Internet Engineering Task Force (IETF)
Request for Comments: 6738
Category: Standards Track
ISSN: 2070-1721

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

October 2012

Diameter IKEv2 SK: Using Shared Keys to Support Interaction between IKEv2 Servers and Diameter Servers

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 Shared Key (SK).

Diameter interworking for Mobile IPv6 between the Home Agent (HA), 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 SK-based authentication available with IKEv2. This document specifies the IKEv2-server-to-Diameter-server communication when the IKEv2 peer authenticates using IKEv2 with SK.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6738.

Table of Contents

1. Introduction

The Internet Key Exchange Protocol version 2 (IKEv2) [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 an IKEv2 peer to be used, such as the Extensible Authentication Protocol (EAP), certificates, and SK.

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-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-Diameter-server communication when the IKEv2 peer authenticates using IKEv2 with SK.

Figure 1 depicts the reference architecture for this document.

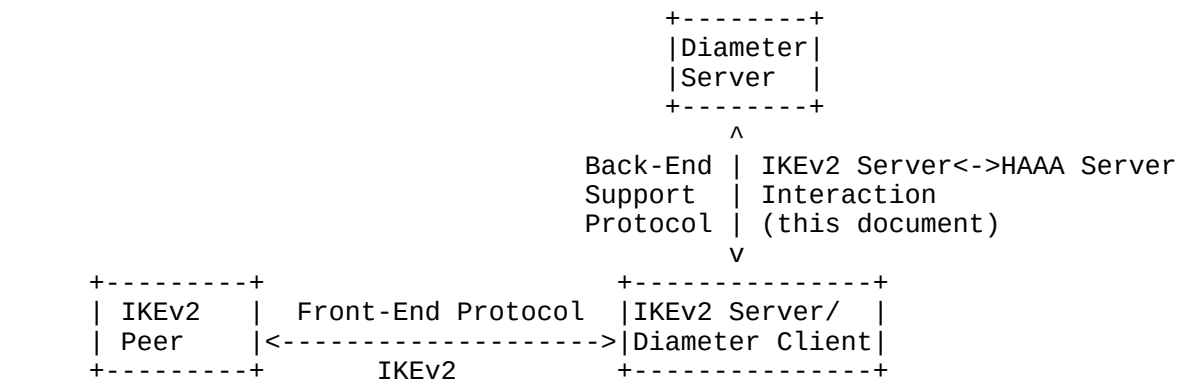

Figure 1: Architecture Overview

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, IKEv2 with SK-based initiator authentication is used for the setup of the IPsec SAs. The HA obtains the SK using the Diameter application specified in this document.

This document assumes that the SK provided to the IKEv2 peer as well as the SK delivered to the IKEv2 server by the Diameter server are established or derived using the same rules. Furthermore, it assumes that these rules are agreed to by the external protocol on a peer side providing the key to the IKEv2 peer, and on the Diameter server side providing the key to the IKEv2 server. This document allows for the SK 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 the SK specific to 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 it specifies the Diameter application needed for this communication. Other protocols leveraging this Diameter application MAY specify their own SK derivation scheme. For example see [X.S0047] and [X.S0058]. This document specifies the default procedure for derivation of the SK used in IKEv2 authentication when protocols leveraging this Diameter application do not specify their own derivation procedure. Selection of either default or other SK derivation procedure is done by the external protocol between the Peer and the Diameter Server, 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
HAAA	Home Authentication, Authorization, and Accounting
IKEv2	Internet Key Exchange Protocol version 2
NAI	Network Access Identifier
PSK	Pre-Shared Key

SA Security Association

SK Shared Key

SPI Security Parameter Index

3. Application Identifier

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

Diameter IKE SK (IKESK) 11

The IKESK Application Identifier is used when the IKEv2 peer is to be authenticated and authorized using IKEv2 with SK-based authentication.

4. Protocol Description

4.1. Support for IKEv2 and Shared Keys

When IKEv2 is used with SK-based initiator authentication, the Diameter commands IKEv2-SK-Request/Answer defined in this document are used between the IKEv2 server and a Home AAA (HAAA) server 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 SK for this IKEv2 peer. If no SK associated with this IKEv2 peer is found, the IKEv2 server MUST send an Authorize-Only (Auth-Request-Type set to "Authorize-Only") Diameter IKEv2-SK-Request message to the HAAA to obtain the SK. If 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), it SHALL be used by the IKEv2 server to populate the User-Name AVP in the Diameter message. Otherwise, it is out of scope of this document how the IKEv2 server maps the value received in the IDi payload to the User-Name AVP and whether or not the User-Name AVP is included in the IKEv2-SK-Request message. In the same Diameter message, the IKEv2 server SHALL also include the IKEv2-Nonces AVP with the initiator and responder nonces (Ni and Nr) exchanged during initial IKEv2 exchange. Finally, the IKEv2 server SHALL include the IKEv2-Identity AVP in the IKEv2-SK-Request message. The Initiator-Identity AVP SHALL be populated with the IDi field extracted from the IKE_AUTH message. If the IDr payload was included in the IKE_AUTH message received from the IKEv2 peer, the IKEv2 server SHALL also include a Responder-Identity AVP populated with the received IDr.

