

Technical Report Part II: Detailed Presentation of Quant-ID

Subproject of the joint project: Quant-ID - Joint project number: KIS6QKH005

Secure Quantum Communication for Critical Identity Access Management Infrastructures - Post-Quantum and Quantum-Secure User Authorization



Pic. 1: Quant-ID title image. Licensed from iStock.

Subproject Duration: 43 months
01.09.2022-31.03.2026

Project Duration:

Company:

Quant-X Security & Coding GmbH
Ricklinger Straße 91
30449 Hannover
Germany

Project Leader/Contact Person:

Xenia Bogomolec (Consortium Coordinator and Applicant)
Email: xb@quant-x-sec.com

Project Objective and Technical Context

The goal of the overall Quant-ID project was the development of reliable digital identities and quantum-secure authorization for users in Identity Access Management (IAM) architectures, with a focus

on end-to-end security provided by quantum random number generators (QRNG) and post-quantum cryptography (PQC), covering network communication as well as electronic signatures and encryption at the application layer. The original objective stemmed from the recognition that the security of modern, highly automated IAM protocols in critical infrastructures heavily depends on the quality of the random values used and the cryptographic methods employed. The subproject conducted by Quant-X therefore focused on three core areas: the security proof of the QRNG developed by Fraunhofer IPMS, the implementation of cryptographic optimizations based on recommendations from the University of Regensburg, and the development of a quantum- and post-quantum-secure authorization server and client.

Regarding the scientific and technical state of the art, the project built upon international developments aimed at PQC implementations for system authentication in dynamic networks (e.g., EuroQCI and QRange in Geneva). However, Quant-ID differentiates itself from these approaches through a specific strategy: instead of assuming dedicated, isolated quantum networks, quantum security is integrated directly into widely used, established IAM protocols such as OAuth 2.0 and OpenID Connect. This enables a cost-effective and low-threshold migration. Requirements from BSI AIS 20/31 for random number generators, the NIST SP 800-90 series, network security, and "JSON Object Signing and Encryption" (JOSE)¹ standards were taken into account. Through the realization of quantum-secure open-source libraries, the security level is intended to be raised not only for critical infrastructures, but potentially for every internet user. Quant-ID thus creates a practical end-to-end solution that strengthens Germany's technological sovereignty in the field of quantum-secure authentication.

The project was characterized by intense interactive collaboration with partners Fraunhofer IPMS, the University of Regensburg, and MTG AG. Quant-X led the consortium and coordinated numerous technical and scientific communication activities with the umbrella project SQuaD, other projects within the Innovation Hub, industrial customers of Quant-X, and the Federal Office for Information Security (BSI). In the following sections, we present Quant-X's activities in detail for each technical area of the project.

The Importance of Random Values and Cryptography in IAM

In modern Identity and Access Management (IAM) architectures based on standards such as OAuth 2.0 and OpenID Connect (OIDC), random values form the foundation of security. IAM protocols rely on cryptographic keys, nonces, identity tokens, refresh tokens, and access tokens being unpredictable. Any weakness in randomness generation opens attack vectors across the complex digital workflows of authentication, authorization, and data access. If an attacker can predict the sequence of generated random values, they can forge tokens or hijack sessions (session hijacking), compromising the entire security model.

Standards such as JSON Object Signing and Encryption (JOSE) require high-quality random numbers for signature generation and encryption to ensure the authenticity and confidentiality of communication between client and server at both the network and application layers. Conventional random number generators (Pseudo-Random Number Generators – PRNG) are often based on algorithms whose output is

¹ [JSON Object Signing and Encryption \(JOSE\)](#)

predictable given knowledge of the input. Quantum Random Number Generators (QRNG), on the other hand, set new standards. Quantum entropy is based on fundamental physical processes. These are not algorithmically computable; instead, they offer genuine, unpredictable randomness. A key advantage for critical infrastructures is mathematically provable high entropy. This ensures that requirements for functionality classes of TRNGs (True Random Number Generators), such as defined in BSI AIS 20/31 or NIST SP 800-90, are not only met but can even be exceeded under optimal conditions.

