IPSECME Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

S. Kampati
Microsoft
W. Pan
Huawei
P. Wouters
Aiven
M. Bharath
Mavenir
M. Chen
CMCC
V. Smyslov
ELVIS-PLUS

7 July 2025

Optimized Rekeys in the Internet Key Exchange Protocol Version 2 (IKEv2)
draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt-05

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-ietf-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/.

Status of This Memo

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

This Internet-Draft will expire on 8 January 2026.

Copyright Notice

Table of Contents

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. This means that the security properties of the IKE or Child SA in practice do not change during a typical rekey.

For example, the Traffic Selectors (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. Further, per RFC 7296, the Traffic Selectors and algorithms should not change when rekeying the Child SA.

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, a Nonce payload, and a new Notify Type payload with the new Security Parameter Index (SPI) are required. For a Child SA rekey, instead of the SA or TS payloads, only an optional KE payload (when using PFS), a Nonce payload, 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. If the responder supports this optimized rekey and is configured to use it, then it includes the OPTIMIZED_REKEY_SUPPORTED in the IKE_AUTH response message. If multiple IKE_AUTH exchanges are sent, the OPTIMIZED_REKEY_SUPPORTED notify payload should be in the first IKE_AUTH request and the last IKE_AUTH response. During the IKE_AUTH exchanges, the entire SA and TS payloads are included as normal. 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, will ignore it. 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 regular rekey should be used.

