

DISCLAIMER

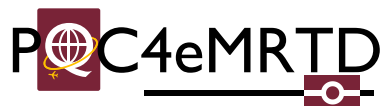
This document, D3.3 – Report on Standardization work on the travel and border landscape and the eMRTD framework, has been prepared as part of the PQC4eMRTD project, under Grant Agreement No 101190400, and is currently under review by the European Commission. It is provided for informational purposes only.



Funded by
the European Union



ECCE
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE





D3.3 – Standardization work on the travel and border landscape and the eMRTD framework

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:	IFAG
Type:	Report
Dissemination Level:	Public
Written by:	Antonio Escobar (IFAG), Detlef Houdeau (IFAG), Damien Bertonnier (THALES CDI), Samo Bardutzky (IPP PFLJUBLJANA)
Approved by:	Matina Maria Trompouki (BSC)
Reviewed by:	Daniel Van Geest (CRYPTONEXT)
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	24/07/2026	Antonio Escobar, Detlef Houdeau	First draft with ToC
v0.2	31/07/2026	Damien Bertonnier	First draft of sections 2.1 and 3
v0.3	13/08/2026	Detlef Houdeau	First draft of sections 2.3 and 2.4
v0.5	15/08/2026	Antonio Escobar	First review of Sections 2 and 3
v0.9	27/08/2026	Antonio Escobar, Samo Bardutzky	First draft of sections 1, 2.2 and 4
v0.10	15/09/2026	Antonio Escobar	Internal review by CRYPTONEXT; corrections to Section 2.3 and references
v0.11	17/09/2026	Antonio Escobar	Consortium partner names aligned with the grant agreement
v0.12	18/09/2026	Antonio Escobar	Added Section 2.5 with the consolidated migration risk analysis
v1.0	30/09/2026	Antonio Escobar	Final approval gate by BSC; consortium partner logos 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	9
1.1	Purpose and scope of D3.3	9
1.2	Relation to D2.3 and other PQC4eMRTD deliverables	9
2.	Standardisation Landscape Relevant to PQC4eMRTD	10
2.1	eMRTD and border-control standardisation	10
2.2	EU Digital Identity Wallet	11
2.3	Post-quantum cryptography standardisation	12
2.4	Crypto-agility and migration aspects for eMRTD	15
2.5	Migration risk analysis	17
3.	Participation in Standardisation Working Groups	18
3.1	Overview of relevant working groups	18
3.2	Active involvement of PQC4eMRTD in relevant working groups	19
3.3	Main technical outcomes and observations	20
4.	Conclusion	22
5.	References	23

List of Tables

Table 1: Commission Implementing Regulations supporting the EUDI Wallet framework.....	12
Table 2: Representative key sizes for selected PQC parameter sets	14
Table 3: Crypto-agility dimensions.....	15
Table 4: CRQC threat assessment for current eMRTD mechanisms (adapted from D2.3 [8])	16
Table 5: Migration risk analysis for eMRTD	18
Table 6: Standards development organisations relevant to D3.3	19
Table 7: PQC4eMRTD contributions to standards development organisations	20

List of Figures

Figure 1: Workflow of PQC4eMRTD with main eMRTD and border-control groups	11
---	----

Acronyms

ACRONYM	DEFINITION
AA	Active Authentication
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
ARF	Architecture and Reference Framework
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germany)
CA	Chip Authentication
CASG	Crypto Agility Sub-Group
CEN	European Committee for Standardization
CMS	Cryptographic Message Syntax
CRQC	Cryptographically Relevant Quantum Computer
CSCA	Country Signing Certification Authority
EAA	Electronic Attestation of Attributes
EAC	Extended Access Control
ECCG	European Cybersecurity Certification Group
eIDAS	electronic identification, authentication and trust services
eMRTD	electronic Machine-Readable Travel Document
ENISA	European Union Agency for Cybersecurity
ESI	Electronic Signatures and Trust Infrastructures
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCC	European Cybersecurity Certification Scheme on Common Criteria
EUDI	European Digital Identity
EUDIW	European Digital Identity Wallet
FCAF	Functional Conformance Assessment Framework
FIPS	Federal Information Processing Standards
FN-DSA	FFT over NTRU-Lattice-Based Digital Signature Algorithm
HQC	Hamming Quasi-Cyclic
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
JTC	Joint Technical Committee
KEM	Key-Encapsulation Mechanism
LAMPS	Limited Additional Mechanisms for PKIX and S/MIME
LDS	Logical Data Structure
LMS	Leighton-Micali Signature
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
MRTD	Machine-Readable Travel Document
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NTWG	New Technologies Working Group
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PAKE	Password-Authenticated Key Exchange
PID	Person Identification Data
PKD	Public Key Directory
PKI	Public Key Infrastructure

ACRONYM	DEFINITION
PKIX	Public-Key Infrastructure using X.509
PoC	Proof of Concept
PQC	Post-Quantum Cryptography
RFC	Request for Comments
RFI	Request for Information
RSA	Rivest–Shamir–Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SC	Subcommittee
SDO	Standards Development Organisation
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SM	Secure Messaging
TA	Terminal Authentication
TAG/TRIP	Technical Advisory Group on the Traveller Identification Programme
TC	Technical Committee
TF	Task Force
WG	Working Group
WP	Work Package
XMSS	eXtended Merkle Signature Scheme

1. Introduction

Electronic machine-readable travel documents are designed for global use over long operational lifetimes. Their security depends on public-key mechanisms for document authenticity, chip authentication, access control and protection of sensitive data. A cryptographically relevant quantum computer would undermine the RSA- and elliptic-curve-based mechanisms used in today's eMRTD ecosystem, while issued documents and inspection infrastructure would continue to operate for many years.

