

DISCLAIMER

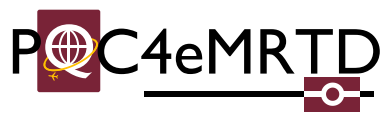
This document, D3.1 – Report on the Standardisation work on quantum-safe X.509 certificates, has been prepared as part of the PQC4eMRTD project, under Grant Agreement No 101190400, and is currently under review by the European Commission. It is provided for informational purposes only.



Funded by
the European Union



ECCE 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE





D3.1 – Standardisation work on quantum-safe X.509 certificates

Project number: 101190400

Project name: Post-Quantum Cryptography for electronic Machine-Readable Travel Documents

Project acronym: PQC4eMRTD

Document Information:	
Work Package No:	3
Lead Beneficiary:	CRYPTONEXT
Type:	Report
Dissemination Level:	Public
Written by:	Adam Anglart (CRYPTONEXT), Daniel Van Geest (CRYPTONEXT)
Approved by:	Matina Maria Trompouki (BSC)
Reviewed by:	Detlef Houdeau (IFAG), Antonio Escobar (IFAG)
Version:	v1.0
Submission Date:	30/09/2026
Due Date:	30/09/2026



**Funded by
the European Union**



ECCE
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

PQC4eMRTD has received funding from the European Union's Digital Europe Programme (DIGITAL) under Grant Agreement No 101190400 and is supported by the European Cybersecurity Competence Centre.

Document Control Page:

Version	Date	Author(s)	Changes
v0.1	10/08/2026	Adam Anglart	Initial version.
v0.2	12/08/2026	Adam Anglart	Added the core of Sections 1–9
v0.3	14/09/2026	Daniel Van Geest	Minor editorial work
v0.4	17/09/2026	Antonio Escobar	Internal review by IFAG; Detlef Houdeau comments implemented, numbered references and citations added
v0.5	18/09/2026	Antonio Escobar	Added Section 4.4 with the consolidated threat and risk scenarios for Passive Authentication; added the List of Tables and the List of Figures; front matter aligned with the project template
v1.0	30/09/2026	Antonio Escobar	Final approval gate by BSC; list of acronyms added; released for submission

The PQC4eMRTD Consortium

#	Partner Legal Name	Short Name	Role	Country
1	INFINEON TECHNOLOGIES AG	IFAG	Coordinator	Germany
2	THALES CDI FRANCE SAS	THALES CDI	Beneficiary	France
3	INSTITUT ZA PRIMERJALNO PRAVO PRI PRAVNI FAKULTETI V LJUBLJANI	IPP PFLJUBLJANA	Beneficiary	Slovenia
4	BARCELONA SUPERCOMPUTING CENTER CENTRO NACIONAL DE SUPERCOMPUTACION	BSC	Beneficiary	Spain
5	CRYPTONEXT SECURITY	CRYPTONEXT	Beneficiary	France



Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. This material is the copyright of PQC4eMRTD consortium parties, and may not be reproduced or copied without permission. The commercial use of any information contained in this document may require a licence from the proprietor of that information.

Table of Contents

1.	Introduction.....	8
1.1	Scope and relation to D2.1	8
1.2	X.509 certificates and eMRTD	8
2.	Quantum-safe X.509 certificate formats.....	9
2.1	Classification	9
2.2	Pure post-quantum and paired certificates	10
2.3	Backward-compatible certificates	12
2.4	Composite certificates	13
2.5	Certificate discovery	14
2.6	Current standardisation status.....	15
3.	Standardisation work completed	16
4.	Assessment for eMRTD	17
4.1	Main constraints.....	17
4.2	Certificate size	17
4.3	Format comparison	18
4.4	Security risk analysis.....	19
5.	Project risks	21
6.	Recommendations	21
7.	Remaining work and conclusion	22
8.	References.....	23
8.1	Standards and published RFCs	23
8.2	Current drafts and supporting records.....	23
	Annex A — Log of standardisation activity	24

List of Tables

Table 1:	Standardisation status of the quantum-safe X.509 certificate formats at 12 August 2026.	16
Table 2:	Certificate sizes for ML-DSA-44 with an ECDSA P-256 baseline.	18
Table 3:	Comparison of certificate formats for the Document Signer certificate.	19
Table 4:	Threat and risk scenarios for the Document Signer certificate in Passive Authentication.....	20
Table 5:	Log of standardisation activity carried out under Task 3.1, January 2025 to 12 August 2026.....	24

List of Figures

Figure 1: The fields of a modern X.509 certificate. The three cryptographic fields are shown with a solid outline.	9
Figure 2: Quantum-safe X.509 certificate formats classified by algorithm count and backward compatibility.	10
Figure 3: A pure post-quantum certificate. The signature algorithm identifier, public key and signature use the post-quantum algorithm.	11
Figure 4: A hybrid-bound pair. The post-quantum certificate contains a digest of the traditional certificate.	11
Figure 5: A traditional and a pure post-quantum certificate used together at protocol level.....	12
Figure 6: A catalyst certificate. Post-quantum information is carried in the extensions of a traditional certificate.	13
Figure 7: A composite certificate. The algorithm identifiers, public key and signature each contain traditional and post-quantum components.	14
Figure 8: Certificate discovery by inclusion, by URI or by local policy.....	15

Acronyms

ACRONYM	DEFINITION
AD	Area Director
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
CFRG	Crypto Forum Research Group
CMS	Cryptographic Message Syntax
CSCA	Country Signing Certification Authority
DER	Distinguished Encoding Rules
DS	Document Signer
ECDSA	Elliptic Curve Digital Signature Algorithm
eMRTD	electronic Machine-Readable Travel Document
ENISA	European Union Agency for Cybersecurity
FIPS	Federal Information Processing Standards
FN-DSA	FFT over NTRU-Lattice-Based Digital Signature Algorithm
HSS	Hierarchical Signature System
ICAO	International Civil Aviation Organization
I-D	Internet-Draft
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IPSECME	IP Security Maintenance and Extensions
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KEM	Key-Encapsulation Mechanism
LAMPS	Limited Additional Mechanisms for PKIX and S/MIME
LDS1	Logical Data Structure version 1
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
NIST	National Institute of Standards and Technology
PA	Passive Authentication
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure using X.509

