Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 13, 2012

V. Cakulev
Alcatel Lucent
A. Lior
Bridgewater Systems
S. Mizikovsky
Alcatel Lucent

August 12, 2011

Diameter IKEv2 PSK: Pre-Shared Key-based Support for IKEv2 Server to Diameter Server Interaction

draft-ietf-dime-ikev2-psk-diameter-09.txt

Abstract

The Internet Key Exchange protocol version 2 (IKEv2) is a component of the IPsec architecture and is used to perform mutual authentication as well as to establish and to maintain IPsec security associations (SAs) between the respective parties. IKEv2 supports several different authentication mechanisms, such as the Extensible Authentication Protocol (EAP), certificates, and pre-shared keys.

Diameter interworking for Mobile IPv6 between the Home Agent, as a Diameter client, and the Diameter server has been specified. However, that specification focused on the usage of EAP and did not include support for pre-shared key based authentication available with IKEv2. This document specifies the IKEv2 Server to the Diameter server communication when the IKEv2 Peer authenticates using the Internet Key Exchange v2 with Pre-Shared Key.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on February 13, 2012.

Copyright Notice

Table of Contents

1. Introduction 3
2. Requirements notation 5
2.1. Abbreviations 5
3. Application Identifier 6
4. Protocol Description 7
4.1. Support for IKEv2 and Pre-Shared Keys 7
4.2. Session Management 8
4.2.1. Session-Termination-Request/Answer 8
4.2.2. Abort-Session-Request/Answer 9
5. Command Codes for Diameter IKEv2 with PSK 10
5.1. IKEv2-PSK-Request (IKEPSKR) Command 10
5.2. IKEv2-PSK-Answer (IKEPSKA) Command 11
6. Attribute Value Pair Definitions 13
6.1. IKEv2-Nonces 13
6.1.1. Ni 13
6.1.2. Nr 13
6.2. Responder-Identity 13
7. AVP Occurrence Tables 14
8. AVP Flag Rules 15
9. IANA Considerations 16
9.1. Command Codes 16
9.2. AVP Codes 16
9.3. AVP Values 16
9.4. Application Identifier 16
10. Security Considerations 17
11. References 18
11.1. Normative References 18
11.2. Informative References 18
Authors' Addresses 20

1. Introduction

The Internet Key Exchange version 2 (IKEv2) protocol [RFC5996] is used to mutually authenticate two parities and to establish a security association (SA) that can be used to efficiently secure the communication between the IKEv2 Peer and Server, for example, using Encapsulating Security Payload (ESP) [RFC4303] and/or Authentication Header (AH) [RFC4302]. The IKEv2 protocol allows several different mechanisms for authenticating a IKEv2 Peer to be used, such as the Extensible Authentication Protocol, certificates, and pre-shared key.

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. [RFC5778] defines the home agent as a Diameter client to the Diameter server communication when the mobile node authenticates using the IKEv2 protocol with the Extensible Authentication Protocol (EAP) [RFC3748] or using the Mobile IPv6 Authentication Protocol [RFC4285]. This document specifies the IKEv2 Server to the Diameter server communication when the IKEv2 Peer authenticates using the Internet Key Exchange v2 with Pre-Shared Key.

Figure 1 depicts the reference architecture for this document.

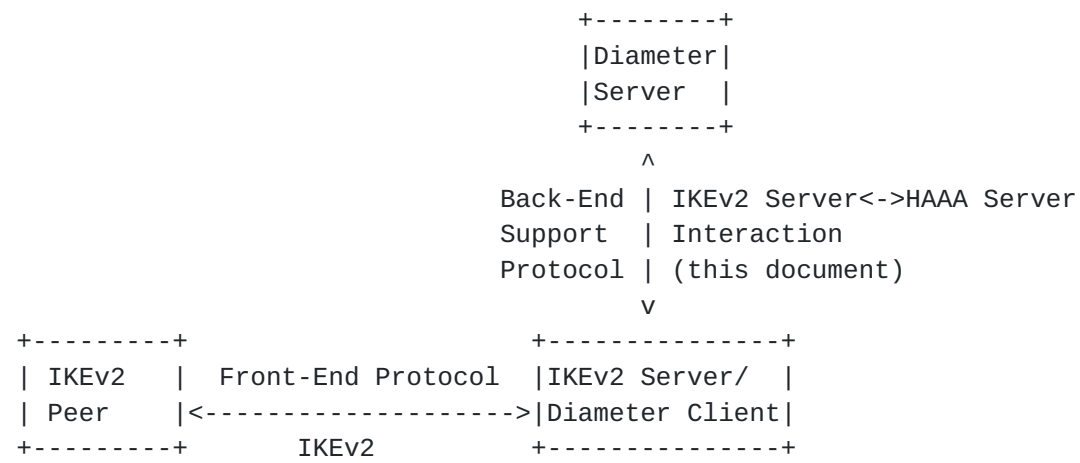

Figure 1: Architecture Overview

An example use case for this architecture is Mobile IPv6 deployment in which the Mobile IPv6 signaling between the Mobile Node and the Home Agent is protected using IPsec. The Mobile node acts as the