Migration to post-quantum cryptography therefore requires more than the selection of new algorithms. It requires coordinated evolution of ICAO and ISO specifications, the document-issuing Public Key Infrastructure, secure elements, personalisation systems, inspection systems, certification and European implementation measures. Global interoperability must be maintained throughout a transition in which classical and PQC-enabled documents and systems coexist.

PQC4eMRTD addresses this challenge by connecting developments in PQC algorithms, certificates and signed data formats with the specific security, privacy and deployment requirements of travel documents. This deliverable reports the project's standardisation activities and consolidates their implications for the eMRTD and border-control landscape.

1.1 Purpose and scope of D3.3

D3.3 reports standardisation work concerning the specification and use of travel documents for border security. Its scope covers the institutional standardisation framework; the document-issuing PKI and Passive Authentication; access-control and chip-authentication mechanisms; relevant PQC algorithms, certificates and signed-object formats; crypto-agility; European regulation and digital identity; and the migration of issuing and inspection infrastructure.

The report first describes the standards and regulatory landscape relevant to eMRTDs, the EU Digital Identity Wallet and PQC. It then examines crypto-agility and migration requirements, documents participation in standards development organisations, and presents the main technical outcomes and observations. Detailed analysis of quantum-safe X.509 and CMS formats is addressed in D3.1, while D3.2 addresses standardisation work on PQC, high-performance computing and quantum-computing hardware and software. Standards and regulatory status are reported as at 12 August 2026.

1.2 Relation to D2.3 and other PQC4eMRTD deliverables

D1.1 established the European regulatory and border-system context for travel documents [25]. D2.3 established the baseline for ICAO and ISO travel-document standards and assessed the impact of a cryptographically relevant quantum computer on existing eMRTD mechanisms [8]. D2.1 analysed the emerging standardisation landscape for quantum-safe X.509 certificates [12].

D3.3 advances these baselines from monitoring to active participation and migration analysis. It is coordinated with D3.1 and D3.2, connecting certificate, CMS and implementation developments to the eMRTD application layer. The resulting observations provide input to WP4 planning for standardisation, regulation, interoperability testing and deployment.

2. Standardisation Landscape Relevant to PQC4eMRTD

2.1 eMRTD and border-control standardisation

The electronic Machine-Readable Travel Document (eMRTD) framework is governed through a layered international and European standardisation system. The International Civil Aviation Organization (ICAO) Doc 9303 establishes the globally interoperable specifications for machine-readable travel documents, including the Logical Data Structure (LDS), the document-signing Public Key Infrastructure (PKI), Passive Authentication (PA) and chip-access mechanisms [9]. Supporting standards from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) include ISO/IEC 14443 for contactless communication and ISO/IEC 19794 for biometric data formats, as summarised in D2.3 [8].

Responsibilities are distributed across several bodies and liaison channels:

- The ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP) provides the strategic and policy forum for traveller identification and the evolution of the global Machine-Readable Travel Document (MRTD) framework.
- The ICAO New Technologies Working Group (NTWG) develops technical strategy, policy, specifications and guidance for the manufacture, issuance, validation and globally interoperable use of MRTDs. Formal ICAO decisions remain state-led.
- ISO/IEC Joint Technical Committee 1, Subcommittee 17, Working Group 3 (JTC1/SC17/WG3) develops traveller-identification standards and technical material in liaison with ICAO. Its Task Force 5 (TF5) Crypto Agility Sub-Group (CASG) addresses quantum threats, cryptographic agility, the document-issuing PKI and PA.
- ISO/IEC JTC1/SC17/WG4 addresses generic interfaces and protocols for security devices, while ISO/IEC JTC1/SC27/WG2 supplies expertise on cryptographic mechanisms. Their work can affect algorithm identifiers, smart-card commands, security-device interfaces and assurance requirements used by eMRTDs.
- National standards bodies, cybersecurity agencies and document-issuing authorities provide expert input through national delegations. Industry and research organisations contribute through these delegations, ISO working groups, information papers, requests for information, demonstrations and accepted presentations.

The European layer adds requirements that are not fully global. Extended Access Control (EAC), including Terminal Authentication (TA) and Chip Authentication (CA), protects access to sensitive biometrics under the European Union (EU) travel-document framework but is not a globally mandatory ICAO Doc 9303 mechanism [8]. EU institutions and the Article 6 committee therefore have an important role in translating international specifications into requirements for EU passports and inspection systems.

The migration also affects operational trust infrastructure. Country Signing Certification Authorities (CSCAs), Document Signers, certificate distribution through bilateral channels or the ICAO Public Key Directory (PKD), personalisation systems and border-control inspection systems must adopt compatible profiles and transition schedules. A cryptographic algorithm is therefore not usable globally merely because it has been standardised by the National Institute of Standards and Technology (NIST) or the

Internet Engineering Task Force (IETF); ICAO/ISO profiles, implementation guidance, certification and interoperability evidence are also required.

Figure 1 summarises the contribution path used by PQC4eMRTD: project results are discussed through ISO/IEC and national expert channels, presented to ICAO NTWG and connected to EU regulatory and deployment stakeholders. Feedback from issuing and inspection authorities supports refinement of protocol and migration proposals.

