

Internet Engineering Task Force  
Internet-Draft  
Intended status: Standards Track  
Expires: July 17, 2020

S. Fluhrer  
P. Kampanakis  
D. McGrew  
Cisco Systems  
V. Smyslov  
ELVIS-PLUS  
January 14, 2020

**Mixing Preshared Keys in IKEv2 for Post-quantum Security**  
**draft-ietf-ipsecme-qr-ikev2-11**

**Abstract**

The possibility of quantum computers poses a serious challenge to cryptographic algorithms deployed widely today. IKEv2 is one example of a cryptosystem that could be broken; someone storing VPN communications today could decrypt them at a later time when a quantum computer is available. It is anticipated that IKEv2 will be extended to support quantum-secure key exchange algorithms; however that is not likely to happen in the near term. To address this problem before then, this document describes an extension of IKEv2 to allow it to be resistant to a quantum computer, by using preshared keys.

**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 July 17, 2020.

**Copyright Notice**

Copyright (c) 2020 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Changes . . . . .	<a href="#">3</a>
<a href="#">1.2.</a>	Requirements Language . . . . .	<a href="#">6</a>
<a href="#">2.</a>	Assumptions . . . . .	<a href="#">6</a>
<a href="#">3.</a>	Exchanges . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Upgrade procedure . . . . .	<a href="#">11</a>
<a href="#">5.</a>	PPK . . . . .	<a href="#">12</a>
<a href="#">5.1.</a>	PPK_ID format . . . . .	<a href="#">12</a>
<a href="#">5.2.</a>	Operational Considerations . . . . .	<a href="#">13</a>
<a href="#">5.2.1.</a>	PPK Distribution . . . . .	<a href="#">13</a>
<a href="#">5.2.2.</a>	Group PPK . . . . .	<a href="#">13</a>
<a href="#">5.2.3.</a>	PPK-only Authentication . . . . .	<a href="#">14</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">14</a>
<a href="#">7.</a>	IANA Considerations . . . . .	<a href="#">16</a>
<a href="#">8.</a>	References . . . . .	<a href="#">17</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">17</a>
<a href="#">8.2.</a>	Informational References . . . . .	<a href="#">18</a>
<a href="#">Appendix A.</a>	Discussion and Rationale . . . . .	<a href="#">19</a>
<a href="#">Appendix B.</a>	Acknowledgements . . . . .	<a href="#">20</a>
	Authors' Addresses . . . . .	<a href="#">20</a>

## [1.](#) Introduction

Recent achievements in developing quantum computers demonstrate that it is probably feasible to build a cryptographically significant one. If such a computer is implemented, many of the cryptographic algorithms and protocols currently in use would be insecure. A quantum computer would be able to solve DH and ECDH problems in polynomial time [[I-D.hoffman-c2pq](#)], and this would imply that the security of existing IKEv2 [[RFC7296](#)] systems would be compromised. IKEv1 [[RFC2409](#)], when used with strong preshared keys, is not vulnerable to quantum attacks, because those keys are one of the inputs to the key derivation function. If the preshared key has sufficient entropy and the PRF, encryption and authentication transforms are quantum-secure, then the resulting system is believed



to be quantum-secure, that is, secure against classical attackers of today or future attackers with a quantum computer.

This document describes a way to extend IKEv2 to have a similar property; assuming that the two end systems share a long secret key, then the resulting exchange is quantum-secure. By bringing post-quantum security to IKEv2, this document removes the need to use an obsolete version of the Internet Key Exchange in order to achieve that security goal.

The general idea is that we add an additional secret that is shared between the initiator and the responder; this secret is in addition to the authentication method that is already provided within IKEv2. We stir this secret into the SK\_d value, which is used to generate the key material (KEYMAT) and the SKEYSEED for the child SAs; this secret provides quantum resistance to the IPsec SAs (and any child IKE SAs). We also stir the secret into the SK\_pi, SK\_pr values; this allows both sides to detect a secret mismatch cleanly.

It was considered important to minimize the changes to IKEv2. The existing mechanisms to do authentication and key exchange remain in place (that is, we continue to do (EC)DH, and potentially PKI authentication if configured). This document does not replace the authentication checks that the protocol does; instead, they are strengthened by using an additional secret key.

