ETSI TR 104 239-1 V1.2.1 (2026-05)

TECHNICAL REPORT

Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 1: General

Reference
RTR/CYBER-QSC-0032

Keywords
cyber security, digital signature, key exchange,
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

Contents

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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 1 of a multi-part deliverable covering implementation guidance for quantum-safe key encapsulation mechanisms and digital signature schemes, as identified below:

Part 1: "General";

Part 2: "ML-KEM" [i.2];

Part 3: "ML-DSA" [i.3];

Part 4: "SLH-DSA" [i.4].

Later parts of this multi-part deliverable will provide implementation guidance for specific algorithms, building on the general guidance provided in the present document.

Modal verbs terminology

In the present document "**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.

1 Scope

The present document provides developers with general guidance to aid the secure implementation of quantum-safe algorithms. This includes an overview of the interfaces and expected security properties of quantum-safe algorithms; some general good practice guidance for cryptographic implementations; some background on side-channel and fault attacks; and a brief discussion of testing and formal verification.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.2] ETSI TR 104 239-2: "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 2: ML-KEM".

[i.3] ETSI TR 104 239-3: " Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 3: ML-DSA".

[i.4] ETSI TR 104 239-4: " Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 4: SLH-DSA".

[i.5] IRTF RFC 7748: "Elliptic Curves for Security".

[i.6] IETF RFC 8017: "PKCS #1: RSA Cryptography Specifications version 2.2".

[i.7] IRTF RFC 8032: "Edwards-Curve Digital Signature Algorithm (EdDSA)".

[i.8] IRTF RFC 9180: "Hybrid Public Key Encryption".

[i.9] IRTF RFC 9474: " RSA Blind Signatures".

[i.10] ISO/IEC 14888-3:2018: "IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms".

[i.11] ISO/IEC 18033-2:2006: "Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers".

[i.12] NCSC: "Timelines for migration to post-quantum cryptography".

[i.13] NIST FIPS 186-5: "Digital Signature Standard (DSS)".

[i.14] NIST FIPS 203: "Module-Lattice-Based Key-Encapsulation Mechanism Standard".

[i.15] NIST FIPS 204: "Module-Lattice-Based Digital Signature Standard".

[i.16] NIST FIPS 205: "Stateless Hash-Based Digital Signature Standard".

[i.17] NIST SP 800-56A Rev. 3: "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography".

[i.18] NIST SP 800-56B Rev. 2: "Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography".

[i.19] NIST SP 800-89: "Recommendation for Obtaining Assurances for Digital Signature Applications".

[i.20] NIST SP 800-90 Series.

[i.21] NIST: "Automated Cryptographic Validation Test System".

[i.22] NIST: "Cryptographic Algorithm Validation Program (CAVP)".

[i.23] NIST: "Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography".

[i.24] J. B. Almeida et al.: "Formally verifying Kyber Episode IV: Implementation correctness". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(3), pp. 164-193, 2023.

[i.25] M. Barbosa et al.: "SoK: Computer-aided cryptography", IEEE™ Symposium on Security and Privacy (SP), pp. 777-795, 2021.

[i.26] G. Becker et al.: "Test Vector Leakage Assessment (TVLA) methodology in practice". International Cryptographic Module Conference 2013.

[i.27] R. Benadjila et al.: "Deep learning for side-channel analysis and introduction to ASCAD database". Journal of Cryptographic Engineering Volume 10 (2020), pp. 163-188, 2020.

[i.28] D. J. Bernstein et al.: "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(2), pp. 209-234, 2025.

[i.29] E. Biham and A. Shamir: "Differential fault analysis of secret key cryptosystems". Advances in Cryptology - CRYPTO' 97. Lecture Notes in Computer Science, vol. 1294, 1997.

[i.30] G. Camurati et al.: "Screaming channels: When electromagnetic side channels meet radio transceivers". CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 163-177, 2018.

[i.31] Cybersecurity & Infrastructure Security Agency, US Government: "Secure-by-Design - Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software".

[i.32] Department of Science, Innovation and Technology, UK Government: "Software Security Code of Practice".

[i.33] fail0verflow: "Console hacking 2010". 27th Chaos Communication Congress, 2010.

[i.34] A. Genêt: "On Protecting SPHINCS+ Against Fault Attacks". IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 80-114, 2023.

[i.35] M. Hastings et al.: "Weak keys remain widespread in network devices". Proceedings of the 2016 Internet Measurement Conference (IMC 16), pp. 49-63, 2016.

[i.36] N. Heninger et al.: "Mining your Ps and Qs: Detection of widespread weak keys in network devices". 21st USENIX Security Symposium (USENIX Security 12), pp. 205-220.

[i.37] X. Hou et al.: "Fully automated differential fault analysis on software implementations of block ciphers". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(3), pp. 1-29, 2019.