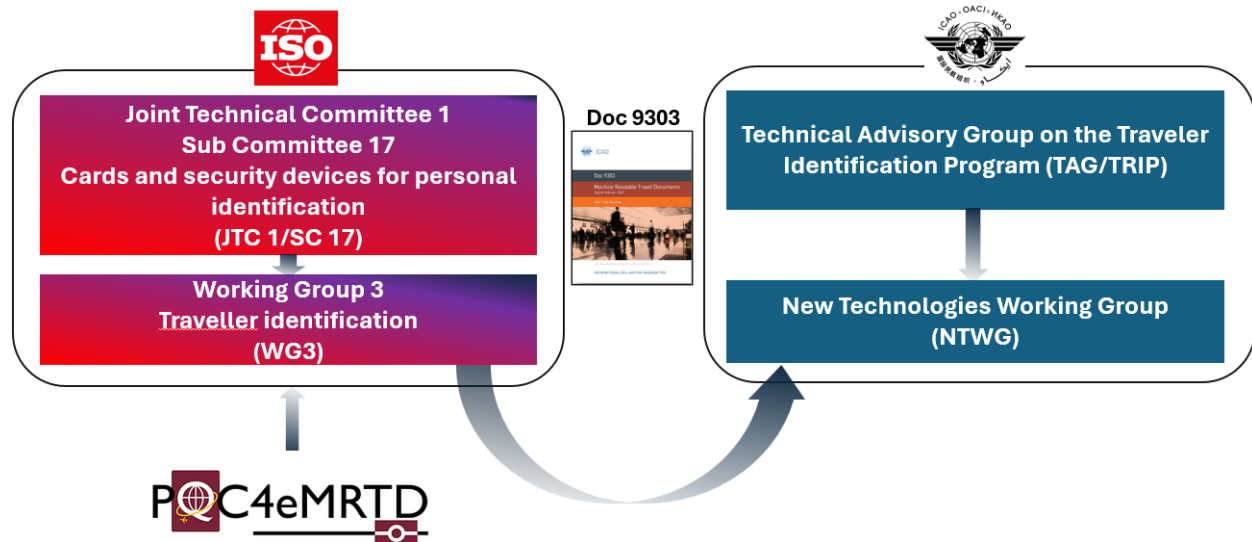


Figure 1: Workflow of PQC4eMRTD with main eMRTD and border-control groups

2.2 EU Digital Identity Wallet

The European Digital Identity Wallet (EUDIW) forms part of the European digital identity standardisation landscape. Its legal basis is the European Digital Identity Framework established by Regulation (EU) 2024/1183, which amended Regulation (EU) No 910/2014 on electronic identification, authentication and trust services (eIDAS) [16]. The revised framework provides for Wallet units through which users can securely store, manage and present person identification data (PID) and electronic attestations of attributes (EAAs), including in cross-border interactions. Commission implementing acts specify technical standards, specifications and procedures for interoperability, security, certification and consistent implementation across the EU.

The initial implementing package adopted in 2024 comprises the acts summarised in Table 1.

Implementing Regulation	Subject matter
Commission Implementing Regulation (EU) 2024/2977 [17]	Person identification data and electronic attestations of attributes issued to EUDI Wallets, including issuance, authenticity, validity and revocation.
Commission Implementing Regulation (EU) 2024/2979 [18]	Integrity and core functionalities of EUDI Wallets and Wallet units.
Commission Implementing Regulation (EU) 2024/2980 [19]	Notifications to the Commission concerning the EUDI Wallet ecosystem.

Implementing Regulation	Subject matter
Commission Implementing Regulation (EU) 2024/2981 [20]	Certification of European Digital Identity Wallets.
Commission Implementing Regulation (EU) 2024/2982 [21]	Protocols and interfaces supported by the European Digital Identity Framework.

Table 1: Commission Implementing Regulations supporting the EUDI Wallet framework

The regulatory and technical framework continues to evolve. Commission Implementing Regulation (EU) 2026/1731 amended Regulations (EU) 2024/2977, 2024/2979, 2024/2980 and 2024/2982 as regards applicable standards and specifications, and entered into force on 11 August 2026 [22].

The coordinated technical framework originated with Commission Recommendation (EU) 2021/946, which called on Member States and the Commission to develop a common Union Toolbox comprising an Architecture and Reference Framework (ARF), common standards and technical specifications, and common guidelines and best practices [23].

The ARF defines the common technical architecture for the EUDIW ecosystem and profiles standards and specifications for interoperable implementations. Version 3.0.0, released on 23 July 2026, aligns the framework with the amending implementing regulations and introduces a Functional Conformance Assessment Framework (FCAF) for Wallet solutions [24].

The EUDIW architecture combines standards and specifications from several European and international organisations. The European Telecommunications Standards Institute (ETSI), including its Technical Committee on Electronic Signatures and Trust Infrastructures (TC ESI), develops standards for trust services, certificate profiles, attestations and cryptographic mechanisms. The European Committee for Standardization (CEN), through CEN/TC 224, covers personal identification and related personal devices. ISO/IEC JTC1/SC17 develops standards for cards, security devices and mobile identification documents. The OpenID Foundation develops credential-issuance and presentation protocols, while the IETF provides underlying Internet and selective-disclosure specifications. The ARF selects and profiles these components for the EUDIW ecosystem [24].

The EUDIW and the ICAO eMRTD framework are distinct systems with different governance and use cases. Their post-quantum transitions nevertheless share dependencies on trust anchors, signed identity data, certificate validation, cryptographic suites, certified components and cross-border interoperability. PQC migration of eMRTD and Digital Travel Credential functions therefore needs to remain compatible with the evolving European digital identity trust and certification framework, without treating the EUDIW as a replacement for ICAO travel documents.

2.3 Post-quantum cryptography standardisation

D2.3 established the initial Post-Quantum Cryptography (PQC) baseline for the travel and border domain [8]. Since then, the standards landscape has matured at algorithm, certificate, message-format and European migration-policy levels. These layers must be considered together because eMRTD security depends on algorithms, encoded security objects, certificates, PKI operations and inspection-system interoperability.

