

ETSI TS 103 744 V1.2.2 (2026-02)



TECHNICAL SPECIFICATION

CYBER;
Quantum-Safe Cryptography (QSC);
Quantum-safe Hybrid Key Establishment

Document Preview

[ETSI TS 103 744 V1.2.2 \(2026-02\)](https://standards.iteh.ai/catalog/standards/etsi/3ed03402-151a-4552-b43a-5e74bb1201b8/etsi-ts-103-744-v1-2-2-2026-02)

<https://standards.iteh.ai/catalog/standards/etsi/3ed03402-151a-4552-b43a-5e74bb1201b8/etsi-ts-103-744-v1-2-2-2026-02>

ReferenceRTS/CYBER-QSC-0031

Keywordskey exchange, quantum safe cryptography

ETSI650 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 may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	8
3.3 Abbreviations	9
4 Purpose of quantum-safe hybrid key establishment.....	9
4.1 Status of quantum-safe key encapsulation mechanisms.....	9
5 Architecture for quantum-safe hybrid key establishment.....	10
5.1 Functional entities	10
5.2 Information relationships (reference points)	10
6 Introductory information	11
6.1 Introduction	11
6.2 Notation.....	11
6.2.1 Radix.....	11
6.2.2 Conventions.....	11
6.2.3 Bit/Byte ordering	11
6.2.4 Integer encoding	11
7 Cryptographic primitives.....	12
7.1 Hash functions (hash).....	12
7.2 Context formatting function (f)	12
7.2.1 Context formatting function (f) description	12
7.2.2 Concatenate-based context formatting function.....	12
7.2.3 Concatenate-and-hash-based context formatting function.....	13
7.3 PseudoRandom Function (PRF).....	14
7.3.1 PRF description	14
7.3.2 PRF to HMAC mapping	14
7.3.3 PRF to KMAC mapping	14
7.4 Key Derivation Functions (KDFs)	15
7.4.1 KDF description.....	15
7.4.2 KDF to HKDF mapping	16
7.4.3 KDF to HMAC mapping	16
7.4.4 KDF to KMAC mapping	17
7.5 Elliptic Curve Diffie-Hellman (ECDH)	17
7.5.1 ECDH description.....	17
7.5.2 Elliptic curve domain parameters	18
7.6 Key Encapsulation Mechanisms (KEMs).....	18
7.6.1 KEM description.....	18
7.6.2 Post-quantum KEMs.....	18
7.7 Primitive parameter sets	18
7.7.1 Parameter set description	18
7.7.2 Parameter sets	19
8 Hybrid key establishment schemes	20
8.1 General	20
8.1.1 Key establishment abstraction	20

8.1.2	Key establishment abstraction to ECDHE	21
8.1.3	Key establishment abstraction to KEM	21
8.2	Concatenate hybrid key establishment scheme	21
8.2.1	Concatenate hybrid key establishment scheme - ephemeral	21
8.2.2	Concatenate hybrid key establishment scheme - static	22
8.2.3	Concatenate hybrid key combiner - CatKDF.....	23
8.3	Cascade hybrid key establishment scheme.....	24
8.3.1	Cascade hybrid key establishment scheme - ephemeral	24
8.3.2	Cascade hybrid key establishment scheme - static	25
8.3.3	Cascade hybrid key combiner - CasKDF.....	26
Annex A (informative): Background		28
A.1	Quantum computing threats to traditional key exchange protocols	28
A.2	Rationale for quantum-safe hybrid key establishment	28
Annex B (informative): Security consideration		30
B.1	Security definitions	30
Annex C (informative): Message Encoding for Test Vector Generation.....		31
C.1	Message Formatting Function for Test Vector Generation.....	31
Annex D (informative): Test Vectors		33
D.1	Test Vectors Repository	33
Annex E (informative): Bibliography.....		34
Annex F (informative): Change history		35
History		36

Document Preview

[ETSI TS 103 744 V1.2.2 \(2026-02\)](https://standards.iteh.ai/catalog/standards/etsi/3ed03402-151a-4552-b43a-5e74bb1201b8/etsi-ts-103-744-v1-2-2-2026-02)

<https://standards.iteh.ai/catalog/standards/etsi/3ed03402-151a-4552-b43a-5e74bb1201b8/etsi-ts-103-744-v1-2-2-2026-02>

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Introduction

Hybrid Key Establishments are constructions that combine a traditional key establishment method, such as elliptic curve Diffie Hellman [1], with a quantum-safe key encapsulation mechanism, such as Module-Lattice-based Key Encapsulation Mechanism (ML-KEM) [11], into a single key establishment method. Hybrid key establishments are a migration technique to move to quantum-safe technology in advance of establishing full security assurance in the underlying post-quantum cryptographic scheme.