Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2020

V. Smyslov
ELVIS-PLUS

March 11, 2020

Announcing Supported Authentication Methods in IKEv2
draft-smyslov-ipsecme-ikev2-auth-announce-01

Abstract

This specification defines a mechanism that allows the Internet Key Exchange version 2 (IKEv2) implementations to indicate the list of supported authentication methods to their peers while establishing IKEv2 Security Association (SA). This mechanism improves interoperability when IKEv2 partners are configured with multiple different credentials to authenticate each other.

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 September 12, 2020.

Table of Contents

1. Introduction

The Internet Key Exchange version 2 (IKEv2) protocol, defined in [RFC7296], performs authenticated key exchange in IPsec. IKEv2, unlike its predecessor IKEv1, defined in [RFC2409], doesn't include a mechanism to negotiate an authentication method that the peers would use to authenticate each other. It is assumed that each peer selects whatever authentication method it thinks is appropriate, depending on authentication credentials it has.

This approach generally works well when there is no ambiguity in selecting authentication credentials. The problem may arise when there are several credentials of different type configured on one peer, while only some of them are supported on the other peer. Another problem situation is when a single credential may be used to produce different types of authentication tokens (e.g. signatures of different formats). Emerging post-quantum signature algorithms may bring additional challenges for implementations, especially if so called hybrid schemes are used (e.g. see [I-D.ounsworth-pq-composite-sigs]).

This specification defines an extension to the IKEv2 protocol that allows peers to announce their supported authentication methods, thus

decreasing risks of SA establishment failure in situations when there are several ways for the peers to authenticate themselves.

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. Protocol Details

The idea is that each party sends a list of authentication methods it supports to its peer. In addition, the sending party may optionally specify that some of the authentication methods are only to be used with particular trust anchors. Upon receiving this information the peer may take it into account while selecting an algorithm for its authentication if several methods are available.

3.1. Exchanges

If the responder is willing to use this extension, it includes a new notification SUPPORTED_AUTH_METHODS in a response message of the IKE_SA_INIT exchange. This notification contains a list of authentication methods supported by the responder.

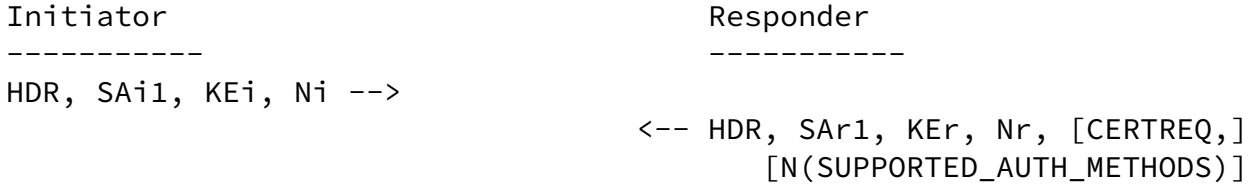

Figure 1: IKE_SA_INIT Exchange

If the initiator doesn't support this extension, it will ignore the received notification as an unknown status notify. Otherwise, it MAY send the SUPPORTED_AUTH_METHODS notification in the IKE_AUTH request message, with a list of authentication methods supported by the

initiator.

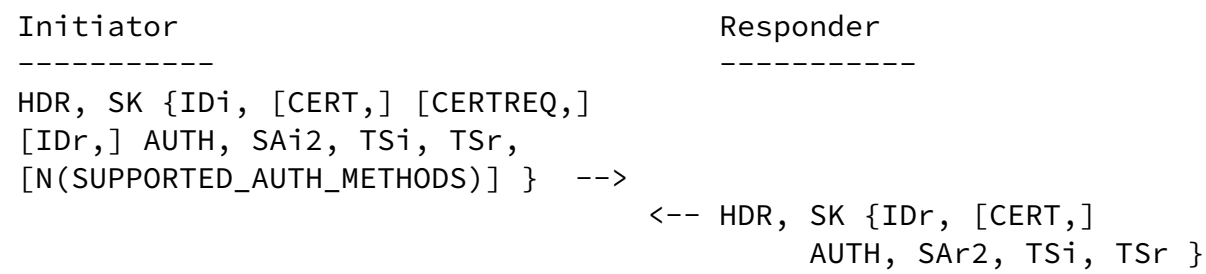

Figure 2: IKE_AUTH Exchange

Since the responder sends the SUPPORTED_AUTH_METHODS notification in the IKE_SA_INIT exchange, it must take care that the size of the response message wouldn't grow too much so that IP fragmentation takes place. If the following conditions are met:

- the SUPPORTED_AUTH_METHODS notification to be included is so large, that the responder suspects that IP fragmentation of the resulting IKE_SA_INIT response message may happen;

- both peers support the IKE_INTERMEDIATE exchange, defined in [I-D.ietf-ipsecme-ikev2-intermediate] (i.e. the responder has received and is going to send the INTERMEDIATE_EXCHANGE_SUPPORTED notification);

then the responder may choose not to send the actual list of the supported authentication methods in the IKE_SA_INIT exchange and instead ask the initiator to start the IKE_INTERMEDIATE exchange for the list to be sent in. In this case the responder includes SUPPORTED_AUTH_METHODS notification containing no data in the IKE_SA_INIT response.

