

ETSI TS 104 145 V1.2.1 (2026-08)



**Cyber Security (CYBER);
Quantum-Safe Cryptography (QSC);
Quantum-Safe Enterprise Transport Security (QSETS)**

get full document from standards.iteh.ai

ReferenceRTS/CYBER-QSC-0035

Keywordsquantum safe cryptography

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Executive summary	5
Introduction	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	8
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Symbols.....	9
3.3 Abbreviations	9
4 Quantum-Safe Enterprise Transport Security	9
4.1 Middlebox Security Protocol requirements mapping	9
4.2 The Quantum-Safe Enterprise Transport Security profile.....	10
4.2.1 Key Encapsulation Mechanisms	10
4.2.2 KEM-based TLS 1.3 key exchange	10
4.2.3 KEM-based QSETS key exchange	11
4.2.4 QSETS middlebox key recovery	11
4.2.5 Visibility information	12
4.2.6 Directly installed seeds	12
4.2.7 Centrally managed seeds	13
4.2.8 Key package.....	13
4.2.9 Protecting the key package	14
4.2.10 Transferring keys	14
4.2.10.1 Protocol overview	14
4.2.10.2 Transfer initiated by the key manager	15
4.2.10.3 Transfer initiated by the key consumer	15
4.3 QSETS Architecture.....	16
4.3.1 QSETS with enterprise clients and servers	16
4.3.2 QSETS with enterprise servers	16
4.3.3 QSETS with enterprise clients	17
5 QSETS key encapsulation operations	18
5.1 Introduction	18
5.2 Supporting functions	18
5.2.1 Encoding.....	18
5.2.2 HKDF	18
5.2.3 Encapsulation seed identifier	18
5.3 ML-KEM.....	19
5.3.1 ML-KEM internal encapsulation	19
5.3.2 Server encapsulation	19
5.3.3 Middlebox key recovery	20
5.4 X25519 with ML-KEM-768.....	20
5.4.1 Hybrid key encapsulation	20
5.4.2 Server encapsulation	21
5.4.3 Middlebox key recovery	22
5.5 ECDH with ML-KEM.....	22
5.5.1 Hybrid encapsulation	22
5.5.2 Server encapsulation	22
5.5.3 Middlebox key recovery	24
6 Security operations.....	24

6.1	Security and conformance analysis	24
6.1.1	Ambiguity resistance	24
6.1.2	Cryptographic binding	24
6.1.3	Forward secrecy	24
6.1.4	FIPS compliance	25
Annex A (normative):	Middlebox visibility information variant.....	26
Annex B (normative):	Requirements for a Quantum-Safe Enterprise Transport Security aware client.....	27
Annex C (informative):	Middlebox ephemeral keys export	28
Annex D (informative):	ETS and QSETS comparison.....	29
D.1	Differences between ETS and QSETS	29
D.2	ETS and QSETS interoperability	29
Annex E (informative):	Bibliography.....	31
History		32

Sample Document

get full document from standards.iteh.ai

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Requirements - such as legal mandates and service agreements - exist for enterprise network and data centre operators and service providers, organizations, and small businesses to be able to observe and audit the content and metadata of encrypted sessions transported across their infrastructures. Enterprise Transport Security (ETS) [2] provides these capabilities for TLS 1.3 [13] when used with traditional Diffie-Hellman key exchanges. However, Diffie-Hellman based ETS is not quantum safe.

The present document specifies an enhanced Quantum-Safe Enterprise Transport Security (QSETS) profile that allows TLS visibility in enterprise networks and data centres while protecting against quantum threats. It also meets the same mandatory requirements for the Middlebox Security Profile (MSP) [1] as ETS.

Introduction

Enterprise Transport Security (ETS), specified in ETSI TS 103 523-3 [2], is an implementation variant of Transport Layer Security (TLS) protocol version 1.3 [13] that provides visibility of TLS sessions in enterprise network and data centre domains.

TLS 1.3 was originally designed to use ephemeral Diffie-Hellman as its primary key exchange mechanism. Ephemeral Diffie-Hellman prevents passive decryption of TLS 1.3 sessions at any scale. However, there are operational circumstances where passive decryption of TLS sessions by authorized entities is required, either in real-time or by storing packets and decrypting them later.