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)}
```

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 regular rekey can be retried when the optimized rekey fails.

Note that, except for the key and identification information such as the SPI, the optimized rekey MUST inherit all other properties of the SA being rekeyed. This means the configurations related to the SA being rekeyed are supposed to have no changes. If there is a change to the configurations, the regular rekey MUST be used instead. After the regular rekey, the next rekey can use the optimized way if there is no change to the configuration.

4. Optimized Rekey of IKE SA

The initiator of an optimized rekey request sends a CREATE_CHILD_SA request with the OPTIMIZED_REKEY notify payload containing the new 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 request with the OPTIMIZED_REKEY notify payload containing the new SPI for the new Child SA. It omits the SA and TS payloads. If the Child SA being rekeyed was negotiated with Perfect Forward Secrecy (PFS), a KEi payload is included as well. If no PFS was negotiated for the Child SA being rekeyed, a KEi payload is not included. If the Child SA being rekeyed was created with IP compression, then IPCOMP_SUPPORTED notifications MUST be sent as they contain the required updated Compression Parameter Indexes (CPIs).

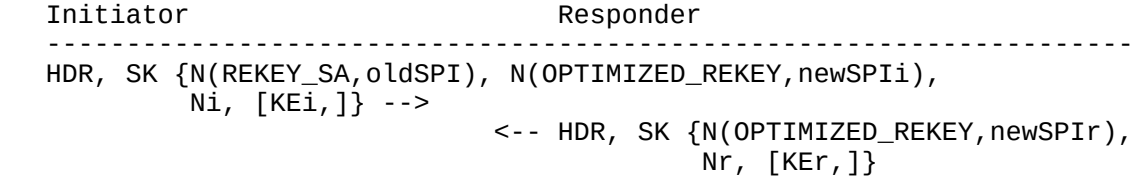
The responder of an optimized rekey request performs the same process. It includes the OPTIMIZED_REKEY notify with its new SPI for the new Child SA and omits the SA and TS payloads. Depending on the PFS and IP compression negotiation of the Child SA being rekeyed, the responder correspondingly includes a KEr payload and/or the IPCOMP_SUPPORTED Notify 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.

Except for the key and identification information such as the SPI and CPI, all other properties of the Child SA being rekeyed MUST be inherited to the one newly created by the optimized rekey. Notify payloads that can affect these properties, such as USE_TRANSPORT_MODE, ESP_TFC_PADDING_NOT_SUPPORTED, ROHC_SUPPORTED [RFC5857] or USE_AGGFRAG [RFC9347] MUST NOT be sent. In contrast, the Post-quantum Preshared Keys (PPKs) defined in [I-D.ietf-ipsecme-ikev2-qr-alt] can be considered as part of the key information since they are used in the session keys calculations, therefore, the PPKs negotiation MUST be included in the optimized Child SA rekey if [I-D.ietf-ipsecme-ikev2-qr-alt] are used.

The CREATE_CHILD_SA message exchange in this case is shown below:



If a responder fails to process the optimized rekey request because for some reasons it cannot re-use SA parameters for the SA being rekeyed (e.g., there is a change in the responder's configuration), it MUST return an error as the notification of type NO_PROPOSAL_CHOSEN. After receiving the error response of the optimized rekey, the initiator can retry a regular rekey.

5.1. Optimized Rekey of the Initial Child SA

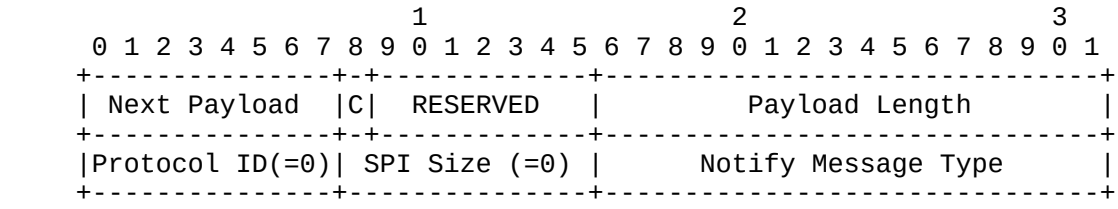
For the initial Child SA that was negotiated as part of an initial IKE exchange (e.g., IKE_AUTH), at the time of its creation the parameters of PFS and KE method(s) for Child SAs are not negotiated. However, [I-D.pwouters-ipsecme-child-pfs-info] provides a mechanism to negotiate these parameters during the creation of the initial Child SA.

If both peers support and use [I-D.pwouters-ipsecme-child-pfs-info], the PFS policy and KE method(s) for the initial Child SA is known during its creation. Therefore, in this situation, when rekeying the initial Child SA for the first time, the optimized way SHOULD be used. If [I-D.pwouters-ipsecme-child-pfs-info] is not supported or used, a regular rekey MUST be used for the first time to negotiate these parameters. Then, the next rekey can use the optimized way.

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.



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

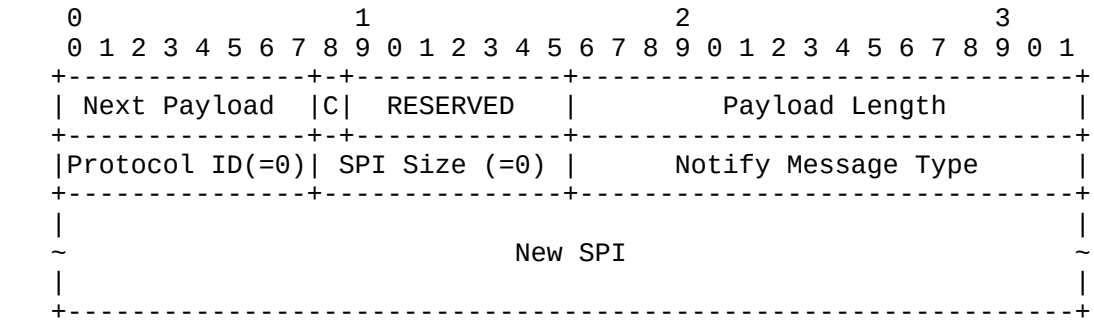
* SPI Size (1 octet) - MUST be 0, meaning no SPI is present.

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

This Notify Message type contains no data.

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) - MUST be 0.

* SPI Size (1 octet) - MUST be 0. The "Security Parameter Index (SPI)" field is not used in this Notify, and the new SPI is placed in the "Notification Data" field.

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

The Notification Data for this notify contains new SPI. Its size depends on the type of SA being rekeyed. In case of IKE SA it MUST be 8 octets. In case of Child SA it MUST be equal to the SPI Size field in the REKEY_SA notification that identifies the SA being rekeyed.

7. Interaction with IKEv2 Extensions

7.1. Multiple Key Exchanges