If the initiator receives the empty SUPPORTED_AUTH_METHODS notification in the IKE_SA_INIT exchange, it means that the responder is going to send the list of the supported authentication methods in the IKE_INTERMEDIATE exchange. If this exchange is to be initiated anyway for some other reason, then the responder MUST use it to send the SUPPORTED_AUTH_METHODS notification. Otherwise, the initiator MAY start the IKE_INTERMEDIATE exchange just for this sole purpose by sending an empty request message.

```
Initiator                                   Responder
-----------                                 -----------
HDR, SK {...}  -->

                                    <-- HDR, SK {...
                                        [N(SUPPORTED_AUTH_METHODS)] }
```

Figure 3: IKE_INTERMEDIATE Exchange

Note, that sending the SUPPORTED_AUTH_METHODS notification and using information obtained from it is optional for both the initiator and the responder.

3.2. SUPPORTED_AUTH_METHODS Notify

The format of the SUPPORTED_AUTH_METHODS notification is shown below.

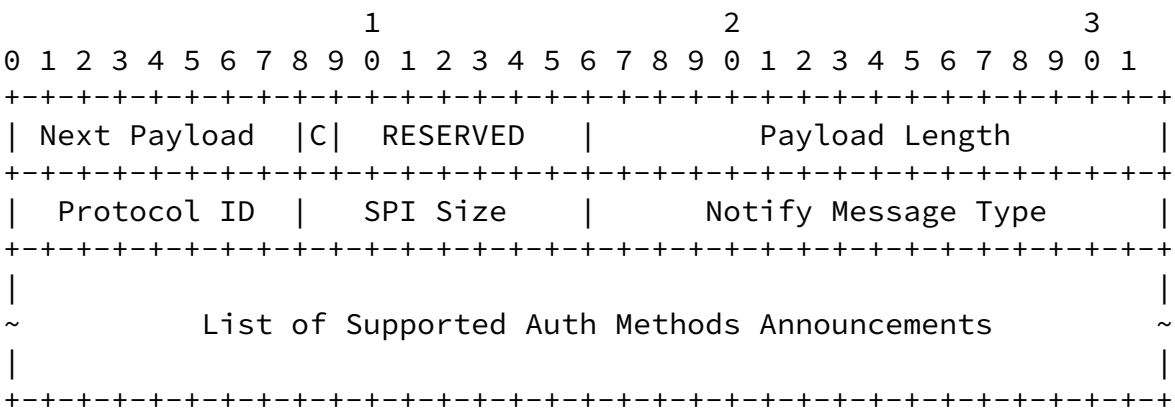

Figure 4: SUPPORTED_AUTH_METHODS Notify

The Notify payload format is defined in Section 3.10 of [RFC7296]. When a Notify payload of type SUPPORTED_AUTH_METHODS is sent, the Protocol ID field is set to 0, the SPI Size is set to 0, meaning there is no SPI field, and the Notify Message Type is set to <TBA by IANA>.

The Notification Data field contains the list of supported authentication methods announcements. Each individual announcement

is a variable-size data blob, which format depends on the announced authentication method. The blob always starts with an octet containing the length of the blob followed by an octet containing the authentication method. Authentication methods are represented as values from the "IKEv2 Authentication Method" registry defined in [IKEV2-IANA]. The meaning of the remaining octets of the blob, if any, depends on the authentication method and is defined below. Note, that for the currently defined authentication methods the length octet fully defines both the format and the semantics of the blob.

If more authentication methods are defined in future, the corresponding documents must describe the semantics of the announcements for these methods. Implementations MUST skip announcements which semantics they don't understand.

3.2.1. 2-octet Announcement

If the announcement contains an authentication method that is not concerned with public key cryptography, then the following format is used.

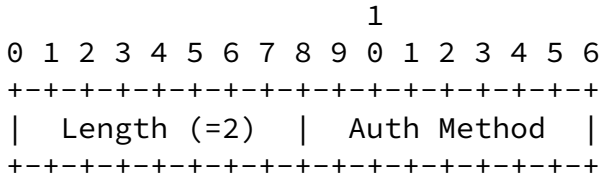

Figure 5: Supported Authentication Method

- Length - the length of the blob, must be 2 for this case.
- Auth Method - the announced authentication method.

This format is applicable for the authentication methods "Shared Key Message Integrity Code" (2) and "NULL Authentication" (13). Note, that authentication method "Generic Secure Password Authentication

Method" (12) would also fall in this category, however it is negotiated separately (see [RFC6467] and for this reason there is no point to announce it via this mechanism.

3.2.2. 3-octet Announcement

If the announcement contains an authentication method that is concerned with public key cryptography, then the following format is used. This format allows to link the announcement with the particular trust anchor from the Certificate Request payload.