ETS relies on long-lived Diffie-Hellman server keys that are re-used across different TLS sessions. The keys can be distributed to real-time decryption middleboxes in advance or can be requested by middleboxes to decrypt sessions post-capture. This greatly reduces the number of keys to be stored and correlated with packet storage systems compared to exporting the ephemeral keys for each TLS session.

Traditional Diffie-Hellman key exchanges are known to be vulnerable to attackers with access to a cryptographically-relevant quantum computer. Consequently, support for post-quantum [i.3] and hybrid [i.5] and [i.4] Key Encapsulation Mechanisms (KEMs) is being added to TLS 1.3.

The present document specifies an enhanced Quantum-Safe Enterprise Transport Security (QSETS) profile that allows visibility of TLS sessions protected by post-quantum or hybrid KEMs.

QSETS relies on long-lived server encapsulation seeds that are used together with session-specific data from the TLS handshake to derive KEM shared secrets and ciphertexts deterministically. The seeds can be distributed to authorized decryption middleboxes allowing them to recover the KEM shared secret and recompute the traffic keys for a TLS session. This only impacts the per-session forward secrecy of the existing TLS 1.3 security architecture, thereby ensuring interoperability and operational effectiveness.

QSETS also requires the server to report visibility information in its certificate, to indicate to the client that long-lived encapsulation seeds are in use for a particular KEM, and to describe the entities that are authorized to receive the seed and decrypt the TLS session.

There are circumstances in which visibility information is not suitable and in which the client has been informed by other means that the connections can be inspected. In such circumstances, annex A can be used. Annex A, which is optional, specifies a variant of QSETS where the visibility information is not sent.

QSETS is compatible with any TLS 1.3 compliant client. Annex B, which is optional, defines the concept of a QSETS aware client whereby a TLS 1.3 client provides additional capabilities in relation to QSETS visibility.

QSETS modifies KEM encapsulation so that it uses a long-lived encapsulation seed. This modification is not suitable in circumstances where the KEM is required to conform to a standard that specifies randomized encapsulation. Annex C briefly describes how to provide TLS session visibility in such circumstances by exporting the ephemeral TLS traffic keys.

1 Scope

The present document specifies the enhanced Quantum Safe Enterprise Transport Security (QSETS) profile to provide quantum-safe secure communication sessions between network endpoints whilst enabling network operations. This allows the use of Transport Layer Security (TLS) version 1.3 [13] with post-quantum [i.3] or hybrid [i.5], [i.4] Key Encapsulation Mechanisms (KEMs) in, for example, compliance constrained environments.

The present document describes three QSETS architectures:

- In the first architecture, both the TLS 1.3 client and the QSETS server are located inside the enterprise.
- In the second architecture, the server is a QSETS server inside the enterprise and the TLS 1.3 client is external to the enterprise. TLS 1.3 is terminated at the enterprise edge such that QSETS is used only inside the enterprise.
- In the third architecture, the TLS 1.3 server is external to the enterprise and the TLS 1.3 client is internal to the enterprise. TLS 1.3 is again terminated at the network edge such that QSETS is used only inside the enterprise.

The present document specifies a modified KEM encapsulation process in which the randomized shared secret and ciphertext are replaced with deterministic values derived from a static encapsulation seed and bound to the TLS session. Annex C describes an alternative approach to providing TLS 1.3 visibility for circumstances in which it is not possible to modify the KEM encapsulation process.

The present document specifies visibility information for indicating the QSETS profile setup. The actions of the client on receiving the visibility information are not normatively defined; however, capabilities for a QSETS aware client are defined in annex B, which is optional. The means by which the QSETS endpoints share the static encapsulation seed are specified. Annex A describes a variant of the QSETS profile for circumstances in which visibility information is not suitable and in which the client has been informed by other means that sessions can be inspected. The means by which the client is informed is out of scope.

