Post-Quantum Use In Protocols
Internet-Draft
Intended status: Standards Track
Expires: 28 December 2025

L. Li
Huawei
F. Liu
Huawei Singapore

26 June 2025

PQC Escape Message for Dynamic Migration
draft-li-pquip-escape-message-01

Abstract

In this contribution, a design of escape message mechanism is proposed, where the service provider sends an escape message to the service consumer using existing non-PQC connection and then starts to re-establish the quantum-safe protocol. The proposed escape message can potentially be used in a variety of protocols, including IPsec, TLS, or between the air interface of a cellphone and a network device. We believe that for largely deployed networks and entities, escape messages can be provided as a plan B for always-live devices of service provider and consumer that cannot complete post-quantum migration in advance and mitigates negative impacts after potential Q-days occur. Different protocols and devices may be implemented escape mechanism in different sepcific ways.

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 28 December 2025.

Copyright Notice

Copyright (c) 2025 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

The post-quantum transition should be gradual in largely deployed networks and entities since one of the important feature of these networks such as telecom network is that a large number of legacy entities and devices have been deployed on the always-live network. Meanwhile, Crypto agility is a basic requirents including incident responses and disaster recovery plans for rapid algorithm and protocol swaps. The transition may cause complex effects in terms of confusing interfaces and reference point.

Considering the increased computational and payload burden of legacy equipment, many stakeholders may take risks and not be willing to embed a large number of equipments to complete the migration ahead of time. Considering billions of cellphones (aka., UE), hundreds of thousands of network entities, we propose to embed the post-quantum migration preparation gradually in advance, and to dynamically trigger and complete the post-quantum transition as required by extra messages and service mechanisms.

Therefore, regarding future quantum attacks (aka, Q-day attacks such as Shor's algorithm [shor]), one of the practical approaches is to notify entities to dynamically perform post-quantum using a new concept message, which we called the PQC escape message. The name was inspired by the history of ESC keys [ISO9995] in the keyboard, when ESC key is originally used for switching different mode in vi family [ESCKEY].

An PQC escape message should be sent in a proper procedure, for example, periodically or broadcast. In addition, except sending the escape message as a simply notification, it can also contain additional usage. It will be discussed in the session of the message design.

We believe that the need for escape messages exists widely in a variety of complex systems, not limit to largely deployed networks such as telecom networks. It is recommended to provide guidance of the format of the escape message. This concept is also important as the part of the cryptographic agility, different protocols and devices may be implemented in different sepcific ways.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. System Architecture

The PQC escape message should be deployed between the service provider and the consumer. In general, the service provider and consumer are only concepts, multiple servers or consumers are also supported as long as having an established secure connection (e.g., IPsec [RFC4301], TLS [RFC8446], etc.).

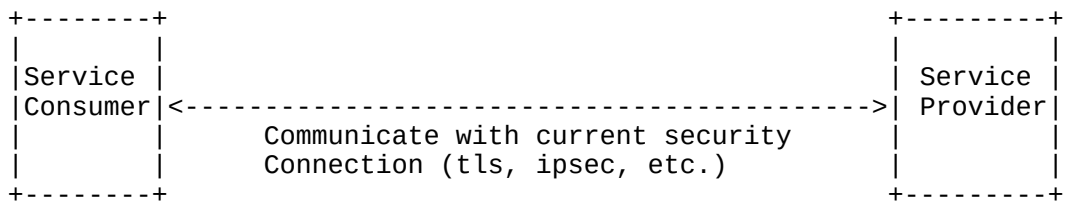

Figure 1 System architecture applied escape message

The service consumer for example can be a UE, an APP client, a security gateway. The service provider for example can be a network function, an APP server, or a security gateway.

4. Message and Mechanism Design

4.1. Requirements

Escape messages should be designed to be as simple and efficient between service providers and consumers. Some requirements are listed as follows:

* 1. the message shall be dedicated for instruction to complete a live quantum transition. A dedicated message format helps the device identify the message rapidly. In term of the implementation level, the device can enter a dedicated mode to improve the success rate and shorten the response time.