NIST published three final United States Federal Information Processing Standards (FIPS) on 13 August 2024:

- FIPS 203 specifies ML-KEM, a module-lattice-based key-encapsulation mechanism (KEM) derived from CRYSTALS-Kyber [1].
- FIPS 204 specifies ML-DSA, a module-lattice-based digital-signature algorithm derived from CRYSTALS-Dilithium [2].
- FIPS 205 specifies SLH-DSA, a stateless hash-based digital-signature algorithm derived from SPHINCS+ [3].

NIST SP 800-208 specifies the stateful hash-based Leighton-Micali Signature (LMS) and eXtended Merkle Signature Scheme (XMSS) [4]. Their state-management requirements restrict the roles for which they are suitable. RFC 9802 consequently treats stateful hash-based signatures as specialised mechanisms for tightly controlled signing environments rather than general-purpose end-entity certificates [13].

Additional algorithmic diversity is under development. NIST is preparing FIPS 206 for FN-DSA, derived from FALCON, and selected the code-based Hamming Quasi-Cyclic (HQC) mechanism for standardisation as a second PQC KEM family. Their final specifications will determine their suitability for future eMRTD profiles.

For eMRTDs, algorithm standards are only the first layer. The CSCA and Document Signer hierarchy uses certificate profiles, while the Document Security Object used for PA is based on Cryptographic Message Syntax (CMS) SignedData. Work in the IETF Limited Additional Mechanisms for PKIX and S/MIME (LAMPS) working group is therefore directly relevant. During the project, CRYPTONEXT contributed to PQC certificate and CMS work, interoperability artefacts and draft reviews. Published Requests for Comments (RFCs) include RFC 9882 for ML-DSA in CMS and RFC 9909 for SLH-DSA algorithm identifiers in X.509 [14] [15]. D2.1 established the certificate-format baseline, which is developed further in D3.1 and which D3.3 uses as an input to the eMRTD migration discussion [12].

Selection for an eMRTD profile must evaluate more than nominal security strength. Public- and private-key size, signature or ciphertext size, signing and verification performance, chip memory, communication limits, Hardware Security Module (HSM) support, side-channel and fault resistance, certificate-chain growth and inspection-system compatibility all affect deployability. National guidance such as the German Federal Office for Information Security (BSI) Technical Guideline TR-02102-1 recommends quantum-safe mechanisms and the periods for which they are considered suitable [5]. Table 2 gives representative key sizes for selected parameter sets as specified in the corresponding algorithm standards [1] [2] [3] and in the FALCON specification [26].

PQC algorithm	Type	NIST security category	Private-key length (bits)	Public-key length (bits)
ML-KEM-512 (derived from CRYSTALS-Kyber), FIPS 203	KEM	1	13,056	6,400
ML-KEM-768	KEM	3	19,200	9,472
ML-KEM-1024	KEM	5	25,344	12,544
ML-DSA-44 (derived from CRYSTALS-Dilithium), FIPS 204	Digital signature	2	20,480	10,496
ML-DSA-65	Digital signature	3	32,256	15,616
ML-DSA-87	Digital signature	5	39,168	20,736
FN-DSA-512 (derived from FALCON), FIPS 206 in preparation	Digital signature	1	10,248	7,176
FN-DSA-1024	Digital signature	5	18,440	14,344
SLH-DSA-SHA2-128s and SLH-DSA-SHAKE-128s (derived from SPHINCS+), FIPS 205	Digital signature	1	512	256
SLH-DSA-SHA2-192s and SLH-DSA-SHAKE-192s	Digital signature	3	768	384
SLH-DSA-SHA2-256s and SLH-DSA-SHAKE-256s	Digital signature	5	1,024	512

Table 2: Representative key sizes for selected PQC parameter sets

Table 2 compares key sizes only. It must not be interpreted as a comparison of signature or ciphertext sizes: SLH-DSA, for example, has small keys but large signatures. Parameter-set selection must therefore be performed for each protocol and PKI role using a complete communication and implementation profile. The FN-DSA values are those of the FALCON submission and remain provisional until FIPS 206 is published. FIPS 205 defines twelve SLH-DSA parameter sets: the SHA2 and SHAKE variants, and the small-signature (s) and fast-signing (f) variants of a given security category, share the same key sizes, so Table 2 lists the s variants only.

Parameter-set selection is further constrained by national guidance. Version 2026-01 of BSI TR-02102-1 recommends only ML-KEM-768 and ML-KEM-1024 for key agreement, and only ML-DSA-65, ML-DSA-87 and the 192-bit and 256-bit SLH-DSA parameter sets for signatures; the NIST category 1 and category 2 rows of Table 2 are therefore outside its recommendations, and FN-DSA is not covered because FIPS 206 has not been published [5]. ANSSI requires the conjectured post-quantum security level to be as high as possible, preferably NIST level V, and states that no closed list of eligible cryptographic algorithms exists for the French security visas [27]. Both agencies currently recommend that quantum-safe mechanisms be deployed in hybrid combination with a classical mechanism, with hash-based signatures as the stated exception. For an eMRTD profile, the category 3 and category 5 parameter sets are therefore the practical candidates; the lower categories are retained in Table 2 as a size reference only.

At the European level, Version 2 of Agreed Cryptographic Mechanisms supports the European Cybersecurity Certification Scheme on Common Criteria (EUCC) and provides guidance to developers and evaluators [6]. It complements rather than replaces national catalogues and product-specific certification requirements.

The Network and Information Systems (NIS) Cooperation Group roadmap defines a coordinated, risk-based migration path and timeline [7]:

- By 31 December 2026, Member States should implement the First Steps, establish initial national roadmaps and initiate planning and pilots for high- and medium-risk use cases.
- By 31 December 2030, high-risk use cases should be migrated, medium-risk pilots and planning completed, and quantum-safe software and firmware upgrade paths enabled by default.
- By 31 December 2035, medium-risk use cases should be migrated and low-risk use cases transitioned as far as feasible.

