

Workgroup: IPSECME Working Group

Internet-Draft:

draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt-10

Published: 21 October 2022

Intended Status: Standards Track

Expires: 24 April 2023

Authors: S. Kampati	W. Pan	P. Wouters	M. Bharath
Microsoft	Huawei	Aiven	Mavenir
M. Chen			
CMCC			

## **IKEv2 Optional SA&TS Payloads in Child Exchange**

### **Abstract**

This document describes a method for reducing the size of the Internet Key Exchange version 2 (IKEv2) CREATE\_CHILD\_SA exchanges used for rekeying of the IKE or Child SA by replacing the SA and TS payloads with a Notify Message payload. Reducing size and complexity of IKEv2 exchanges is especially useful for low power consumption battery powered devices.

### **About This Document**

This note is to be removed before publishing as an RFC.

Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt/>.

Discussion of this document takes place on the ipsec Working Group mailing list (<mailto:ipsec@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/ipsec/>. Subscribe at <https://www.ietf.org/mailman/listinfo/ipsec/>.

Source for this draft and an issue tracker can be found at <https://github.com/mcr/ipsecme-ikev2-sa-ts-payloads.git>.

### **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 24 April 2023.

## Copyright Notice

Copyright (c) 2022 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 (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

- [1. Introduction](#)
- [2. Conventions Used in This Document](#)
  - [2.1. Requirements Language](#)
- [3. Negotiation of Support for OPTIMIZED REKEY](#)
- [4. Optimized Rekey of the IKE SA](#)
- [5. Optimized Rekey of Child SAs](#)
- [6. Payload Formats](#)
  - [6.1. OPTIMIZED REKEY SUPPORTED Notify](#)
  - [6.2. OPTIMIZED REKEY Notify](#)
- [7. IANA Considerations](#)
- [8. Operational Considerations](#)
- [9. Security Considerations](#)
- [10. Acknowledgments](#)
- [11. Normative References](#)
- [Authors' Addresses](#)

## 1. Introduction

The Internet Key Exchange protocol version 2 (IKEv2) [[RFC7296](#)] is used to negotiate Security Association (SA) parameters for the IKE SA and the Child SAs. Cryptographic key material for these SAs have a limited lifetime before it needs to be refreshed, a process referred to as "rekeying". IKEv2 uses the CREATE\_CHILD\_SA exchange to rekey either the IKE SA or the Child SAs.

When rekeying, a full set of negotiation parameters are exchanged. However, most of these parameters will be the same as before, and some of these parameters **MUST NOT** change.

For example, the Traffic Selector (TS) negotiated for the new Child SA **MUST** cover the Traffic Selectors negotiated for the old Child SA. And in practically all cases, a new Child SA does not need to cover a wider set of Traffic. In the rare case where this would be needed, either a standard rekey could be used or a new Child SA could be negotiated followed by a deletion of the replaced Child SA.

Similarly, IKEv2 states that the cryptographic parameters negotiated for rekeying **SHOULD NOT** be different. This means that the security properties of the IKE or Child SA in practise do not change during a typical rekey.

This document specifies a method to omit these parameters and replace them with a single Notify Message declaring that all these parameters are identical to the originally negotiated parameters.

Large scale IKEv2 gateways such as Evolved Packet Data Gateway (ePDG) in 4G networks or Centralized Radio Access Network (cRAN/Cloud) gateways in 5G networks typically support more than 100,000 IKE/IPsec connections. At any point in time, there will be hundreds or thousands of IKE SAs and Child SAs that are being rekeyed. This takes a large amount of bandwidth and CPU power and any protocol simplification or bandwidth reducing would result in a significant resource saving.

For Internet of Things (IoT) devices which utilize low power consumption technology, reducing the size of the CREATE\_CHILD\_SA exchange for rekeying reduces its power consumption, as sending bytes over the air is usually the most power consuming operation of such a device. Reducing the CPU operations required to verify the rekey exchanges parameters will also save power and extend the lifetime for these devices.

When using identical parameters for the IKE SA or Child SA rekey, the SA and TS payloads can be omitted thanks to the optimization defined in this document. For an IKE SA rekey, instead of the (large) SA payload, only a Key Exchange (KE) payload and a new Notify Type payload with the new SPI are required. For a Child SA payload, instead of the SA or TS payloads, only an optional nonce payload (when using PFS) and a new Notify Type payload with the new SPI are needed. This makes the rekey exchange packets much smaller and the peers do not need to verify that the SA or TS parameters are compatible with the old SA parameters.