IKEv2 Peer and the Home Agent acts as an IKEv2 server. In this use case Internet Key Exchange v2 (IKEv2) with pre-shared key based initiator authentication is used for the setup of the IPsec SAs. The HA obtains the pre-shared key using the Diameter application specified herein to obtain the pre-shared key.

This document does not assume that the IKEv2 Server has the pre-shared key (PSK) with the IKEv2 Peer. Instead, it allows for the PSK to be obtained for a specific IKEv2 session and exchanged between IKEv2 Server and the Home Authentication, Authorization and Accounting (HAAA) server. The protocol provides IKEv2 attributes to allow the HAAA to compute a PSK specific key for the session if desired (see Section 10). This is accomplished through the use of a new Diameter application specifically designed for performing IKEv2 authorization decisions. This document focuses on the IKEv2 server, as a Diameter client, communicating to the Diameter server and specifies the Diameter application needed for this communication. It is left to protocols leveraging this Diameter application to specify PSK derivation. For example see [X.S0047] and [X.S0058]. This document specifies the default procedure for derivation of the PSK used in IKEv2 authentication when protocols leveraging this Diameter application do not specify their own derivation procedure. Selection of either default or other PSK derivation procedure is left to agreement between the HAAA server and the IKEv2 Peer, and is outside the scope of this document.

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].

2.1. Abbreviations

AH	Authentication Header
AVP	Attribute Value Pair
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
ESP	Home Authentication, Authorization and Accounting
IKEv2	Internet Key Exchange version 2
NAI	Network Access Identifier
PSK	Pre-Shared Key
SA	Security Association
SPI	Security Parameter Index

3. Application Identifier

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

Diameter IKE PSK (IKEPSK) TBD1 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 Keys

When IKEv2 is used with PSK-based initiator authentication, the Diameter commands IKEv2-PSK-Request/Answer defined in this document are used between IKEv2 server and a Home AAA server (HAAA) 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 [RFC5996] to identify the IKEv2 Peer and the SPI if available to determine the correct 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 and SPI if available to the HAAA to obtain the PSK. The IDi payload extracted from the IKE_AUTH message contains an identity that is meaningful for the Diameter infrastructure, such as a Network Access Identifier (NAI), and SHALL be used by the IKEv2 Server to populate the User-Name AVP in the Diameter message. The IKEv2 Server SHALL also include in the same Diameter message the IKEv2-Nonces AVP with the initiator and responder nonces (Ni and Nr) exchanged during initial IKEv2 exchange. Finally, if IDr payload was included in IKE_AUTH message received from the IKEv2 Peer, the IKEv2 Server SHALL also include in this same message the Responder-Identity AVP containing the received IDr.

The IKEv2 Server sends the IKEv2-PSK-Request message to the IKEv2 Peer's HAAA. The Diameter message is routed to the correct HAAA as per [RFC3588].

Upon receiving Diameter IKEv2-PSK-Request message from the IKEv2 Server, the HAAA SHALL use the User-Name AVP to retrieve the associated keying material. When the default PSK generation procedure specified in this document is used, the PSK derivation follows the methodology similar to that specified in Section 3.1 of [RFC5295], specifically:

```
PSK = KDF(Root Key Material, key label | "\0" | Ni | Nr | IDi | length)
```

Where:

- KDF is the default key derivation function based on HMAC-SHA-256 as specified in Section 3.1.2 of [RFC5295].
- Root Key Material is the key available to the protocol leveraging this Diameter application, e.g., the long term shared secret that would be provisioned to be used for IKEV2, or the Extended Master

Session Key (EMSK) as the result of prior EAP authentication etc. Selection of this value is left up to the protocol leveraging this Diameter application.