Another advantage of a high-performance quantum entropy source is that it supports the high performance demands of IAM systems. Systems such as the demonstrator developed in Quant-ID require a steady and rapid supply of random values under heavy loads. Vacuum fluctuations in particular enable very high output rates, ensuring the security of IAM protocols without compromising system performance.

In summary, the transition to quantum entropy in IAM protocols represents a technological safeguard that extends beyond classical cryptographic security, creating a robust and future-proof trust model.

QRNG Requirements and Security Proof

Quant-X supported the Fraunhofer IPMS and the University of Regensburg with the QRNG design requirements and the security proof of the QRNG. Following initial literature research, it became clear that the proof was closely tied to the design requirements of the device and would take place in parallel with the implementation by Fraunhofer IPMS. Therefore, a new strategy for the security proof was developed and coordinated with the project sponsor VDI/VDE and the BMBF (now BMFTR). The project established an entropy team featuring experts from Fraunhofer IPMS, Quant-X, and the University of Regensburg. This team held bi-weekly online meetings to optimally coordinate their highly interconnected activities. Ilja Gerhardt and René Schwonnek, internationally recognized quantum entropy experts from Leibniz University Hannover, and the BSI AIS 20/31 team supported the group on key technical questions.

Selection of Methods and Quantum Entropy Source

The entropy team began with a literature review of various QRNGs, simulations of selected quantum entropy sources (e.g., phase noise), and the evaluation of different analytical methods for the physical setup. In addition, the Rényi entropy family was evaluated with respect to the project's requirements. Given the objective of building a certifiable QRNG, the team decided to utilize min-entropy in the security proof. Furthermore, various randomness extraction methods and statistical validation techniques for the quality of raw and post-processed data were evaluated and tested. Initial results comparing phase noise were presented as a poster titled *"Gain-Switching in Phase Noise Quantum Random Number Generators: An Experimental and Stochastic Analysis"* at the Physics and Security Conference in Bad Honnef and discussed with other quantum security experts. Following these initial analyses, Fraunhofer IPMS decided to develop a QRNG based on vacuum fluctuations. The primary reasons were the mathematical provability of true randomness, very high output rates, and the physical stability of the quantum source against environmental influences.

Understanding the Term "QRNG Security Proof"

The goal of a QRNG security proof is to demonstrate that the output values generated by the respective QRNG are truly random. In theoretical physics, true randomness only exists in quantum mechanical systems. Classical physical systems are deterministic, even if they are highly complex. The authors of the Reference Standard for the Entangled Quantum Random Number Generator with the Public Randomness Certification – Theoretical Concepts (Definitions, True Randomness, Use Cases) by EITCI² describe the availability of true random number generators as follows: *"Most of the currently used RNG devices are based upon deterministic processes and classical (deterministic) chaos, that is the generation of randomness is based upon classical physics laws. In this case, in PRNGs randomness is not true, but is fully dependent on the complexity of the system involved in the physical process of randomness generation and in principle can be predicted with sufficient knowledge of initial conditions regarding the physical system and computational power to simulate its behavior."*

The vacuum fluctuation QRNG implemented by Fraunhofer IPMS for Quant-ID is not based on entanglement. However, the physical prerequisites cited by EITCI also apply to systems that do not rely on entanglement. Implementations of physical systems always deviate from theory because every system interacts with its environment. Therefore, from the perspective of the Quant-ID consortium, relying solely on the quantum mechanical properties of a QRNG is insufficient to assume true randomness. The deviation between physical implementation and theory must be evaluated within a validation framework. Demonstrating the quantum nature of a system remains very demanding. For instance, the Bell test proves the quantum property of systems based on entanglement, but its setup is extremely complex and drastically reduces the QRNG output rate, making it impractical for digital industrial applications. Since the vacuum fluctuation QRNG in Quant-ID does not rely on entanglement, the Bell test is inapplicable regardless of these drawbacks. The project therefore had to rely on alternative methods. For security proof and verification, we examined three classes: "device-dependent", "device-independent", and "semi device-independent". Depending on the context, these three classes are referred to as "QRNG classes", "security proof classes", or "protocol classes", reflecting the close coupling between the QRNG architecture, the implemented protocol, and provable security.

