Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 19 April 2026

V. Smyslov
ELVIS-PLUS

16 October 2025

Using the Internet Key Exchange Protocol Version 2 (IKEv2) for PSP Key Management
draft-smyslov-ipsecme-ikev2-psp-00

Abstract

This document specifies how the Internet Key Exchange Version 2 (IKEv2) protocol can be used for supplying keys for the PSP Security Protocol (PSP).

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 https://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 19 April 2026.

Table of Contents

1. Introduction 2
2. Terminology and Notation 2
3. PSP 3
4. PSP Key Management Using IKEv2 3
4.1. The IKE_SA_INIT Exchange 3
4.2. The IKE_AUTH Exchange 4
4.3. The Modified CREATE_CHILD_SA Exchange 4
5. Security Considerations 5
6. IANA Considerations 5
7. References 6
7.1. Normative References 6
7.2. Informative References 7
Author's Address 7

1. Introduction

Internet Key Exchange Version 2 (IKEv2) protocol [RFC7296] is used in IPsec architecture [RFC4301] for the purpose SA negotiation and key management. It provides authenticated key exchange and calculates session keys for the Encapsulating Security Payload (ESP) protocol [RFC4303].

PSP Security Protocol (PSP) is defined in [PSP]. The protocol utilizes the concept of so called "stateless encryption" by keeping only global state for decrypting incoming packets. This concept implies that the receiving side of Security Association (SA) provides the sending side with a key at the time this SA is being created.

PSP is considered as an alternative for ESP for high-speed communications (e.g., inside data centers). However, IKEv2 cannot directly be used for providing keys for PSP, since the way IPsec keys are being obtained in IKEv2 implies that they are derived from the ephemeral key exchange and thus are unpredictable. This is incompatible with the way keys are used in PSP where each side must independently generate keys used for decryption for a particular SA based on some global key.

2. Terminology and Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. PSP

PSP [PSP] is a security protocol created by Google for encryption on IP level. PSP was designed to address the high-speed encryption requirements of large-scale data centers. To avoid storing per-SA decryption keys on the receiver side, the decryption keys are derived from the SPI (that is present in the packet) plus a global secret known only to the receiver side.

PSP specification does not address key management issues. It assumes that at the time an SA is being created the sender asks the receiver to create an SA encryption key, which the receiver then somehow communicates securely to the sender.

4. PSP Key Management Using IKEv2

IKEv2 cannot directly be used for providing keys for PSP, because its specification [RFC7296] assumes that keying material for Child SAs is derived using initial ephemeral key exchange. Thus, peers contribute to this keying material, but cannot control it and for this reason cannot provide each other with arbitrary keys.

On the other hand, IKEv2 extension for group key management [I-D.ietf-ipsecme-g-ikev2] does allow this functionality as it is needed for providing members of a group with identical keys. This specification re-uses the ability to download arbitrary keys in IKEv2 from [I-D.ietf-ipsecme-g-ikev2]. Note that unlike [I-D.ietf-ipsecme-g-ikev2] this specification is for unicast (peer-to-peer) communication.

Since both peers have to provide each other with keying material, it is not possible to do that in the IKE_AUTH exchange (as in [RFC7296]), since the initiator in this case would send its key (which is sensitive information) to the not-yet-authenticated responder. For this reason, peers MUST create IKE SA childless as specified in [RFC6023]. Once childless IKE SA is created, peers can use the modified CREATE_CHILD_SA exchange to create or rekey Child SAs utilizing PSP.

4.1. The IKE_SA_INIT Exchange

Peers wishing to use IKEv2 for providing keys for PSP MUST negotiate the Key Wrap Algorithm (KWA) transform (Section 4.4.2.1.2 of [I-D.ietf-ipsecme-g-ikev2]) in the IKE_SA_INIT exchange. If the initiator is not sure that the responder supports PSP and if using PSP is optional for the initiator, then the initiator MAY include two proposals into the IKE_SA_INIT request - one with the Key Wrap Algorithm transform (aiming for responders supporting PSP) and the

other without it.

The responder supporting PSP key management, besides negotiation of the KWA transform, MUST also include the CHILDLESS_IKEV2_SUPPORTED notification (Section 4 of [RFC6023]) in the IKE_SA_INIT response.

Even if the KWA transform is negotiated, it does not mean that this IKE SA is for creating PSP SAs only - such an SA MAY be used for creating both ESP and PSP SAs.

4.2. The IKE_AUTH Exchange

The PSP Child SA cannot be created in the IKE_AUTH exchange. On the other hand, peers may create the ESP Child SA in this exchange if they want to. Otherwise, the IKE SA is created childless and the IKE_AUTH exchange is as defined in Section 5 of [RFC6023].