### **1.1. Changes**

RFC EDITOR PLEASE DELETE THIS SECTION.

Changes in this draft in each version iterations.

[draft-ietf-ipsecme-qr-ikev2-11](#)

- o Updates the IANA section based on Eric V.'s IESG Review.
- o Updates based on IESG Reviews (Alissa, Adam, Barry, Alexey, Mijra, Roman, Martin).

[draft-ietf-ipsecme-qr-ikev2-10](#)

- o Addresses issues raised during IETF LC.

[draft-ietf-ipsecme-qr-ikev2-09](#)

- o Addresses issues raised in AD review.

[draft-ietf-ipsecme-qr-ikev2-08](#)



- o Editorial changes.

[draft-ietf-ipsecme-qr-ikev2-07](#)

- o Editorial changes.

[draft-ietf-ipsecme-qr-ikev2-06](#)

- o Editorial changes.

[draft-ietf-ipsecme-qr-ikev2-05](#)

- o Addressed comments received during WGLC.

[draft-ietf-ipsecme-qr-ikev2-04](#)

- o Using Group PPK is clarified based on comment from Quynh Dang.

[draft-ietf-ipsecme-qr-ikev2-03](#)

- o Editorial changes and minor text nit fixes.

- o Integrated Tommy P. text suggestions.

[draft-ietf-ipsecme-qr-ikev2-02](#)

- o Added note that the PPK is stirred in the initial IKE SA setup only.

- o Added note about the initiator ignoring any content in the PPK\_IDENTITY notification from the responder.

- o fixed Tero's suggestions from 2/6/1028

- o Added IANA assigned message types where necessary.

- o fixed minor text nits

[draft-ietf-ipsecme-qr-ikev2-01](#)

- o Nits and minor fixes.

- o prf is replaced with prf+ for the SK\_d and SK\_pi/r calculations.

- o Clarified using PPK in case of EAP authentication.

- o PPK\_SUPPORT notification is changed to USE\_PPK to better reflect its purpose.



[draft-ietf-ipsecme-qr-ikev2-00](#)

- o Migrated from [draft-fluhrer-qr-ikev2-05](#) to [draft-ietf-ipsecme-qr-ikev2-00](#) that is a WG item.

[draft-fluhrer-qr-ikev2-05](#)

- o Nits and editorial fixes.
- o Made PPK\_ID format and PPK Distributions subsection of the PPK section. Also added an Operational Considerations section.
- o Added comment about Child SA rekey in the Security Considerations section.
- o Added NO\_PPK\_AUTH to solve the cases where a PPK\_ID is not configured for a responder.
- o Various text changes and clarifications.
- o Expanded Security Considerations section to describe some security concerns and how they should be addressed.

[draft-fluhrer-qr-ikev2-03](#)

- o Modified how we stir the PPK into the IKEv2 secret state.
- o Modified how the use of PPKs is negotiated.

[draft-fluhrer-qr-ikev2-02](#)

- o Simplified the protocol by stirring in the preshared key into the child SAs; this avoids the problem of having the responder decide which preshared key to use (as it knows the initiator identity at that point); it does mean that someone with a quantum computer can recover the initial IKE negotiation.
- o Removed positive endorsements of various algorithms. Retained warnings about algorithms known to be weak against a quantum computer.

[draft-fluhrer-qr-ikev2-01](#)

- o Added explicit guidance as to what IKE and IPsec algorithms are quantum resistant.

[draft-fluhrer-qr-ikev2-00](#)





- o We switched from using vendor ID's to transmit the additional data to notifications.
- o We added a mandatory cookie exchange to allow the server to communicate to the client before the initial exchange.
- o We added algorithm agility by having the server tell the client what algorithm to use in the cookie exchange.
- o We have the server specify the PPK Indicator Input, which allows the server to make a trade-off between the efficiency for the search of the clients PPK, and the anonymity of the client.
- o We now use the negotiated PRF (rather than a fixed HMAC-SHA256) to transform the nonces during the KDF.