The 3 Security Proof Classes

The three security proof classes—device-dependent, device-independent, and semi-device-independent proof—were investigated for feasibility regarding the vacuum fluctuation QRNG under consideration of project requirements (application as an online QRNG for OpenID Connect). Specifically, we took into account criteria from our project's internal security proof strategy, available research findings on vacuum fluctuation QRNGs from other experts, prerequisites for potential BSI certification, setup complexity, and industrial exploitation potential.

² [EITCI-OSG-EQRNG THEORETICAL CONCEPTS](#)

Device-dependent (Practical) QRNG is based on complete, trustworthy modeling of the physical quantum process. This approach enables high output rates at moderate cost. Quantum randomness is often mixed with classical randomness, which can be minimized through proper modeling. Post-processing in this case cannot reduce side information, and in the worst case, might even decrease quantum entropy. The required absolute trust in the implementation's correctness can be problematic when dealing with external suppliers without certification.

The class of device-independent (Self-Testing) QRNGs includes devices whose output is tested for randomness due to a lack of trust in the physical process. Security analysis for such protocols must account for faulty or even malicious device scenarios. Classical randomness tests can be combined with quantum tests, such as verifying the presence of quantum entanglement (e.g., via Bell tests). For these devices, neither the source nor the measurement is trusted. Since Quant-ID does not use entanglement, the Bell test is not applicable. Furthermore, the complex testing procedures make these processes too slow for real-time industrial requirements and vulnerable to Denial-of-Service attacks via manipulation. On the other hand, verifiable testing builds trust with a broader audience.

The hybrid approach is called semi-device-independent (Semi-test) QRNG. These devices distinguish between components that are fully relied upon due to exact implementation characterization and components tested due to a lack of trust. The advantages include higher output rates and a simpler setup compared to device-independent QRNGs. Plausibility checks, integrity verification, and sender authentication (in QKD) achieve higher security than a device-dependent QRNG. However, it must be ensured that the device cannot be tampered with during preparation and measurement.

Provides protection against Man-in-the-Middle scenarios. This class is a strong candidate for the Quant-ID project, offering distinct advantages in cloud environments (as a TRNG). However, it is more complex to implement than a purely device-dependent solution.

State of Requirements for QRNG Security Proofs from Research and Standardization

The authors of "100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations"³ describe the requirements for a QRNG security proof as follows: *"In order to obtain true unpredictability, it is critical to map any imperfections in the measurement setup and to know how much information is available to the environment. Information is leaked to the environment via side-information channels, which can be classified as either classical or quantum. Classical side information is any noise of a classical origin. Quantum side-information channels arise due to the environment being entangled with the system used to extract the random numbers. Security proofs have been proposed that take into account classical side information as well as quantum side information. In addition to the side-information leakage, imperfect analog-to-digital converters (ADC) also give rise to reduced performance. Therefore, the nonlinear behavior of the ADC must also be accounted for."*

³ [100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations](#)

According to the BSI, an RNG security proof must include a stochastic model (a family of distributions across multiple parameters) that describes the physical setup along with all classical and quantum side information. Min-entropy is then generally calculated for this model (dependent on the parameters, independent of experimental QRNG data). During an initial RNG operation, real-time experimental data is used to determine the parameters and compute the min-entropy of the device. The parameters and the min-entropy are then subsequently used during the startup test and online test to evaluate the quality of the entropy. The total failure tests detect total failure of the RNG. Online and total failure tests run continuously during the RNG operation. This enables real-time verification of whether output data meets the required quality. This process (along with additional statistical tests) is required by the BSI and the NIST for standardization.

