication between two parties and establishes a security association (SA) that includes shared secret information that can be used to efficiently establish SAs for Encapsulating Security Payload (ESP) [RFC4303] and/or Authentication Header (AH) [RFC4302], and a set of cryptographic algorithms to be used by the SAs to protect the traffic that they carry. IKEv2 protocol allows several different mechanisms for authenticating a IKEv2 Peer to be used, such as the Extensible Authentication Protocol, certificates, and pre-shared secrets.

From a service provider perspective it is important to ensure that a user is authorized to use the services. Therefore, the IKEv2 Server must verify that the IKEv2 Peer is authorized for the requested services possibly with the assistance of the operator’s Diameter servers. Moreover, this document does not assume that the IKEv2 Server has the pre-shared secrets (PSK) with the IKEv2 Peer. Instead, it allows for PSK to be derived for a specific IKEv2 session and exchanged between IKEv2 Server and HAAA. This is accomplished through the use of a new Diameter application specifically designed for performing IKEv2 authorization decisions. This document specifies the Diameter support for shared secrets (PSK) based IKEv2.
2. Requirements notation

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].
3. Application Identifier

This specification defines a new Diameter application and its respective Application Identifier:

Diameter IKE PSK (IKEPSK) TBD by IANA

The IKEPSK Application Identifier is used when the IKEv2 Peer is to be authenticated and authorized using IKEv2 with PSK-based authentication.
4. Protocol Description

4.1. Support for IKEv2 and Pre-Shared Secrets

When IKEv2 is used with PSK-based initiator authentication, the Diameter commands IKEv2-PSK-Request and IKEv2-PSK-Answer defined in this document are used to authorize the IKEv2 Peer for the services. Upon receiving the IKE_AUTH message from the IKEv2 Peer, the IKEv2 Server uses the information received in IDi to determine if it has the PSK for this IKEv2 Peer. If there is no PSK found associated with this IKEv2 Peer, the IKEv2 Server MUST send an Authorize-Only (Auth-Request-Type set to "Authorize-Only") Diameter IKEv2-PSK message with the IKEv2 Peer's IDi payload to the HAAA to obtain the PSK. The IDi payload extracted from the IKE_AUTH message has to contain an identity that is meaningful for the Diameter infrastructure, such as a Network Access Identifier (NAI), since it is used by the IKEv2 Server to populate the User-Name AVP in the Diameter message. The IKEv2 Server also includes in the Session-Key-Nonces AVP of the same Diameter message the initiator and responder nonces (Ni and Nr) exchanged during initial IKEv2 exchange.

This message is routed to the IKEv2 Peer’s HAAA. Upon receiving Diameter IKEv2-PSK message from the IKEv2 Server, the HAAA shall use the User-Name AVP to retrieve the associated keying material. If HAAA also receives Session-Key-Nonces AVP with Ni and Nr nonces included, the HAAA may use the nonces to generate the PSK. It is outside of scope of this document how the HAAA obtains or generates the PSK. For example, if the HAAA previously performed EAP based access authentication and authorization of the IKEv2 Peer, it can use the available EMSK to generate the PSK [RFC5295]. The HAAA returns the PSK to the IKEv2 Server using the Master-Security-Association AVP.

Once the IKEv2 Server receives the PSK from the HAAA, the IKEv2 Server verifies the IKE_AUTH message received from the IKEv2 Peer. If the verification of AUTH is successful, the IKEv2 Server sends the IKE message back to the IKEv2 Peer.

4.2. Session Management

The HAAA may maintain state or may be stateless. This is indicated by presence or absence of the Auth-Session-State AVP. The IKEv2 Server MUST support the Authorization Session State Machine defined in [RFC3588].

This specification makes an assumption that each IKE_SA created between the IKEv2 Peer and the IKEv2 Server as a result of a successful IKEv2 negotiation exchange together with CHILD_SAs set up
through that particular IKE_SA correspond to one currently active PSK and one active Diameter session.

4.2.1. Session-Termination-Request/Answer

In the case where session tracking is being used, when the IKEv2 Server terminates the SA it SHALL send a Session-Termination-Request (STR) message [RFC3588] to inform the HAAA that the authorized session has been terminated.

The Session-Termination-Answer (STA) message [RFC3588] is sent by the HAAA to acknowledge the notification that the session has been terminated.

4.2.2. AbortSession-Request/Answer

The Abort-Session-Request (ASR) message [RFC3588] is sent by the HAAA to the IKEv2 Server to terminate the authorized session. When the IKEv2 Server receives the ASR message, it MUST delete the corresponding IKE_SA and all CHILD_SAs set up through it.

The Abort-Session-Answer (ASA) message [RFC3588] is sent by the IKEv2 Server in response to an ASR message.
5. Command Codes for Diameter IKEv2 with PSK

This section defines new Command-Code values that MUST be supported by all Diameter implementations conforming to this specification.

