Towards Post-Quantum-Ready Automated Certificate Lifecycle Management in Operational Technology

Ayham Alhulaibi*, Tobias Frauenschläger† and Jürgen Mottok†
* Maschinenfabrik Reinhausen, 93059 Regensburg, Germany
e-mail: a.alhulaibi@reinhausen.com
† Laboratory for Safe and Secure Systems (LaS³), OTH Regensburg, 93053 Regensburg, Germany
e-mail: {tobias.frauenschlaeger, juergen.mottok}@oth-regensburg.de

***Abstract*—Operational Technology (OT) systems increasingly depend on robust and automated certificate lifecycle management to maintain secure operations across long device lifespans and constrained environments. As quantum-capable adversaries emerge, these systems must also support cryptographic agility and prepare for a seamless transition to Post-Quantum Cryptography (PQC). This work presents a crypto-agile, post-quantum-ready testbed architecture that extends existing standards, such as Enrollment over Secure Transport (EST) and Bootstrapping Remote Secure Key Infrastructure (BRSKI), to support hybrid certificates, hardware-based key storage, and protocol flexibility for device bootstrapping and certificate management. A work-in-progress prototype implementation demonstrates support for both traditional and PQC algorithms across device types. Planned evaluations target performance on constrained devices, PQC readiness, and compatibility with alternative protocols. The system lays a foundation for secure and standards-compliant certificate management in future-proof OT deployments.**

Keywords-Post-Quantum Cryptography; Public Key Infrastructure; Automated Device Onboarding; BRSKI; Security Token; Operational Technology Security.

I. Introduction

The convergence of Information Technology (IT) and Operational Technology (OT) has brought increased efficiency and connectivity to critical infrastructure sectors, such as water supply, energy distribution, and industrial automation. However, this interconnection expands the attack surface and raises the urgency for adopting scalable and robust cybersecurity mechanisms [1]. Among the most critical challenges is the secure provisioning and lifecycle management of device certificates in environments with remaining manual processes [2].

In OT contexts, device onboarding and certificate management must account for long operational lifespans, constrained computational resources, and limited maintenance windows [3]. Compounding these challenges is the increasing need to prepare for quantum-capable adversaries, which threaten to break widely deployed, traditional cryptographic schemes, such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) [4][5]. Ensuring long-term security in OT deployments thus requires not only Public Key Infrastructure (PKI) automation but also cryptographic agility and support for transitioning to PQC [6].

In order to address these challenges, we currently work on a testbed to evaluate the migration to PQC for the entire certificate lifecycle management (enrollment, renewal, revocation, and algorithm migration) within OT environments, including automated device onboarding. Our proposed architecture extends existing standards by addressing two key requirements missing or underexplored in prior work: (i) support for hardware-based secure key storage through a generic and agile interface, and (ii) end-to-end readiness for PQC, including hybrid certificates that combine traditional and PQ algorithms for transitional security [7]. In this context, *crypto-agility* refers to a system's ability to support multiple cryptographic algorithms throughout its lifetime without requiring major redesign or loss of interoperability [8]. By supporting crypto-agility and standard-compliant interfaces, the system enables future-proof, maintainable deployments without requiring protocol redesigns or vendor-specific extensions.

This paper presents a work-in-progress report on the design and early implementation of this testbed. Our main contributions are as follows:

- A system architecture for automated certificate lifecycle management in OT environments, combining secure onboarding, renewal, and revocation processes with cryptographic agility and hardware-backed key protection.
- A modular prototype implementation with support for PKCS#11-based security tokens and hybrid post-quantum/traditional certificates.
- An evaluation strategy covering both constrained device performance and the system's cryptographic and protocol agility.

The remainder of this paper is structured as follows: Section II presents fundamentals and discusses related work. Section III presents the final system architecture with its key components. Section IV outlines the current implementation status. Section V describes the remaining future work. Finally, Section VI concludes the paper.

