Migrating Time and Security-Critical PKIs to Post-Quantum Cryptography: SWIM and C-ITS

Anni Karinsalo, Sara Nikula and Sami Lehtonen
VTT Technical Research Centre of Finland, Oulu/Espoo, Finland

anni.karinsalo@vtt.fi
sara.nikula@vtt.fi
sami.lehtonen@vtt.fi

Abstract: Public Key Infrastructures (PKIs) are foundational to time- and security-critical systems such as air traffic management and cooperative intelligent transport systems (C-ITS). These PKIs rely almost exclusively on classical public-key cryptography, which will become vulnerable once cryptographically relevant quantum computers emerge. Migrating such systems to post-quantum cryptography (PQC) is therefore necessary but non-trivial, as these environments impose strict constraints on latency, bandwidth, interoperability, long system lifetimes, and regulatory compliance. This paper presents a comparative, constraint-driven analysis of PQC migration for time- and security-critical PKIs. Focusing on System-Wide Information Management (SWIM) and C-ITS, we examine how PQC signature and key sizes, verification costs, and certificate structures affect real-time communication, certificate validation, and session establishment. In particular, we analyze the impact of certificate size growth and verification latency on time-critical messaging using published benchmarks and protocol specifications. Rather than proposing new cryptographic primitives or implementations, this work synthesizes existing benchmarks, standardization documents, and protocol specifications to identify feasibility limits, migration risks, and design trade-offs. The analysis shows that certificate chain length and signature overhead can dominate session establishment time in short communication windows, particularly in C-ITS environments, even when individual cryptographic operations remain computationally efficient. We further discuss the operational risks introduced by hybrid cryptographic deployments, including increased system complexity, negotiation failures, and insecure fallback behavior. In addition, we highlight how long system lifetimes and slow standardization cycles in safety-critical sectors complicate timely cryptographic transitions. The results indicate that migration feasibility is often determined by system-level constraints, such as certificate handling, protocol overhead, interoperability requirements, and regulatory alignment, rather than by the performance of individual PQC algorithms alone. Based on this analysis, we present a benchmarking-based migration framework tailored to critical PKIs, highlighting where hybrid cryptographic approaches are unavoidable, where they introduce new risks, and which classes of PQC algorithms are conditionally viable under strict timing and bandwidth constraints. The paper concludes with concrete recommendations for system designers and policymakers to support crypto-agile PQC migration without compromising operational safety.

Keywords: Post-Quantum cryptography, Public key infrastructure, PQC migration, Cooperative intelligent transport systems, System wide information management

1. Introduction

Public Key Infrastructures (PKIs) form the backbone of secure digital communication by enabling authentication, integrity, and trust establishment between distributed entities. In time- and security-critical systems, such as air traffic management, cooperative intelligent transport systems (C-ITS), and other cyber-physical infrastructures, PKIs are not merely supporting components but safety-relevant mechanisms. In these environments, failures or delays in cryptographic operations can directly affect operational continuity and, in extreme cases, human safety.

Most currently deployed PKIs rely on classical public-key cryptographic algorithms, primarily RSA (Moriarty et al., 2016) and elliptic curve cryptography (ECC) (Miller, 1985, Koblitz, 1987). These algorithms are widely considered vulnerable to sufficiently powerful quantum computers due to Shor's algorithm. While cryptographically relevant quantum computers (CRQC) do not yet exist, the long operational lifetimes of critical systems, combined with the risk of "harvest now, decrypt later" attacks, make proactive migration planning unavoidable. Consequently, post-quantum cryptography (PQC) has emerged as a strategic requirement rather than a theoretical concern.

Migrating PKIs to PQC is significantly more complex in time- and security-critical systems than in conventional IT environments. Such systems impose strict constraints on latency, bandwidth, computational resources, interoperability, and regulatory compliance. PQC algorithms typically introduce substantially larger keys and signatures, which can stress communication channels and certificate validation mechanisms. In addition, critical PKIs are governed by international standards and certification processes that evolve more slowly than cryptographic research, further constraining feasible migration paths and limiting near-term deployment options.

