QUASAR

Quantum Technologies for Future-Ready and Secure Air Traffic Management

Programm / Ausschreibung	WRLT 24/26, WRLT 24/26, Take Off 2025	**Status**	laufend
Projektstart	01.12.2026	**Projektende**	30.11.2027
Zeitraum	2026 - 2027	**Projektlaufzeit**	12 Monate
Projektförderung	€ 199.990		
Keywords	Post-Quantum Migration; Air Traffic Management; Cryptographic Bill of Materials; Aviation Cybersecurity; Quantum-Resilient Systems		

Projektbeschreibung

Fortschritte im Bereich des Quantencomputings stellen langfristig eine potenzielle Bedrohung für heute eingesetzte kryptographische Verfahren dar. Besonders sicherheitskritische Infrastrukturen wie das Air Traffic Management (ATM) müssen sich frühzeitig mit möglichen Auswirkungen und geeigneten Gegenmaßnahmen auseinandersetzen.

Das Projekt QUASAR analysiert systematisch die potenziellen Auswirkungen quantenfähiger Angriffe auf kryptographische Komponenten im ATM-Kontext. Dazu werden relevante Standards und bestehende Sicherheitsmechanismen untersucht sowie repräsentative Anwendungsfälle identifiziert und in Form eines strukturierten Cryptographic Bill of Materials (CBOM) dokumentiert.

Auf dieser Grundlage bewertet das Projekt kryptographische Schwachstellen, priorisiert Risiken und entwickelt strategische Ansätze für eine zukünftige Migration zu post-quanten-sicherer Kryptographie (PQC). Die Ergebnisse werden in Form eines migrationsorientierten Fahrplans und strategischer Empfehlungen aufbereitet und bilden die Grundlage für zukünftige Forschungs- und Implementierungsprojekte zur quantensicheren Absicherung von ATM-Systemen.

Abstract

Advances in quantum computing pose a potential long-term threat to currently deployed cryptographic mechanisms. Safety-critical infrastructures such as Air Traffic Management (ATM) must therefore assess possible impacts early and prepare appropriate mitigation strategies.

The QUASAR project systematically analyzes the potential impact of quantum-enabled attacks on cryptographic components within the ATM domain. Relevant standards and existing security mechanisms are reviewed, and representative use cases are identified and documented through a structured Cryptographic Bill of Materials (CBOM).

Based on this foundation, the project evaluates cryptographic vulnerabilities, prioritizes risks, and develops strategic approaches for a future migration towards post-quantum cryptography (PQC). The results are consolidated into a migration-oriented roadmap and strategic recommendations that support future research and implementation projects aimed at securing ATM systems against quantum threats.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- FREQUENTIS AG