### **1.2. 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.

## **2. Assumptions**

We assume that each IKE peer has a list of Post-quantum Preshared Keys (PPK) along with their identifiers (PPK\_ID), and any potential IKE initiator selects which PPK to use with any specific responder. In addition, implementations have a configurable flag that determines whether this post-quantum preshared key is mandatory. This PPK is independent of the preshared key (if any) that the IKEv2 protocol uses to perform authentication (because the preshared key in IKEv2 is not used for any key derivation, and thus doesn't protect against quantum computers). The PPK specific configuration that is assumed to be on each node consists of the following tuple:

Peer, PPK, PPK\_ID, mandatory\_or\_not

## **3. Exchanges**

If the initiator is configured to use a post-quantum preshared key with the responder (whether or not the use of the PPK is mandatory), then it MUST include a notification USE\_PPK in the IKE\_SA\_INIT request message as follows:



If the responder did include the USE\_PPK notification, then the initiator selects a PPK, along with its identifier PPK\_ID. Then, it computes this modification of the standard IKEv2 key derivation from [Section 2.14 of \[RFC7296\]](#):



```

SKEYSEED = prf(Ni | Nr, g^air)
{SK_d' | SK_ai | SK_ar | SK_ei | SK_er | SK_pi' | SK_pr' }
      = prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr }

```

```

SK_d  = prf+ (PPK, SK_d')
SK_pi = prf+ (PPK, SK_pi')
SK_pr = prf+ (PPK, SK_pr')

```

That is, we use the standard IKEv2 key derivation process except that the three resulting subkeys SK\_d, SK\_pi, SK\_pr (marked with primes in the formula above) are then run through the prf+ again, this time using the PPK as the key. The result is the unprimed versions of these keys which are then used as inputs to subsequent steps of the IKEv2 exchange.

Using a prf+ construction ensures that it is always possible to get the resulting keys of the same size as the initial ones, even if the underlying PRF has output size different from its key size. Note, that at the time of this writing, all PRFs defined for use in IKEv2 [[IKEV2-IANA-PRFS](#)] had output size equal to the (preferred) key size. For such PRFs only the first iteration of prf+ is needed:

```

SK_d  = prf (PPK, SK_d' | 0x01)
SK_pi = prf (PPK, SK_pi' | 0x01)
SK_pr = prf (PPK, SK_pr' | 0x01)

```

Note that the PPK is used in SK\_d, SK\_pi and SK\_pr calculation only during the initial IKE SA setup. It MUST NOT be used when these subkeys are calculated as result of IKE SA rekey, resumption or other similar operation.

The initiator then sends the IKE\_AUTH request message, including the PPK\_ID value as follows:

Initiator	Responder
-----	
HDR, SK {IDi, [CERT,] [CERTREQ,]	
[IDr,] AUTH, SAi2,	
TSi, TSr, N(PPK_IDENTITY, PPK_ID), [N(NO_PPK_AUTH)]} --->	

PPK\_IDENTITY is a status notification with the type 16436; it has a protocol ID of 0, no SPI and a notification data that consists of the identifier PPK\_ID.

A situation may happen when the responder has some PPKs, but doesn't have a PPK with the PPK\_ID received from the initiator. In this case the responder cannot continue with PPK (in particular, it cannot authenticate the initiator), but the responder could be able to



continue with normal IKEv2 protocol if the initiator provided its authentication data computed as in normal IKEv2, without using PPKs. For this purpose, if using PPKs for communication with this responder is optional for the initiator (based on the mandatory\_or\_not flag), then the initiator MUST include a NO\_PPK\_AUTH notification in the above message. This notification informs the responder that PPK is optional and allows for authenticating the initiator without using PPK.

NO\_PPK\_AUTH is a status notification with the type 16437; it has a protocol ID of 0 and no SPI. The Notification Data field contains the initiator's authentication data computed using SK\_pi', which has been computed without using PPKs. This is the same data that would normally be placed in the Authentication Data field of an AUTH payload. Since the Auth Method field is not present in the notification, the authentication method used for computing the authentication data MUST be the same as method indicated in the AUTH payload. Note that if the initiator decides to include the NO\_PPK\_AUTH notification, the initiator needs to perform authentication data computation twice, which may consume computation power (e.g., if digital signatures are involved).