Evaluation of Research Results from Other Experts

First, it should be noted that few organizations or experts focus on vacuum fluctuation QRNGs. Furthermore, not all publications include a formal security proof or verification. We examined a selection of 8 publications on vacuum fluctuation QRNGs, among which "100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations" presents an improved implementation of a QRNG setup⁴ by the same authors, Tobias Gehring and Cosmo Lupo. Only these two publications contain security proofs with stochastic modeling satisfying BSI TRNG requirements. Further details are summarized in the next section. Another analyzed implementation⁵ incorporates a security proof accounting for experimental constraints, such as digitization resolution or excessive local oscillator noise caused by unbalanced detection. Regarding output rates and statistical test results, this QRNG setup is less promising for our use case. Two other well-known publications in the expert community include statistical tests but lack formal security proof. Additionally, we examined three less prominent publications on vacuum fluctuation QRNGs from ResearchGate representing implementations without security proofs, providing crucial insights into the current state of research and additional evaluation methodologies.

Security Proof according to Bruynsteen, Gehring, Lupo, Bauwelinck, and Yin

The measurement implementation of the system described in "100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations" uses homodyne detection, achieving an impressive data rate of 100 Gbit/s. This capacity is enabled by combining a continuous noise source with high-bandwidth photodiodes, leading to significant improvements within the shot-noise-limited bandwidth. To analyze autocorrelation, the effect of a digital equalizer was tested, as detailed in the publication. Following measurement, randomness extraction is performed using Toeplitz hashing ($n = 8192$, $m = 5120$). The security proof is comprehensive: it accounts for both classical and quantum side information and integrates the non-linear behavior of the analog-to-digital converter (ADC). Quality and reliability of generated random

⁴ [Homodyne-based QRNG at 2.9 Gbps secure against quantum side-information.pdf](#)

⁵ [Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations](#)

numbers are verified by passing the NIST SP 800-22 and Die-harder statistical test suites at 100 Gbit/s, using the min-entropy framework as a methodological foundation.

This architecture meets all our requirements. Overall, we welcome that this publication executes a complete QRNG security proof due to the following factors: complexity and state-of-the-art QRNG validation, solid foundation for potential BSI certification, and potential industrial exploitation in critical infrastructures. The security proof is device-dependent (practical). The noted downside—requiring trust in device implementation—can be mitigated through potential BSI certification. Advantages related to data integrity and confidentiality verified via S-value measurements in device-independent and semi-device-independent classes do not apply here, as the system is not entanglement-based and thus ineligible for Bell tests. These aspects must be addressed separately, e.g., by evaluating threat scenarios and corresponding countermeasures.

The quantum property of the setup is verified at runtime via the integrated security proof, measuring classical side information and eliminating it during extraction under conservative min-entropy estimates. This aligns with our project's security proof strategy, allowing us to execute all work packages without restriction. The output rate of 100 Gbit/s provides a solid foundation for industrial exploitation beyond the project demonstrator. The setup's low structural complexity minimizes operational overhead and makes test runs less error-prone, while increasing capacity to evaluate an adequate number of test runs.

FMEA for the Physical Setup of the QRNG

For certifiability of the QRNG as TRG.3 according to BSI AIS 20/31 and NIST SP 800-90, tests before startup and at runtime must be defined. As a preparatory step, Quant-X conducted a Failure Mode and Effects Analysis (FMEA). The FMEA systematically evaluates potential failure points in the QRNG to identify, assess, and derive suitable tests or countermeasures ensuring operational safety. A gap analysis compared BSI TRNG requirements with NIST SP 800-90c. The FMEA focused on evaluating concepts for total failure tests and online tests per selected standards. The objective was to systematically identify, rate, and prioritize potential failure modes in the experimental QRNG system, producing a structured risk assessment to guide technical choices during development. Ultimately, the FMEA ensures any failure impacting entropy quality is anticipated, traceable, and testable. It was built using a bottom-up approach combining system analysis, literature review, and expert judgment: system decomposition, component identification, failure mode research, and evaluation metrics (severity, occurrence, detection).