ACRONYM	DEFINITION
PQ	Post-Quantum
PQC	Post-Quantum Cryptography
PQCC	Post-Quantum Cryptography Coalition
PQUIP	Post-Quantum Use In Protocols
RAM	Random Access Memory
RFC	Request for Comments
S/MIME	Secure/Multipurpose Internet Mail Extensions
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
TLS	Transport Layer Security
URI	Uniform Resource Identifier
WG	Working Group
X9	Accredited Standards Committee X9
XMSS	eXtended Merkle Signature Scheme

1. Introduction

1.1 Scope and relation to D2.1

Task 3.1 covers participation in the preparation and review of standards for quantum-safe X.509 certificates [22]. This report records work carried out by the project and provides recommendations for hybrid post-quantum and traditional certificates. All document statuses and measurements reported here are stated as at 12 August 2026, the reporting cut-off date for this deliverable. Annex A logs the standardisation activity carried out under Task 3.1 over the reporting period.

D2.1 described the formats available at month 4 [21]. This deliverable updates their status and adds an assessment for travel documents. D3.2 reports standardisation work on PQC, high-performance computing and quantum-computing hardware and software, and D3.3 reports standardisation work in the travel-document bodies.

Most formats covered by this report are developed in the Internet Engineering Task Force Limited Additional Mechanisms for PKIX and S/MIME (IETF LAMPS) working group. Adoption as a working-group draft indicates group interest but does not make the text stable. A published Standards Track Request for Comments (RFC) records an IETF-reviewed specification and provides the most reliable basis for implementation.

1.2 X.509 certificates and eMRTD

An X.509 certificate links a public key to an identity and is signed by a certification authority. The cryptographic algorithm affects three fields: the signature algorithm identifier, the subject public-key information and the signature. The remaining fields retain their ASN.1 structure, although certificate profiles and extensions may still require changes. Figure 1 shows these fields within a modern certificate.

The diagram illustrates the structure of a Traditional X.509 certificate. It consists of a header 'Traditional X.509 certificate' followed by a series of fields. The fields are: Version, Serial Number, Signature Algo Id, Issuer Name, Validity Period, Subject Name, Subject Public Key Info, Issuer Unique ID, Subject Unique ID, Extensions, and Signature. The fields are grouped into two categories: 'determined by the traditional algorithm' (indicated by a 'T' icon) and 'unchanged by the transition' (indicated by a 'U' icon). The fields 'Signature Algo Id', 'Subject Public Key Info', and 'Signature' are marked with a 'T' icon, indicating they are determined by the traditional algorithm. The other fields are marked with a 'U' icon, indicating they are unchanged by the transition.

T determined by the traditional algorithm U unchanged by the transition

Figure 1: The fields of a modern X.509 certificate. The three cryptographic fields are shown with a solid outline.

Passive Authentication (PA) verifies the data stored on an electronic Machine-Readable Travel Document (eMRTD). The inspection system checks a Document Signer certificate against the issuing State’s Country Signing Certification Authority (CSCA) certificate and then verifies the signed security object on the chip. ICAO Doc 9303 [1] [2] requires the Document Signer certificate to be carried in that security object, so certificate size affects both chip storage and transmission time.

Travel documents remain in use for many years, while inspection systems are not always upgraded at the same time as documents are issued. A suitable format must therefore balance post-quantum protection, compatibility with existing terminals, certificate size and the ability to change algorithms during the document lifetime.

2. Quantum-safe X.509 certificate formats

2.1 Classification

The formats can be classified by the number of certificates and algorithms they carry, whether a legacy verifier can process them, and whether they store cryptographic material directly or by reference. Figure 2 places the formats on these axes.

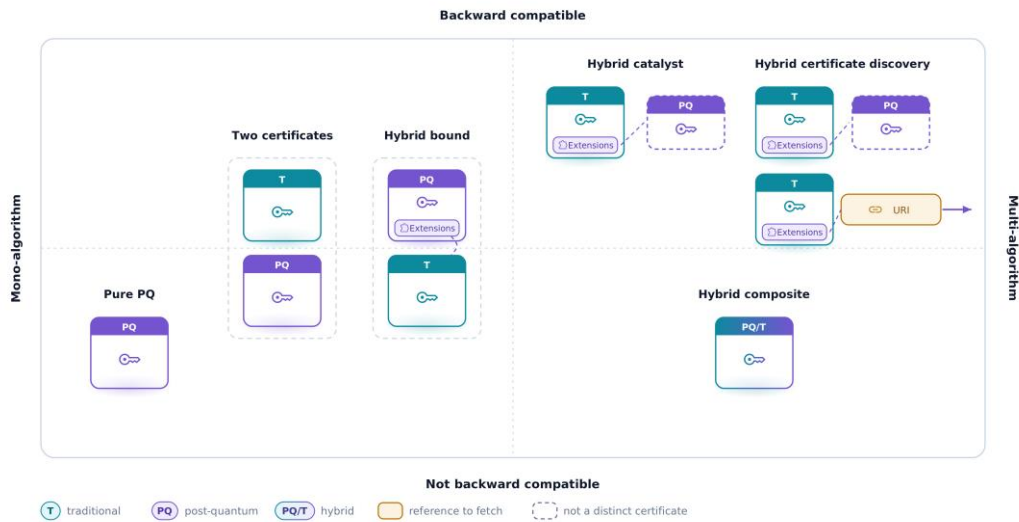
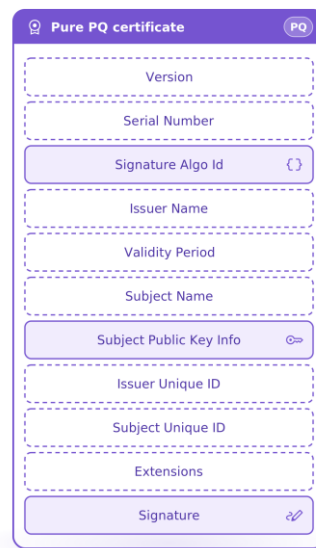


Figure 2: Quantum-safe X.509 certificate formats classified by algorithm count and backward compatibility.

