



**Cyber Security (CYBER);
Quantum-Safe Cryptography (QSC);
Secure Implementation Guidance for
Key Encapsulation Mechanisms and Digital Signature Schemes;
Part 3: ML-DSA**

get full document from standards.iteh.ai

Reference

DTR/CYBER-QSC-0027-3

Keywords

cyber security, digital signature,
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	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	8
3.3 Abbreviations	8
4 Introduction	9
5 ML-DSA interfaces	10
5.1 Parameters	10
5.2 Key generation	10
5.2.1 Key formats	10
5.2.2 Full key generation	11
5.2.3 Seeded key generation	11
5.3 Signature generation.....	11
5.3.1 Overview	11
5.3.2 Pure ML-DSA.....	12
5.3.3 HashML-DSA.....	13
5.3.4 External μ	13
5.4 Signature verification	15
5.4.1 Pure ML-DSA.....	15
5.4.2 HashML-DSA.....	15
5.4.3 External μ	16
6 General implementation considerations	17
6.1 Perform input validation.....	17
6.1.1 Signature generation inputs	17
6.1.2 Signature verification inputs.....	17
6.1.3 HashML-DSA inputs	18
6.1.4 External μ inputs.....	18
6.1.5 Internal algorithms	18
6.2 Perform output validation.....	19
6.2.1 Rejection sampling checks.....	19
6.2.2 Pairwise consistency test	19
6.2.3 Self testing	20
6.3 Prevent leakage of intermediate values	20
6.3.1 Zeroise intermediate values after use.....	20
6.3.2 Limit external access to internal functions	21
6.4 Handle errors gracefully	21
6.4.1 Specified errors.....	21
6.4.2 Unspecified errors.....	21
6.4.3 Verification failures	22
6.5 Randomness	22
7 Side-channel and fault attack considerations	22
7.1 Key Generation	22
7.1.1 Overview	22
7.1.2 Timing Analysis Considerations.....	23
7.1.3 Power Analysis Considerations	23
7.1.4 Fault Attack Considerations.....	24

7.2	Signature generation.....	24
7.2.1	Overview	24
7.2.2	Timing Analysis Considerations.....	25
7.2.3	Power Analysis Considerations	25
7.2.4	Fault Attack Considerations.....	26
7.3	Signature verification	26
7.3.1	Overview	26
7.3.2	Timing Analysis Considerations.....	26
7.3.3	Power Analysis Considerations	26
7.3.4	Fault Attack Considerations.....	26
8	Testing and formal verification considerations	27
8.1	Testing Considerations	27
8.2	Formal Verification Considerations	28
Annex A:	NIST FIPS 204 algorithms	29
A.1	Pure digital signature (external)	29
A.2	Pre-hash digital signature (external).....	29
A.3	De-randomized digital signature (internal only)	29
A.4	Sampling.....	29
A.5	Arithmetic.....	30
A.6	Encoding.....	30
Annex B:	ML-DSA security properties.....	31
B.1	Unforgeability	31
B.2	Beyond unforgeability	32
Annex C:	Hybrid ML-DSA	33
C.1	Deployment considerations	33
C.2	Implementation considerations.....	33
Annex D:	Change history	35
History		36

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

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.2].

The present document provides implementation guidance for the Module-Lattice-based Digital Signature Algorithm (ML-DSA).

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 guidance to aid the secure implementation of the quantum-safe digital signature algorithm ML-DSA as specified by NIST FIPS 204 [i.7]. This highlights some potential ML-DSA implementation hazards; identifies some side-channel and fault attack issues specific to ML-DSA; considers some testing and formal verification aspects relevant to ML-DSA; and briefly discusses the secure usage of ML-DSA.