1.1 Scope of This Paper

This paper addresses PQC migration from a systems and PKI-engineering perspective rather than from an algorithm-design or implementation standpoint. We focus on authenticated communication, certificate chain validation, and session establishment, as these are the dominant contributors to cryptographic overhead in PKI-based communication. The paper does not present new cryptographic constructions or experimental implementations; instead, it synthesizes published benchmarks, standardization documents, and protocol specifications to analyse feasibility limits and design trade-offs. We have concentrated specifically on session establishment and certificate chain validation. These two are the main factors in communication between end users and the main contributor in the PKI-based overhead. This work assumes the widely accepted cryptanalytic threat model used by NIST and ETSI, rather than attempting to validate quantum feasibility independently.

Our analysis handles two representative case studies: System-Wide Information Management (SWIM) (ICAO, 2018), which contains emerging aviation data exchange architectures, and Cooperative Intelligent Transport Systems (C-ITS), which enable real-time vehicle-to-everything (V2X) communication. These case studies are used to illustrate how PQC-related performance characteristics interact with real-world timing, bandwidth, and interoperability constraints. Based on this analysis, we derive a migration framework for time- and security-critical PKIs and identify conditions under which hybrid cryptographic approaches are unavoidable, as well as the risks they introduce.

The remainder of this paper is structured as follows. Section 2 provides background on PQC, SWIM, and C-ITS. Section 3 examines these systems as case-study PKIs, focusing on hybrid certificates, algorithm applicability, and certificate lifecycle considerations. Section 4 analyses the main challenges and constraints of PQC migration in time- and security-critical PKIs. Section 5 presents a benchmarking framework for evaluating PQC feasibility under strict performance constraints. Section 6 discusses design implications and migration guidance for system designers and policymakers, followed by conclusions and directions for future work.

Please note: we use the term ‘critical PKI’ as a synonym for time- and security-critical for simplicity.

2. Background and Scope

Ensuring the integrity and origin of transmitted information is traditionally achieved using signature algorithms based on the discrete logarithm problem or the factorization of large numbers. Since 2016, NIST has led the standardization of PQC algorithms. In 2024, NIST published its first PQC standards for digital signatures and key establishment (NIST, 2024a; NIST, 2024b; NIST 2024c). NIST disallows asymmetric cryptography vulnerable to quantum computers by year 2035 (NIST, 2024d).

PKI is a widely adopted framework for secure digital communication and identity verification. In brief, PKI enables entities to authenticate each other and ensure data integrity using asymmetric cryptography, trusted certificate authorities and certificate status queries.

2.1 System-Wide Information Management (SWIM) in Aviation PKIs

Air Traffic Management (ATM) systems rely on short-lived, time-critical communications with strict security and latency requirements.

SWIM is a framework that integrates global real-time data exchange between various aviation systems using common standards, infrastructure, and shared air traffic data. Reference implementations are currently undergoing testing with the aim of future deployment for ATM data management and planning. SWIM is primarily developed under EUROCONTROL in Europe. However, it also plays a significant role in the United States, where joint U.S.-EU strategies are being developed to ensure global harmonization and interoperability, reflecting SWIM’s growing importance in international air traffic management (SESAR-NextGen, 2018). The European Commission (2021) defines the SWIM Yellow Profile as a ground distribution mechanism in which the technical infrastructure can run over any IP-based network.

The European Aviation Common Public Key Infrastructure (EACP) (EUROCONTROL, 2022a) is a European-wide, globally supported shared PKI aimed at enabling secure communication within the European aviation context. EACP provides a trust framework for SWIM communication and data management and will also define rules for local implementations. EACP aligns with European Commission’s mandate (European Commission, 2022) for a common aviation PKI. The European ATM Master Plan (European Commission, 2021) serves as the implementation roadmap for applying EACP to SWIM. Within EACP, civil and military stakeholders may either

operate a local PKI in which they act as a certification authority, use the central EACP CA, or adopt a hybrid approach.