* 2. the escape message shall contain a common security protection design including the integrity protection. This prevents attackers from sending false indications and causing the device to enter the migration state accidently.

* 3. the message shall be a standardized message format. A pre-shared key may be configured on both sides of the device to be migrated, which can be used for the protection of migration and a furtherly negotiation a post-quantum algorithm key. The sepcific format can be discussed in dedicated working group which are not in the scope of this docuement.

The pre-shared key can be either a dedicated pre-shared key. Optionally, it can also be the symmetric (pre-shared) key already used in the currently connection of TLS or IPsec, etc. Specifically, the following two mode can be used as options.

4.2. Basic steps of escape message

From the perspective of IETF PQUIP and this use case, the following analysis can be considered.

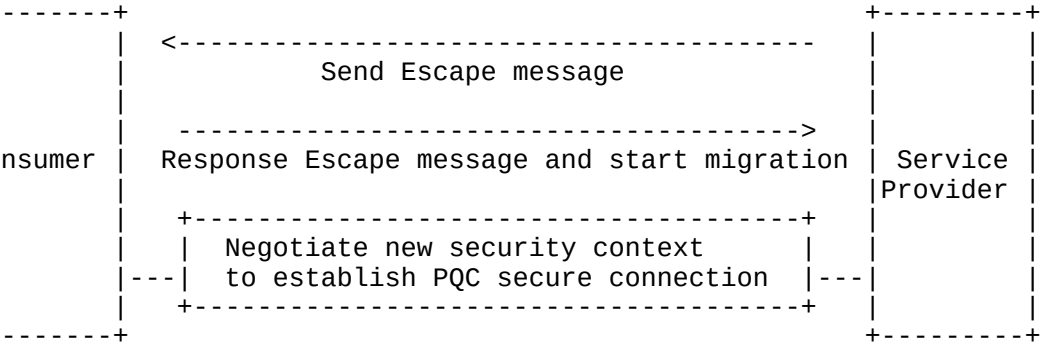

Figure 2. Basic steps of escape message

The following steps shall be performed between consumer and service provider:

* 1. The service provider sends escape message to the consumer.

* 2. The consumer responses the escape message and starts to PQC migration. Noted that before the begnining of the consumer migration, provider may also be required to send a comfirmation message to consumer to make sure the both service provider and consumer are in the same page to avoid any incosistances

* 3. The consumer and service provider negotiate the new PQC security context and to establish PQC security connection. There are several ways to negotiate with new PQC security context. For example, If the consumer and service provider have established an IPsec connection through traditional IKE [RFC7296], the multiple key exchanges of IKEv2 as defined in RFC 9370 [RFC9370] can be used to re-negotiate a new quantum-safe security key after receiving the escape message.

The consumer and service provider preconfigure the escape message. During the migration point (for example, service provider detected the quantum attack in Q-day, or as instructions of the system administrator). The service provider can send the escape message with above flows to consumer. Then, the consumer will response escape message to start the PQC migration. Finally, the consumer and the service provider shall start to negotiate new security context of including ML-KEM, ML-DSA or hybrid key exchanges, etc.

The PQC escape message above is a concept, and its specific existence varies in different protocols and scenarios. It is expacted that this capability should be widely supported during PQC transitions. The following examples are some specific scenarios. Specifically, the IKEv2 indication is an already supported feature in RFC. Cellphone identifier is another transition example that could be done in future.

5. Message example: IPsec/IKEv2

As it is already supported in RFC 9242 [RFC9242], the initiator indicates its support for Intermediate Exchange by including a notification of type INTERMEDIATE_EXCHANGE_SUPPORTED in the IKE_SA_INIT request message. If the responder also supports this exchange, it includes this notification in the response message. The same functionality is also supported in RFC 9370, where the indication message INTERMEDIATE_EXCHANGE_SUPPORTED can be considered an escape message, triggered between the IKEv2 initiator and responder when post-quantum key negotiation needs to be triggered.

