

Whitepaper: Quant-ID – Quantum-Safe User Authorization for Critical Identity Access Management (IAM) Infrastructures

Subproject of the Joint Project: Quant-ID | Reference Number: KIS6QKH005
Secure Quantum Communication for Critical Identity Access Management Infrastructures –
Post-Quantum and Quantum-Secure User Authorization



Fig. 1: Quant-ID Cover Image. Licensed from iStock.

Project Duration: 43 Months (01.09.2022 – 31.03.2026)

Project Member: Quant-X Security & Coding GmbH

Address: Ricklinger Straße 91, 30449 Hannover, Germany

Project Lead / Contact: Xenia Bogomolec

Executive Summary

The overall objective of the Quant-ID project was the development of reliable digital identities and quantum-safe authorization for users within Identity Access Management (IAM) architectures. The primary focus was on end-to-end protection using Quantum Random Number Generators (QRNG) and Post-Quantum Cryptography (PQC), spanning network communications, electronic signatures, and application-layer encryption. By integrating quantum security directly into established IAM protocols such as OAuth 2.0 and OpenID Connect, Quant-ID delivers a cost-effective, practical end-to-end solution that strengthens technological sovereignty in quantum-safe authentication.

Problem Statement

The security of modern, highly automated IAM protocols in critical infrastructures relies fundamentally on two pillars: the quality of the random numbers used and the robustness of the underlying cryptographic algorithms. Traditional approaches often require dedicated, isolated quantum networks (e.g., EuroQCI or

QRange in Geneva), creating significant cost and deployment barriers. Furthermore, upcoming quantum computing capabilities threaten classical encryption schemes, requiring a seamless transition toward Post-Quantum Cryptography (PQC) without disrupting existing digital infrastructure.

The Quant-ID Solution: Integrating QRNG and PQC into OAuth/OpenID Connect

Rather than relying on isolated physical networks, Quant-ID directly embeds quantum safety into widely adopted, standard IAM protocols—specifically OAuth 2.0 and OpenID Connect. This enables a cost-effective and low-threshold migration path. The solution complies with BSI AIS 20/31 standards for random number generators, the NIST SP 800-90 series, NIST PQC standards, network security benchmarks, and an experimental version of PQC in JSON Object Signing and Encryption (JOSE) standards. By realizing quantum-safe digital authorization, Quant-ID elevates security levels across critical infrastructures and general internet deployments.

Technical Approach

The subproject led by Quant-X Security & Coding GmbH focused on three core areas: supporting the security proof and validation of the vacuum-fluctuation-based QRNG developed by Fraunhofer IPMS, specifying post-quantum cryptography for OAuth and OpenID Connect based on recommendations from the University of Regensburg, and developing a quantum- and post-quantum-secure authorization server and clients. Key aspects of the technical implementation include:

Quantum Entropy Generation: Fraunhofer IPMS developed a QRNG based on vacuum fluctuations, offering very high output rates with mathematically provable high entropy suitable for high-load IAM systems. Quant-X supported design requirements from information security and compliance perspective, entropy output validation, and QRNG integration to a Linux hosting environment. The BSI AIS 20/31 team provided advisory guidance on certifiability.

IAM & Open-Source Architecture: Quant-X implemented an authorization server and two clients on a IBM VPC Debian 13 hosting environment with OpenID Core interfaces, incorporating open-source libraries from global OAuth/OpenID Connect experts Roland Hedberg and Giuseppe de Marco.

NIST Standardisation & Re-architecture: Following NIST's August 2024 PQC standardization, Quant-X transitioned from experimental to standardized libraries, undergoing a complete realigning of its hosting environment and application architecture in 2025.

Cloud Demonstrator Deployment: A functional demonstrator for quantum-safe authorization was successfully deployed on an IBM Virtual Private Cloud (VPC) instance. Quantum random numbers are streamed directly from Fraunhofer IPMS's laboratory via a dedicated online interface into the cloud hosting environment's entropy pool.