2.2 Pure post-quantum and paired certificates

A **pure post-quantum certificate** replaces the traditional signature algorithm, public key and signature, as shown in Figure 3. It is simple to specify, but it provides no hybrid protection and a legacy verifier cannot recognise the algorithm identifiers. Module-Lattice-Based Digital Signature Algorithm (ML-DSA, FIPS 204) [5] [11] [12], Stateless Hash-Based Digital Signature Algorithm (SLH-DSA, FIPS 205) [6] [10] [13], Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM, FIPS 203) [4] [14] [15] and the stateful Hierarchical Signature System/eXtended Merkle Signature Scheme (HSS/XMSS) [9] family now have published IETF documents for X.509 or Cryptographic Message Syntax (CMS) use. The subject-key algorithm and the issuing signature algorithm are chosen independently: ML-KEM certificates carry a key-encapsulation key and do not produce certificate or Passive Authentication signatures.



PQ determined by the post-quantum algorithm unchanged by the transition

Figure 3: A pure post-quantum certificate. The signature algorithm identifier, public key and signature use the post-quantum algorithm.

A **hybrid-bound** arrangement uses a traditional certificate and a pure post-quantum certificate. The post-quantum certificate contains a digest of the traditional certificate, binding both to the same holder. RFC 9763 [8] specifies the Related Certificate extension used for this purpose, as shown in Figure 4.

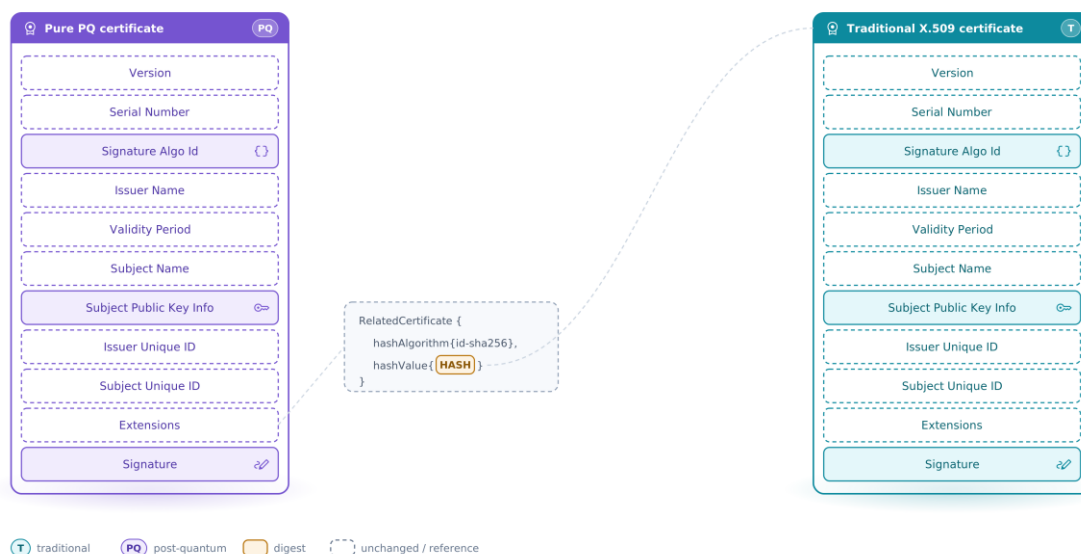


Figure 4: A hybrid-bound pair. The post-quantum certificate contains a digest of the traditional certificate.

The two certificates may also be combined at protocol level without changing either certificate format. This is straightforward but requires both complete objects to be stored and

transmitted, and the certificates are not bound unless the protocol adds that property. See Figure 5.

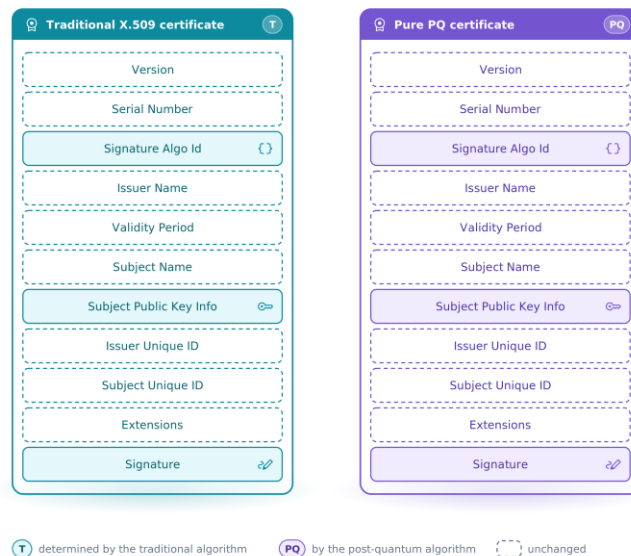


Figure 5: A traditional and a pure post-quantum certificate used together at protocol level.

2.3 Backward-compatible certificates

A catalyst certificate as shown in Figure 6 retains the traditional algorithm, public key and signature in their usual fields and adds a post-quantum algorithm identifier, public key and signature in extensions. A legacy terminal can verify the traditional signature, while an updated terminal can require both signatures. This construction is specified in the International Telecommunication Union Telecommunication Standardization Sector [3] (ITU-T) standard for X.509. Backward compatibility also creates a downgrade path, so profiles must require the alternative signature when post-quantum protection is expected.