II. Background and Related Work

PKIs are critical for securing industrial and OT systems, enabling authenticated communication and device identity management. In such environments, automated certificate provisioning is essential to replace manual processes that are error-prone and difficult to scale. A foundational protocol for certificate management in such systems is EST [9]. EST defines a secure, certificate-based protocol for retrieving Certification Authority (CA) certificates, requesting new client certificates, and renewing or rekeying existing ones. EST is

widely used in automated certificate provisioning workflows, as it supports mutual TLS authentication and standard X.509 certificate [10] handling.

In order to enable secure and automated device onboarding, the Internet Engineering Task Force (IETF) specified the BRSKI protocol [11], which builds on EST. In BRSKI, a new device (the *pledge*) presents its manufacturer-issued *Initial Device Identity certificate* (IDevID) to a *domain registrar* (the operator's administrative and security boundary, whose identity is represented by the *pinned-domain-cert*). The registrar then contacts the *Manufacturer Authorized Signing Authority* (MASA), which returns a signed voucher (a data object containing metadata [12]) that binds the pledge to the local domain (i. e., the local OT network). This voucher allows the pledge to verify the registrar's identity (via the *pinned-domain-cert* and a pre-installed MASA root certificate). Once trust is established, the pledge uses EST to request its *local operational certificate* (LDevID), completing the onboarding. Several extensions and variations of BRSKI have been proposed to support broader use cases. *BRSKI-AE* [13] enables the use of alternative enrollment protocols, such as CMPv2 [14]. Furthermore, extensions introduce support for registrar-initiated onboarding (BRSKI-PRM) or enable the usage of more efficient encoding formats (cBRSKI). Together, these variants support a range of network conditions, device capabilities, and operational constraints.

In order to protect private keys, OT systems increasingly rely on hardware security tokens, partly even required by regulations like IEC 62443 [15]. The PKCS#11 interface [16] provides a standard interface to such tokens, including Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs), smart cards, and secure elements. It abstracts key storage, signing, and other cryptographic operations, ensuring tamper-resistant credential protection and interoperability across vendors.

Existing work has explored the applicability of BRSKI in industrial and resource-constrained environments. Heinl *et al.* [2] analyze BRSKI adoption in OT networks in accordance with IEC 62443, creating a testbed similar to ours. They also add support for hardware-based security tokens in the form of TPMs. However, their setup misses a generic interface for security tokens and does not consider the PQC migration. Krieger *et al.* [17] demonstrate an embedded BRSKI client running on a microcontroller. While suitable for Bluetooth Low Energy-based constrained networks, it does not address the challenges of PQ readiness or hardware-based key storage. Rüst *et al.* [18] present an implementation of cBRSKI for wireless building automation devices using mbedTLS and support for various secure elements. They note the integration overhead of vendor-specific interfaces and call for harmonization, a gap we address through standardized PKCS#11 support. Again, the PQC migration is not addressed.

In contrast to prior work, our approach focuses explicitly on *post-quantum readiness* and *cryptographic agility*, enabling the use of hybrid classical/PQ certificates and hardware-based key storage. This positions our system as a forward-looking solution for scalable and future-proof device onboarding and PKI certificate lifecycle management in critical OT environments. Building on these foundations, we introduce an architecture designed to integrate crypto-agility and secure key storage into standard onboarding and lifecycle management protocols.

III. System Architecture and Design

Figure 1 depicts our complete, post-quantum-ready onboarding and certificate management architecture for OT networks. The design follows the BRSKI protocol layered over EST, with targeted extensions to support PQC and hardware-based key protection. For deterministic and low-complexity deployments, we omit automatic registrar discovery via mDNS/DHCP and instead preconfigure pledges with the registrar address. The architecture comprises four core components:

Pledge: A constrained embedded device to be onboarded. It holds a pre-installed IDevID certificate and initiates the BRSKI workflow. The pledge supports traditional and post-quantum key types and is capable of generating hybrid or PQC-only Certificate Signing Requests (CSRs) for EST enrollment. Secure key storage is provided via PKCS#11-based tokens, including TPMs or secure elements. All BRSKI and EST interactions are protected with a PQC-enabled Transport Layer Security (TLS) client stack, enabling both backward compatibility and security against future adversaries.