The actual FMEA table is omitted from this report due to confidentiality constraints. The analysis followed standard FMEA methodology, breaking down the setup into functional modules (e.g., laser source, photodetector, amplifier, ADC). For each module, potential failure modes, causes, effects, and preventive measures were systematically cataloged. The structure recorded failure descriptions, system impact, occurrence probability, detection probability, and Risk Priority Numbers (RPN), allowing critical evaluation of individual parts and overall architecture. Out of 37 failure modes potentially relevant to total failure testing, 9 were confirmed relevant, predominantly involving component failures. FMEA entries were reviewed during

the consortium meeting in Dresden in June 2025 regarding technical plausibility, duplication, and completeness (integrating missing modes like power instability or firmware faults). This review refined entries, eliminated overlaps, and integrated high-impact modes (e.g., software crashes, entropy estimator drift). Finally, the FMEA was aligned with total failure and online testing strategies, ensuring every high-RPN element has a corresponding test or mitigation mechanism. Every critical entropy-affecting block was observable at runtime.

Definition and Implementation of QRNG Tests

Following the gap analysis between standards, Fraunhofer IPMS targeted the BSI AIS PTG.3 functionality class for post-project certification. This class mandates startup, online, and total failure tests. The startup test runs prior to operational start to detect complete noise source failure or severe statistical defects upon boot, preventing output of insecure or predictable random numbers before cryptographic operation begins. Online tests continuously evaluate random number quality during operation to catch gradual degradation or shifting statistical properties. Total failure tests rapidly detect complete noise source failure, preventing output of zero-entropy or severely weakened values. Reacting almost instantaneously to sudden physical defects, its design is based on technical failure analyses of the noise source. All three test types use statistical methods on raw QRNG data, primarily based on the NIST Randomness Test Suite (NIST SP 800-22). Test selection and parameterization depend heavily on the entropy source and overall TRNG architecture. The entropy team consulted with the BSI AIS 20/31 team and a NIST suite expert to address generic BSI requirements accommodating diverse entropy sources. Specific test details remain confidential. Fraunhofer IPMS successfully implemented these tests by project end while maintaining a very high output rate of 4.1 Gb/s.

Post-Quantum Cryptography in Identity Access Management

Digital identity and access management are foundational to securing data safety. To facilitate secure access across complex web infrastructures, protocols like OAuth and OpenID Connect (OIDC) were defined for use over HTTPS. Today, these protocols are ubiquitous across public and private networks. Beyond enabling social logins, OAuth and OIDC are vital for high-security, user-friendly Single Sign-On (SSO) experiences, particularly within major cloud ecosystems. A key example is Microsoft, where users logging onto a Windows desktop gain seamless access to all MS 365 applications, even across disparate servers in the Microsoft Cloud.

The security and trustworthiness of these protocols rely fundamentally on cryptography. Transport Layer Security (TLS) specifies cryptographic mechanisms at the network layer, while JSON Object Signing and Encryption (JOSE) defines mechanisms at the application layer. JOSE is a framework introduced by IANA⁶

⁶ [Internet Assigned Numbers Authority](https://www.iana.org/)

encompassing proposed standards: JSON Web Signing (JWS), JSON Web Encryption (JWE), JSON Web Key (JWK), JSON Web Token (JWT), and JSON Web Algorithms (JWA).

The "Harvest Now, Decrypt Later" scenario refers to state actors or cybercriminals intercepting classically encrypted data to decrypt it once cryptographically relevant quantum computers become available. Extensive data must remain confidential for decades. In 2025, a BSI survey revealed that data across many German organizations should have been PQC-encrypted six years prior to effectively mitigate this threat.

The risk that classically signed data can be forged once cryptographically relevant quantum computers arrive is termed "Trust Now, Forge Later". The integrity of IAM data must often be preserved for decades. For instance, an attacker with a quantum computer could forge financial transaction signatures or access tokens, posing severe risks to privileged accounts like system administrators, emergency users, or security engineers.

Both scenarios grow increasingly realistic given quantum computing advancements. Independent estimates suggest cryptographically relevant quantum computers could arrive sooner than anticipated. For example, Google and Cloudflare announced plans in spring 2026 to complete PQC migrations by 2029.