EACP uses the X.509 v3 (ITU, 2000) certificate format, and current CAs rely on ECDSA and RSA signature algorithms (EUROCONTROL, 2022b). SWIM documentation assumes that ECC-224 and RSA-2048 remain secure until approximately 2030, while larger key sizes are projected to remain secure until around 2035. Public SWIM documentation does not disclose any concrete strategy for migration to PQC-compliant algorithms.

2.2 Cooperative Intelligent Transport Systems

Critical communication in intelligent transport systems occurs between nodes called Intelligent Transportation System's Stations (ITS-Ss), including vehicles on the road and static roadside communication points. These nodes communicate using an underlying PKI. ETSI standards define the message and certificate formats used by intelligent transport systems. Some of the defined message types are CAM (ETSI, 2019a) and DENM (ETSI, 2019b), which are used to alert other vehicles to noteworthy events. At the time of writing, ETSI TS 103 097 defines the certificate structures used in C-ITS. Regarding signature types, it refers to IEEE 1609.2, which specifies several elliptic curve options. ETSI TS 102 941 defines the communication between vehicles (ITS stations) and PKI entities in the context of secure and privacy-preserving V2X systems. It specifies the trust models, certificate and credential handling, and secure communication interfaces between vehicles and PKI entities. Currently, ETSI's C-ITS standards provide no support for PQC signatures (ETSI 2022, ETSI 2021, IEEE 2023).

3. Case Study PKIs: PQC Applicability to SWIM and C-ITS

In this section, we examine the practical applicability of PQC to SWIM and C-ITS. As publicly accessible, PQC-enabled SWIM implementations were not available at the time of writing, we use C-ITS as the primary empirical reference case and generalize relevant findings to SWIM messaging and PKI validation constraints.

3.1 Hybrid Certificates

The most widely deployed certificate format for PKIs is X.509 v3, which supports only a single subject public key. This design poses a fundamental limitation for combining classical and post-quantum cryptography within a single certificate. While custom extensions can be used to embed additional public keys, such approaches are not standardized and require explicit support from both the issuing authority and the validating peer. To address this limitation, the Internet Engineering Task Force (IETF) has proposed composite signature schemes in which a single signature is formed from multiple algorithms, such as ECDSA and ML-DSA (Ounsworth et al., 2024).

Alternatively, and more commonly, two separate X.509 certificates are issued and combined using certificate chains or alternate trust anchors, as also supported by NIST. This approach requires communication protocols that can negotiate which certificate and signature algorithm to use, such as TLS 1.3 with PQC extensions. However, under current C-ITS standards, a major limitation is that existing certificate profiles do not support the concurrent use of multiple signature algorithms. Given that vehicles may remain in operation for several decades, it is impractical to transition to post-quantum algorithms in a single coordinated update. As a result, simultaneous support for multiple signature types during extended transition periods becomes unavoidable (Yoshizawa and Preneel, 2023). While ETSI (2023) does not recommend hybrid solutions and instead emphasizes crypto-agility and rapid algorithm replacement, this assumption conflicts with the operational realities of long-lived vehicular systems.

Hybrid certificates introduce risks for both the developer and the user. From the developer perspective, hybrid deployments require maintaining two parallel PKI stacks, one based on classical cryptography and one on post-quantum algorithms. This entails operating two certificate hierarchies and implementing negotiation, fallback, and failover logic between cryptographic stacks. In time-critical systems, this additional complexity introduces risks of increased latency, software defects, and misconfiguration. In the worst case, race conditions or logic errors may cause the system to select an insecure fallback algorithm under load or timing pressure, thereby silently degrading the security level of the communication.