According to the protocol requirements, if the indication message is not carried, any ADDKE Transform may be skipped or considered unreadable information. These ADDKEs can be used to negotiate payloads for post-quantum capabilities (i.e., key encapsulation using post-quantum algorithms). In other words, the indication message INTERMEDIATE_EXCHANGE_SUPPORTED corresponds to the send/response escape message in Figure 2 in IKE_SA_INIT stage of the PQC hybrid key exchange.

6. Message example: the UE and Network in telco network

Regarding the post-quantum migration of UE (e.g., mobile phones), according to GSMA analysis[PQ03], the UE SUPI (Subscription Permanent Identifier) may be related to post-quantum migration, where SUPI needs to be encrypted to Subscription Concealed Identifier (SUCI) using the non-PQC algorithm ECIES during access. It is expected to use a post-quantum way for protecting SUCI when accessing the network.

Therefore, an example scenarios of PQC escape message is to let the UE receive a post-quantum escape indication, which can be sent from network equipment, e.g., periodically broadcasted. When the UE receives this indication (e.g., broadcast), it should encrypt the SUPI using the post-quantum cryptographic algorithm according to the indication to obtain a post-quantum secured SUCI. Then, use the post-quantum secure SCUI in the initial message for network access. Network equipment can authenticate the device through the post-quantum secure SUCI.

Based on the discussion of emails, some exceptional situations may need to be handled, as following.

* Indication should be as a proper format, which if the legacy device receives, it can be discard and do nothing and continue use non-PQC way to access the network, but the network shall verify if it is legacy for example based on its subscription. This is to prevent any potential attacker jamming to use weak crypto in a non-legacy device access procedure

* If a device is already migrated and it still receives the escape message, the device shall know it has migrated successfully and may ignore any newly recived indication.

* It is suggested the escape message should be carried in broadcasting way. And may send to all reachable devices periodically, until the majority of the device has complete the migration. It is helpful to prevent any potential attackers that tries to block any escape messages.

7. IANA Considerations

This document has no IANA considerations.

8. Security Consideration

The escape message is a compromise approach for dynamic PQC migration, usually it is expected after an attack has been discovered. It is still recommended that quantum migration should be performed in advance. Escape can be a plan B.

During the escape message procedure, Although basic steps can be implemented easily, it is worth to say that the key being used in non-PQC TLS or IPsec may already be leaked during the key exchange phase because of Q-day attacks. For example, assume that an attacker has captured the key during the establishement of non-PQC TLS or IPsec connection, and uses a quantum attack (e.g., HNDL attack). In this case, the attacker can obtain the information and data in the connection, including subsequent escape messages and PQC security context negotiation content, which potential brings security risks.

/*TODO: Consideration of escape message enhancement when potential non quantum-safe keys already be leaked.

9. References

9.1. Normative Reference

[ISO9995] ISO/IEC, "Information technology — Keyboard layouts for text and office systems", ISO/IEC 9995-1:2009, ISO/IEC JTC 1/SC 35, October 2009, <https://www.iso.org/standard/51645.html>.

[PQ03] GSMA, "Post Quantum Cryptography Guidelines for Telecom Use Cases v2.0", PQ 03, Task Force PQTN, October 2024, <https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/>.

[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>.

[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>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9242] Smyslov, V., "Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9242, DOI 10.17487/RFC9242, May 2022, <https://www.rfc-editor.org/info/rfc9242>.

[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/info/rfc9370>.

9.2. Informative References

[ESCKEY] Wikipedia, "the ESC key", 10 February 2025, <https://en.wikipedia.org/wiki/Esc_key#References>.

[shor] Shor, P.W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", DOI 10.1109/SFCS.1994.365700, 6 August 2002, <https://ieeexplore.ieee.org/document/365700/authors#authors>.

Acknowledgments

TODO

Authors' Addresses

Lun Li
Huawei
Email: lilun20@huawei.com

Faye Liu
Huawei Singapore
Email: liufei19@huawei.com