The European Commission and NIST have defined PQC migration roadmaps. Combiners mixing classical and PQC algorithms were added to TLS, and the post-quantum signature algorithm ML-DSA was incorporated into JWA for use with JWS. Critical European systems are expected to migrate by end-of-year 2030. Digital signature algorithms ECDSA, EdDSA, and RSA with 122-bit security will be deprecated by NIST after 2030 and disallowed after 2035. At 128-bit security or higher, these methods remain valid until end-of-year 2035. Similar timelines apply to key exchange mechanisms (Finite Field DH, MQV, ECDH, MQC, RSA), most of which are represented in JWA. Simultaneously, vulnerable IAM systems top OWASP Top 10 risks ("Broken Access Control" and "Cryptographic Failures"). PQC also introduces performance challenges; identity providers already struggle with token generation overhead. Hence, exploring PQC in OAuth and OIDC is urgent to guide stakeholders and accelerate global post-quantum IAM adoption.

Differentiation from Other PQC in IAM Projects

The publication "Post-Quantum Electronic Identity: Adapting OpenID Connect and OAuth 2.0 to the Post-Quantum Era"⁷, published prior to FIPS-203, FIPS-204, and FIPS-205 standardization, evaluated PQC in OAuth 2.0 and OIDC. The authors compared classical and PQC algorithms regarding size and performance (ECDSA, RSA 2048, Dilithium/FIPS-204, Falcon, SPHINCS+/FIPS-205, ECDHE, Kyber/FIPS-203). They identified the access token as the primary PQC-critical asset. In contrast, we identify other authorization flow data as PQC-critical: Client Secret, Client Request URI, username/password, Refresh Token, and PII in ID tokens. Access tokens are short-lived (5-60 minutes) and thus less vulnerable to quantum decryption threats.

The publication "Post-Quantum Electronic Identity" uses the OAuth 2.0 Authorization Code Grant Flow in a standard network environment as a reference. The authors concluded that PQC candidates offer

⁷ [Post-Quantum Electronic Identity: Adapting OpenID Connect and OAuth 2.0 to the Post-Quantum Era](#)

competitive performance against RSA and ECDSA, though network architecture significantly impacts latency. They emphasized the need for further research into hybrid schemes and latency mitigation techniques.

The OpenID Foundation initiated a workshop series on PQC across OAuth 2.0 and OIDC standards, including FAPI and OpenID Connect Federation 1.0. Our project focused on the OIDC Core specification, analyzing three complete authorization flows implemented in a high-security virtual environment with FIPS-compliant components: Authorization Code Flow (with and without PKCE) and Implicit Flow. We evaluated all transmitted data for long-term confidentiality and integrity requirements, investigated hybrid schemes, assessed advanced cryptographic properties, and addressed cybersecurity threats across the entire implementation.

Basic Terminology in the Context of IAM

This section outlines protocols relevant to integrating post-quantum cryptography into IAM, focusing on OAuth 2.0 and OIDC. OIDC is an interoperable authentication protocol suite built on OAuth 2.0, standardized by the OpenID Foundation. For deeper technical context, refer to OAuth 2.0 RFCs 6749, 6750, 7636, and the OIDC Core specification.

We adopt standard terminology from these specifications: An Authorization Server provides authorization services to Relying Parties (client apps) and securely stores persistent secrets (Client Secrets, password hashes, access tokens, session data, private keys). A Resource Server hosts digital resources (files, datasets) protected by authentication and authorization schemes (identity-based, group-based, or scope-based).

Authorization Flows

Authorization flows rely on Authorization Grants—credentials representing resource owner authorization used by clients to request access tokens. OAuth 2.0 defines Authorization Code Grant, Implicit Grant, Resource Owner Password Credentials Grant, and Client Credentials Grant. RFC 8252 defines native app browser flows, while OIDC Core specifies Authorization Code, Implicit, and Hybrid flows. PKCE enhances security for public clients. We focus on Authorization Code Flow, Authorization Code Flow with PKCE, and Implicit Flow.

