RISC-V Solutions for Post Quantum Computing for Machine Readable Travel Documents

PQC4eMRTD

Leonidas Kosmidis, Matina Maria Trompouki, Eric Rufart, Jannis Wolf, Guillermo Vidal, Marc Solé
Barcelona Supercomputing Center (BSC)

Goal

To push previous Post-Quantum-Cryptography (PQC) research results towards the international standardisation working groups in order to unlock the implementation of Quantum-Resistant (QR) protocols, mainly in the fields of digital identities and electronic Machine-Readable Travel Documents (eMRTDs).

Focus

Focus on standardisation and dissemination to strengthen Europe's efforts on the transition to PQC by supporting European and international standardisation activities, delivering a comprehensive European PQC industrial migration roadmap and raising awareness regarding PQC endeavours

PQC

In 2017, the US National Institute of Standards and Technology (NIST) started its post-quantum cryptography project and asked for submissions of post-quantum key exchange, public-key encryption, and signature schemes to a competition-like standardization effort. In 2022, the first algorithms chosen for standardization were announced, with finalized written standards published in 2024.

Governmental applications are critical, especially due to the fact that identity theft or misuse can have major consequences. Government ID applications include travel documents (ePassport) and ID cards – often equipped with digital signature functionality.

PQC4eMRTD Consortium

infineon · Barcelona Supercomputing Center, Centro Nacional de Supercomputación · THALES · inštitutzaprimerjalnopravo · CRYPTONEXT SECURITY

Contact Us

https://www.pqc4emrtd-project.eu/
@pqc4emrtd
/company/pqc4emrtd-project

Project ID

Project Runtime: January 2024 – December 2025 (24 months)
Call: DIGITAL-ECCC-2024-DEPLOY-CYBER-06; Standardisation and awareness of the European transition to post-quantum cryptography; Coordination and Support Actions (CSA)
Budget: 1M€

More Information

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

PQC4eMRTD has received funding from the European Union's DIGITAL research and innovation programme under Grant Agreement No 101190400 and is supported by the European Cybersecurity Competence Centre.