From the user perspective, mixed cryptographic environments introduce a risk of compatibility failures and service disruptions. A client device may support only a single cryptographic algorithm, while the server offers a certificate based on a different algorithm. Without standardized support for dual keying or hybrid validation, such mismatches lead to failed connections or ambiguous certificate errors. As a result, essential operations such as authentication, software updates, or safety messaging may fail unexpectedly. In the worst case, users or systems may disable certificate validation or encryption to restore connectivity, thereby exposing the communication to downgrade attacks or complete loss of confidentiality and integrity.

3.2 Algorithm Applicability and Optimization

NIST is evaluating additional PQC signature schemes with improved or alternative security assumptions (Alagic et al., 2024). Table 1 lists the combined lengths of the public key and signature for algorithms that have either already been standardized or selected for the second round of additional signatures. The algorithms are categorized based on the underlying mathematical problem, and if multiple algorithms based on the same problem have been submitted to the competition, their averages are shown.

Table 1: Average total lengths of signature and public key of digital signature algorithms that are already standardized by NIST or chosen for the second round of additional digital signatures

type	bytes
lattice	1998
hash	7888
multivariate	18903
code-based	17537
symmetric	5038
MPC-in-the-head	8165
isogeny	214
average (all PQC)	9935
RSA (classical)	512
ECDSA (classical)	97

Algorithms based on different mathematical problems exhibit widely varying public key sizes, signature lengths, and computational performance. Consequently, replacing classical signature schemes with post-quantum alternatives impacts both the size of transmitted messages and the time required for signing and verification operations. These effects are particularly relevant in vehicular and aviation communication, where message sizes are tightly constrained and authentication must be completed within short communication windows.

The size of a signature impacts the total length of the transmitted messages. The size of certificates is influenced by both the signatures and the public keys, as they must at least include the signature and public key of the certificate authority, as well as the public key of the certificate owner. (Nikula, Halunen, Vallivaara, 2022) constructed DENM messages defined in (ETSI, 2019b) and calculated that the total length of DENM messages was 300 bytes + length of digital signature + length of public key. If the PKI uses intermediate certificate authorities, the messages become even longer, as their signatures and public keys must also be included in the certificates.

Table 2 presents the size of the DENM message calculated as described in Nikula, Halunen, Vallivaara (2022) assuming the use of the specified signature algorithm, along with the verification time promised by the lowest security level of the signature algorithm (Bos et al., 2025, Aardal et al., 2025, Beullens et al., 2024, Aumasson et al., 2022, Alagic et al., 2022) and ECDSA verification time taken from Nikula, Halunen, Vallivaara (2022).

Table 2: Lengths of DENM messages constructed with different PQC digital signature algorithms and their verification times

type	name	DENM length, bytes	verification time, seconds
lattice	FALCON	1799	3.58×10^{-5}
lattice	HAWK	935	6.44×10^{-5}
hash	SPHINCS+	8124	1.5×10^{-3}
isogeny	SQIsign	450	1.5×10^{-3}
multivariate	MAYO	2110	9.06×10^{-5}
code-based	CROSS	13241	4.22×10^{-4}
elliptic curve (classical)	ECDSA	338	7.8×10^{-5}

Using larger signatures and public keys to form certificates introduces a significant performance constraint. Yoshizawa and Preneel (2023) estimate that the effective channel capacity is reduced by approximately half

when even a subset of vehicles transitions to quantum-safe signature algorithms. Consistently with this observation, ETSI (2023) concludes that none of the NIST-standardized signature schemes, ML-DSA (Dilithium), FN-DSA (Falcon), or SLH-DSA (SPHINCS+), are currently suitable for deployment in C-ITS communication. The primary reason is the large size of public keys and signatures, which causes authentication-related data to consume a disproportionate share of the available channel capacity. For example, signatures produced by the lowest security level of SLH-DSA are approximately thirty times larger than those of elliptic curve schemes (NIST, 2024a; NIST, 2024b), making certificate-based authentication impractical under current C-ITS bandwidth constraints.