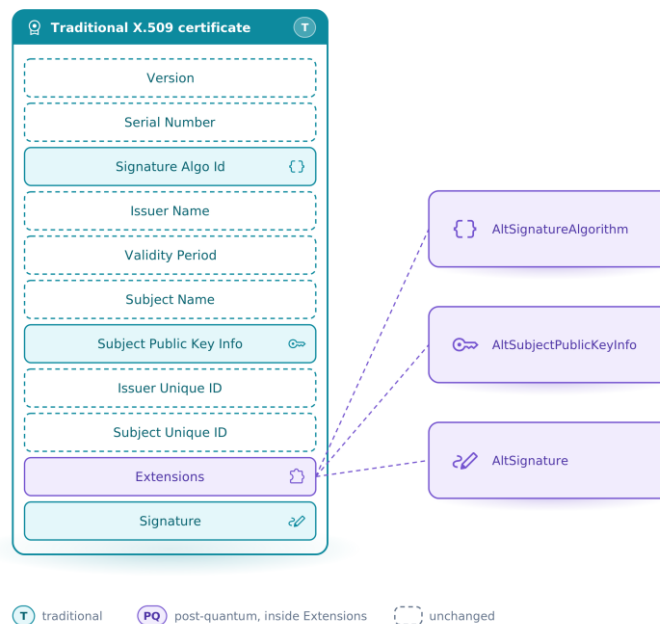


Figure 6: A catalyst certificate. Post-quantum information is carried in the extensions of a traditional certificate.

2.4 Composite certificates

A composite certificate carries one public key and one signature, each containing a traditional and a post-quantum component. See Figure 7. The certificate remains structurally conventional, but new object identifiers and verification algorithms are required. Composite certificates avoid the partial acceptance possible with catalyst certificates and are smaller than the other hybrid arrangements measured in this report. The Composite ML-DSA X.509 draft [16] had been approved by the Internet Engineering Steering Group (IESG) and was in the RFC Editor queue at the cut-off date; the Composite ML-KEM draft [17] remained under IESG review.

Composite certificate

Version

Serial Number

Signature Algo Id

Issuer Name

Validity Period

Subject Name

Subject Public Key Info

Issuer Unique ID

Subject Unique ID

Extensions

Signature

Legend: PQ/T hybrid — one field, two components unchanged by the transition

Figure 7: A composite certificate. The algorithm identifiers, public key and signature each contain traditional and post-quantum components.

2.5 Certificate discovery

Certificate discovery uses a Subject Information Access extension to reference a related certificate by Uniform Resource Identifier (URI), to include the certificate directly, or to leave retrieval to local policy [18]. Revision 03 defines no certificate-digest field, so discovery alone does not bind the two certificates: the relying party must validate the related certificate and apply a subject-equivalence policy. The inclusion form does not reduce storage because the related certificate is embedded. The URI form reduces on-chip storage but makes verification dependent on retrieval from the referenced location. That dependency is unsuitable for the Document Signer certificate at border inspection, although it may be useful for distributing CSCA material between States. See Figure 8.

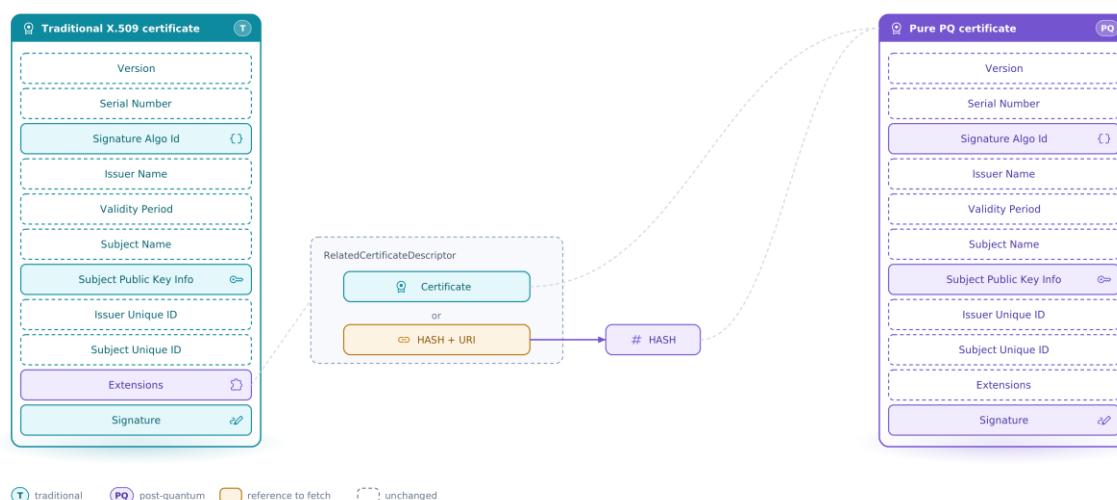


Figure 8: Certificate discovery by inclusion, by URI or by local policy.

Three formats described in D2.1 are no longer active candidates. The chameleon, external public-key and Sun certificate drafts remained individual drafts and expired. Their main functions are now covered by RFC 9763 or the certificate-discovery draft [18].

2.6 Current standardisation status

Table 1 summarises the status verified on 12 August 2026. Published RFCs provide stable references. Drafts in the IESG or RFC Editor process are close to publication but can still change.

Family	Format	Reference at cut-off	State	Change since D2.1 (M4)
Mono-algorithm	Pure PQ — ML-DSA	RFC 9881 (Oct 2025)	Published RFC	WG draft → RFC
Mono-algorithm	Pure PQ — SLH-DSA	RFC 9909 (Dec 2025)	Published RFC	WG draft → RFC
Mono-algorithm	Pure PQ — ML-KEM	RFC 9935 (Mar 2026)	Published RFC	WG draft → RFC
Mono-algorithm	Pure PQ — HSS/XMSS	RFC 9802 (Jun 2025)	Published RFC	WG draft → RFC
Mono-algorithm	Pure PQ — FrodoKEM	draft-smyslov-lamps-frodokem-certificates-03	Individual I-D, active	New since D2.1
Mono-algorithm	Hybrid bound	RFC 9763 (Jun 2025)	Published RFC	WG draft → RFC
Mono-algorithm	Two certificates	No format change; see pure PQ	Not applicable — protocol level	Unchanged