The IKEv2 server sends the IKEv2-SK-Request message to the IKEv2 peer's HAAA. The Diameter message is routed to the correct HAAA per [RFC6733].

Upon receiving a Diameter IKEv2-SK-Request message from the IKEv2 server, the HAAA SHALL use the User-Name AVP (if present) and/or Initiator-Identity AVP to retrieve the associated keying material. When the default SK-generation procedure specified in this document is used, the peer side that provides the SK to the IKEv2 peer, as well as the Diameter server, SHALL use the same SK derivation that follows the methodology similar to that specified in Section 3.1 of [RFC5295], specifically:

SK = KDF(PSK, 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].
- Pre-Shared Key (PSK) is the key available to the protocol leveraging this Diameter application, e.g., the long-term shared secret, 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 'sk4ikev2@ietf.org'.
- | denotes concatenation
- "\0" is a NULL octet (0x00 in hex)
- Length is a 2-octet unsigned integer in network byte order of the output key length, in octets.

When applications using this protocol define their own SK-generation algorithm, it is strongly RECOMMENDED that the nonces Ni and Nr be used in the computation. It is also RECOMMENDED that IDi be used. IDr SHOULD NOT be used in the SK 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 SKs being generated. The HAAA returns the SK to the IKEv2 server using the Key AVP as specified in [RFC6734].

Once the IKEv2 server receives the SK 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 [RFC6733].

4.2.1. Session-Termination-Request/Answer

In the case where the HAAA is maintaining session state, when the IKEv2 server terminates the SA, it SHALL send a Session-Termination-Request (STR) message [RFC6733] to inform the HAAA that the authorized session has been terminated.

The Session-Termination-Answer (STA) message [RFC6733] 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 [RFC6733] 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 [RFC6733] is sent by the IKEv2 server in response to an ASR message.

5. Command Codes for Diameter IKEv2 with SK

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

Command Name	Abbrev.	Code	Section Reference	Application
IKEv2-SK-Request	IKESKR	329	Section 5.1	IKESK
IKEv2-SK-Answer	IKESKA	329	Section 5.2	IKESK

Table 1: Command Codes

5.1. IKEv2-SK-Request (IKESKR) Command

The IKEv2-SK-Request message, indicated with the Command Code set to 329 and the 'R' bit set in the Command Flags field, is sent from the IKEv2 server to the HAAA to initiate IKEv2 with SK authorization. In this case, the Application-Id field of the Diameter header MUST be set to the Diameter IKE SK Application-Id (11).

Message format

```
      <IKEv2-SK-Request> ::= < Diameter Header: 329, 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 ]
                             { IKEv2-Identity }
                             [ Auth-Session-State ]
                             { IKEv2-Nonces }
                           * [ Proxy-Info ]
                           * [ Route-Record ]
                             ...
                           * [ AVP ]
```

The IKEv2-SK-Request message MUST include an IKEv2-Nonces AVP containing the Ni and Nr nonces swapped during initial IKEv2 exchange. The IKEv2-SK-Request message MAY contain a Key-SPI AVP (Key-SPI AVP is specified in [RFC6734]). If included, it contains the SPI that HAAA SHALL use, in addition to the other parameters (e.g., Initiator-Identity), to identify the appropriate SK. The IKEv2-SK-Request message MUST include IKEv2-Identity AVP. The Initiator-Identity AVP SHALL contain IDi as received in IKE_AUTH message. The Responder-Identity AVP SHALL be included in the IKEv2-SK-Request message, if IDr payload was included in the IKE_AUTH message received from the IKEv2 peer. If included, the Responder-Identity AVP contains the received IDr.

5.2. IKEv2-SK-Answer (IKESKA) Command

The IKEv2-SK-Answer (IKESKA) message, indicated by the Command Code field set to 329 and the 'R' bit cleared in the Command Flags field, is sent by the HAAA to the IKEv2 server in response to the IKESKR command. In this case, the Application-Id field of the Diameter header MUST be set to the Diameter IKE SK Application-Id (11).

Message format

```
        <IKEv2-SK-Answer> ::= < Diameter Header: 329, 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-SK-Answer message SHALL include the Key AVP as specified in [RFC6734]. The value of the Key-Type AVP SHALL be set to IKEv2 SK (3). The Keying-Material AVP SHALL contain the SK. If the Key-SPI AVP is received in IKEv2-SK-Request, the Key-SPI AVP SHALL be included in the Key AVP. The Key-Lifetime AVP may be included; if so, then the associated key SHALL NOT be used by the receiver of the answer if the lifetime has expired. Finally, the Responder-Identity AVP may be included.

6. Attribute-Value Pair Definitions

This section defines new AVPs for IKEv2 with SK.

6.1. IKEv2-Nonces

The IKEv2-Nonces AVP (Code 587) 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 SK generation.