4.3. The Modified CREATE_CHILD_SA Exchange

Modified CREATE_CHILD_SA exchange is used for creating the PSP SA. The following modifications are made.

* The SA payload MUST contain one or more Proposal substructures with the Protocol ID field set to a new Security Protocol Identifier PSP (<TBA by IANA>). Note that SPI Size for PSP is the same as for ESP (4 octets). Proposals with other Security Protocol Identifiers MUST NOT be present.

* These Proposal substructures MUST only contain one or more Transform substructures with new Transform Type "PSP Parameters (PSP)" (<TBA by IANA>). See Section 6, Paragraph 2, Item 1 for Possible Transform IDs for this Transform Type. Transform substructures with other Transform Types MUST NOT be present.

* The CREATE_CHILD_SA messages MUST NOT contain the Key Exchange (KE) and the Nonce (Ni and Nr) payloads. Instead, both request and response MUST contain exactly one Key Download (KD) payload, defined in Section 4.5 of [I-D.ietf-ipsecme-g-ikev2]. The sender of a KD payload provides a keying material for the PSP SA that it will use as a receiver to its peer.

* The KD payloads MUST contain exactly one or more Group Key Bag substructure, defined in Section 4.5.2 of [I-D.ietf-ipsecme-g-ikev2]. The Protocol field of this substructures MUST be set to Security Protocol Identifier PSP (<TBA by IANA>), the SPI MUST match that in one of the Proposal substructures in the SA payload.

* Each Key Bag MUST contain exactly one SA_KEY attribute, defined in Section 4.5.2.1 of [I-D.ietf-ipsecme-g-ikev2], in which the wrapped keying material (See Section 4.5.4 of [I-D.ietf-ipsecme-g-ikev2]) for the PSP SA is provided. The Key ID and the KWK ID fields MUST be set to zero, meaning that this attribute contains the keying material for an SA and this keying material is protected with the default Key Wrap Key SK_w that is calculated as

  SK_w = prf+(SK_d, "Key Wrap for PSP")

* The size of the provided keying material MUST be sufficient to get keys for any of the proposed PSP parameters.

The modified CREATE_CHILD_SA exchange is shown below.

```
Initiator                          Responder
-------------------------------------------------------------------
HDR, SK {[N(REKEY_SA),]
     SA, KD, TSi, TSr}   --->

                           <---    HDR, SK {SA, KD, TSi, TSr}
```

Figure 1: CREATE_CHILD_SA Exchange for PSP

The USE_TRANSPORT_MODE notification can be used in case of PSP to indicate that the PSP SA is to be created using transport mode, as with ESP.

The REKEY_SA notification can be present and plays the same role as with ESP SA - indicates the SA to be replaced with a newly created SA.

5. Security Considerations

To be added.

6. IANA Considerations

This document requests IANA to make the following changes in the "Internet Key Exchange Version 2 (IKEv2) Parameters" registry group [IKEV2-IANA].

1. Create new registry "Transform Type <TBA> - PSP Parameters Transform IDs". The registration policy for this registry is Expert Review Policy [RFC8126]. The initial values of the new registry are:

Value	PSP Parameters
0	Reserved
1	PSP Header Version 0, AES-GCM-128
2	PSP Header Version 0, AES-GCM-256
3	PSP Header Version 0, AES-GMAC-128
4	PSP Header Version 0, AES-GMAC-256
Unassigned	5-1023
Private Use	1024-65535

2. Add new Transform Type "PSP Parameters (PSP)" in the "Transform Type Values" registry.

Type	Description	Used In
<TBA>	PSP Parameters (PSP)	(PSP)

3. Add new Security Protocol Identifier in the "IKEv2 Security Protocol Identifiers" registry.

Protocol ID	Protocol
<TBA>	PSP

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC6023] Nir, Y., Tschofenig, H., Deng, H., and R. Singh, "A Childless Initiation of the Internet Key Exchange Version 2 (IKEv2) Security Association (SA)", RFC 6023, DOI 10.17487/RFC6023, October 2010, <https://www.rfc-editor.org/info/rfc6023>.

[I-D.ietf-ipsecme-g-ikev2] Smyslov, V. and B. Weis, "Group Key Management using IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-g-ikev2-23, 31 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-g-ikev2-23>.

[PSP] "PSP Architecture Specification", November 2022, <https://github.com/google/psp/blob/main/doc/PSP_Arch_Spec.pdf>.

7.2. Informative References

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[IKEV2-IANA] IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml>.

Author’s Address

Valery Smyslov
ELVIS-PLUS
Russian Federation
Email: svan@elvis.ru