Communication in aviation can be compared to communication in intelligent transportation systems, as both involve time-critical messaging that may require rapid responses. The signing time is crucial when creating a message, and the verification time is crucial when receiving a message. Sarıbas and Tonyalı (2022) compared the use of classical and quantum-safe algorithms for TLS handshakes. The results indicate that the performance times of quantum-safe signature algorithms are often even better than those of classical digital signatures. Furthermore, Nikula, Halunen, Vallivaara (2022) claim that lattice-based signature options are suitable for C-ITS communication in terms of performance.

In every communication session, both parties must validate each other's certificate chains by verifying each signature and checking the validity of each certificate in the chain. This requires the exchange of several kilobytes of authentication data, even when the actual application payload may be a few hundred bytes. The communication range of a roadside unit is typically 50 – 200m. For a vehicle travelling at 70 km/h, this corresponds to a communication window of approximately 3s at a range of 50m, and even less at larger distances. Communication between two vehicles is typically reliable only when they travel in the same direction; for oncoming vehicles, the available communication window is extremely short. Since communication sessions are initiated by certificate exchange and validation, certificate size has a direct impact on the probability of successful session establishment. If the certificate chain is too long, the handshake process may consume a significant portion of the available communication time. It is therefore not sufficient that cryptographic operations are computationally feasible; they must also complete within the limited communication window.

4. PQC Migration Challenges and Constraints

Migrating critical PKIs to PQC introduces a set of systemic challenges that extend beyond the choice of cryptographic algorithms. In PKI systems, authentication mechanisms are dependent on real-time communication, bandwidth limitations, long system lifetimes, and regulatory constraints. PQC migration is constrained not only by cryptographic performance, but also by interoperability and backward-compatibility requirements, latency budgets, channel capacity, and sector-specific certification processes. These constraints fundamentally limit the feasibility and pace of migration in critical infrastructures.

When digital certificates are updated to be PQC compatible across certification authorities (CAs), registration authorities, key management systems, directory services, and end users, this requires supporting new cryptographic algorithms in certificate issuance processes and modifying validation and revocation mechanisms. The greatest challenge in this migration is that all related systems utilizing the certificates must be interoperable with the new algorithms. Ensuring backwards compatibility during the transition period is crucial for security.

As illustrated by the C-ITS case study in the previous section, many PQC algorithms introduce increased computational overhead and larger key sizes due to performance and latency constraints. This can impact system performance, especially in real-time communication systems like SWIM and C-ITS. The larger keys and signatures, such as those presented in Table 2, affect certificate issuance, storage, and revocation mechanisms, requiring re-evaluation of key management protocols. Moreover, certificate size affects protocol overhead in mechanisms such as TLS, as certificate fragmentation during transmission increases latency and retransmission risk (Kampanakis et al., 2018).

Certificate agility enables flexible issuance, revocation, and updating of certificates, for example through hybrid certificates and certificate inventories. PKI automation supports this process by enabling automated certificate rotation using systems such as the Automatic Certificate Management Environment (ACME) (Barnes et al., 2019). In this model, lifecycle management is delegated to an ACME client, which must itself be secure and support the selected PQC signature algorithms to avoid introducing new operational vulnerabilities.

Even though technical advances may occur rapidly, regulations and standardizations affect the migration to PQC. Critical PKIs are subject to stringent regulatory requirements and their migration to PQC must particularly align

with evolving international standards from organizations such as ICAO (International Civil Aviation Organization), ETSI, and NIST.

5. Benchmarking Framework for Migrating Critical PKIs

PQC causes new performance constraints in systems where low latency, high availability, and high integrity are essential. Depending on the deployment environment, such as embedded and IoT systems, resource efficiency may also be a mandatory requirement. To evaluate the feasibility of PQC in critical PKIs, we propose a benchmarking framework based on the following performance and communication parameters.