When the responder receives this encrypted exchange, it first computes the values:

```
SKEYSEED = prf(Ni | Nr, g^air)
{SK_d' | SK_ai | SK_ar | SK_ei | SK_er | SK_pi' | SK_pr' }
    = prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr )
```

The responder then uses the SK\_ei/SK\_ai values to decrypt/check the message and then scans through the payloads for the PPK\_ID attached to the PPK\_IDENTITY notification. If no PPK\_IDENTITY notification is found and the peers successfully exchanged USE\_PPK notifications in the IKE\_SA\_INIT exchange, then the responder MUST send back AUTHENTICATION\_FAILED notification and then fail the negotiation.

If the PPK\_IDENTITY notification contains a PPK\_ID that is not known to the responder or is not configured for use for the identity from IDi payload, then the responder checks whether using PPKs for this initiator is mandatory and whether the initiator included NO\_PPK\_AUTH notification in the message. If using PPKs is mandatory or no NO\_PPK\_AUTH notification is found, then the responder MUST send back AUTHENTICATION\_FAILED notification and then fail the negotiation. Otherwise (when PPK is optional and the initiator included NO\_PPK\_AUTH notification) the responder MAY continue regular IKEv2 protocol, except that it uses the data from the NO\_PPK\_AUTH notification as the authentication data (which usually resides in the AUTH payload), for the purpose of the initiator authentication.





Note, that Authentication Method is still indicated in the AUTH payload.

This table summarizes the above logic for the responder:

Received USE_PPK	Received NO_PPK_AUTH	Configured with PPK	PPK is Mandatory	Action
No	*	No	*	Standard IKEv2 protocol
No	*	Yes	No	Standard IKEv2 protocol
No	*	Yes	Yes	Abort negotiation
Yes	No	No	*	Abort negotiation
Yes	Yes	No	Yes	Abort negotiation
Yes	Yes	No	No	Standard IKEv2 protocol
Yes	*	Yes	*	Use PPK

If PPK is in use, then the responder extracts the corresponding PPK and computes the following values:

```
SK_d  = prf+ (PPK, SK_d')
SK_pi = prf+ (PPK, SK_pi')
SK_pr = prf+ (PPK, SK_pr')
```

The responder then continues with the IKE\_AUTH exchange (validating the AUTH payload that the initiator included) as usual and sends back a response, which includes the PPK\_IDENTITY notification with no data to indicate that the PPK is used in the exchange:

Initiator	Responder
-----	
	<-- HDR, SK {IDr, [CERT, AUTH, SAR2, TSi, TSr, N(PPK_IDENTITY)}

When the initiator receives the response, then it checks for the presence of the PPK\_IDENTITY notification. If it receives one, it marks the SA as using the configured PPK to generate SK\_d, SK\_pi, SK\_pr (as shown above); the content of the received PPK\_IDENTITY (if any) MUST be ignored. If the initiator does not receive the PPK\_IDENTITY, it MUST either fail the IKE SA negotiation sending the AUTHENTICATION\_FAILED notification in the Informational exchange (if the PPK was configured as mandatory), or continue without using the PPK (if the PPK was not configured as mandatory and the initiator included the NO\_PPK\_AUTH notification in the request).

If EAP is used in the IKE\_AUTH exchange, then the initiator doesn't include AUTH payload in the first request message, however the responder sends back AUTH payload in the first reply. The peers then



exchange AUTH payloads after EAP is successfully completed. As a result, the responder sends AUTH payload twice - in the first IKE\_AUTH reply message and in the last one, while the initiator sends AUTH payload only in the last IKE\_AUTH request. See more details about EAP authentication in IKEv2 in [Section 2.16 of \[RFC7296\]](#).

The general rule for using PPK in the IKE\_AUTH exchange, which covers EAP authentication case too, is that the initiator includes PPK\_IDENTITY (and optionally NO\_PPK\_AUTH) notification in the request message containing AUTH payload. Therefore, in case of EAP the responder always computes the AUTH payload in the first IKE\_AUTH reply message without using PPK (by means of SK<sub>pr'</sub>), since PPK\_ID is not yet known to the responder. Once the IKE\_AUTH request message containing the PPK\_IDENTITY notification is received, the responder follows the rules described above for the non-EAP authentication case.

