

SPQR-AT

Sichere Post-Quantum-Resilienz für Österreichische Banken

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS CS F&E-Dienstleistungen (CS FED_2025)	Status	laufend
Projektstart	01.11.2026	Projektende	31.10.2028
Zeitraum	2026 - 2028	Projektlaufzeit	24 Monate
Barwert der Projektförderung	€ 198.923		
Keywords	Kryptographie, Post-Quantum-Sicherheit, Finanzinstitutionen		

Projektbeschreibung

Das Projekt SPQR-AT widmet sich der Frage, wie Finanzinstitutionen in Österreich auf die bevorstehenden sicherheitstechnischen Herausforderungen der Post-Quantum-Ära vorbereitet werden können. Da herkömmliche kryptografische Verfahren wie RSA oder ECC durch leistungsfähige Quantencomputer angreifbar werden, besteht dringender Handlungsbedarf. Es müssen organisatorische wie technische Grundlagen geschaffen werden, um langfristige Sicherheit und regulatorische Konformität gewährleisten zu können. Besonders im Finanzsektor – einem Bereich der kritischen Infrastruktur mit erheblichen Abhängigkeiten von verlässlichen digitalen Signaturen und geschützten Kommunikationskanälen – müssen Lösungen frühzeitig definiert, getestet und für die Praxis aufbereitet werden.

Das Projekt verfolgt daher zwei Hauptlinien:

- * Einerseits die Erstellung fundierter, praxisnaher Empfehlungen für den Einsatz von Post-Quantum-Kryptografie (PQC) in Finanzinstituten, ergänzt durch ein Modell für eine Cryptographic Bill of Materials (CBOM).
- * Andererseits die Entwicklung eines Prototyps der demonstriert, wie PQC-Signaturen unter Nutzung von Cloud-Ressourcen sicher erzeugt werden können – abgesichert durch Remote Attestation, um die Vertrauenswürdigkeit des ausführenden Systems sicherzustellen.

Ein zentrales Arbeitspaket ist die Analyse aktueller Kryptografie-Einsatzszenarien im Finanzsektor. Diese Bestandsaufnahme erfolgt durch Literaturstudien, Erfahrungsaustausch mit der österr. Finanzmarktaufsicht (FMA) sowie durch zwei Workshops mit Expertinnen und Experten aus der Praxis (ua der Nationalbank). Daraus werden jene Szenarien abgeleitet, in denen PQC künftig notwendig sein wird – etwa bei

- * der Sicherstellung der langfristigen Gültigkeit von Dokumentensignaturen,
- * bei Kommunikationskanälen oder
- * bei ausgelagerten IT-Dienstleistungen kleinerer Institute.

Auf Basis dieser Erkenntnisse werden PQ-Algorithmen hinsichtlich Sicherheit, Performance, Implementierungsreife und

regulatorischer Anforderungen evaluiert.

Parallel dazu wird eine Checkliste entwickelt, mit der Finanzinstitute ihren tatsächlichen Kryptografie-Einsatz identifizieren und bewerten können – ein essenzieller Bestandteil für die Entwicklung einer CBOM. Diese dient sowohl der internen Prüfung als auch der externen Aufsicht und schafft Transparenz, welche Algorithmen, Parameter und Systemkomponenten wo im Einsatz sind. Ergänzend wird ein exemplarischer Ausschnitt einer CBOM erstellt, der als Vorlage für Institute und die FMA dient.

Der Prototyp bildet ein weiteres Kernelement des Projekts: Er zeigt, wie PQC-Signaturen in einem Cloud-Umfeld sicher erstellt werden können, ohne dass der Dienstleister Zugriff auf die Daten erhält. Remote Attestation stellt sicher, dass ausschließlich geprüfter, unveränderter Code ausgeführt wird. Messungen zu Laufzeiten, Ressourcenbedarf und praktischem Aufwand ermöglichen erstmals eine realistische Einschätzung der zukünftigen Belastungen durch PQ-Signaturen – ein besonders relevanter Aspekt, da manche PQ-Verfahren deutlich höhere Anforderungen an CPU, Speicher und Bandbreite stellen.

Abschließend werden die Projektergebnisse sowohl der FMA als auch der wissenschaftlichen Gemeinschaft und der Öffentlichkeit zugänglich gemacht. Durch strukturierte Veröffentlichungen, Workshops und die Bereitstellung des Prototypen als Open-Source-Lösung wird sichergestellt, dass das Projekt einen nachhaltigen Beitrag zur digitalen Resilienz des österreichischen Finanzsektors leistet.

Abstract

The project SPQR-AT addresses how financial institutions in Austria can prepare for the upcoming security challenges of the post-quantum era. Since conventional cryptographic methods such as RSA or ECC are vulnerable to attacks by powerful quantum computers, there is an urgent need for action. Organizational and technical foundations must be established to ensure long-term security and regulatory compliance. Particularly in the financial sector - a sector of the critical infrastructure with significant dependence on reliable digital signatures and secure communication channels - solutions must be defined, tested, and prepared for practical application at an early stage.

The project therefore pursues two main objectives:

- * Firstly, the development of well-founded, practical recommendations for the use of post-quantum cryptography (PQC) in financial institutions, supplemented by a model for a Cryptographic Bill of Materials (CBOM).
- * Secondly, the project develops a prototype that demonstrates how PQC signatures can be securely generated using cloud resources - secured by remote attestation to ensure the trustworthiness of the executing system.

A key work package is dedicated to analyzing current cryptography use cases in the financial sector. This inventory is compiled through literature reviews, an exchange of experience with the Austrian Financial Markets Authority (FMA), and two workshops with experts from the field of financial institutions (incl. the Austrian National Bank). From this, scenarios will be derived in which PQC will be necessary in the future, for example

- * ensuring the long-term validity of document signatures,
- * securing communication channels, or
- * secure outsourced IT services for smaller institutions.

Based on these findings, PQ algorithms will be evaluated with regard to security, performance, implementation readiness, and regulatory requirements.

In parallel, a checklist is being developed to help financial institutions identify and assess their actual use of cryptography – an essential component for developing a CBOM (Cryptographic Bill of Materials). This CBOM supports both internal audits and external oversight, creating transparency regarding which algorithms, parameters, and system components are in use and where. Additionally, an exemplary excerpt of a CBOM is being created to serve as a template for institutions and the FMA.

The prototype forms the second core element of the project: It demonstrates how PQC (Post Quantum Cryptography) signatures can be securely generated in a cloud environment without the service provider gaining access to the data. Remote attestation ensures that only verified and unmodified code is executed. Measurements of runtimes, resource requirements, and practical effort enable for the first time a realistic assessment of the future burden of PQ signatures – a particularly relevant aspect, as some PQ methods place significantly higher demands on CPU, memory, and bandwidth.

Finally, the project results will be made available to the FMA, the scientific community, and the public. Structured publications, workshops, and providing the prototype as open-source ensure that the project makes a sustainable contribution to the digital resilience of the Austrian financial sector.

Projektkoordinator

- Universität Linz

Projektpartner

- Finanzmarktaufsichtsbehörde