Key generation time: the time required to generate public-private key pairs, especially in when using ephemeral keys. Comparing this with existing RSA/ECDSA key generation times helps understand migration usefulness.

Signature generation and verification time: Signature generation is critical for senders (e.g. vehicles broadcasting safety messages). Verification time is often more performance-critical (e.g. C-ITS road-side units verifying thousands of messages per second). PQC offer trade-offs: FALCON is faster at verification, but more complex to implement securely.

Ciphertext and signature sizes: Larger PQC signatures and ciphertexts can overload communication and increase packet fragmentation. This is important in bandwidth-limited or latency-sensitive systems. For example, a typical PQC signature (Dilithium 2 2.4 KB) is orders of magnitude larger than ECDSA (64 bytes).

Memory and computation footprint: analysing RAM and CPU use in cryptographic operations. Embedded devices, like onboard units (OBUs), have strict resource constraints. Computationally intensive PQC algorithms may be impractical without hardware acceleration.

Latency impact on system-level operations: combined latency of cryptographic operations across protocol stacks. In time-critical domains, even small latency increase can lead to delays or lost messages. Benchmarking must reflect end-to-end scenarios such as certificate validation and message authentication in real-time SWIM or V2X exchanges.

Network throughput and scalability by assessing how the increased size of cryptographic algorithms impacts network throughput. Systems should be then stress tested under high load to determine the number of cryptographic operations per second that can be sustained without degradation.

Hardware acceleration potential: Some PQC can benefit significantly from hardware acceleration. Benchmarking should compare software-only with hardware-accelerated implementations if applicable.

Protocol integration overheads: measuring the added complexity and processing delay with PQC integrated into existing protocols. Hybrid schemes cause additional cryptographic load in multi-algorithm handshakes, which should be reflected in benchmarking.

6. Design Implications and Migration Recommendations

While benchmarking frameworks support the technical evaluation of PQC, effective migration in critical PKIs additionally requires coordinated design strategies, crypto-agile system architectures, and operational planning across the entire PKI ecosystem. For example, regarding the previous C-ITS case study, while the effect of overhead and latency can be estimated, the PQC-enabled system must always be tested against a real-life environment. Standards, specifications and other requirements can give estimate values, but the real-life situation is extremely difficult to simulate, since any deviation may cumulate unexpectedly.

Algorithm selection should be guided by system-specific constraints, including latency budgets, computational resources, and key and signature sizes. For example, in latency-sensitive SWIM environments, Falcon may be preferable for verification-heavy workloads, whereas Dilithium may be better suited for balanced signing and verification scenarios. There is no universally applicable algorithm for all critical PKIs, and algorithm choices must therefore be adapted to the operational context.

PQC migration should be implemented in phases, with initial deployment in non-critical system components. Support for classical cryptography should be maintained during transition periods to reduce migration risk and preserve service continuity. Hybrid solutions provide backward compatibility but increase system complexity and are therefore best suited as transitional rather than permanent solutions. Bindel et al. (2017) show that backward compatibility in standards such as X.509, TLS, and S/MIME requires post-quantum alternatives to be embedded as non-critical certificate extensions.

Certificate lifecycles must be adapted by adjusting validity periods and issuance workflows to account for PQC key sizes and operational overhead. Short-lived certificates may reduce exposure but increase management complexity.

Computational overhead introduced by PQC can be mitigated through cryptographic accelerators, FPGAs, and other secure hardware platforms that support high-throughput signing and verification operations.

Standardization progress should be continuously monitored using resources from organizations such as NIST and ETSI. Participation in hackathons, interoperability testing events, and working groups supports early validation of deployment readiness.

Monitoring frameworks can be used to assess PQC performance and security in operational environments, while periodic audits verify compliance with operational and regulatory requirements. As monitoring tools are highly system-specific, their deployment must be tailored to the operational characteristics and risk profile of each PKI.