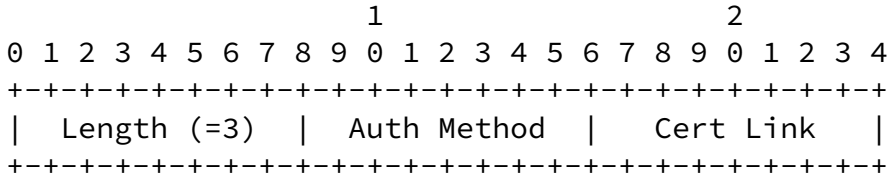

Figure 6: Supported Authentication Method

- Length - the length of the blob, must be 3 for this case.
- Auth Method - the announced authentication method.
- Cert Link - allows linking this announcement to the particular CA.

If the Cert Link field contains non-zero value N, it means that the announced authentication method is intended to be used only with the N-th trust anchor (CA certificate) from the Certificate Request payload(s) sent by this peer. If it is zero, then this authentication method may be used with any of CAs, that are not linked to any other announcement. If multiple CERTREQ payloads were sent, the CAs from all of them are treated as a single list for the purpose of the linking. If no Certificate Request payload were

receives, the content of this field MUST be ignored and treated as zero.

This format is applicable for the authentication methods "RSA Digital Signature" (1), "DSS Digital Signature" (3), "ECDSA with SHA-256 on the P-256 curve" (9), "ECDSA with SHA-384 on the P-384 curve" (10) and "ECDSA with SHA-512 on the P-512 curve" (11). Note however, that these authentication methods are currently superseded by the "Digital

Signature" (14) authentication method, which has a different announcement format, described below.

3.2.3. Multi-octet Announcement

The following format is currently used only with the "Digital Signature" (14) authentication method.

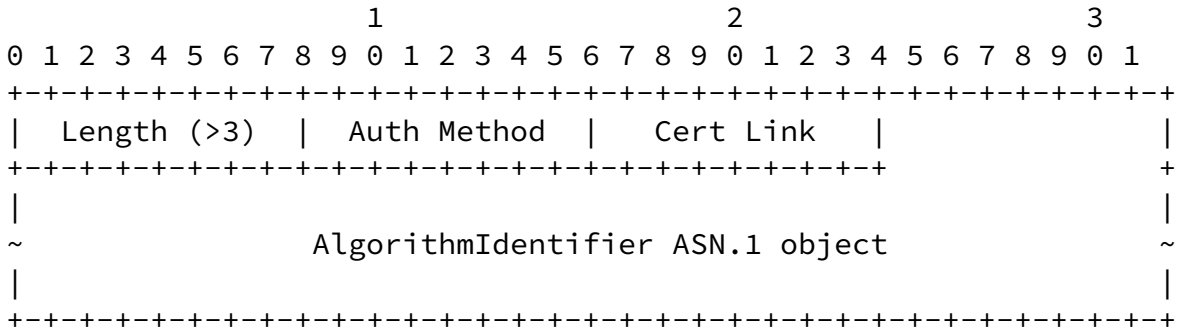

Figure 7: Supported Authentication Method

- Length - the length of the blob, must be greater than 3 for this case.
- Auth Method - the announced authentication method, currently may only be 14 ("Digital Signature").
- Cert Link - allows linking this announcement to the particular CA; see Section 3.2.2 for details.
- AlgorithmIdentifier ASN.1 object - contains DER-encoded ASN.1 object AlgorithmIdentifier.

The "Digital Signature" authentication method, defined in [RFC7427], supersedes previously defined signature authentication methods. In this case the real authentication algorithm is identified via AlgorithmIdentifier ASN.1 object. Appendix A in [RFC7427] contains examples of Commonly Used ASN.1 Objects.

4. Security Considerations

Security considerations for IKEv2 protocol are discussed in [RFC7296]. It is assumed that this extension of the IKEv2 doesn't add new vulnerabilities to the protocol.

5. IANA Considerations

This document also defines a new Notify Message Types in the "Notify Message Types - Status Types" registry:

<TBA>	SUPPORTED_AUTH_METHODS

6. References

6.1. 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>.

[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>.

[RFC7427] Kivinen, T. and J. Snyder, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)", RFC 7427, DOI 10.17487/RFC7427, January 2015, <https://www.rfc-editor.org/info/rfc7427>.

[I-D.ietf-ipsecme-ikev2-intermediate] Smyslov, V., "Intermediate Exchange in the IKEv2 Protocol", draft-ietf-ipsecme-ikev2-intermediate-03 (work in progress), December 2019.

[IKEV2-IANA] IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-7>.

6.2. Informative References

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, DOI 10.17487/RFC2409, November 1998, <https://www.rfc-editor.org/info/rfc2409>.

[RFC6467] Kivinen, T., "Secure Password Framework for Internet Key Exchange Version 2 (IKEv2)", RFC 6467, DOI 10.17487/RFC6467, December 2011, <https://www.rfc-editor.org/info/rfc6467>.

[I-D.ounsworth-pq-composite-sigs] Ounsworth, M. and M. Pala, "Composite Keys and Signatures For Use In Internet PKI", draft-ounsworth-pq-composite-sigs-02 (work in progress), January 2020.

Author's Address

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd) 124460
RU

Phone: +7 495 276 0211
Email: svan@elvis.ru