Project Outcomes

The Quant-ID project successfully demonstrated that while PQC exhibits different network behavior compared to classical cryptography, it can be integrated into high-load IAM systems without impairing user experience. Key achievements include:

Modular Architecture: Developed solutions are highly modular, permitting flexible exploitation of both the hardware QRNG system and the software components.

Academic & Industry Outreach: Results were presented at numerous national and international conferences, including the OAuth Security Workshop 2026 in Leipzig, strengthening links between the global expert community and German quantum security research.

End-to-End Demonstrator: Successfully built and validated a cloud-based proof-of-concept demonstrating practical, quantum-safe authentication and authorization.

Future Outlook

Quant-X Security & Coding GmbH is actively advancing commercialization and exploitation plans, evaluating new strategic partnerships to accelerate deployment. Focus areas include applying the QRNG as an entropy source in virtualized cloud infrastructures and delivering post-quantum-safe IAM aligned with upcoming NIST and European Union PQC transition roadmaps.

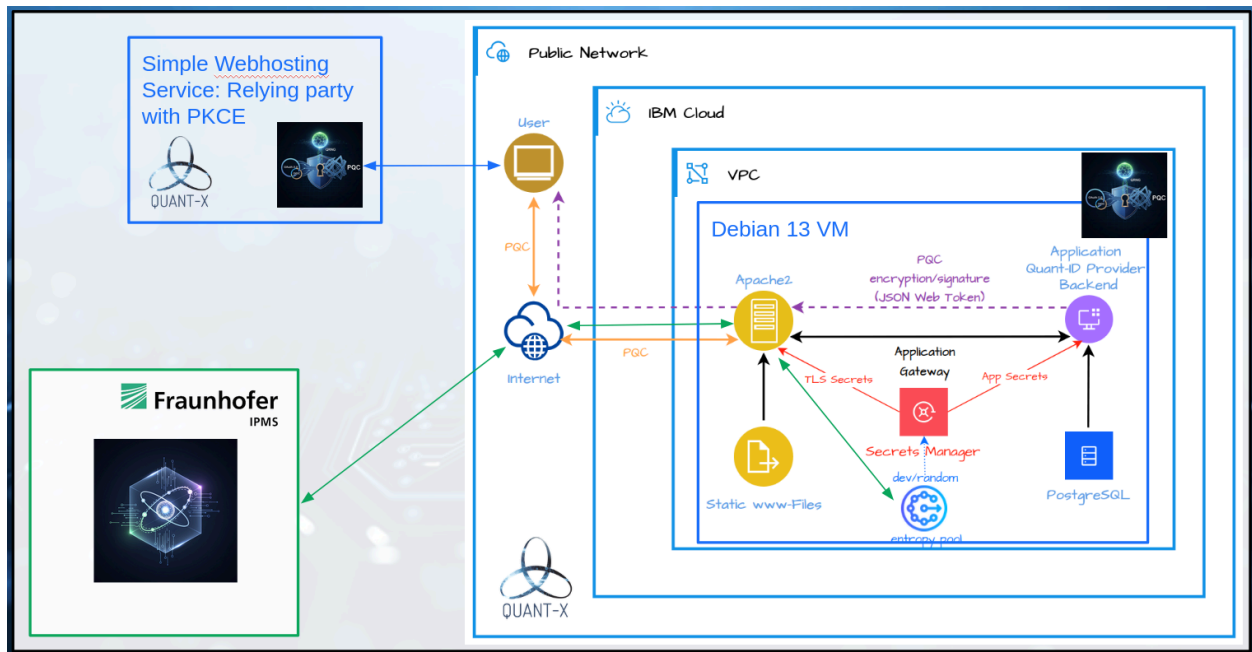


Fig. 2: Diagram of the Quant-ID Demonstrator. Copyright: Quant-X Security & Coding GmbH.