The roadmap does not assign an automatic category to every eMRTD mechanism. PQC4eMRTD must apply the risk criteria separately to long-term confidentiality, document authenticity, biometric access control, inspection availability, document lifetime and infrastructure dependencies. ICAO and ISO must then profile approved algorithms, parameter sets, object identifiers, certificate and CMS encodings, hybridisation rules and failure behaviour before global deployment can begin.

2.4 Crypto-agility and migration aspects for eMRTD

Crypto-agility is the ability to identify, govern and replace cryptographic mechanisms without losing security, interoperability or service continuity. It is required for the PQC transition, but it is also needed when algorithms, parameters, implementations or assurance requirements change for other reasons.

Crypto-agility comprises the five dimensions shown in Table 3. Effective migration requires all five; supporting an additional algorithm in software is insufficient unless certificate policy, procurement, HSMs, readers and regulatory approval can evolve with it.

Agility dimension	Goal of the agility dimension
Knowledge and governance	Decision-makers understand the cryptographic threat, dependencies, approved mechanisms and ownership of transition decisions.
System and asset knowledge	The organisation maintains an inventory of algorithms, keys, certificates, protocols, products and dependencies across issuing and inspection systems.
Agility in processes	Risk, procurement, certification, incident, approval and migration processes can introduce or retire cryptographic mechanisms in a controlled manner.
Agility in systems	Interfaces, data formats, capacity and update mechanisms permit replacement or coexistence of cryptographic components.
Agility of algorithms and profiles	Approved alternatives, parameter sets, identifiers, negotiation rules and security policies are available for each protocol role.

Table 3: Crypto-agility dimensions

Applied to eMRTDs, these dimensions create a system-of-systems problem:

- Document lifetime and coexistence: passports are commonly valid for up to ten years. Classical-only, hybrid and PQC-enabled documents may therefore coexist across several issuance cycles.
- Chip and communication constraints: secure elements have bounded memory and processing capacity, while larger keys, signatures and protocol messages can affect contactless communication time and implementation resistance.
- PKI and trust distribution: CSCAs, Document Signers, certificate policies, HSMs, master lists, bilateral exchange and the ICAO PKD need compatible profiles and rollover procedures.

- Inspection infrastructure: border readers, middleware, validation services and back-end systems must accept new objects without rejecting valid legacy documents or silently downgrading security.
- Assurance and governance: algorithm approval, Common Criteria protection profiles, product certification, operational accreditation, procurement and EU legal requirements must evolve with the technical specification.
- Protocol and object agility: algorithm identifiers, data structures, certificate formats, negotiation and error handling must be unambiguous. Hybrid designs need binding and downgrade resistance so that an attacker cannot remove the PQC component or force a weaker validation path.

D2.3 reproduced the threat assessment shown in Table 4 [8]. It ranks PA as the highest priority because a Cryptographically Relevant Quantum Computer (CRQC) would compromise the document-signing PKI and the authenticity of signed document data. The assessment nevertheless identifies material risks to Password Authenticated Connection Establishment (PACE), Chip Authentication, Active Authentication and TA. The absence of a direct break for symmetric Secure Messaging does not make the complete protocol stack quantum-safe.

Cryptographic protocol for border and travel	Impact of a CRQC on current protocol implementation	Threat severity
Passive Authentication (PA)	Cryptographic protection of an eMRTD would be entirely compromised. Both the document-issuing PKI and the data stored by an eMRTD would be affected.	High
Chip Authentication (CA) / Active Authentication (AA)	Protection against cloning or substitution of the eMRTD chip would no longer be available.	Medium
Password Authenticated Connection Establishment (PACE)	The inspection procedure of an eMRTD chip would no longer be protected from sniffing and/or eavesdropping.	Medium
Terminal Authentication (TA)	Protection of highly sensitive biometric data on a chip would no longer be available.	Medium
Secure Messaging (SM)	No Shor-type break of the symmetric algorithms; generic quantum key search, and compromise of PACE or Chip Authentication, can still affect confidentiality.	Dependent on algorithms, key lengths and key establishment

Table 4: CRQC threat assessment for current eMRTD mechanisms (adapted from D2.3 [8])

Migration strategy distinguishes prioritisation from overall scope. Migrating Passive Authentication first addresses the highest-ranked threat, whereas deferring PACE, Chip Authentication and Terminal Authentication prolongs dependence on quantum-vulnerable public-key mechanisms and can require a second infrastructure transition. A coordinated transition can reduce repeated deployment effort but depends on the concurrent availability of specifications, proofs, implementations and interoperability testing.

The following migration principles follow from the project baseline and the EU roadmap [7] [8]:

- Maintain a cryptographic inventory and dependency map covering documents, certificates, HSMs, personalisation, inspection and trust-distribution systems.
- Define algorithm and parameter profiles per role, including identifiers, object encodings, key and signature sizes, validation policy and explicit failure behaviour.
- Specify classical/PQC binding, downgrade resistance and policy handling for any hybrid or dual-mode design.

- Plan CSCA and Document Signer rollover, certificate-chain coexistence, master-list/PKD distribution and revocation or retirement procedures.
- Update chips, operating systems, personalisation equipment, HSMs, readers and back-end validation services with sufficient capacity and secure update paths.
- Align ICAO/ISO specifications, EU legal measures, security certification, national implementation and procurement schedules.
- Validate conformance, negative/error cases, performance and interoperability across multiple document issuers and inspection-system vendors before issuance.
- Monitor algorithm, implementation and certification developments and retain a controlled rollback or replacement path.