- Key label is set to 'psk4ikev2@ietf.org'.
- | denotes concatenation
- "\0" is a NULL octet (0x00 in hex)
- length is a 2-octet unsigned integer in network byte order

When applications using this protocol define their own PSK generation algorithm it is strongly RECOMMENDED that the nonces Ni and Nr are used in the computation. It is also RECOMMENDED that IDi be used. IDr SHOULD NOT be used in the PSK generation algorithm. Applications that want to use IDr in the computation should take into consideration that the IDr asserted by the IKEv2 peer may not be the same as the IDr returned by the IKEv2 responder. This mismatch will result in different PSKs being generated. The HAAA returns the PSK to the IKEv2 Server using the Key AVP as specified in [I-D.ietf-dime-local-keytran].

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

4.2.1. Session-Termination-Request/Answer

In the case where HAAA is maintaining session state, 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. Abort-Session-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.

Command-Name	Abbrev.	Code	Reference	Application
IKEv2-PSK-Request	IKEPSKR	TBD2	Section 5.1	IKEPSK
IKEv2-PSK-Answer	IKEPSKA	TBD2	Section 5.2	IKEPSK

Table 1: Command Codes

5.1. IKEv2-PSK-Request (IKEPSKR) Command

The IKEv2-PSK-Request message, indicated with the Command-Code set to TBD2 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 TDB1).

Message format

```
<IKEv2-PSK-Request> ::= < Diameter Header: TBD2, 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 }
                        [ Key-SPI ]
                        [ Responder-Identity ]
                        [ Auth-Session-State ]
                        { IKEv2-Nonces }
                      * [ Proxy-Info ]
                      * [ Route-Record ]
                        ...
                      * [ AVP ]
```

The IKEv2-PSK-Request message MUST include a IKEv2-Nonces AVP containing the Ni and Nr nonces exchanged during initial IKEv2 exchange. The IKEv2-PSK-Request message MAY contain a Key-SPI AVP (Key-SPI AVP is specified in [I-D.ietf-dime-local-keytran]). If included, it contains the Security Parameter Index (SPI) that HAAA SHALL use to identify the appropriate PSK. Responder-Identity AVP SHALL be included in the IKEv2-PSK-Request message, if IDr payload was included in the IKE_AUTH message received from the IKEv2 Peer. If included, Responder-Identity AVP contains the received IDr.

5.2. IKEv2-PSK-Answer (IKEPSKA) Command

The IKEv2-PSK-Answer (IKEPSKA) message, indicated by the Command-Code field set to TBD2 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 IKE PSK Application ID (value of TDB1).

Message format

```
<IKEv2-PSK-Answer> ::= < Diameter Header: TBD2, PXY >
                       < Session-Id >
                       { Auth-Application-Id }
                       { Auth-Request-Type }
                       { Result-Code }
                       { Origin-Host }
                       { Origin-Realm }
                       [ User-Name ]
                       [ Key ]
                       [ Responder-Identity ]
                       [ Auth-Session-State ]
                       [ 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 is successful then the IKEv2-PSK-Answer message SHALL include the Key AVP as specified in [I-D.ietf-dime-local-keytran]. The value of the Key-Type AVP SHALL

be set to IKEv2-PSK (TBD3). The Keying-Material AVP SHALL contain the PSK. If Key-SPI AVP is received in IKEv2-PSK-Request, Key-SPI AVP SHALL be included in Key AVP. The Key-Lifetime AVP may be included and if it is included then the associated key SHALL NOT be used by the receiver of the answer if the lifetime has expired. Finally, Responder-Identity AVP may be included. If the Responder-Identity AVP is present in both the request and the answer messages, it SHOULD be the same.

6. Attribute Value Pair Definitions

This section defines new AVPs for the IKEv2 with PSK.

6.1. IKEv2-Nonces

The IKEv2-Nonces AVP (Code TBD4) 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: TBD4>
                 {Ni}
                 {Nr}
                *[AVP]
```

6.1.1. Ni

The Ni AVP (AVP Code TBD5) is of type OctetString and contains the IKEv2 initiator nonce.

6.1.2. Nr

The Nr AVP (AVP Code TBD6) is of type OctetString and contains the IKEv2 responder nonce.

6.2. Responder-Identity

The Responder-Identity AVP (AVP Code TBD7) is of type UTF8String and contains the identity of the responder. In the scope of this specification, the value is extracted from the IKEv2 IDr payload, if available in the IKE_AUTH message sent by the IKEv2 Peer.