Family	Format	Reference at cut-off	State	Change since D2.1 (M4)
Backward-compatible	Hybrid catalyst / Chimera	ITU-T X.509 (10/2019), Ed. 9; ANSI X9.146 (draft)	Published international standard, in force	Unchanged; X9.146 work added
Multi-algorithm	Hybrid composite — ML-DSA	draft-ietf-lamps-pq-composite-sigs-19	IESG approved 22 Apr 2026; RFC Editor queue	WG draft → RFC Editor queue
Multi-algorithm	Hybrid composite — ML-KEM	draft-ietf-lamps-pq-composite-kem-18	IESG processing (Waiting for AD Go-Ahead)	Not covered in D2.1
Indirection	Hybrid certificate discovery	draft-ietf-lamps-certdiscovery-03	Adopted WG draft, active	New; supersedes external public key and sun
Not pursued	Chameleon (delta)	draft-bonnell-lamps-chameleon-certs-07	Individual I-D, expired	Described in D2.1 §3.2; not adopted
Not pursued	External public key	draft-ounsworth-lamps-pq-external-pubkeys-05	Individual I-D, expired	Described in D2.1 §3.4; superseded
Not pursued	Sun	draft-sun-lamps-hybrid-scheme-01	Individual I-D, expired	Described in D2.1 §3.4; superseded

Table 1: Standardisation status of the quantum-safe X.509 certificate formats at 12 August 2026.

3. Standardisation work completed

The project’s main standardisation venue was the IETF LAMPS working group. Four contributed documents became RFCs during the reporting period. CryptoNext authors are listed first on RFC 9802 and RFC 9936 [9] [15] and are co-authors of RFC 9882 and RFC 9909 [12] [13]. These publications cover stateful hash-based signatures and SLH-DSA in X.509, together with ML-DSA and ML-KEM in CMS.

The project authored or contributed text to seven working-group drafts covering X.509 and CMS. It also contributed to the two composite X.509 drafts. CryptoNext authorship covers the working-group draft for FN-DSA in the Cryptographic Message Syntax [19], together with individual drafts on the parameterised SIGNED ASN.1 type and on Composite ML-DSA for Transport Layer Security (TLS) 1.3.

CryptoNext produced post-quantum certificate and CMS interoperability test artefacts for the IETF 122, 123 and 124 hackathons and for the January 2026 LAMPS interim hackathon [20]. At the cut-off date, cross-testing covered sixteen independent implementations. Independent open-source work, in particular the Open Quantum Safe project, publishes post-quantum X.509

and Transport Layer Security implementations that are widely used for interoperability testing across the wider ecosystem [23].

The project commented on nine further IETF documents, delivered a formal review for the IETF Independent Stream Editor and responded to the European Union Agency for Cybersecurity (ENISA) consultation on Agreed Cryptographic Mechanisms version 3.0. Presentations were delivered at IETF 122, IETF 124 and IETF 126. A project author also co-authored the Post-Quantum Cryptography Coalition publication on dual-signature downgrade risks.

4. Assessment for eMRTD

4.1 Main constraints

Four constraints determine whether a certificate format is suitable for Passive Authentication:

- Chip storage. ICAO Doc 9303 [2] requires the Document Signer certificate to be stored in the security object on the chip.
- Transmission time. The certificate is transmitted over the contactless interface at every inspection.
- Legacy terminals. Many inspection systems cannot be upgraded at the same time as documents are issued.
- Document lifetime. A certificate may need to remain verifiable for more than ten years without replacing the document.

Random Access Memory (RAM) use and signature-processing time remain important, but they depend mainly on the selected algorithm and implementation rather than on the certificate format. Those measurements must be obtained before a profile is selected.

4.2 Certificate size

Table 2 gives the complete Distinguished Encoding Rules (DER) size of self-signed certificates using ML-DSA-44 at NIST security category 2, with a traditional baseline for comparison. The post-quantum and composite values were measured from the CryptoNext interoperability test artefacts produced for the IETF Hackathon [20]. The traditional Elliptic Curve Digital Signature Algorithm (ECDSA) P-256 baseline was generated with the same profile. Catalyst and hybrid-bound values were calculated from the measured components and the published ASN.1 structure.

Format	Basis	Size (bytes)	Ratio to traditional	Transmission at 424 kbit/s (ms)
Traditional — ECDSA P-256	Generated locally, OpenSSL 3.6.3	431	1.0	8
Pure PQ — ML-DSA-44	Measured artefact	4 009	9.3	76
Hybrid composite — MLDSA44-ECDSA-P256-SHA256	Measured artefact	4 180	9.7	79
Hybrid catalyst — ECDSA P-256 with ML-DSA-44	Calculated from measured components	4 238	9.8	80
Two certificates — traditional and pure PQ	Calculated (sum of two measured artefacts)	4 440	10.3	84
Hybrid bound pair — with RelatedCertificate	Calculated (sum plus 65-byte extension)	4 505	10.5	85

Table 2: Certificate sizes for ML-DSA-44 with an ECDSA P-256 baseline.

The main increase comes from replacing elliptic-curve cryptography, not from hybridisation. The pure ML-DSA certificate is 4 009 bytes, compared with 431 bytes for ECDSA P-256. Composite adds 171 bytes to the pure post-quantum certificate and is the smallest measured hybrid option. Passive Authentication validates the Document Signer certificate against CSCA trust material that inspection systems obtain independently, so the CSCA certificate is not stored on the chip. The chip budget must instead cover the complete Document Security Object, which carries the Document Signer certificate together with the CMS signature, the signed attributes and the data-group hashes.

ML-DSA-44 is the parameter set present in the measured artefacts and corresponds to NIST security category 2. BSI TR-02102-1 recommends only the category 3 and category 5 parameter sets, ML-DSA-65 and ML-DSA-87 [24]. Their larger public keys and signatures add the same amount to every post-quantum format in Table 2, so the sizes reported here are a lower bound for a deployed profile and the ranking of the formats is unchanged.

4.3 Format comparison

Table 3 compares the formats against the deployment constraints. Pure post-quantum and unbound two-certificate arrangements are not recommended for Passive Authentication. Hybrid-bound certificates are valid but larger than the other hybrid options. Catalyst and composite certificates are the two preferred formats.