An implementation sequence comprises international profile and protocol agreement; EU and national legal assessment; prototype and security-proof completion; certification-profile updates; PKI and infrastructure preparation; multi-vendor interoperability testing; national procurement and rollout; and long-term mixed-fleet operation. The competent bodies establish the applicable timelines and legal procedures.

These findings form a direct handover to Work Package 4 (WP4), which must turn the standards options into dated standardisation, regulation, testing and field-trial migration plans.

2.5 Migration risk analysis

Table 5 consolidates the risks that arise from the migration itself. It complements Table 4: where Table 4 states the effect of a CRQC on each eMRTD mechanism, Table 5 states what can go wrong while that effect is being removed, and the measure that contains it. Severity is stated as High where the risk defeats the objective of the migration or the confidentiality of data already recorded, and Medium where it delays or fragments deployment.

#	Risk scenario	Affected layer	Consequence if not contained	Severity	Containment measure
M1	Migration is confined to Passive Authentication and the remaining mechanisms are deferred without a dated plan	Chip protocols: PACE, Chip Authentication, Terminal Authentication, Active Authentication	The document retains a dependence on quantum-vulnerable public-key mechanisms, and a second infrastructure transition may become necessary	High	Treat the priority given to Passive Authentication as a sequence, not a scope, and fix the order and dates for the remaining mechanisms
M2	The post-quantum component of a hybrid object is stripped, or a verifier is driven onto the classical validation path	Certificate and Document Security Object formats; inspection software	Verification succeeds on the classical component alone, so post-quantum protection is lost without any indication to the operator	High	Cryptographic binding between the components, explicit validation rules, and downgrade and stripping resistance stated in the profile
M3	Encrypted chip–terminal exchanges are recorded before migration and retained until a CRQC becomes available	Biometric and personal data carried in secure messaging established through PACE and Chip Authentication	Confidentiality is lost retrospectively for data that is captured now and decrypted later	High	Keep the confidentiality mechanisms inside the migration scope and apply the risk criteria of the NIS Cooperation Group roadmap

#	Risk scenario	Affected layer	Consequence if not contained	Severity	Containment measure
M4	Classical, hybrid and post-quantum documents circulate at the same time across issuance cycles	Inspection infrastructure; mixed document population	Readers reject valid documents, or accept them by falling back to the weaker mechanism without recording the fact	High	A validation policy for mixed populations, with negative and error-case conformance testing completed before issuance begins
M5	Post-quantum keys, signatures and protocol messages exceed the capacity of the secure element or the contactless interface	Secure elements; contactless communication	Documents cannot be personalised as specified, or inspection time and implementation attack resistance degrade below acceptable levels	Medium	Select parameter sets per role against complete communication and implementation budgets rather than key size alone
M6	CSCA and Document Signer rollover is not coordinated with the introduction of the new profiles	Document-issuing PKI, master lists, ICAO Public Key Directory, bilateral exchange	Certificate chains cannot be validated across States, and cross-border acceptance of valid documents fails	Medium	Define rollover, coexistence and retirement procedures together with the profile, and exercise them before the first issuance
M7	Certification and assurance frameworks are updated later than the technical specification	Common Criteria protection profiles, EUCC, national approval and procurement	Certified products are not available when the specification is ready, and deployment stalls after the technical work is complete	Medium	Align the update of certification profiles with the ICAO and ISO milestones, and begin the assurance work in parallel
M8	International specifications are not final when the milestones of the NIS Cooperation Group roadmap fall due	International specifications measured against the EU roadmap	Member States implement divergent national solutions, and cross-border interoperability is lost for the lifetime of those documents	Medium	Monitor and contribute to the specification timelines, and retain a controlled rollback or replacement path

Table 5: Migration risk analysis for eMRTD

Risks M1 to M4 concern the security properties of the migrated system and are addressed by the specification and by the validation policy applied to it. Risks M5 to M8 concern capacity, governance and timing, and are addressed by the migration plan. The mitigations in Table 5 require implementation, validation and residual-risk review; WP4 carries both groups forward as dated actions with named owners.

3. Participation in Standardisation Working Groups

3.1 Overview of relevant working groups

PQC4eMRTD uses several connected forums because no single body controls the full eMRTD cryptographic stack. Table 6 summarises the decision-making, application-profile, primitive/format, certification and EU implementation channels across the relevant standards development organisations (SDOs).

Body or group	Role relevant to D3.3	PQC4eMRTD participation or dependency
ICAO TAG/TRIP and NTWG	Global policy, requirements and guidance for interoperable MRTDs; NTWG evaluates new technologies and work priorities.	Project presentations, demonstrations and information supplied through accepted forums and state/ISO channels.
ISO/IEC JTC1/SC17/WG3	Traveller-identification standards and technical material supporting ICAO Doc 9303.	IFAG and THALES CDI experts participate; TF5/CASG is the main crypto-agility channel.
ISO/IEC JTC1/SC17/WG4 and SC27/WG2	Security-device interfaces/protocols and cryptographic-mechanism expertise.	Dependencies for smart-card commands, algorithm integration, device interfaces and assurance.
IETF LAMPS	X.509, CMS and algorithm identifiers used by certificate and signed-object ecosystems.	CRYPTONEXT contributions in D3.1 supply certificate/CMS building blocks relevant to PA and the issuing PKI.
European Cybersecurity Certification Group (ECCG) / European Union Agency for Cybersecurity (ENISA), EU institutions and Article 6 committee	ECCG/ENISA provide EU cryptographic and EUCC certification guidance. EU institutions and the Article 6 committee govern legal and technical implementation of EU travel-document requirements.	Legal and migration alignment involving IFAG, IPP PFLJUBLJANA and project stakeholder contacts.
National bodies and agencies	National positions, algorithm catalogues, certification and expert representation.	Engagement through BSI, the French National Cybersecurity Agency (ANSSI), national standards bodies and issuing/inspection authorities.