Registrar: The designated onboarding coordinator within the operator domain. It terminates BRSKI and EST requests from pledges, communicates with the MASA to validate voucher requests, and relays certificate enrollment messages to the CA. The registrar supports hybrid TLS handshakes to accommodate PQC-ready pledges. It enforces local policy decisions (e. g., which pledges to accept) and handles certificate issuance with the CA.

Certificate Authority (CA): Responsible for issuing LDevID certificates based on authenticated enrollment requests received via EST. The CA supports hybrid and PQC-only certificates. It is integrated with a PKCS#11 interface to manage key material in security tokens. This ensures keys are protected and compliance with security regulations is achieved.

MASA: Validates pledges and issues vouchers, binding them to a domain registrar. While MASA is typically vendor-operated and external, our prototype includes a minimal MASA implementation with PQC support for voucher signing and TLS. Its goal is to enable local testing of end-to-end onboarding flows without focusing on full MASA lifecycle functionality.

Our architecture emphasizes *crypto-agility* and *hardware security* as key design goals. PKCS#11 integration ensures compatibility with a wide range of security tokens and simplifies token management across the stack. By supporting hybrid certificates and PQC-native flows at every layer (TLS, voucher validation, and enrollment), our system enables future-proof certificate lifecycle management for OT environments facing both legacy compatibility and quantum-capable threats.

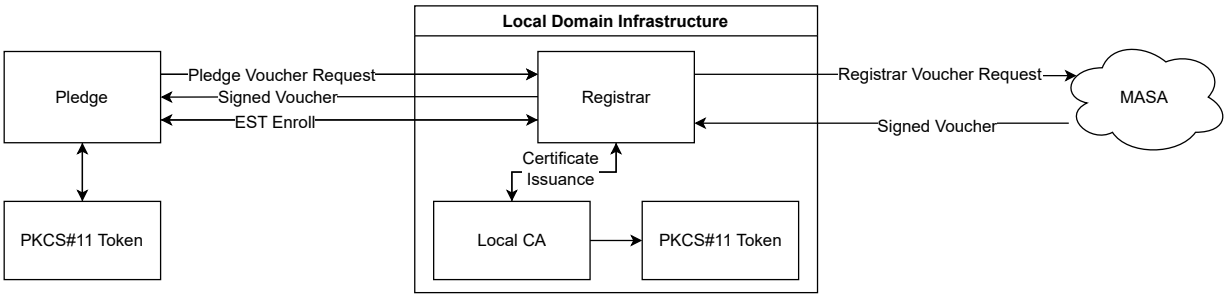

Figure 1. Testbed architecture with the various logical components required to cover the full certificate lifecycle.

While the depicted components in Figure 1 follow the standard BRSKI/EST layering, our work introduces the following targeted extensions:

- Support for PQC-enabled TLS handshakes and hybrid certificates across pledge, registrar, and CA.
- Integration of PKCS#11-based secure key storage in both resource-constrained pledges and backend components.
- PQC support for voucher handling and issuance within the MASA

These additions ensure crypto-agility and post-quantum readiness and are highlighted in the prototype implementation described in Section IV.

IV. Implementation Status

A. Platform Support

Our current prototype implementation is developed in Go [19] and targets Linux and Windows platforms. Both the EST server and the pledge client are based on a fork of an open-source EST implementation [20]. This fork has been extended to support BRSKI functionality, hybrid and post-quantum cryptography, and integration with PKCS#11-based security tokens. The prototype includes an EST server extended with registrar functionality for BRSKI, a pledge client implementing EST and BRSKI voucher exchange, and a minimal MASA implementation for testing.

All components use the WolfSSL library for cryptographic operations via wrapper bindings, including TLS, X.509 [10] handling, and PQC algorithm support. The system is designed to enable automated onboarding in OT environments, with particular focus on cryptographic agility and secure key storage. A lightweight C-based pledge implementation targeting microcontrollers (e. g., with the Real-Time Operating System Zephyr) is under active development and forms an essential part of future work.