## 2. Conventions Used in This Document

### 2.1. Requirements Language

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. Negotiation of Support for OPTIMIZED REKEY

To indicate support for the optimized rekey negotiation, the initiator includes the OPTIMIZED\_REKEY\_SUPPORTED notify payload in the IKE\_AUTH exchange request. During this initial key request, the entire SA and TS payloads are included as normal. A responder that supports the optimized rekey exchange includes the OPTIMIZED\_REKEY\_SUPPORTED notify payload in its response. Note that the notify indicates support for optimized rekey for both IKE and Child SAs.

A responder that does not support the optimized rekey exchange processes the SA and TS payloads as normal, and does not include the new Notify. As per regular IKEv2 processing, a responder that does not recognize this new Notify, **MUST** ignore the notify. Responders may have been administratively configured with the optimization turned off for local reasons. The absence of the Notify indicates to the initiator that the optimization is not available, and normal, full rekey should be done.

When a peer wishes to rekey an IKE SA or Child SA, it **MAY** use the optimized rekey method during the CREATE\_CHILD\_SA exchange. If both peers have exchanged OPTIMIZED\_REKEY\_SUPPORTED notifies, peers **SHOULD** use the optimized rekey method for rekeys. Non-optimized, regular rekey requests **MUST** always be accepted.

The IKE\_AUTH message exchange in this case is shown below:

Initiator	Responder
-----	
HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr, N(OPTIMIZED_REKEY_SUPPORTED)} -->	<-- HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr, N(OPTIMIZED_REKEY_SUPPORTED)}

#### 4. Optimized Rekey of the IKE SA

The initiator of an optimized rekey request sends a CREATE\_CHILD\_SA payload with the OPTIMIZED\_REKEY notify payload containing the new Security Parameter Index (SPI) for the new IKE SA. It omits the SA payload.

The responder of an optimized rekey request replies with an included OPTIMIZED\_REKEY notify with its new IKE SPI and also omits the SA payload.

Both parties send their nonce and KE payloads just as they would do for a regular IKE SA rekey.

Using the old SPI from the IKE header and the two new SPIs respectively from the initiator and responder's OPTIMIZED\_REKEY payloads, both parties can perform the IKE SA rekey operation.

The CREATE\_CHILD\_SA message exchange in this case is shown below:

Initiator	Responder
-----	
HDR, SK {N(OPTIMIZED_REKEY,newSPIi), Ni, KEi} -->	<-- HDR, SK {N(OPTIMIZED_REKEY,newSPIr), Nr, KEr}

#### 5. Optimized Rekey of Child SAs

The initiator of an optimized rekey request sends a CREATE\_CHILD\_SA payload with the OPTIMIZED\_REKEY notify payload containing the new Security Parameter Index (SPI) for the new Child SA. It omits the SA and TS payloads. If the current Child SA was negotiated with Perfect Forward Secrecy (PFS), a KEi payload **MUST** be included as well. If no PFS was negotiated for the current Child SA, a KEi payload **MUST NOT** be included.

The responder of an optimized rekey request performs the same process. It includes the OPTIMIZED\_REKEY notify with its new IKE SPI and omits the SA and TS payloads. Depending on the PFS negotiation of the current Child SA, the responder includes a KEr payload.

Both parties send their nonce payloads just as they would do for a regular Child SA rekey.

Using the old SPI from the REKEY\_SA payload and the two new SPIs respectively from the initiator and responder's OPTIMIZED\_REKEY payloads, both parties can perform the Child SA rekey operation.

The CREATE\_CHILD\_SA message exchange in this case is shown below:

Initiator	Responder
-----	
HDR, SK {N(REKEY_SA,oldSPI), N(OPTIMIZED_REKEY,newSPIi), Ni, [KEi,]} -->	<-- HDR, SK {N(OPTIMIZED_REKEY,newSPIr), Nr, [KEr,]}

## 6. Payload Formats

### 6.1. OPTIMIZED\_REKEY\_SUPPORTED Notify

The OPTIMIZED\_REKEY\_SUPPORTED Notify Message type notification is used by the initiator and responder to indicate their support for the optimized rekey negotiation.

1										2										3											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+-----+-----+-----+-----+										+-----+-----+-----+-----+										+-----+-----+-----+-----+											
Next Payload  C  RESERVED										Payload Length																					
+-----+-----+-----+-----+										+-----+-----+-----+-----+										+-----+-----+-----+-----+											
Protocol ID(=0)  SPI Size (=0)										Notify Message Type																					
+-----+-----+-----+-----+										+-----+-----+-----+-----+										+-----+-----+-----+-----+											

\*Protocol ID (1 octet) - **MUST** be 0.