<table>
<thead>
<tr>
<th>Command-Name</th>
<th>Abbrev.</th>
<th>Code</th>
<th>Reference</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKEv2-PSK-Request</td>
<td>IKEPSKR</td>
<td>TBD</td>
<td>Section 5.1</td>
<td>IKEPSK</td>
</tr>
<tr>
<td>IKEv2-PSK-Answer</td>
<td>IKEPSKA</td>
<td>TBD</td>
<td>Section 5.2</td>
<td>IKEPSK</td>
</tr>
</tbody>
</table>

Figure 1: Command Codes

5.1. IKEv2-PSK-Request (IKEPSKR) Command

The IKEv2-PSK-Request message, indicated with the Command-Code set to TBD and the ‘R’ bit set in the Command Flags field is sent from the IKEv2 Server to the HAAA to initiate IKEv2 with PSK authorization. In this case, the Application-ID field of the Diameter Header MUST be set to the Diameter IKE PSK Application ID (value of TBD).

Message format

```plaintext
<IKEv2-PSK-Request> ::= < Diameter Header: TBD, REQ, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
[ Destination-Host ]
[ NAS-Identifier ]
[ NAS-IP-Address ]
[ NAS-IPv6-Address ]
[ NAS-Port ]
{ Origin-State-Id }
{ User-Name }
{ Auth-Session-State }
{ Session-Key-Nonces }
* [ Proxy-Info ]
* [ Route-Record ]
...
* [ AVP ]
```

IKEv2-PSK-Request message MUST include a Session-Key-Nonces AVP containing Ni and Nr nonces exchanged during initial IKEv2 exchange.
5.2. IKEv2-PSK-Answer (IKEPSKA) Command

The IKEv2-PSK-Answer (IKEPSKA) message, indicated by the Command-Code field set to TBD and the 'R' bit cleared in the Command Flags field, is sent by the HAAA to the IKEv2 Server in response to the IKEPSKR command. In this case, the Application-ID field of the Diameter Header MUST be set to the Diameter Mobile IPv6 IKE PSK Application ID (value of TDB).

Message format

```plaintext
<IKEv2-PSK-Answer> ::= < Diameter Header: TBD, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Auth-Request-Type }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
{ User-Name }
[ Master-Security-Association ]
{ Error-Message }
{ Error-Reporting-Host }
* [ Failed-AVP ]
{ Origin-State-Id }
* [ Redirect-Host ]
{ Redirect-Host-Usage }
{ Redirect-Max-Cache-Time }
* [ Proxy-Info ]
* [ Route-Record ]
...
* [ AVP ]
```

If the authorization procedure was successful then the IKEv2-PSK-Answer message shall include the Master-Security-Association.
6. Attribute Value Pair Definitions

This section defines new AVPs for the IKEv2 with PSK.

6.1. The Master-Security-Association

The Master-Security-Association AVP (AVP Code TBD) is of type Grouped and contains the session related information for use with the PSK based IKEv2.

Master-Security-Association ::= < AVP Header: TBD >
   ( Key )
   [ MSA-Lifetime ]
   [ MSA-SPI ]
   * [ AVP ]

6.1.1. Key

Key AVP (AVP Code TBD) is of type OctetString and contains the PSK. The PSK is placed in this AVP most significant byte first. Exactly how the PSK is derived is beyond the scope of this document.

6.1.2. MSA-Lifetime

MSA-Lifetime AVP (AVP Code TBD) is of type Unsigned32 and represents the period of time (in seconds) for which the PSK is valid. The associated PSK shall not be used if the lifetime has expired.

6.1.3. MSA-SPI

MSA-SPI AVP (AVP Code TBD) is of type Unsigned32 and contains an SPI associated with the PSK.

6.2. Session-Key-Nonces

The IKEv2-Nonces AVP (Code TBD) is of type Grouped and contains the nonces exchanged between the IKEv2 Peer and the IKEv2 Server during IKEv2 initial exchange. The nonces are used for PSK generation.

IKEv2-Nonces ::= < AVP Header: TBD >
   {Ni}
   {Nr}
   *[AVP]
6.2.1. Ni

The Ni AVP (AVP Code TBD) is of type Unsigned32 and contains the IKEv2 initiator nonce.

6.2.2. Nr

The Nr AVP (AVP Code TBD) is of type Unsigned32 and contains the IKEv2 responder nonce.
7. AVP Occurrence Tables

The following tables present the AVPs defined in this document and their occurrences in Diameter messages. Note that AVPs that can only be present within a Grouped AVP are not represented in this table.

The table uses the following symbols:

0:

The AVP MUST NOT be present in the message.

0+:

Zero or more instances of the AVP MAY be present in the message.

0-1:

Zero or one instance of the AVP MAY be present in the message.

1:

One instance of the AVP MUST be present in the message.

+-------------------+
|   Command-Code    |
|---------+---------|
+-------------------+
|   AVP Name       |
|---------+---------|
|--- IKEPSKR | IKEPSKA |
+---------+---------+
| Master-Security-Assocation |   0     |   0-1   |
| Sessio-Key-Nonces         | 0-1     |     0   |
+---------------------------+
8. AVP Flag Rules

The following table describes the Diameter AVPs, their AVP Code values, types, possible flag values, and whether the AVP MAY be encrypted. The Diameter base [RFC3588] specifies the AVP Flag rules for AVPs in Section 4.5.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Defined Code in 5.1</th>
<th>Value Type</th>
<th>SHOULD</th>
<th>MUST</th>
<th>MAY</th>
<th>ENCR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master-Security-Association</td>
<td>TBD</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Key</td>
<td>TBD 5.1.1</td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>MSA-Lifetime</td>
<td>TBD 5.1.2</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSA-SPI</td>
<td>TBD 5.1.3</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Session-Key-Nonces</td>
<td>TBD 5.2</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Ni</td>
<td>TBD 5.2.1</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Nr</td>
<td>TBD 5.2.2</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>Y</td>
</tr>
</tbody>
</table>

AVP Flag Rules Table
9. IANA Considerations

This section contains the namespaces that have either been created in this specification or had their values assigned to existing namespaces managed by IANA.

9.1. Command Codes

IANA is requested to allocate a command code value for the IKEv2-PSK-Request message (IKEPSKR) and for the IKEv2-PSK-Answer message (IKEPSKA) from the Command Code namespace defined in [RFC3588]. See Section 4 for the assignment of the namespace in this specification.

9.2. AVP Codes

This specification requires IANA to register the following new AVPs from the AVP Code namespace defined in [RFC3588].

- Master-Security-Association
- Key
- MSA-Lifetime
- MSA-SPI
- Session-Key-Nonces
- Ni
- Nr

The AVPs are defined in Section 6.

9.3. Application Identifier

This specification requires IANA to allocate one new value "Diameter IKE PSK" from the Application Identifier namespace defined in [RFC3588].

<table>
<thead>
<tr>
<th>Application Identifier</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter IKE PSK (IKEPSK)</td>
<td>TBD</td>
</tr>
</tbody>
</table>
10. Security Considerations

Any authentication and key agreement protocol with pre-shared keys between an end-user client and AAA infrastructure relies on the assumption that the client and network can mutually authenticate each other. In context of, for example, 3GPP networks, the HAAA sharing a PSK with the IKEv2 Server is similar to the HSS sharing an authentication vector with the SGSN or MME in AKA based mutual authentication protocols.

The basic security assumptions in sharing the PSK are based on the following standard considerations.

- The security tunnel between the HAAA and the IKEv2 Server is typically a mutually authenticated tunnel, with ciphering and integrity protection for every packet. The existence of such tunnels ensures that on-going trust and security are enforced, and in particular the HAAA can guarantee that the IKEv2 Server is not misbehaving.

- The protocol under discussion relies on the fact an IKEv2 Peer has successfully authenticated with the system and has, for example, an EMSK stored in the HAAA. The fact that the PSK is derived from the EMSK proves to the HAAA of the existence of an authenticated and active IKEv2 Peer.

- If the HAAA is to treat an IKEv2 Server as adversarial, then we claim that under no circumstances can an IKEv2 Peer communicate with that IKEv2 Server. Recall that any authentication and key agreement protocol with pre-shared keys between an end-user client and AAA infrastructure relies on the assumption that the client and network can mutually authenticate each other, and furthermore the client trusts the network elements that the AAA communicates with and delegates post authentication security parameters to be legitimate. If the HAAA is to treat the IKEv2 Server as adversarial, then the trust assumption is no longer valid. This in turn implies that the IKEv2 Peer is no longer guaranteed that the network elements it is communicating with are trusted.

Hence the following two assumptions are critical to ensure secure communications:

- The HAAA server and the IKEv2 Server share a trust relationship; for instance, may be owned and managed by the same network operator.
Moreover, transfer of keys between the HAAA and the IKEv2 Server rely on an existing security association between the above network elements.

In addition, the security considerations of the Diameter Base protocol [RFC3588] are applicable to this document.
11. References

11.1. Normative References


11.2. Informative References


Authors’ Addresses

Violeta Cakulev
Alcatel Lucent
600 Mountain Ave.
3D-517
Murray Hill, NJ 07974
US

Phone: +1 908 582 3207
Email: cakulev@alcatel-lucent.com

Avi Lior
Bridgewater Systems
303 Terry Fox Drive
Otawa, Ontario K2K 3J1
Canada

Phone: +1 613-591-6655
Email: avi@bridgewatersystems.com