B. BRSKI Workflow and Voucher Handling

The implementation supports the complete BRSKI voucher exchange flow. The registrar handles authenticated voucher requests from pledges and validates the incoming messages using the pledge's IDevID certificate. After verifying pledge identity and request integrity, the registrar constructs the registrar voucher request, encapsulating domain metadata and pledge identity. This request is forwarded to the MASA, which verifies the registrar's credentials and issues a signed voucher containing a *pinned-domain-cert*. The registrar forwards the voucher to the pledge to complete the trust establishment.

Voucher artifacts are encoded and signed using Cryptographic Message Syntax (CMS) [21]. PQC support for CMS is still under development [22][23], and is not yet implemented in our prototype. Supporting PQC-capable CMS structures is an essential item on our roadmap.

C. Enrollment and Certificate Lifecycle Support

After successful voucher validation, the pledge initiates certificate enrollment via EST. In our implementation, the registrar and CA are combined into a single application with modular separation between protocol handling and certificate logic. The registrar manages EST endpoints, including CA certificate distribution, CSR attribute provisioning, and enrollment via mutually authenticated TLS (mTLS). The CA is designed for cryptographic agility and lifecycle flexibility. It supports:

- Issuance of traditional, PQC-only, and hybrid X.509 certificates [10], based on configurable templates.
- Template-driven control of signature algorithms, validity periods, and metadata constraints.
- Hardware-based signing via PKCS#11 tokens.

Lifecycle operations include:

- Certificate renewal and rekeying, including transitions between algorithm profiles (e. g., classical→hybrid→PQC).
- Revocation via Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP), with future extensions for transparency logging and PQC awareness.
- Backward-compatible fallback modes to support legacy devices during migration.

The full EST flow already supports PQC, both for the TLS handshake and for issued certificates, while ensuring backward compatibility for legacy clients. This ensures compatibility during the transition period and provides a robust foundation for long-term cryptographic resilience in OT deployments.

V. Planned Future Work

A. Evaluation of Constrained Clients

Our primary evaluation target is the microcontroller-based pledge implementation, as it represents the most resource-constrained component in the proposed architecture. The evaluation will focus on metrics relevant to embedded OT devices:

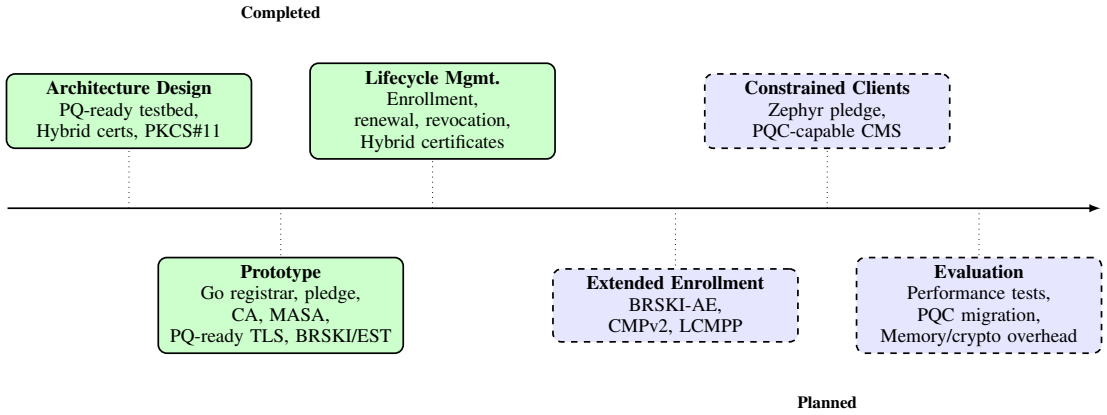

Figure 2. Roadmap of contributions (green) and planned extensions (blue).

- Enrollment performance: Time required to complete voucher acquisition and certificate enrollment over EST.
- Memory usage: Stack and heap consumption during onboarding and certificate renewal.
- Hardware-backed key operations: Comparison of cryptographic performance with and without secure key storage.

Initial tests using Zephyr on representative microcontroller platforms will guide optimizations of the pledge client and its integration with constrained TLS and PKI libraries.