Format	Certificate size (bytes)	Legacy terminal can verify	Downgrade resistance	Specification maturity at cut-off	Verdict for the Document Signer certificate
Pure PQ (ML-DSA-44)	4 009	No	Not applicable — no traditional component	Published RFC 9881	Not recommended — no hybrid property
Two certificates	4 440	Yes, traditional alone	Weak — no binding between the pair	No format change required	Not recommended — unbound pair
Hybrid bound (RFC 9763)	4 505	Yes, traditional alone	Moderate — digest binds the pair	Published RFC 9763	Fallback only — largest option
Hybrid catalyst	4 238	Yes, by design	Conditional — verifier must be configured to require the alternative signature	Published ITU-T X.509 (2019)	Recommended where terminals cannot be upgraded in step
Hybrid composite	4 180	No	Strong — one algorithm, no partial acceptance	RFC Editor queue (approved 22 Apr 2026)	Recommended where terminals can be upgraded in step
Certificate discovery (URI form)	Reduced only where the related certificate is held elsewhere	Yes, traditional alone	Not provided by discovery alone	Adopted WG draft, revision 03	Not recommended for the DS certificate; suitable for CSCA distribution

Table 3: Comparison of certificate formats for the Document Signer certificate.

Catalyst is appropriate where existing terminals must continue to verify newly issued documents. Updated terminals must be configured to require the alternative signature; otherwise the traditional signature becomes an unintended downgrade path.

Composite is appropriate where terminal software can be upgraded before deployment. It is smaller, uses one certificate and one verification path, and has been tested across multiple implementations. Its limitation is timing: the X.509 signature specification had not yet been published as an RFC at the cut-off date.

The size values do not establish absolute feasibility because available chip capacity has not been supplied, and the transmission figures exclude protocol framing and processing time. These two measurements must be completed before deployment planning is finalised.

4.4 Security risk analysis

Table 4 states the threat and risk scenarios that determine the choice of certificate format for Passive Authentication. Each scenario names the asset affected, the consequence if the

scenario is not addressed, and the recommendation in Section 6 that addresses it. Severity is stated as High where the scenario defeats the authenticity of the document or prevents inspection outright, and Medium where it degrades deployment, capacity or continuity.

#	Threat or risk scenario	Asset affected	Consequence	Severity	Mitigation
T1	A cryptographically relevant quantum computer recovers a Document Signer or CSCA private key from its public key	Document-issuing PKI; Document Security Object	A forged or altered eMRTD is accepted as authentic, and the trust chain used by inspection systems no longer establishes origin	High	R1
T2	A verifier accepts a catalyst certificate on the traditional signature alone and never evaluates the alternative signature	Document Signer certificate; inspection system	Post-quantum protection is lost while the document continues to verify, so the downgrade is not detected	High	R3
T3	A pure post-quantum certificate is issued with no traditional fall-back	Document Signer certificate; legacy inspection systems	Terminals that have not been upgraded cannot verify newly issued documents, and inspection fails at the border	High	R1, R2
T4	A traditional and a post-quantum certificate are issued as two unbound objects	Certificate chain	Nothing ties the two certificates to the same subject, so verifying one carries no assurance about the other	High	R1
T5	The hybrid Document Security Object exceeds the capacity of the chip or the time budget of the contactless interface	Chip storage; contactless transmission	The document cannot carry the security object as specified, or Passive Authentication no longer completes within the inspection time budget	Medium	R5
T6	Passive Authentication depends on retrieving the Document Signer certificate over a network at the time of inspection	Availability of inspection	Inspection fails wherever connectivity is unavailable, and the retrieval path becomes an additional point of attack	High	R4, R10
T7	A certificate profile is fixed on a specification that is still in the standardisation process	Certificate and CMS profiles	A late change to the specification invalidates deployed profiles and breaks interoperability between issuers and inspection systems	Medium	R7, R8, R9
T8	An algorithm or parameter set must be replaced within the ten-year validity of an issued document	Certificate profile; documents in circulation	Documents remain in circulation carrying a mechanism that can no longer be relied upon, with no defined replacement path	Medium	R6

Table 4: Threat and risk scenarios for the Document Signer certificate in Passive Authentication.

Scenarios T1, T2 and T4 concern the cryptographic properties of the certificate format and are addressed by binding the traditional and post-quantum credentials in a single object and by requiring both components to be evaluated. T3 concerns compatibility and requires a transition profile matched to the inspection systems in service; a composite certificate alone does not provide that compatibility, which is why R2 retains the catalyst format where terminals cannot be upgraded in step. Scenarios T5 to T8 concern deployment, and are addressed by sizing the security object against measured chip and interface budgets, by fixing profiles only on stable specifications, and by defining algorithm replacement for future issuance together with a reissuance path for documents already in circulation.

5. Project risks

Critical risk 3 materialised. Composite ML-DSA for X.509 reached the RFC Editor queue, but Composite ML-KEM remained in IESG processing and certificate discovery remained a working-group draft. The project mitigated this risk by contributing directly to the specifications and by making the affected recommendations conditional on publication.

Risk 1 partly materialised for FN-DSA. FIPS 203, 204 and 205 [4] [5] [6] were final before the project began, while FIPS 206 [7] had not been published at the cut-off date. Certificate and CMS work for FN-DSA cannot be completed until the standard is final. Risk 2 did not materialise at algorithm level, but changes to the composite ML-KEM encoding required corresponding implementation updates.

6. Recommendations

The following recommendations are based on the document status and measurements available on 12 August 2026.

- R1.** Use hybrid post-quantum and traditional certificates for Passive Authentication. Do not use a pure post-quantum certificate without a traditional fall-back.
- R2.** Use catalyst certificates where inspection systems cannot be upgraded together. Use composite certificates where coordinated terminal upgrades are possible.
- R3.** Require catalyst verifiers to check the alternative signature. Record acceptance based only on the traditional signature as a downgrade.
- R4.** Do not make Passive Authentication depend on retrieving the Document Signer certificate over a network during inspection.