\*SPI Size (1 octet) - **MUST** be 0, meaning no SPI is present.

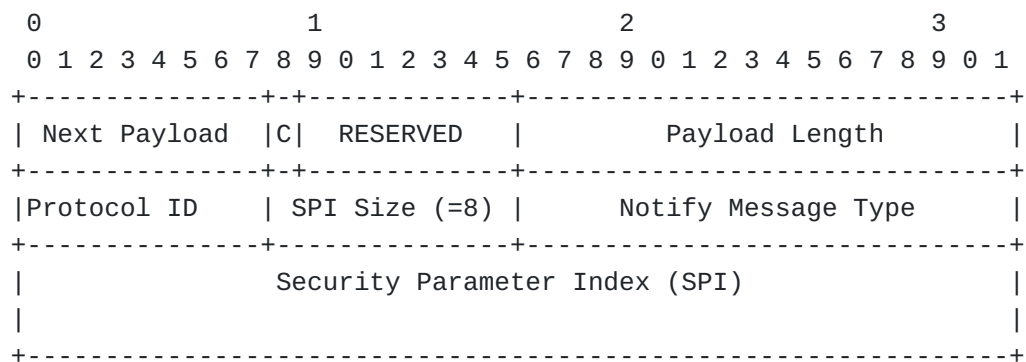
\*Notify Message Type (2 octets) - **MUST** be set to the value TBD1.

This Notify Message type contains no data.

The Critical bit **MUST** be 0. A non-zero value **MUST** be ignored.

### 6.2. OPTIMIZED\_REKEY Notify

The OPTIMIZED\_REKEY Notify Message type is used to perform an optimized IKE SA or Child SA rekey.



\*Protocol ID (1 octet) - For an IKE SA rekey, this field **MUST** contain (1). For Child SAs, this field **MUST** contain either (2) to indicate AH or (3) to indicate ESP.

\*SPI Size (1 octet) - **MUST** be 8 when rekeying an IKE SA. **MUST** be 4 when rekeying a Child SA.

\*Notify Message Type (2 octets) - **MUST** be set to the value TBD2.

\*SPI (4 octets or 8 octets) - Security Parameter Index. The new SPI.

The Critical bit **MUST** be 1. A value of 0 **MUST** be ignored.

## 7. IANA Considerations

This document defines two new Notify Message Types in the "IKEv2 Notify Message Types - Status Types" registry. IANA is requested to assign codepoints in this registry.

NOTIFY messages: status types	Value
-----	
OPTIMIZED_REKEY_SUPPORTED	TBD1
OPTIMIZED_REKEY	TBD2

## 8. Operational Considerations

Some implementations allow sending rekey messages with a different set of Traffic Selectors or cryptographic parameters in response to a configuration update. IKEv2 [RFC7296] states this **SHOULD NOT** be done. Whether or not optimized rekeying is used, a configuration change that changes the Traffic Selectors or cryptographic parameters **MUST NOT** use the optimized rekey method. It **SHOULD** also not use a regular rekey method but instead start an entire new IKE and Child SA negotiation with the new parameters.

## 9. Security Considerations

The optimized rekey removes sending unnecessary new parameters that originally would have to be validated against the original parameters. In that sense, this optimization enhances the security of the rekey process by reducing the complexity and code required.

## 10. Acknowledgments

Special thanks go to Valery Smyslov and Antony Antony.

## 11. 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>>.
- [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>>.
- [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>>.

## Authors' Addresses

Sandeep Kampati  
Microsoft  
India

Email: [skampati@microsoft.com](mailto:skampati@microsoft.com)

Wei Pan  
Huawei Technologies  
101 Software Avenue, Yuhatai District  
Nanjing  
Jiangsu,  
China

Email: [william.panwei@huawei.com](mailto:william.panwei@huawei.com)

Paul Wouters  
Aiven

Email: [paul.wouters@aiven.io](mailto:paul.wouters@aiven.io)

Meduri S S Bharath

Mavenir Systems Pvt Ltd  
Manyata Tech Park  
Bangalore  
Karnataka  
India

Email: [bharath.meduri@mavenir.com](mailto:bharath.meduri@mavenir.com)

Meiling Chen  
China Mobile  
32 Xuanwumen West Street, West District  
Beijing  
100053  
China

Email: [chenmeiling@chinamobile.com](mailto:chenmeiling@chinamobile.com)