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 TR 103 966: "CYBER Security (CYBER); Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Schemes".
- [i.2] ETSI TR 104 239-1: "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 1: General".
- [i.3] IETF RFC 9881: "Internet X.509 Public Key Infrastructure - Algorithm identifiers for the Module-Lattice-based Digital Signature Algorithm".
- [i.4] IRTF RFC 8032: "Edwards-curve Digital Signature Algorithm (EdDSA)".
- [i.5] ISO/IEC 24759:2025: "Information security, cybersecurity and privacy protection - Test requirements for cryptographic modules".
- [i.6] NIST FIPS 186-5: "Digital Signature Standard (DSS)".
- [i.7] NIST FIPS 204: "Module-Lattice-Based Digital Signature Standard".
- [i.8] NIST: "[FAQ - FIPS 204 - Computing mu](#)".
- [i.9] NIST SP 800-57A Rev. 6 (Initial Public Draft): "Recommendation for Key Management: Part 1 - General".
- [i.10] NIST SP 800-89: "Recommendation for Obtaining Assurances for Digital Signature Applications".
- [i.11] NIST: "[Cryptographic Algorithm Validation Program \(CAVP\)](#)".
- [i.12] NIST: "[Automated Cryptographic Validation Test System](#)".
- [i.13] NIST: "[Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program](#)".
- [i.14] S. Bai et al.: "CRYSTALS-Dilithium: Algorithm specifications and supporting documentation (Version 3.1)". NIST Post-Quantum Cryptography Standardization Process.

- [i.15] S. Bauer and F. De Santis: "Forging Dilithium and Falcon signatures by single fault injection". FDTC 2023.
- [i.16] B. Benčina et al.: "Post-quantum cryptographic analysis of SSH". S&P, 2025.
- [i.17] F. Bergsma et al.: "Multi-ciphersuite security of the Secure Shell (SSH) protocol". ACM CCS, 2014.
- [i.18] F. Bergsma et al.: "Multi-ciphersuite security of the Secure Shell (SSH) protocol". IACR ePrint 2013/813, June 5, 2020.
- [i.19] D.J. Bernstein et al.: "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations". CHES, 2025.
- [i.20] J. Brendel et al.: "The provable security of Ed25519: Theory and practice". S&P, 2021.
- [i.21] K. Chalkias, F. Garillot and V. Nikolaenko: "Taming the many EdDSAs". SSR, 2020.
- [i.22] Community Cryptography Specification Project: "[Project Wycheproof](#)".
- [i.23] Community Cryptography Specification Project: "[Community Cryptography Test Vectors \(CCTV\)](#)".
- [i.24] J.-S. Coron et al.: "Improved gadgets for the high-order masking of Dilithium". CHES, 2023.
- [i.25] J.-S. Coron et al.: "Improved high-order masked generation of masking vector and rejection sampling in Dilithium". CHES, 2024.
- [i.26] C. Cremers et al.: "BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures". S&P, 2021.
- [i.27] Cryspen: "[libcrux](#)".
- [i.28] Cybersecurity & Infrastructure Security Agency, US Government: "Secure-by-Design - Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software".
- [i.29] C. Decker and R. Wattenhofer: "Bitcoin transaction malleability and MtGox". ESORICS, 2014.
- [i.30] Department of Science, Innovation and Technology, UK Government: "Software Security Code of Practice".
- [i.31] J. Don et al.: "On the (In)Security of the BUFF transform". CRYPTO, 2024.
- [i.32] A. Fiat and A. Shamir: "How to prove yourself: Practical solutions to identification and signature problems". CRYPTO, 1986.
- [i.33] B. Gierlichs et al.: "Mutual information analysis". CHES, 2008.
- [i.34] T. Hollebeek, S. Schmieg and B. Westerbaan, "Use of ML-DSA in TLS 1.3 (work in progress)". IETF Internet-Draft, draft-ietf-tls-mldsa.
- [i.35] K. Jackson, C. Miller and D. Wang: "Evaluating the security of CRYSTALS-Dilithium in the Quantum Random Oracle Model". EUROCRYPT, 2024.
- [i.36] E. Karatsiolis et al.: "Public key linting for ML-KEM and ML-DSA". ACNS, 2025.
- [i.37] E. Kiltz, V. Lyubashevsky and C. Schaffner: "A concrete treatment of Fiat-Shamir signatures in the Quantum Random-Oracle Model". EUROCRYPT, 2018.
- [i.38] V. Lyubashevsky: "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures". ASIACRYPT, 2009.
- [i.39] Monero: "[Disclosure of a Major Bug In Cryptonote Based Currencies](#)".
- [i.40] P.Q. Nguyen and O. Regev: "Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures". EUROCRYPT, 2006.

