

ETSI TS 104 146 V1.1.1 (2026-08)



Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Authenticated Quantum Safe Hybrid Key Establishment

get full document from standards.iteh.ai

Reference

DTS/CYBER-QSC-0030

Keywords

Quantum 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	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	6
3.1 Terms.....	6
3.2 Symbols.....	6
3.3 Abbreviations	7
4 Overview of Authenticated Quantum-Safe Hybrid Key Establishment.....	7
4.1 Motivation and Objectives	7
4.2 Use Cases and Applications Scenarios.....	7
4.3 Comparison with Existing Standards	8
5 Protocol Architecture	8
5.1 Functional Entities and Roles.....	8
5.2 Information Relationships (Reference Points).....	8
6 Cryptographic Primitives	8
6.1 Notation.....	8
6.2 Hash Function	8
6.3 Elliptic Curve Diffie-Hellman (ECDH)	8
6.4 Post-Quantum Key Encapsulation Mechanisms (PQ KEMs).....	8
6.5 Quantum-Based Cryptographic Component Integration	9
6.6 Message Authentication Code	9
6.7 Digital Signature Schemes (DSSs).....	9
6.8 Key Derivation Functions (KDFs)	9
6.9 Authenticated Encryption with Associated Data (AEAD)	10
7 Protocol Specifications.....	10
7.1 General	10
7.1.1 Key Establishment Abstraction Framework	10
7.1.2 Authenticated Quantum-Safe Hybrid Key Establishment	12
7.1.3 Security Aspects	15
History	17

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

The present document specifies a method for authenticated quantum-safe hybrid key establishment by securely combining quantum-safe cryptographic key-material with a quantum-safe authentication mechanism for any two communicating entities.

Introduction

Authenticated Quantum-Safe Hybrid Key Establishment (AQSHKE) is a secure cryptographic protocol that ensures an authenticated, confidential, and integrity-protected channel between any two communicating entities, even in the event of a Cryptographically Relevant Quantum Computer (CRQC). Such security guarantee is established using (optional) traditional asymmetric cryptography, post-quantum and symmetric cryptography, and quantum-based cryptographic components.

1 Scope

The present document specifies a method for establishing authenticated quantum-safe shared cryptographic key material from multiple sources of quantum-safe key material. Specifically, such key material can be derived from (optional) traditional cryptography, post-quantum and symmetric cryptography, and quantum-based cryptographic components with a post-quantum authentication mechanism.

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 103 744 \(V1.2.2\)](#): "CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment".
- [2] [ISO/IEC 18033-2:2006/Amd 2:2026](#): "Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers — Amendment 2".
- [3] [ETSI GS QKD 014 \(V1.1.1\)](#): "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API".
- [4] [ETSI GS QKD 004 \(V2.1.1\)](#): "Quantum Key Distribution (QKD); Application Interface".
- [5] [NIST SP 800-38B](#): "Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication".
- [6] [ISO/IEC 9797-1:2011](#): "Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher".
- [7] [FIPS 204](#): "Module-Lattice-Based Digital Signature Standard".
- [8] [FIPS 205](#): "Stateless Hash-Based Digital Signature Standard".
- [9] [FIPS 186-5](#): "Digital Signature Standard (DSS)".
- [10] [IETF RFC 5869](#): "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".
- [11] [IETF RFC 5116](#): "An Interface and Algorithms for Authenticated Encryption".
- [12] [IETF RFC 9846](#): "The Transport Layer Security (TLS) Protocol Version 1.3".