The Authorization Code Flow is used for trusted Relying Parties (e.g., full-stack web applications) that can securely store Client Secrets. When requesting protected resources, the client authenticates with the Authorization Server to receive an authorization code. The user authenticates at the server login interface. Upon successful verification, the authorization code is issued to the client, which exchanges it for access, refresh, and ID tokens to access resource servers on behalf of the user.

Authorization Code Flow with PKCE is recommended for Public Clients (e.g., single-page web applications) lacking secure persistent storage for secrets like Client Secrets. PKCE prevents authorization code interception and replay attacks by generating an ephemeral random Code Verifier on the user device and

sending its cryptographic hash (Code Challenge) to the server. During token exchange, the original Code Verifier is transmitted and verified. Generating the Code Verifier requires a high-entropy source.

Implicit Flow was originally designed for Public Clients but is now restricted to simple login scenarios. Using Implicit Flow for token requests introduces severe vulnerabilities (e.g., CSRF attacks and access token leakage via URL fragments). PKCE was designed specifically to eliminate these security risks for public clients.

The OAuth and OIDC community continuously monitors emerging security threats. Beyond working groups, the annual OAuth Security Workshop (OSW) serves as a primary exchange forum. Quant-X presented its Quant-ID results at OSW 2026 in Leipzig, evaluating industry partnerships and future project initiatives.

Cryptography and Entropy in OAuth and OpenID Connect

Cryptography and entropy form the core of security in OAuth 2.0 and OIDC. TLS protects confidentiality and integrity across all static and ephemeral secrets. Static secrets include user credentials, Relying Party credentials, and private keys for TLS and JOSE, as well as the Client Request URI. Ephemeral secrets include authorization codes, state, nonces, and PKCE challenge parameters. Access and refresh tokens feature configurable lifespans ranging from 30 minutes to 90 days.

The Authorization Server signs issued tokens to prove authenticity, while Relying Parties validate these signatures. Compromising a signing key enables attackers to impersonate any user, including superusers and system administrators. Incidents involving identity key compromise in hyperscaler IAM highlights these risks⁸. The "Trust Now, Forge Later" threat underscores the critical need for post-quantum signature schemes to protect long-term signing keys in identity protocols.

JSON Web Tokens can also be encrypted at the application layer to preserve confidentiality across TLS endpoints against web hosting or cloud providers. High-entropy sources are essential not only for key generation but also for tokens, nonces, codes, client URIs, and state parameters.

Cryptographic Primitives and Their Impact on Performance

Key cryptographic primitives in OAuth and OIDC include digital signatures, symmetric encryption, and Key Encapsulation Mechanisms (KEMs). Digital signatures ensure integrity and origin verification for tokens, while KEMs enable token encryption. Approved algorithms are specified in JOSE JWA, into which post-quantum standards ML-DSA-44, ML-DSA-65, and ML-DSA-87 were recently incorporated.

Quant-X supported cryptographic analysis by the University of Regensburg by evaluating classical JWA algorithms. In 2023, lattice-based ML-DSA (formerly Dilithium2) was identified as a prime candidate for token signatures. ML-DSA key generation is slower than ECC but significantly faster than RSA. Signature generation in ML-DSA-65 is up to 10x faster than RSA-2048. At high security levels (NIST Level 5), ML-DSA-87 (~75 µs) outperforms ECDSA (>400 µs). Verification is up to 20x faster than high-level ECC

⁸ [Black Hat | Webinar: UnAuthorized: The Previously Untold Findings](#)

(P-521). However, ML-DSA signatures are 9–40x larger than ECC/RSA, causing network packet fragmentation and increasing latency impacts. Public keys are 5–80x larger, though since client fetching occurs infrequently, the overall network impact of public keys is minor compared to token signatures.

Another notable candidate is Unbalanced Oil and Vinegar (UOV), a multivariate signature scheme offering significantly smaller signatures and faster timings, albeit with public keys ~200x larger than ML-DSA.

Falcon-512 (FN-DSA / FIPS-206) shares similar properties to ML-DSA, featuring 3.5x smaller signatures at the cost of ~3x slower signing speeds.