- [i.41] M. Ounsworth et al, "Composite Module-Lattice-based Digital Signature Algorithm (ML-DSA) for use in X.509 Public Key Infrastructure (work in progress)". IETF Internet-Draft, draft-ietf-lamps-pq-composite-sigs.
- [i.42] Post-Quantum Cryptography Alliance: "[mlds-native](#)".
- [i.43] Post-Quantum Cryptography Alliance: "[mlkem-native](#)".
- [i.44] P. Ravi et al.: "Exploiting determinism in lattice-based signatures: Practical fault attacks on pqm4 implementations of NIST candidates". Asia CCS, 2019.
- [i.45] P. Ravi et al.: "On configurable SCA countermeasures against single trace attacks for the NTT". SPACE, 2020.
- [i.46] Sebastien Riou: "[BTVG-MLDSA](#)".
- [i.47] M. Stevens, A. Lenstra and B. de Weger: "Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities". EUROCRYPT, 2007.
- [i.48] Symbolic Software: "[Crucible](#)".
- [i.49] Symbolic Software: "[Even More Bugs in CE Labs' libcrux: ML-DSA](#)".
- [i.50] UK National Cyber Security Centre: "[Next steps in preparing for post-quantum cryptography](#)".
- [i.51] R. Wang et al.: "Unpacking needs protection: A single-trace secret key recovery attack on Dilithium". IACR Communications in Cryptology, 2024.
- [i.52] P. Wuille, J. Nick and T. Ruffing: "[BIP 340: Schnorr Signatures for secp256k1](#)".

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:

$\ a\ _{\infty}$	Maximum absolute value of a coefficient in a
$\text{wt}(a)$	Number of non-zero coefficients in a
(a, b)	Ordered pair of values a and b
$a b$	Concatenation of the byte strings a and b
$a = b$	Return true if the values a and b are equal and false otherwise
$a \leftarrow b$	Assign the value b to the variable a

3.3 Abbreviations

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

AES	Advanced Encryption Standard
BIP	Bitcoin Improvement Proposal
BUFF	Beyond Unforgeability
CPA	Correlational Power Analysis
CVE	Common Vulnerabilities and Exposures
DPA	Differential Power Analysis
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm

EUF-CMA	Existential Unforgeability against Chosen-Message Attacks
FIPS	Federal Information Processing Standard
ISO	International Organization for Standardization
LWE	Learning With Errors
MBS	Message-Bound Signatures
ML-DSA	Module-Lattice-based Digital Signature Algorithm
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism
M-S-UFO	Malicious-Strong Universal Exclusive Ownership
NIST	National Institute of Standards and Technology
NR	Non Re-signability
NTT	Number Theoretic Transform
PKCS	Public Key Cryptography Standards
PQC	Post-Quantum Cryptography
RBG	Random Bit Generator
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm Keccak
SIS	Short Integer Solution
SP	Special Publication
SSH	Secure Shell
SUF-CMA	Strong Unforgeability against Chosen-Message Attacks
TLS	Transport Layer Security

4 Introduction

The Module-Lattice-based Digital Signature Algorithm (ML-DSA) is a post-quantum signature algorithm selected for standardization following the multi-year NIST Post-Quantum Cryptography (PQC) Standardization Process. It is specified in NIST FIPS 204 [i.7] and support for ML-DSA is being integrated into internet protocols such as TLS [i.34].

NOTE: ML-DSA is based on the CRYSTALS-Dilithium submission to the NIST PQC Process [i.14].

ML-DSA received a significant amount of analysis during the NIST PQC Process, but its security also depends on the way in which it is implemented and used. The present document builds on the general guidance in ETSI TR 104 239-1 [i.2] to provide developers with some specific guidance to aid the secure implementation of ML-DSA:

- It describes the ML-DSA interfaces, including the difference between the "pure" ML-DSA and HashML-DSA algorithms, and different options for private key formats (clause 5).
- It extends the general implementation considerations from ETSI TR 104 239-1 [i.2] with ML-DSA specific aspects such as input validation, consistency checks, and error handling (clause 6).
- It discusses different side-channel considerations for ML-DSA key generation, signature generation and signature verification (clause 7).
- It touches on testing and formal validation for ML-DSA implementations (clause 8).

The present document also gives some background on ML-DSA security properties (annex B) and some considerations on the use of ML-DSA in hybrid schemes (annex C).

As with ETSI TR 104 239-1 [i.2], the guidance is primarily aimed at secure implementations in software, although some of the recommendations will also be relevant to hardware implementations. Developers implementing ML-DSA should also ensure that they follow best practice for developing secure systems in general [i.28], [i.30].