- R5.** Plan chip storage and inspection time for the complete Document Security Object and its protocol overhead, not for the Document Signer certificate alone. Budget CSCA trust-anchor storage separately in the inspection system.
- R6.** Specify algorithm agility in the eMRTD certificate profile and allow several parameter sets under one ASN.1 definition where the security analysis permits. Define a reissuance strategy for documents whose mechanisms must be retired before expiry; issued Logical Data Structure version 1 (LDS1) documents cannot be rewritten in the field.
- R7.** Adopt Composite ML-DSA for the eMRTD certificate profile once the X.509 specification is published as an RFC.
- R8.** Defer a decision on Composite ML-KEM for eMRTD until the specification completes IESG processing.
- R9.** Do not plan eMRTD deployment around FN-DSA until FIPS 206 is published. Repeat the certificate-size measurements after publication.
- R10.** Consider certificate discovery for distributing CSCA material between States, but not for the Document Signer certificate stored on the chip.

7. Remaining work and conclusion

Work Package 4 should complete the following actions before preparing the migration plan:

- Obtain the certificate capacity available in the logical data structure of the target chip platforms from the chip and document manufacturers.
- Measure end-to-end inspection time with a complete hybrid certificate chain, including protocol and chip-processing overhead.
- Re-check the publication status of Composite ML-DSA, Composite ML-KEM, certificate discovery and FIPS 206, and update the profile references accordingly.
- Confirm how the final ENISA Agreed Cryptographic Mechanisms guidance affects the certificate-profile choices.

The project has advanced four contributed documents to RFC publication and has produced implementation artefacts for the principal quantum-safe certificate formats. The measurements show that moving from elliptic-curve cryptography accounts for most of the certificate-size increase. Adding a traditional fall-back to a post-quantum certificate has a comparatively small cost.

Catalyst and composite certificates are therefore the preferred options for the Document Signer certificate. Catalyst supports gradual deployment across existing terminals. Composite is smaller and avoids partial verification, but it requires coordinated software upgrades and a

stable published specification. The choice should be made for each deployment according to those operational conditions.

8. References

8.1 Standards and published RFCs

- [1] ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021, Part 10, Logical Data Structure for Storage of Biometrics and Other Data in the Contactless Integrated Circuit.
- [2] ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021, Part 12, Public Key Infrastructure for MRTDs.
- [3] ITU-T Recommendation X.509, edition 9, October 2019, including Amendment 1 of October 2024.
- [4] NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, August 2024.
- [5] NIST FIPS 204, Module-Lattice-Based Digital Signature Standard, August 2024.
- [6] NIST FIPS 205, Stateless Hash-Based Digital Signature Standard, August 2024.
- [7] NIST FIPS 206, FN-DSA, in development; not published at 12 August 2026.
- [8] RFC 9763, Related Certificates for Use in Multiple Authentications within a Protocol, June 2025.
- [9] RFC 9802, Use of the HSS and XMSS Hash-Based Signature Algorithms in Internet X.509 Public Key Infrastructure, June 2025.
- [10] RFC 9814, Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax, July 2025.
- [11] RFC 9881, Internet X.509 Public Key Infrastructure Algorithm Identifiers for ML-DSA, October 2025.
- [12] RFC 9882, Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax, October 2025.
- [13] RFC 9909, Internet X.509 Public Key Infrastructure Algorithm Identifiers for SLH-DSA, December 2025.
- [14] RFC 9935, Internet X.509 Public Key Infrastructure Algorithm Identifiers for ML-KEM, March 2026.
- [15] RFC 9936, Use of ML-KEM in the Cryptographic Message Syntax, March 2026.

8.2 Current drafts and supporting records

- [16] draft-ietf-lamps-pq-composite-sigs-19, Composite ML-DSA for use in X.509 Public Key Infrastructure, 21 April 2026.
- [17] draft-ietf-lamps-pq-composite-kem-18, Composite ML-KEM for use in X.509 Public Key Infrastructure, 23 July 2026.
- [18] draft-ietf-lamps-certdiscovery-03, A Mechanism for X.509 Certificate Discovery, 21 May 2026.
- [19] draft-ietf-lamps-cms-fn-dsa-00, Use of FN-DSA in the Cryptographic Message Syntax, 20 May 2026.
- [20] IETF Hackathon, post-quantum certificate and CMS interoperability test artefacts, CryptoNext contribution, 23 July 2026.
- [21] PQC4eMRTD D2.1, Report on the state of standardization for quantum-safe X.509 certificates, 2025.
- [22] European Commission Grant Agreement 101190400, PQC4eMRTD, DIGITAL-ECCC-2024-DEPLOY-CYBER-06, 2024.
- [23] Open Quantum Safe project, post-quantum X.509 and Transport Layer Security interoperability resources. <https://openquantumsafe.org/applications/x509.html>

[24] BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2026-01, 23 January 2026.

Annex A — Log of standardisation activity

Table 5: Log of standardisation activity carried out under Task 3.1, January 2025 to 12 August 2026.