The present document also discusses the Middlebox Security Profile (MSP) mapping for QSETS, based on the mapping for Enterprise Transport Security (ETS) from ETSI TS 103 523-3 [2]. Annex D provides a broader comparison between ETS and QSETS.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the [ETSI docbox](#).

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

- [1] [ETSI TS 103 523-1](#): "CYBER; Middlebox Security Protocol; Part 1: MSP Framework and Template Requirements".
- [2] [ETSI TS 103 523-3](#): "CYBER; Middlebox Security Protocol; Part 3: Enterprise Transport Security".
- [3] IANA: "[Transport Layer Security \(TLS\) Parameters](#)".

NOTE: Registry for TLS 1.3 and later SignatureScheme values: TLS Signature Scheme registry and TLS Supported Groups registry.

[4] [IETF RFC 2818](#): "HTTP Over TLS".

NOTE: Obsoleted by IETF RFC 9110.

[5] [IETF RFC 4073](#): "Protecting Multiple Contents with the Cryptographic Message Syntax (CMS)".

[6] [IETF RFC 5280](#): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[7] [IETF RFC 5869](#): "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[8] [IETF RFC 5958](#): "Asymmetric Key Packages".

[9] [IETF RFC 6031](#): "Cryptographic Message Syntax (CMS) Symmetric Key Package Content Type".

[10] [IETF RFC 7193](#): "The application/cms Media Type".

[11] [IETF RFC 7748](#): "Elliptic Curves for Security".

[12] [IETF RFC 7906](#): "NSA's Cryptographic Message Syntax (CMS) Key Management Attributes".

[13] [IETF RFC 8446](#): "The Transport Layer Security (TLS) Protocol Version 1.3".

NOTE: Obsoleted by IETF RFC 9846.

[14] [Recommendation X.509 \(10/19\)](#) | [ISO/IEC 9594-8](#): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[15] [FIPS 203](#): "Module-Lattice-Based Key-Encapsulation Mechanism Standard".

[16] [NIST SP 800-56A Rev. 3](#): "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography".

[17] [NIST SP 800-185](#): "SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

- [i.1] IETF RFC 5083: "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type".
- [i.2] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".
- [i.3] IETF draft-ietf-tls-mlkem (work in progress): "ML-KEM Post-Quantum Key Agreement for TLS 1.3", D. Connolly.
- [i.4] IETF draft-ietf-tls-ecdhe-mlkem (work in progress): "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3", K. Kwiatkowski, P. Kampanakis, B. Westerbaan and D. Stebila.
- [i.5] IETF draft-ietf-tls-hybrid-design (work in progress): "Hybrid key exchange in TLS 1.3", D. Stebila, S. Fluhrer and S. Gueron.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

$a b$	Concatenation of the byte strings a and b
$a[i : j]$	Sub-string $a_i \dots a_{j-1}$ of the byte string $a = a_0 \dots a_{n-1}$
c	Ciphertext
K	Shared secret
pk	Public key
sk	Private key
m	Key Encapsulation Mechanism (KEM) plaintext

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AEAD	Authenticated Encryption with Associated Data
ASN	Abstract Syntax Notation
CMS	Cryptographic Message Syntax
Decaps	Decapsulation
DER	Distinguished Encoding Rules
ECDH	Elliptic Curve Diffie-Hellman
Encaps	Encapsulation
ETS	Enterprise Transport Security
FFDH	Finite Field Diffie-Hellman
FIPS	Federal Information Processing Standards
HKDF	HMAC-based Key Derivation Function
HMAC	Hashed Message Authentication Code
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
KEM	Key Encapsulation Mechanism
KeyGen	Key Generation
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism
MSP	Middlebox Security Protocol
PFS	Perfect Forward Secrecy
QSETS	Quantum-Safe Enterprise Transport Security
TLS	Transport Layer Security

4 Quantum-Safe Enterprise Transport Security

4.1 Middlebox Security Protocol requirements mapping

ETSI TS 103 523-1 [1] defines a set of Middlebox Security Protocol (MSP) Template Requirements that underpin all MSP profile specifications. These are based around the principles of Data Protection, Transparency, Access Control and Good Citizen.