```
IKEv2-Nonces ::= < AVP Header: 587 >
                 {Ni}
                 {Nr}
                *[AVP]
```

6.1.1. Ni

The Ni AVP (AVP Code 588) is of type OctetString and contains the IKEv2 initiator nonce as contained in Nonce Data field.

6.1.2. Nr

The Nr AVP (AVP Code 589) is of type OctetString and contains the IKEv2 responder nonce as contained in Nonce Data field.

6.2. IKEv2-Identity

The IKEv2-Identity AVP (Code 590) is of type Grouped and contains the Initiator and possibly Responder identities as included in IKE_AUTH message sent from the IKEv2 peer to the IKEv2 server.

```
IKEv2-Identity ::= < AVP Header: 590 >
                   {Initiator-Identity}
                   [Responder-Identity]
                  *[AVP]
```

6.2.1. Initiator-Identity

The Initiator-Identity AVP (AVP Code 591) is of type Grouped and contains the identity type and identification data of the IDi payload of the IKE_AUTH message.

```
Initiator-Identity ::= < AVP Header: 591 >
                       {ID-Type}
                       {Identification-Data}
                      *[AVP]
```

6.2.1.1. ID-Type

The ID-Type AVP (AVP Code 592) is of type Enumerated and contains the ID type value of IDi payload of the IKE_AUTH message.

6.2.1.2. Identification-Data

The Identification-Data AVP (AVP Code 593) is of type OctetString and contains the Identification Data field of IDi payload of the IKE_AUTH message.

6.2.2. Responder-Identity

The Responder-Identity AVP (AVP Code 594) is of type Grouped and contains the identity type and identification data of the IDr payload of the IKE_AUTH message.

```
Responder-Identity ::= < AVP Header: 594 >
                       {ID-Type}
                       {Identification-Data}
                      *[AVP]
```

6.2.2.1. ID-Type

The ID-Type AVP (AVP Code 592) is of type Enumerated and contains the ID type value of IDr payload of the IKE_AUTH message.

6.2.2.2. Identification-Data

The Identification-Data AVP (AVP Code 593) is of type OctetString and contains the Identification Data field of IDr payload of the IKE_AUTH message.

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.

AVP Name	Command Code	
	IKESKR	IKESKA
Key	0	0-1
Key-SPI	0-1	0
IKEv2-Nonces	1	0
IKEv2-Identity	1	0
Responder-Identity	0	0-1

IKESKR and IKESKA 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 protocol [RFC6733] specifies the AVP Flag rules for AVPs in Section 4.5.

Attribute Name	AVP Code	Section Defined	Value Type	AVP Flag Rules: MUST	AVP Flag Rules: MUST NOT
Key	581	Note 1	Grouped	M	V
Keying-Material	583	Note 1	OctetString	M	V
Key-Lifetime	584	Note 1	Integer64	M	V
Key-SPI	585	Note 1	Unsigned32	M	V
Key-Type	582	Note 1	Enumerated	M	V
IKEv2-Nonces	587	6.1	Grouped	M	V
Ni	588	6.1.1	OctetString	M	V
Nr	589	6.1.2	OctetString	M	V
IKEv2-Identity	590	6.2	Grouped	M	V
Initiator-Identity	591	6.2.1	Grouped	M	V
ID-Type	592	6.2.1.1	Enumerated	M	V
Identification-Data	593	6.2.1.2	OctetString	M	V
Responder-Identity	594	6.2.2	Grouped	M	V

AVP Flag Rules Table

Note 1: The Key, Keying-Material, Key-Lifetime, Key-SPI, and Key-Type AVPs are defined in [RFC6734].

9. IANA Considerations

9.1. Command Codes

IANA has allocated a Command Code value for the following new command from the Command Code namespace defined in [RFC6733].

Command Code	Value
IKEv2-SK-Request/Answer	329

9.2. AVP Codes

This specification requires IANA to register the following new AVPs from the AVP Code namespace defined in [RFC6733].

- IKEv2-Nonces - 587
- Ni - 588
- Nr - 589
- IKEv2-Identity - 590
- Initiator-Identity - 591
- ID-Type - 592
- Identification-Data - 593
- Responder-Identity - 594

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 3 signifies that IKEv2 SK is being sent.

9.4. Application Identifier

This specification requires IANA to allocate one new value "Diameter IKE SK" from the Application Identifier namespace defined in [RFC6733].

Application Identifier	Value
Diameter IKE SK (IKESK)	11

10. Security Considerations

The security considerations of the Diameter base protocol [RFC6733] 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 SK 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 [RFC6733].

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, it relies on the security properties of the intermediating AAA inter-connection networks, AAA brokers, and Diameter agents. Furthermore, any agents that process IKEv2-SK-Answer messages can see the contents of the Key AVP.

To mitigate the threat of exposing a long-lived PSK, this specification expects that the HAAA derive and return the associated SK to the IKEv2 server. Given that SK derivation is security-critical, for the SK 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 the IKEv2-SK-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

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

[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.

[RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

[RFC6734] Zorn, G., Wu, W., and V. Cakulev, "Diameter Attribute-Value Pairs for Cryptographic Key Transport", RFC 6734, October 2012.

11.2. Informative References

[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.ietf@lior.org

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