Initiator	Responder
-----	
HDR, SK {IDi, [CERTREQ, [IDr,] SAi2, TSi, TSr]} -->	<-- HDR, SK {IDr, [CERT,] AUTH, EAP}
HDR, SK {EAP} -->	<-- HDR, SK {EAP (success)}
HDR, SK {AUTH, N(PPK_IDENTITY, PPK_ID) [, N(NO_PPK_AUTH)]} -->	<-- HDR, SK {AUTH, SAR2, TSi, TSr [, N(PPK_IDENTITY)]}

Note that the diagram above shows both the cases when the responder uses PPK and when it chooses not to use it (provided the initiator has included NO\_PPK\_AUTH notification), and thus the responder's PPK\_IDENTITY notification is marked as optional. Also, note that the IKE\_SA\_INIT exchange in case of PPK is as described above (including exchange of the USE\_PPK notifications), regardless whether EAP is employed in the IKE\_AUTH or not.

#### **4. Upgrade procedure**

This algorithm was designed so that someone can introduce PPKs into an existing IKE network without causing network disruption.

In the initial phase of the network upgrade, the network administrator would visit each IKE node, and configure:



- o The set of PPKs (and corresponding PPK\_IDs) that this node would need to know.
- o For each peer that this node would initiate to, which PPK will be used.
- o That the use of PPK is currently not mandatory.

With this configuration, the node will continue to operate with nodes that have not yet been upgraded. This is due to the USE\_PPK notification and the NO\_PPK\_AUTH notification; if the initiator has not been upgraded, it will not send the USE\_PPK notification (and so the responder will know that the peers will not use a PPK). If the responder has not been upgraded, it will not send the USE\_PPK notification (and so the initiator will know to not use a PPK). If both peers have been upgraded, but the responder isn't yet configured with the PPK for the initiator, then the responder could do standard IKEv2 protocol if the initiator sent NO\_PPK\_AUTH notification. If both the responder and initiator have been upgraded and properly configured, they will both realize it, and the Child SAs will be quantum-secure.

As an optional second step, after all nodes have been upgraded, then the administrator should then go back through the nodes, and mark the use of PPK as mandatory. This will not affect the strength against a passive attacker, but it would mean that an active attacker with a quantum computer (which is sufficiently fast to be able to break the (EC)DH in real-time) would not be able to perform a downgrade attack.

## **5. PPK**

### **5.1. PPK\_ID format**

This standard requires that both the initiator and the responder have a secret PPK value, with the responder selecting the PPK based on the PPK\_ID that the initiator sends. In this standard, both the initiator and the responder are configured with fixed PPK and PPK\_ID values, and do the look up based on PPK\_ID value. It is anticipated that later specifications will extend this technique to allow dynamically changing PPK values. To facilitate such an extension, we specify that the PPK\_ID the initiator sends will have its first octet be the PPK\_ID Type value. This document defines two values for PPK\_ID Type:

- o PPK\_ID\_OPAQUE (1) - for this type the format of the PPK\_ID (and the PPK itself) is not specified by this document; it is assumed to be mutually intelligible by both by initiator and the



responder. This PPK\_ID type is intended for those implementations that choose not to disclose the type of PPK to active attackers.

- o PPK\_ID\_FIXED (2) - in this case the format of the PPK\_ID and the PPK are fixed octet strings; the remaining bytes of the PPK\_ID are a configured value. We assume that there is a fixed mapping between PPK\_ID and PPK, which is configured locally to both the initiator and the responder. The responder can use the PPK\_ID to look up the corresponding PPK value. Not all implementations are able to configure arbitrary octet strings; to improve the potential interoperability, it is recommended that, in the PPK\_ID\_FIXED case, both the PPK and the PPK\_ID strings be limited to the Base64 character set [[RFC4648](#)].

## **5.2. Operational Considerations**

The need to maintain several independent sets of security credentials can significantly complicate a security administrator's job, and can potentially slow down widespread adoption of this specification. It is anticipated, that administrators will try to simplify their job by decreasing the number of credentials they need to maintain. This section describes some of the considerations for PPK management.