Table 6: Standards development organisations relevant to D3.3

The CASG originated from an August 2023 request to establish the activity, followed by initiation of the NTWG work in February 2024 [8]. The September 2024 NTWG report records the subsequent shift towards the document-issuing PKI and Passive Authentication as the highest-priority work area [10].

Two information-paper tracks are material to D3.3. Developments regarding Cryptographic Agility and Post Quantum Cryptography for eMRTDs addresses the broader threat and agility problem. Quantum safe mechanisms for the Document Issuing PKI and Passive Authentication analyses signature, PKI, certificate and hybridisation options. The latter was circulated as ISO/IEC JTC1/SC17/WG3 N188, release 0.02 dated 4 June 2025, following discussion at the NTWG meeting in Ottawa [11].

The three D3 reports are complementary: D3.1 covers quantum-safe X.509 and CMS work, D3.2 covers standardisation work on PQC, high-performance computing and quantum-computing hardware and software, and D3.3 applies those inputs to the travel-document protocols, PKI, regulatory context and global deployment path.

3.2 Active involvement of PQC4eMRTD in relevant working groups

Table 7 summarises the principal standardisation and technical activities undertaken by the consortium.

Date/status	Forum	Documented PQC4eMRTD-related activity	Output and status
18-20 Sep 2024 Pre-project technical background	ICAO NTWG Request for Information (RFI) and NTWG, Copenhagen	THALES CDI presented “Introducing Post Quantum Algorithms in eMRTD” and demonstrated hybrid multi-certificate PA, classical PACE and a Kyber-based PQC Password-Authenticated Key Exchange (PAKE) with inspection-system considerations.	Technical demonstration and contribution to the ICAO discussion [10].
15-21 Mar 2025 Completed	IETF 122 Hackathon and LAMPS meeting	CRYPTONEXT worked on PQC certificate and CMS interoperability artefacts and presented or progressed SLH-DSA X.509, ML-KEM CMS and CMS security guidance.	Published outputs and D3.1 input to the certificate and signed-object layer are described in Section 2.3.
7-9 May 2025 Completed	ICAO NTWG, Ottawa	THALES CDI presented the project objectives and plan. WG3/TF5 subsequently updated its analysis of quantum-safe mechanisms for the document-issuing PKI and Passive Authentication.	Presentation and WG3 N188 update [11].
2025-2026 Ongoing	ISO/IEC JTC1/SC17/WG3 TF5/CASG	Participation in discussions on crypto agility, document-issuing PKI, PA, certificate formats and hybridisation; the PKI/PA paper was circulated to Member States for implementation feedback.	Working-group participation and information-paper development [11].

Table 7: PQC4eMRTD contributions to standards development organisations

The activities combine implementation prototypes, interoperability work, standards contributions and working-group analysis. Presentations and proofs of concept (PoCs) establish technical feasibility, while normative adoption is performed by the relevant standards and policy bodies.

3.3 Main technical outcomes and observations

The standardisation activities produced the following technical outcomes and observations.

1. Passive Authentication and the issuing PKI are the immediate priority. A CRQC would undermine the authenticity of signed document data and the trust chain used by inspection systems. This priority is consistent across D2.3, the September 2024 NTWG report and WG3 N188 [8] [10] [11].
2. Priority does not define the complete migration scope. PACE, Chip Authentication, Terminal Authentication and Active Authentication (AA) protect confidentiality, access control and anti-cloning properties. Deferring their migration retains a residual dependency on quantum-vulnerable public-key mechanisms.
3. A staged and a coordinated migration have different trade-offs. A PA-first stage can mature earlier without waiting for every protocol. A coordinated transition can reduce repeated PKI, reader, certification and procurement changes and can address privacy mechanisms within the same programme. The selection depends on technical maturity, national infrastructure and deployment constraints.

4. Hybrid support includes both cryptographic mechanisms and validation policy. Classical and PQC components require cryptographic binding, explicit validation rules, downgrade and stripping resistance, and a controlled mechanism for algorithm retirement.

5. The Copenhagen demonstration covered hybrid multi-certificate Passive Authentication and a Kyber-based PQC PAKE in a representative document and inspection-system context. The Ottawa activity presented the project objectives and plan and informed the subsequent WG3 analysis of quantum-safe mechanisms for the document-issuing PKI and Passive Authentication. End-to-end deployment additionally involves final protocol specifications, security proofs, certified implementations, performance assessment and multi-vendor interoperability.

6. European deployment must align standards, law and assurance. ICAO/ISO profiles must connect to EU travel-document requirements, the NIS Cooperation Group roadmap, EUCC/national cryptographic guidance and Common Criteria certification. The same transition decision must be implementable by issuing authorities, PKI operators, document manufacturers and border-control operators [6] [7].

7. The results feed WP4 planning for the migration sequence, algorithm and parameter profiles, certificate and CMS formats, hybridisation rules, protocol proofs, certification updates, test strategy, regulatory route and deployment milestones.

Work continues on normative profiles, security proofs and standardisation for PQC-enabled PACE, EAC and coordinated eMRTD migration.

4. Conclusion

The transition of eMRTDs to post-quantum cryptography is a coordinated standards and infrastructure migration rather than a direct algorithm substitution. It affects the ICAO and ISO specification framework, the document-issuing PKI, certificate and CMS profiles, secure elements, personalisation systems, border-control infrastructure, certification and European implementation measures.