7. Conclusion

This paper examined the migration of time- and security-critical Public Key Infrastructures to post-quantum cryptography from a systems and PKI-engineering perspective. Using SWIM and C-ITS as representative case studies, we showed that PQC migration in such environments is constrained less by cryptographic correctness than by operational requirements related to latency, bandwidth, interoperability, and regulatory compliance. Our analysis indicates that direct replacement of classical algorithms with PQC counterparts is generally infeasible in critical PKIs without structural changes to certificate handling and communication protocols. In particular, increased certificate and signature sizes, combined with verification-heavy workloads, can significantly affect end-to-end performance even when individual cryptographic operations remain computationally efficient. These effects are amplified in environments with short communication windows and strict timing guarantees.

As a result, hybrid cryptographic approaches emerge as a pragmatic transitional solution, despite introducing additional complexity and new risk vectors. Hybridization should be understood as an intermediate step that enables crypto-agility while standards and implementations mature. Migration must be phased, context-aware, and aligned with sector-specific standardization.

The contribution of this work is a constraint-driven synthesis of existing benchmarks, standards, and protocol specifications, that highlights feasibility limits and design trade-offs for PQC adoption in critical PKIs. This paper provides concrete guidance for system designers and policymakers tasked with planning long-term cryptographic transitions in security-relevant infrastructures.

Future work should focus on system-level validation of PQC-enabled PKIs under realistic traffic conditions, as well as on the evolution of standards that better accommodate multi-algorithm operation and cryptographic agility. Such efforts will be essential to ensure that the transition to post-quantum cryptography strengthens, rather than compromises, the safety and reliability of critical digital infrastructures.

Acknowledgements

This work has been funded by the European Defence Fund research and innovation project SESIOP, under the programme grant agreement No. 101070052, and Business Finland project Beyond the Limits of Post-Quantum Cryptography, under the agreement No. 100/31/2024.

Ethical Clearance: Ethical clearance was not required for this research.

AI Declaration: Copilot AI has been used for language refinement.

References

Aardal, M.A., Adj, G., Aranha, D.F., Basso, A., Martínez, I.A.C., Chávez-Saab, J., Santos, M.C.-R., Dartois, P., Feo, L.D., Duparc, M., Eriksen, J.K., Fouotsa, T.B., Filho, D.L.G., Hess, B., Kohel, D., Leroux, A., Longa, P., Maino, L., Meyer, M., Nakagawa, K., Onuki, H., Panny, L., Patranabis, S., Petit, C., Pope, G., Reijnders, K., Robert, D., Henríquez, F.R., Schaeffler, S. and Wesolowski, B. (2025). SQISign algorithm specifications and supporting documentation version 2.0. https://sqisign.org/spec/sqisign-20250205.pdf.

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A. and Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process (NIST IR 8413-upd1). https://doi.org/10.6028/NIST.IR.8413-upd1.

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D. and Waller, N. (2024). Status report on the first round of the additional digital signature schemes for the NIST postquantum cryptography standardization process (NIST IR 8528). https://doi.org/10.6028/NIST.IR.8528.

Aumasson, J.-P., Bernstein, D.J., Beullens, W., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S.-L., Hülsing, A., Kampanakis, P., Kölbl, S., Lange, T., Lauridsen, M.M., Mendel, F., Niederhagen, R., Rechberger, C., Rijneveld, J., Schwabe, P. and Westerbaan, B. (2022). SPHINCS+ submission to the NIST post-quantum project, v.3.1. https://sphincs.org/data/sphincs+-r3.1-specification.pdf.

Barnes, R., Hoffman-Andrews, J., McCarney, D. and Kasten, J. (2019). Automatic Certificate Management Environment (ACME). RFC 8555. https://www.rfc-editor.org/info/rfc8555.

Beullens, W., Campos, F., Celi, S., Hess, B. and Kannwischer, M.J. (2024). MAYO round 2 version. https://pqmayo.org/assets/specs/mayo-round2.pdf.