### **5.2.1. PPK Distribution**

PPK\_IDs of the type PPK\_ID\_FIXED (and the corresponding PPKs) are assumed to be configured within the IKE device in an out-of-band fashion. While the method of distribution is a local matter and out of scope of this document or IKEv2, [[RFC6030](#)] describes a format for the transport and provisioning of symmetric keys. That format could be reused using the PIN profile (defined in [Section 10.2 of \[\[RFC6030\]\(#\)\]](#)) with the "Id" attribute of the <Key> element being the PPK\_ID (without the PPK\_ID Type octet for a PPK\_ID\_FIXED) and the <Secret> element containing the PPK.

### **5.2.2. Group PPK**

This document doesn't explicitly require that PPK is unique for each pair of peers. If it is the case, then this solution provides full peer authentication, but it also means that each host must have as many independent PPKs as the peers it is going to communicate with. As the number of peers grows the PPKs will not scale.

It is possible to use a single PPK for a group of users. Since each peer uses classical public key cryptography in addition to PPK for key exchange and authentication, members of the group can neither impersonate each other nor read other's traffic, unless they use quantum computers to break public key operations. However group





members can record any traffic they have access to that comes from other group members and decrypt it later, when they get access to a quantum computer.

In addition, the fact that the PPK is known to a (potentially large) group of users makes it more susceptible to theft. When an attacker equipped with a quantum computer gets access to a group PPK, all communications inside the group are revealed.

For these reasons using group PPK is NOT RECOMMENDED.

### **5.2.3. PPK-only Authentication**

If quantum computers become a reality, classical public key cryptography will provide little security, so administrators may find it attractive not to use it at all for authentication. This will reduce the number of credentials they need to maintain to PPKs only. Combining group PPK and PPK-only authentication is NOT RECOMMENDED, since in this case any member of the group can impersonate any other member even without help of quantum computers.

PPK-only authentication can be achieved in IKEv2 if the NULL Authentication method [[RFC7619](#)] is employed. Without PPK the NULL Authentication method provides no authentication of the peers, however since a PPK is stirred into the SK\_pi and the SK\_pr, the peers become authenticated if a PPK is in use. Using PPKs MUST be mandatory for the peers if they advertise support for PPK in IKE\_SA\_INIT and use NULL Authentication. Additionally, since the peers are authenticated via PPK, the ID Type in the IDi/IDr payloads SHOULD NOT be ID\_NULL, despite using the NULL Authentication method.

## **6. Security Considerations**

Quantum computers are able to perform Grover's algorithm [[GROVER](#)]; that effectively halves the size of a symmetric key. Because of this, the user SHOULD ensure that the post-quantum preshared key used has at least 256 bits of entropy, in order to provide 128 bits of post-quantum security. That provides security equivalent to Level 5 as defined in the NIST PQ Project Call For Proposals [[NISTPQCFP](#)].

With this protocol, the computed SK\_d is a function of the PPK. Assuming that the PPK has sufficient entropy (for example, at least  $2^{256}$  possible values), then even if an attacker was able to recover the rest of the inputs to the PRF function, it would be infeasible to use Grover's algorithm with a quantum computer to recover the SK\_d value. Similarly, all keys that are a function of SK\_d, which include all Child SAs keys and all keys for subsequent IKE SAs (created when the initial IKE SA is rekeyed), are also quantum-secure



(assuming that the PPK was of high enough entropy, and that all the subkeys are sufficiently long).

An attacker with a quantum computer that can decrypt the initial IKE SA has access to all the information exchanged over it, such as identities of the peers, configuration parameters and all negotiated IPsec SAs information (including traffic selectors), with the exception of the cryptographic keys used by the IPsec SAs which are protected by the PPK.

Deployments that treat this information as sensitive or that send other sensitive data (like cryptographic keys) over IKE SA MUST rekey the IKE SA before the sensitive information is sent to ensure this information is protected by the PPK. It is possible to create a childless IKE SA as specified in [\[RFC6023\]](#). This prevents Child SA configuration information from being transmitted in the original IKE SA that is not protected by a PPK. Some information related to IKE SA, that is sent in the IKE\_AUTH exchange, such as peer identities, feature notifications, Vendor ID's etc. cannot be hidden from the attack described above, even if the additional IKE SA rekey is performed.