#	Date	Body / working group	Document or event	Action taken	Outcome	Evidence
1	07/01/2025 – 27/03/2025	IETF Hackathon	PQC certificate artefacts	Interoperability artefacts for PQ certificates and CMS; compatibility matrices added and updated	Accepted into the IETF Hackathon artefact set	IETF Hackathon artefact set, January–March 2025
2	H1 2025	IETF LAMPS	draft-ietf-lamps-x509-slhdsa	Authored revisions 04–08	Published as RFC 9909, Dec 2025	RFC 9909
3	H1 2025	IETF LAMPS	draft-ietf-lamps-cms-kyber	Authored revisions 08–09	Published as RFC 9936, Mar 2026	RFC 9936
4	H1 2025	IETF LAMPS	draft-ietf-lamps-cms-ml-dsa	Review and approval of revisions 02–05	Published as RFC 9882, Oct 2025	RFC 9882
5	H1 2025	IETF LAMPS / IESG	draft-ietf-lamps-x509-shbs	Updates in response to RFC Editor feedback	Published as RFC 9802, Jun 2025	RFC 9802
6	H1 2025	IETF LAMPS	cms-euf-cma-signeddata	Published revision 01 as an individual draft	Adopted by the working group	draft-ietf-lamps-cms-euf-cma-signeddata
7	15–16/03/2025	IETF 122 Hackathon (remote)	PQC certificate artefacts	Interoperability artefacts for PQ certificates and CMS; compatibility matrix updated to the current artefact format	Artefacts cross-tested by other implementers	IETF 122 Hackathon artefact set
8	17–21/03/2025	IETF 122 — LAMPS	draft-ietf-lamps-x509-slhdsa	Presented draft updates at the working-group session	Draft advanced; published Dec 2025	Session recording
9	17–21/03/2025	IETF 122 — LAMPS	draft-ietf-lamps-cms-kyber	Presented draft updates at the working-group session	Draft advanced; published Mar 2026	Session recording
10	17–21/03/2025	IETF 122 — LAMPS	cms-euf-cma-signeddata	Presented the draft at the working-group session	Subsequently adopted by the working group	Session recording
11	04/2025	PQCC (MITRE)	Artifact Signing: Dual, Post-Quantum/Traditional Hybrid Signatures and Downgrades	Co-authored the publication	Published April 2025	pqcc.org

#	Date	Body / working group	Document or event	Action taken	Outcome	Evidence
12	06/2025	IETF LAMPS / RFC Editor	RFC 9802	Carried the document through RFC Editor processing	Published, first author CryptoNext	rfc-editor.org/info/rfc9802
13	19–25/07/2025	IETF 123 Hackathon (in person)	PQC certificate artefacts	Artefacts for Composite ML-DSA and Composite ML-KEM; object identifiers updated to the current drafts	Artefacts cross-tested by other implementers	IETF 123 Hackathon artefact set
14	21/07/2025	IETF Hackathon	PQC certificate artefacts	Added automated validation of Hackathon artefacts with OpenSSL 3.5	Continuous validation adopted for the artefact set	IETF Hackathon artefact set, July 2025
15	10/2025	IETF LAMPS / RFC Editor	RFC 9882	Co-authored; carried to publication	Published October 2025	rfc-editor.org/info/rfc9882
16	01–08/11/2025	IETF 124 Hackathon (in person)	PQC certificate artefacts	Artefacts for the current Composite ML-DSA and Composite ML-KEM; CMS automated tests with OpenSSL 3.6	Artefacts cross-tested by other implementers	IETF 124 Hackathon artefact set
17	01–08/11/2025	IETF 124 — LAMPS	Best Practices for Signed Attributes in CMS SignedData	Presented draft updates at the working-group session	Draft advanced to working-group revision 02	Session recording
18	12/2025	IETF LAMPS / RFC Editor	RFC 9909	Co-authored; carried to publication	Published December 2025	rfc-editor.org/info/rfc9909
19	19–27/01/2026	IETF LAMPS interim hackathon	PQC certificate artefacts	Artefacts updated for the interim event; composite KEM object identifiers moved to production values	Interoperability tables rebuilt	IETF LAMPS interim hackathon artefact set
20	27/02/2026	IETF LAMPS	draft-ietf-lamps-cms-euf-cma-signeddata	Published working-group revision 02	In Area Director evaluation at the cut-off date	draft-ietf-lamps-cms-euf-cma-signeddata-02
21	03/2026	IETF LAMPS / RFC Editor	RFC 9936	First author; carried to publication	Published March 2026	rfc-editor.org/info/rfc9936
22	14–20/03/2026	IETF 125, Shenzhen	—	No participation; LAMPS session followed remotely from published materials	Draft work continued over the same period	
23	20/05/2026	IETF LAMPS	draft-turner-lamps-cms-fn-dsa	Authored; put forward for adoption	Adopted by the working group as draft-ietf-lamps-cms-fn-dsa-00	datatracker.ietf.org/doc/draft-ietf-lamps-cms-fn-dsa/
24	02/06/2026	IETF Hackathon	PQC certificate artefacts	Updated CryptoNext artefacts for Composite ML-KEM; corrected CHOICE private-key testing	Merged	IETF Hackathon artefact set, June 2026

#	Date	Body / working group	Document or event	Action taken	Outcome	Evidence
25	15/06/2026	ENISA	Agreed Cryptographic Mechanisms v3.0	Submitted a response to the public review, opened 2 June 2026	Held by ENISA as a consultation contribution; disposition not known at the cut-off date	ENISA public consultation on Agreed Cryptographic Mechanisms v3.0
26	22/06/2026	IETF (individual)	draft-vangeest-lamps-update-asn1-signed-type-00	Authored and submitted	Active individual draft	datatracker.ietf.org/doc/draft-vangeest-lamps-update-asn1-signed-type/
27	20/07/2026	IETF Hackathon	PQC certificate artefacts	Added CryptoNext artefacts for FrodoKEM	Merged into the Hackathon artefact set	IETF Hackathon artefact set, July 2026
28	23/07/2026	IETF 126 — LAMPS, Vienna	draft-vangeest-lamps-update-asn1-signed-type-00	Presented the draft at the working-group session, agenda item 6c	Defect in RFC 5912 affecting composite ML-DSA decoders recorded in the minutes	Minutes and recording, IETF 126 LAMPS session
29	26/07/2026	IETF Independent Stream	draft-housley-asn1-layman-guide-01	Formal review at the request of the Independent Stream Editor, with formatting and technical corrections	Review delivered to the Editor and authors; not published	—
30	01/2025 – 08/2026	IETF LAMPS, CFRG, IPSECME, PQUIP	Nine IETF documents reviewed under Task 3.1	Comments by mailing list, at meetings and in direct correspondence	Comments submitted to the respective working groups	IETF mail archive
31	Throughout	PQCC (MITRE)	State of the Migration tracker	Supplied IETF status updates	Tracker maintained	pqcc.org
32	Throughout	PKI Consortium PQC WG	—	Regular attendance	Attendance only; no attributable standardisation output	