B. Enrollment Flexibility and PQ Transition

Our planned future work will also extend the system to support alternative enrollment workflows using BRSKI-Alternative Enrollment (BRSKI-AE), enabling the integration of certificate management protocols, such as Certificate Management Protocol (CMPv2) and lightweight profiles like Lightweight CMP (LCMPP) [24]. This allows comparative analysis of EST-based and alternative enrollment approaches, particularly in scenarios with asynchronous provisioning or intermittent network connectivity.

In parallel, we plan to evaluate the system's cryptographic agility by transitioning from traditional to hybrid and post-quantum certificates. Planned experiments include the migration of IDevID and LDevID certificates to post-quantum formats, as well as lifecycle testing of hybrid certificates, covering renewal and revocation processes.

Together, these extensions will assess the testbed's readiness for long-term cryptographic transitions and its ability to support diverse PKI profiles across industrial use cases.

VI. Conclusion

This work presents a crypto-agile, post-quantum-ready certificate management architecture tailored for OT environments. Building on standardized protocols, such as BRSKI and EST, our system enables secure and automated device onboarding, coupled with full certificate lifecycle support. A key feature of the architecture is its support for hybrid and PQC-only certificates, allowing gradual migration without disrupting legacy compatibility. The integration of PKCS#11-based secure key storage further strengthens credential protection and aligns with regulatory requirements in critical infrastructure.

By decoupling enrollment and transport mechanisms from specific cryptographic primitives, the system remains adaptable to future algorithmic changes. Planned extensions, such as constrained pledge evaluations, PQC support in CMS, and the integration of alternative enrollment protocols via BRSKI-AE (e. g., CMPv2) to enable secure air-gapped provisioning. Ultimately, this work lays the foundation for long-term, crypto-agile PKI deployments in OT systems, enabling secure, automated, and standards-aligned certificate management in the post-quantum era.

To clearly separate outcomes from open directions, Figure 2 summarizes our contributions to date and places them in the context of the planned extensions. This roadmap highlights the concrete results of the present work while outlining the future steps towards full post-quantum readiness.

Acknowledgments

The presented work is part of the research project *KRITIS Scalable Safe and Secure Modules* (KRITIS³M), which is funded by the Project Management Jülich (PtJ) and the German Federal Ministry for Economic Affairs and Climate Action (BMWK) under funding code 03EI6089A.

References

[1] Waterfall team, *How Industrial Cybersecurity Works in 2025*, Jun. 2025. [Online]. Available: https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/industrial-cyber-security/ (Retrieved: 09/04/2025).

[2] M. P. Heinl, A. Reuter, S. N. Peters, and M. Bever, "Leveraging BRSKI to Protect the Hardware Supply Chain of Operational Technology: Opportunities and Challenges", in *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing*, ser. SAC '25, Association for Computing Machinery, May 2025, pp. 245–254. DOI: 10.1145/3672608.3707707.

[3] M. P. Heinl, M. Pursche, N. Puch, S. N. Peters, and A. Giehl, "From Standard to Practice: Towards ISA/IEC 62443-Conform Public Key Infrastructures", in *Computer Safety, Reliability, and Security*, Springer Nature Switzerland, 2023, pp. 196–210. DOI: 10.1007/978-3-031-40923-3_15.

[4] C. Gidney, *How to factor 2048 bit RSA integers with less than a million noisy qubits*, arXiv:2505.15917 [quant-ph], May 2025. DOI: 10.48550/arXiv.2505.15917.

[5] C. Chevignard, P.-A. Fouque, and A. Schrottenloher, "Reducing the Number of Qubits in Quantum Factoring", in *Advances in Cryptology – CRYPTO 2025*, Y. Tauman Kalai and S. F. Kamara, Eds., vol. 16001, Series Title: Lecture Notes in Computer Science, Springer Nature Switzerland, 2025, pp. 384–415. DOI: 10.1007/978-3-032-01878-6_13. [Online]. Available: https://link.springer.com/10.1007/978-3-032-01878-6_13 (Retrieved: 09/05/2025).

[6] P. Viorel, *Preparing ICS for Future Threats with Quantum-Resistant Cybersecurity*, Nov. 2024. [Online]. Available: https://www.iiot-world.com/ics-security/cybersecurity/preparing-ics-future-threats-quantum-cybersecurity/ (Retrieved: 09/04/2025).

[7] J. Fan *et al.*, "Impact of post-quantum hybrid certificates on PKI, common libraries, and protocols", *International Journal of Security and Networks*, vol. 16, no. 3, pp. 200–211, 2021. DOI: 10.1504/IJSN.2021.117887.

[8] T. Frauenschläger and J. Mottok, "Problems and New Approaches for Crypto-Agility in Operational Technology", in *12th European Congress Embedded Real Time Systems - ERTS 2024*, Jun. 2024. [Online]. Available: https://hal.science/hal-04614197.

[9] M. Pritikin, P. E. Yee, and D. Harkins, *Enrollment over Secure Transport*, RFC 7030, Oct. 2013. DOI: 10.17487/RFC7030.

[10] ITU-T, *Recommendation ITU-T X.509*, Oct. 2019. [Online]. Available: https://www.itu.int/rec/T-REC-X.509-201910-I/en.

[11] M. Pritikin, M. Richardson, T. Eckert, M. H. Behringer, and K. Watsen, *Bootstrapping Remote Secure Key Infrastructure (BRSKI)*, RFC 8995, May 2021. DOI: 10.17487/RFC8995.

[12] K. Watsen, M. Richardson, M. Pritikin, and T. Eckert, *A Voucher Artifact for Bootstrapping Protocols*, RFC 8366, May 2018. DOI: 10.17487/RFC8366.

[13] D. von Oheimb, S. Fries, and H. Brockhaus, *BRSKI with Alternative Enrollment (BRSKI-AE)*, RFC 9733, Mar. 2025. DOI: 10.17487/RFC9733.

[14] T. Mononen, T. Kause, S. Farrell, and D. C. Adams, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, RFC 4210, Sep. 2005. DOI: 10.17487/RFC4210.

[15] International Electrotechnical Commission, "Industrial communication networks – Network and system security", Standard IEC/TS 62443:2009, 2009.

[16] D. Bong and G. Scott, *PKCS #11 Specification Version 3.2*, OASIS Standard, Apr. 2025. [Online]. Available: https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.2/pkcs11-spec-v3.2.html.

[17] J. Krieger, T. Hilbig, and T. Schreck, "Device Identity Bootstrapping in Constrained Environments: A BLE-Based BRSKI Extension", in *2025 20th European Dependable Computing Conference (EDCC)*, IEEE Computer Society, Apr. 2025, pp. 93–99. DOI: 10.1109/EDCC66201.2025.00024.

[18] A. Rüst, A. R. D. Schellenbaum, T. Schläpfer, C. Stauffer, and O. Camenzind, "Authenticating wireless nodes in building automation : Challenges and approaches", in *Wireless Congress: Systems & Applications*, Nov. 2018. DOI: 10.21256/ZHAW-2750.

[19] The Go Project, *The Go Programming Language*. [Online]. Available: https://go.dev/ (Retrieved: 09/05/2025).

[20] GlobalSign, *Globalsign/est*, May 2025. [Online]. Available: https://github.com/globalsign/est (Retrieved: 09/05/2025).

[21] R. Housley, *Cryptographic Message Syntax (CMS)*, RFC 5652, Sep. 2009. DOI: 10.17487/RFC5652.

[22] S. Ben, R. Adam, and D. V. Geest, "Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)", Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-cms-ml-dsa-06, Jul. 2025, Work in Progress, 30 pp. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-ml-dsa/06/.

[23] M. Ounsworth, J. Gray, M. Pala, J. Klaußner, and S. Fluhrer, "Composite ML-DSA for use in X.509 Public Key Infrastructure and CMS", Internet Engineering Task Force, Internet-Draft draft-ietf-lamps-pq-composite-sigs-07, Jul. 2025, Work in Progress, 198 pp. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/07/.

[24] H. Brockhaus, D. von Oheimb, and S. Fries, *Lightweight Certificate Management Protocol (CMP) Profile*, RFC 9483, Nov. 2023. DOI: 10.17487/RFC9483.