[RFC9370] defines the use of multiple key exchange methods for the purpose of IKE SA and Child SA establishment in IKEv2. If multiple key exchange methods are used for an SA, then optimized rekey of this SA MUST use the same key exchange methods. It means that the CREATE_CHILD_SA will be followed by some IKE_FOLLOWUP_KE exchanges and the number of these exchanges will be determined by the number of additional key exchange methods used for the SA being rekeyed.

7.2. IKE Session Resumption

IKE Session Resumption [RFC5723] defines an IKEv2 extension, that allows peers to quickly restore IKE SA when it is for some reason deleted. When used with optimized rekey, the following rules apply.

* Support for optimized rekeys MUST be re-negotiated during the resumption (in the IKE_AUTH exchange).

* If support for optimized rekey is negotiated during resumption, then all IKE SA algorithms, including key exchange methods, are taken from the resumption ticket (i.e., from the SA being resumed), since they are not negotiated in the IKE_SA_RESUME exchange.

* The initial Child SA created during the resumption is considered as been created with key exchange methods for the IKE SA, that were stored in the resumption ticket. This is despite the fact, that during the resumption no key exchanges (e.g., Diffie-Hellman) take place, the session keys are derived from the keys stored in the resumption ticket.

7.3. Mixing Preshared Keys in the CREATE_CHILD_SA Exchanges

[I-D.ietf-ipsecme-ikev2-qr-alt] defines how PPKs can be mixed into the session keys calculations. In particular, this document allows PPKs to be used in the CREATE_CHILD_SA exchanges when SAs are being rekeyed. If peers support [I-D.ietf-ipsecme-ikev2-qr-alt] and a PPK was used for the SA being rekeyed, then they MUST NOT silently re-use this PPK in case of optimized rekey and MUST re-negotiate the use of PPKs in the CREATE_CHILD_SA exchange.

8. 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

9. 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. But if there is a configuration change that changes the Traffic Selectors, cryptographic parameters, or other properties of the SA, the regular rekey should be used to make the configuration change active, since the optimized rekey can’t express such changes.

Two peers MUST have the same PFS policy and contain mutally acceptable KE method(s), otherwise, the rekey (regardless of regular or optimized way) of the initial Child SA created in the IKE_AUTH exchange would fail. This issue is also discussed in detail in [I-D.pwouters-ipsecme-child-pfs-info].

10. 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.

11. Acknowledgments

Special thanks go to Antony Antony and Tobias Brunner.

12. References

12.1. Normative References

[I-D.ietf-ipsecme-ikev2-qr-alt]
Smyslov, V., "Mixing Preshared Keys in the IKE_INTERMEDIATE and in the CREATE_CHILD_SA Exchanges of IKEv2 for Post-quantum Security", Work in Progress, Internet-Draft, draft-ietf-ipsecme-ikev2-qr-alt-10, 23 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-qr-alt-10>.

[I-D.pwouters-ipsecme-child-pfs-info]
Wouters, P., "IKEv2 support for Child SA PFS policy notification", Work in Progress, Internet-Draft, draft-pwouters-ipsecme-child-pfs-info-01, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-pwouters-ipsecme-child-pfs-info-01>.

[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/rfc/rfc2119>.

[RFC5723] Sheffer, Y. and H. Tschofenig, "Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption", RFC 5723, DOI 10.17487/RFC5723, January 2010, <https://www.rfc-editor.org/rfc/rfc5723>.

[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/rfc/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/rfc/rfc8174>.

[RFC9370] Tjhai, CJ., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9370, DOI 10.17487/RFC9370, May 2023, <https://www.rfc-editor.org/rfc/rfc9370>.

12.2. Informative References

[RFC5857] Ertekin, E., Christou, C., Jasani, R., Kivinen, T., and C. Bormann, "IKEv2 Extensions to Support Robust Header Compression over IPsec", RFC 5857, DOI 10.17487/RFC5857, May 2010, <https://www.rfc-editor.org/rfc/rfc5857>.

[RFC9347] Hopps, C., "Aggregation and Fragmentation Mode for Encapsulating Security Payload (ESP) and Its Use for IP Traffic Flow Security (IP-TFS)", RFC 9347, DOI 10.17487/RFC9347, January 2023, <https://www.rfc-editor.org/rfc/rfc9347>.

Authors' Addresses

Sandeep Kampati
Microsoft
India
Email: skampati@microsoft.com

Wei Pan
Huawei Technologies
101 Software Avenue, Yuhuatai District
Nanjing
Jiangsu,
China
Email: william.panwei@huawei.com

Paul Wouters
Aiven
Email: paul.wouters@aiven.io

Meduri S S Bharath
Mavenir Systems Pvt Ltd
Manyata Tech Park
Bangalore
Karnataka
India
Email: bharath.meduri@mavenir.com

Meiling Chen
China Mobile
32 Xuanwumen West Street, West District
Beijing
100053
China
Email: chenmeiling@chinamobile.com

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd)
124460
Russian Federation
Phone: +7 495 276 0211
Email: svan@elvis.ru