Bindel, N., Herath, M., McKague, M. and Stebila, D. (2017). Transitioning to a quantum-resistant public key infrastructure. In *PQCrypto 2017*, Utrecht, The Netherlands, 26–28 June. Springer, pp. 384–405.

Bos, J.W., Bronchain, O., Ducas, L., Fehr, S., Huang, Y.-H., Pornin, T., Postlethwaite, E.W., Prest, T., Pulles, L.N. and van Woerden, W. (2025). HAWK version 1.1 (February 5, 2025). https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/hawk-spec-round2-web.pdf.

ETSI (2019a). *ETSI EN 302 637-2 V1.4.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.*

ETSI (2019b). *ETSI EN 302 637-3 V1.3.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service.*

ETSI (2021). *ETSI TS 103 097 V2.1.1: Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; Release 2.*

ETSI (2022). *ETSI TS 102 941 V2.2.1: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2.*

ETSI (2023). *ETSI TR 103 949 V1.1.1: Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS Migration Study.*

European Commission (2021). *Commission Implementing Regulation (EU) 2021/116 of 1 February 2021 on the establishment of the Common Project One supporting the implementation of the European Air Traffic Management Master Plan.* Official Journal of the European Union.

European Commission (2022). *Commission Decision of 12.8.2022 approving the SESAR deployment programme 2022.* https://www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022D1344.

EUROCONTROL (2022a). *SWIM Common PKI: Common PKI Specifications (D2.1).* Brussels: EUROCONTROL/SESAR Deployment Manager.

EUROCONTROL (2022b). *SWIM Common PKI and Policies & Procedures for Establishing a Trust Framework: Certificate Policy, Annex A3.a of D1.2 Final Trust Framework.* Brussels: EUROCONTROL/SESAR Deployment Manager.

ICAO (2018). *Manual on System-Wide Information Management (SWIM).* Montreal: ICAO (Doc 10039).

ITU (2025). Recommendation X.509: The directory – authentication framework. https://www.itu.int/rec/T-REC-X.509.

Kampanakis, P., Panburana, P., Daw, E. and Van Geest, D. (2018). The viability of post-quantum X.509 certificates. *Cryptology ePrint Archive*, Paper 2018/063.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), pp. 203–209.

Nikula, S., Halunen, K. and Vallivaara, V. (2022). Quantum-safe signing of notification messages in intelligent transport systems. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, 448, pp. 11–25.

NIST (2024a). *Module-Lattice-Based Digital Signature Standard (FIPS 204).* https://doi.org/10.6028/NIST.FIPS.204.

NIST (2024b). *Stateless Hash-Based Digital Signature Standard (FIPS 205).* https://doi.org/10.6028/NIST.FIPS.205.

NIST (2024c). *Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203).* https://doi.org/10.6028/NIST.FIPS.203.

NIST (2024d). *NIST IR 8547: Transition to Post-Quantum Cryptography Standards, Initial Public Draft.* https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf.

Ounsworth, M., Gray, J., Pala, M. and Klaußner, J. (2024). Composite ML-DSA for use in Internet PKI. https://www.ietf.org/archive/id/draft-ounsworth-pq-composite-sigs-13.html.

Sarıbas, S. and Tonyalı, S. (2022). Performance evaluation of TLS 1.3 handshake on resource-constrained devices using NIST's third-round post-quantum key encapsulation mechanisms and digital signatures. In *2022 7th International Conference on Computer Science and Engineering (UBMK)*, pp. 294–299.

SESAR-NextGen (2018). *NextGen – SESAR State of Harmonisation: Third Edition.* https://sesar.eu/sites/default/files/documents/StateOfHarmonization_Ed3.pdf.

Yoshizawa, T. and Preneel, B. (2023). Post-quantum impacts on V2X certificates – already at the end of the road. In *2023 IEEE 97th Vehicular Technology Conference*.