In addition, the policy SHOULD be set to negotiate only quantum-secure symmetric algorithms; while this RFC doesn't claim to give advice as to what algorithms are secure (as that may change based on future cryptographical results), below is a list of defined IKEv2 and IPsec algorithms that should not be used, as they are known to provide less than 128 bits of post-quantum security

- o Any IKEv2 Encryption algorithm, PRF or Integrity algorithm with key size less than 256 bits.
- o Any ESP Transform with key size less than 256 bits.
- o PRF\_AES128\_XCBC and PRF\_AES128\_CBC; even though they are defined to be able to use an arbitrary key size, they convert it into a 128-bit key internally.

[Section 3](#) requires the initiator to abort the initial exchange if using PPKs is mandatory for it, but the responder does not include the USE\_PPK notification in the response. In this situation, when the initiator aborts negotiation it leaves a half-open IKE SA on the responder (because IKE\_SA\_INIT completes successfully from the responder's point of view). This half-open SA will eventually expire and be deleted, but if the initiator continues its attempts to create IKE SA with a high enough rate, then the responder may consider it as a Denial-of-Service (DoS) attack and take protection measures (see [\[RFC8019\]](#) for more detail). In this situation, it is RECOMMENDED



that the initiator caches the negative result of the negotiation and doesn't make attempts to create it again for some time. This period of time may vary, but it is believed that waiting for at least few minutes will not cause the responder to treat it as DoS attack. Note, that this situation would most likely be a result of misconfiguration and some re-configuration of the peers would probably be needed.

If using PPKs is optional for both peers and they authenticate themselves using digital signatures, then an attacker in between, equipped with a quantum computer capable of breaking public key operations in real time, is able to mount downgrade attack by removing USE\_PPK notification from the IKE\_SA\_INIT and forging digital signatures in the subsequent exchange. If using PPKs is mandatory for at least one of the peers or PSK is used for authentication, then the attack will be detected and the SA won't be created.

If using PPKs is mandatory for the initiator, then an attacker able to eavesdrop and to inject packets into the network can prevent creating an IKE SA by mounting the following attack. The attacker intercepts the initial request containing the USE\_PPK notification and injects a forged response containing no USE\_PPK. If the attacker manages to inject this packet before the responder sends a genuine response, then the initiator would abort the exchange. To thwart this kind of attack it is RECOMMENDED, that if using PPKs is mandatory for the initiator and the received response doesn't contain the USE\_PPK notification, then the initiator doesn't abort the exchange immediately. Instead it waits for more response messages retransmitting the request as if no responses were received at all, until either the received message contains the USE\_PPK or the exchange times out (see [section 2.4 of \[RFC7296\]](#) for more details about retransmission timers in IKEv2). If neither of the received responses contains USE\_PPK, then the exchange is aborted.

If using PPK is optional for both peers, then in case of misconfiguration (e.g., mismatched PPK\_ID) the IKE SA will be created without protection against quantum computers. It is advised that if PPK was configured, but was not used for a particular IKE SA, then implementations SHOULD audit this event.

## **7. IANA Considerations**

This document defines three new Notify Message Types in the "Notify Message Types - Status Types" registry

(<https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-16>):



16435	USE_PPK	[THIS RFC]
16436	PPK_IDENTITY	[THIS RFC]
16437	NO_PPK_AUTH	[THIS RFC]

This document also creates a new IANA registry "IKEv2 Post-quantum Preshared Key ID Types" in IKEv2 IANA registry (<https://www.iana.org/assignments/ikev2-parameters/>) for the PPK\_ID types used in the PPK\_IDENTITY notification defined in this specification. The initial values of the new registry are:

PPK_ID Type	Value	Reference
-----	-----	-----
Reserved	0	[THIS RFC]
PPK_ID_OPAQUE	1	[THIS RFC]
PPK_ID_FIXED	2	[THIS RFC]
Unassigned	3-127	[THIS RFC]
Private Use	128-255	[THIS RFC]

The PPK\_ID type value 0 is reserved; values 3-127 are to be assigned by IANA; values 128-255 are for private use among mutually consenting parties. To register new PPK\_IDs in the unassigned range, a Type name, a Value between 3 and 127 and a Reference specification need to be defined. Changes and additions to the unassigned range of this registry are by the Expert Review Policy [[RFC8126](#)]. Changes and additions to the private use range of this registry are by the Private Use Policy [[RFC8126](#)].

## 8. References

### 8.1. 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>>.
- [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>>.





## 8.2. Informational References

- [GROVER] Grover, L., "A Fast Quantum Mechanical Algorithm for Database Search", Proc. of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (STOC 1996), 1996.
- [I-D.hoffman-c2pq]  
Hoffman, P., "The Transition from Classical to Post-Quantum Cryptography", [draft-hoffman-c2pq-06](#) (work in progress), November 2019.
- [IKEV2-IANA-PRFS]  
"Internet Key Exchange Version 2 (IKEv2) Parameters, Transform Type 2 - Pseudorandom Function Transform IDs", <<https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-6>>.
- [NISTPQCFP]  
NIST, "NIST Post-Quantum Cryptography Call for Proposals", 2016, <<https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf>>.
- [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>>.
- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", [RFC 4648](#), DOI 10.17487/RFC4648, October 2006, <<https://www.rfc-editor.org/info/rfc4648>>.
- [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>>.
- [RFC6030] Hoyer, P., Pei, M., and S. Machani, "Portable Symmetric Key Container (PSKC)", [RFC 6030](#), DOI 10.17487/RFC6030, October 2010, <<https://www.rfc-editor.org/info/rfc6030>>.
- [RFC7619] Smyslov, V. and P. Wouters, "The NULL Authentication Method in the Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 7619](#), DOI 10.17487/RFC7619, August 2015, <<https://www.rfc-editor.org/info/rfc7619>>.



- [RFC8019] Nir, Y. and V. Smyslov, "Protecting Internet Key Exchange Protocol Version 2 (IKEv2) Implementations from Distributed Denial-of-Service Attacks", [RFC 8019](#), DOI 10.17487/RFC8019, November 2016, <<https://www.rfc-editor.org/info/rfc8019>>.
- [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>>.

## **Appendix A. Discussion and Rationale**

The idea behind this document is that while a quantum computer can easily reconstruct the shared secret of an (EC)DH exchange, they cannot as easily recover a secret from a symmetric exchange. This document makes the SK\_d, and hence the IPsec KEYMAT and any child SA's SKEYSEED, depend on both the symmetric PPK, and also the Diffie-Hellman exchange. If we assume that the attacker knows everything except the PPK during the key exchange, and there are  $2^n$  plausible PPKs, then a quantum computer (using Grover's algorithm) would take  $O(2^{n/2})$  time to recover the PPK. So, even if the (EC)DH can be trivially solved, the attacker still can't recover any key material (except for the SK\_ei, SK\_er, SK\_ai and SK\_ar values for the initial IKE exchange) unless they can find the PPK, which is too difficult if the PPK has enough entropy (for example, 256 bits). Note that we do allow an attacker with a quantum computer to rederive the keying material for the initial IKE SA; this was a compromise to allow the responder to select the correct PPK quickly.

Another goal of this protocol is to minimize the number of changes within the IKEv2 protocol, and in particular, within the cryptography of IKEv2. By limiting our changes to notifications, and only adjusting the SK\_d, SK\_pi, SK\_pr, it is hoped that this would be implementable, even on systems that perform most of the IKEv2 processing in hardware.

A third goal was to be friendly to incremental deployment in operational networks, for which we might not want to have a global shared key, or quantum-secure IKEv2 is rolled out incrementally. This is why we specifically try to allow the PPK to be dependent on the peer, and why we allow the PPK to be configured as optional.

A fourth goal was to avoid violating any of the security properties provided by IKEv2.



## [Appendix B](#). Acknowledgements

We would like to thank Tero Kivinen, Paul Wouters, Graham Bartlett, Tommy Pauly, Quynh Dang and the rest of the IPSecME Working Group for their feedback and suggestions for the scheme.

### Authors' Addresses

Scott Fluhrer  
Cisco Systems

Email: [sfluhrer@cisco.com](mailto:sfluhrer@cisco.com)

Panos Kampanakis  
Cisco Systems

Email: [pkampana@cisco.com](mailto:pkampana@cisco.com)

David McGrew  
Cisco Systems

Email: [mcgrew@cisco.com](mailto:mcgrew@cisco.com)

Valery Smyslov  
ELVIS-PLUS

Phone: +7 495 276 0211  
Email: [svan@elvis.ru](mailto:svan@elvis.ru)