Passive Authentication and the document-issuing PKI form the immediate priority because their compromise would undermine the authenticity of signed document data and the trust chain used by inspection systems. The overall migration scope also includes PACE, Chip Authentication, Terminal Authentication and Active Authentication, which protect confidentiality, access control and anti-cloning properties. A staged migration and a coordinated migration offer different balances between technical readiness, security coverage and repeated infrastructure change.

The project has progressed from landscape monitoring to active standardisation engagement. Its activities include contributions concerning PQC certificate and CMS formats and analysis of quantum-safe mechanisms for the document-issuing PKI and Passive Authentication. These activities build on the pre-project THALES CDI demonstration in Copenhagen of hybrid multi-certificate Passive Authentication and a Kyber-based PQC password-authenticated key exchange. These activities inform the development of normative profiles.

A secure transition requires cryptographic agility throughout the ecosystem. Hybrid mechanisms require explicit binding and downgrade resistance; CSCA and Document Signer rollover requires coordinated certificate policy and trust distribution; and document, personalisation and inspection systems require compatible capacity, interfaces and update paths. Certification and multi-vendor interoperability testing are integral to deployment.

The EUDIW and ICAO eMRTD frameworks remain distinct, but their transitions share dependencies on trust anchors, signed identity data, certified components and cross-border validation. Alignment between international travel-document standards and the European digital identity, cryptographic and certification frameworks supports consistent migration across related identity infrastructures.

The transition must preserve the privacy properties of the current eMRTD framework, including confidentiality of sensitive biometric data, controlled access to protected data groups and resistance to unauthorised or avoidably traceable interactions.

The remaining work concerns the completion of protocol profiles and security proofs, selection of algorithms and parameters for each role, definition of hybrid certificate and signed-object policies, updates to certification profiles, and preparation of migration and interoperability programmes. These results provide the technical basis for WP4 standardisation, regulatory and testing plans.

5. References

- [1] NIST, FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard, final publication, 13 August 2024. <https://csrc.nist.gov/pubs/fips/203/final>
- [2] NIST, FIPS 204: Module-Lattice-Based Digital Signature Standard, final publication, 13 August 2024. <https://csrc.nist.gov/pubs/fips/204/final>
- [3] NIST, FIPS 205: Stateless Hash-Based Digital Signature Standard, final publication, 13 August 2024. <https://csrc.nist.gov/pubs/fips/205/final>
- [4] NIST Special Publication 800-208: Recommendation for Stateful Hash-Based Signature Schemes, final publication, October 2020. <https://csrc.nist.gov/pubs/sp/800/208/final>
- [5] BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2026-01, 23 January 2026. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html
- [6] ENISA / European Cybersecurity Certification Group (ECCG), EUCC Guidelines on Cryptography: Agreed Cryptographic Mechanisms, Version 2, May 2025. https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en
- [7] European Commission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>
- [8] PQC4eMRTD, Deliverable D2.3: Report on the state of standardization in the travel and border landscape, Version 1.0, 30 April 2025.
- [9] International Civil Aviation Organization (ICAO), Doc 9303: Machine Readable Travel Documents, official publication series. <https://www.icao.int/publications/doc-series/doc-9303>
- [10] ICAO New Technologies Working Group, Meeting Report, Copenhagen, 18-20 September 2024, Version 1.0 (final).
- [11] ISO/IEC JTC1/SC17/WG3 N188, TF5 Information Paper: Quantum safe mechanisms for the Document Issuing PKI and Passive Authentication, Release 0.02, 4 June 2025.
- [12] PQC4eMRTD, Deliverable D2.1: Report on the state of standardization for quantum-safe X.509 certificates, Version 1.0, 5 May 2025.
- [13] IETF, RFC 9802: Use of the HSS and XMSS Hash-Based Signature Algorithms in Internet X.509 Public Key Infrastructure, June 2025. <https://www.rfc-editor.org/rfc/rfc9802.html>
- [14] IETF, RFC 9882: Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS), October 2025. <https://www.rfc-editor.org/rfc/rfc9882.html>
- [15] IETF, RFC 9909: Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA, December 2025. <https://www.rfc-editor.org/rfc/rfc9909.html>
- [16] European Parliament and Council, Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30 April 2024. <https://data.europa.eu/eli/reg/2024/1183/oj>
- [17] European Commission, Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets. https://data.europa.eu/eli/reg_impl/2024/2977/oj

- [18] European Commission, Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 as regards the integrity and core functionalities of European Digital Identity Wallets. https://data.europa.eu/eli/reg_impl/2024/2979/oj
- [19] European Commission, Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem. https://data.europa.eu/eli/reg_impl/2024/2980/oj
- [20] European Commission, Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 as regards the certification of European Digital Identity Wallets. https://data.europa.eu/eli/reg_impl/2024/2981/oj
- [21] European Commission, Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 as regards protocols and interfaces to be supported by the European Digital Identity Framework. https://data.europa.eu/eli/reg_impl/2024/2982/oj
- [22] European Commission, Commission Implementing Regulation (EU) 2026/1731 of 15 July 2026 amending Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980 and 2024/2982 as regards applicable standards and specifications. https://data.europa.eu/eli/reg_impl/2026/1731/oj
- [23] European Commission, Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework. <https://data.europa.eu/eli/reco/2021/946/oj>
- [24] European Digital Identity Cooperation Group, European Digital Identity Wallet Architecture and Reference Framework, Version 3.0.0, released 23 July 2026. <https://eudi.dev/3.0.0/>
- [25] PQC4eMRTD, Deliverable D1.1: Report on regulations on travel & borders on the EU, Version 1.0, 30 April 2025.
- [26] Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU, Specification v1.2, 1 October 2020, NIST Post-Quantum Cryptography Standardization Round 3 submission. <https://falcon-sign.info/>
- [27] ANSSI, Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique, 14 April 2022. <https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique>