Towards Automated Post-Quantum Certificate Management for the Industrial Internet of Things

KIRON MIRDHA[*], Robert Bosch GmbH, Germany
SEBASTIAN PAUL, Robert Bosch GmbH, Germany

The Industrial Internet of Things (IIoT) is characterized by its high interconnectedness enabling data exchange across private and public networks. In order to protect the authenticity of industrial devices and applications against cyber-attacks, current best practices typically involve public-key infrastructures (PKIs). While PKI solutions are well established in the Web, recent studies suggest that their realization in industrial applications is often insufficient.

Moreover, the long lifespan of IIoT devices necessitates protecting them against future threats, such as attacks aided by quantum computers. Especially the ongoing standardization efforts of post-quantum cryptography (PQC) motivate research on its applicability in industrial networks.

Our work aims to reduce the complexity of certificate management for IIoT devices by automating administrative PKI tasks. Furthermore, we address the quantum threat by incorporating post-quantum certificates. Our design is based on the Lightweight Certificate Management Protocol Profile for X.509 digital certificates. It considers the requirements of industrial networks and automates the three main functions of certificate management: certificate issuance, renewal, and revocation status check. We analyze the security of the proposed protocol in the symbolic model using a formal verification tool. Additionally, we show that the PQC signature schemes CRYSTALS-Dilithium and Falcon are viable post-quantum alternatives — even for time-sensitive industrial applications.

Keywords: Post-Quantum Cryptography, Certificate Management, Industrial Networks

[*] Also with Karlsruhe Institute of Technology.

Authors' addresses: Kiron Mirdha, fixed-term.Kiron.Mirdha@de.bosch.com, Robert Bosch GmbH, Renningen, Germany; Sebastian Paul, Sebastian.Paul2@de.bosch.com, Robert Bosch GmbH, Renningen, Germany.