7. AVP Occurrence Tables

The following tables present the AVPs defined or used 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
Key	0	0-1
Key-SPI	0-1	0
IKEv2-Nonces	1	0
Responder-Identity	0-1	0-1

IKEPSKR and IKEPSKA Commands AVP Table

8. AVP Flag Rules

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

Attribute Name	AVP Code	Defined in	Value Type	AVP Flag rules: MUST	MAY	SHOULD NOT	MUST NOT
Key	TBD	Note 1	Grouped	M	P		V
Keying-Material	TBD	Note 1	OctetString	M	P		V
Key-Lifetime	TBD	Note 1	Integer64	M	P		V
Key-SPI	TBD	Note 1	Unsigned32	M	P		V
Key-Type	TBD	Note 1	Enumerated	M	P		V
IKEv2-Nonces	TBD4	6.1	Grouped	M	P		V
Ni	TBD5	6.1.1	OctetString	M	P		V
Nr	TBD6	6.1.2	OctetString	M	P		V
Responder-Identity	TBD7	6.2	UTF8String	M	P		V

AVP Flag Rules Table

Note 1: Key, Keying-Material, Key-Type, Key-SPI and Key-Lifetime AVPs are defined in [I-D.ietf-dime-local-keytran].

9. IANA Considerations

Upon publication of this memo as an RFC, IANA is requested to assign values as described in the following sections.

9.1. Command Codes

IANA is requested to allocate a command code value for the following new command from the Command Code namespace defined in [RFC3588].

Command Code	Value
IKEv2-PSK-Request/Answer	TBD2

9.2. AVP Codes

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

- IKEv2-Nonces - TBD4
- Ni - TBD5
- Nr - TBD6
- Responder-Identity - TBD7

The AVPs are defined in Section 6.

9.3. AVP Values

IANA is requested to create a new value for the Key-Type AVP. The new value TBD3 signifies that IKEv2 PSK is being sent.

9.4. Application Identifier

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

Application Identifier	Value
Diameter IKE PSK (IKEPSK)	TBD1

10. Security Considerations

The security considerations of the Diameter Base protocol [RFC3588] are applicable to this document (e.g., it is expected that Diameter protocol is used with security mechanism and that Diameter messages are secured).

In addition, the assumption is that the IKEv2 Server and the Diameter Server where the PSK is generated are in a trusted relationship. Hence, the assumption is that there is an appropriate security mechanism to protect the communication between these servers. For example the IKEv2 Server and the Diameter server would be deployed in the same secure network or would utilize transport layer security as specified in [RFC3588].

The Diameter messages between the IKEv2 Server and the HAAA may be transported via one or more AAA brokers or Diameter agents. In this case, the IKEv2 Server to the Diameter server AAA communication is hop-by-hop protected, hence relies on the security properties of the intermediating AAA inter- connection networks, AAA brokers, and Diameter agents. Furthermore, any agents that process IKEv2-PSK-Answer messages can see the contents of the Key AVP.

To mitigate the threat of exposing long lived PSK, this specification expects that the HAAA derives and returns the associated PSK to the IKEv2 Server. Given that PSK derivation is security-critical, for the PSK derivation this specification recommends the use of short lived secrets, possibly based on a previous network access authentication, if such secrets are available. To ensure key freshness and to limit the key scope, this specification strongly recommends the use of nonces included in IKEv2-PSK-Request. The specifics of key derivation depend on the security characteristics of the system that is leveraging this specification (for example see [X.S0047] and [X.S0058]), therefore this specification does not define how the Diameter server derives required keys for these systems. For systems and protocols that leverage this Diameter application but do not specify the key derivation procedure, this document specifies the default key derivation procedure that preserves expected security characteristics.

11. References

11.1. Normative References

[I-D.ietf-dime-local-keytran]
Zorn, G., Wu, W., and V. Cakulev, "Diameter Attribute-Value Pairs for Cryptographic Key Transport", draft-ietf-dime-local-keytran-10 (work in progress), May 2011.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", RFC 5295, August 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

11.2. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[RFC5778] Korhonen, J., Tschofenig, H., Bournelle, J., Giaretta, G., and M. Nakhjiri, "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", RFC 5778, February 2010.

[X.S0047] 3GPP2: X.S0047, "Mobile IPv6 Enhancements", February 2009.

[X.S0058] 3GPP2: X.S0058, "WiMAX-HRPD Interworking: Core Network Aspects", June 2010.

Authors' Addresses

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

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

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

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

Semyon Mizikovsky
Alcatel Lucent
600 Mountain Ave.
3C-506
Murray Hill, NJ 07974
US

Phone: +1 908 582 0729
Email: Simon.Mizikovsky@alcatel-lucent.com