JOSE currently recommends RSA-OAEP and ECDH with AES Key Wrap for JWT encryption. We propose adopting ML-KEM into JWA for quantum-secure token encryption. ML-KEM comes with minimal CPU overhead compared to classical methods, though larger public key sizes (~2.2 KB total for key and ciphertext) increase network latency via packet fragmentation, which means that the payload forces the network to transmit over multiple TCP packets. For example, in low-latency testing environments, ML-KEM-768 shows identical end-to-end network timings to RSA-2048. When moving to degraded network conditions such as mobile networks or networks with high packet loss, the packet fragmentation results in higher latency. For example, if a packet is dropped under a 5% packet loss condition, ML-KEM requires a retransmission that can cause its overall network handshake latency to reach up to 180 ms in heavily throttled tests.

Symmetric primitives are used throughout OAuth 2.0 and OIDC for encryption and hashing. In general, doubling key sizes maintains security levels in quantum setting. AES-256 already fulfills NIST Quantum security category 5 and requires no modification. AES-128 is classified as a category 1 and AES 192 is a NIST category 3 post-quantum algorithm. They can be continued to be used for applications that process data with shorter confidentiality requirements. The continued use of AES-128 and AES-192 offer the chance to lower the overall impact of resource consumption and performance in environments with restricted computational resources.

Integration of PQC and QRNG in Authorization Server and Clients

Quant-X developed an OAuth/OIDC authorization server, a confidential client, and a public client utilizing certified open-source libraries by Roland Hedberg and Giuseppe de Marco. Benchmarks across FIPS-203, FIPS-204, and FIPS-205 were conducted on a Linux desktop (Intel i9-13900H) and an IBM VPC VM (Debian 13, Intel Xeon Cascade Lake), confirming desktop performance was ~1.74x higher. Experimental PQC modules were implemented into custom versions of JWA, JWK, JWT, JWS, and JWE. Transitioning to final FIPS standards in August 2024 required rebuilding hosting environments (Debian 13, OpenSSL 3.5.2) and updating essential server/client components. TLS connections used X25519MLKEM768 certificates restricted exclusively to TLS 1.3 to prevent downgrade attacks.

In the demonstrator, QRNG output is fed via an online interface directly into the Debian 13 VM entropy pool, making quantum entropy available system-wide to the application server, database, and web proxy via standard OS random interfaces.

Conclusion for PQC in IAM

The impact of PQC on IAM must be evaluated per use case and architecture. Centralized authorization servers benefit significantly from efficient signature verification. Key generation efficiency is less critical as keys are typically generated infrequently offline. For clients, signature verification overhead and packet size increases have negligible end-user impact during login. However, servers acting simultaneously as clients face compounded overhead from combined TLS and application-layer PQC, increasing cloud infrastructure operational costs. Greater algorithm flexibility and hybrid combiners are desirable. Draft standards FIPS-206 and FIPS-207, alongside BSI recommendations for FrodoKEM and Classic McEliece, represent positive steps. While hash-based SLH-DSA is approved, its large signature sizes and slow operations make it unviable for IAM systems.

Scientific Communication and Publications

Quant-X maintained active communication through articles, presentations, posters, and conference booths throughout the project lifecycle. Engagements included annual SQuaD meetings, the National IT Security Research Conferences 2023 and 2025, Quantum Effects 2023, 2024 and 2025, the Quantum Communication Symposium Germany 2024 at PTB, poster presentations at Physics and Security 2024, a public science article on Cyberunity⁹, presentations at the 3rd International Conference on Lasers, Optics & Photonics in Edinburgh, and lectures at ING-DiBa and SAP. On March 31, 2026, the project concluded with a public online demonstration showcasing the QRNG, its IAM host integration, and quantum-secure authorization.

Supplementary Project Information

The vast majority of project funding (97%) covered personnel costs, with 1.8% allocated to travel and 1.2% to other costs (workshops, software, and hosting licenses). Work performed in Quant-ID addresses critical needs driven by quantum threat vectors like "Harvest Now, Decrypt Later" and "Trust Now, Forge Later". The chosen strategy of directly integrating PQC and QRNG into existing IAM standards (OAuth 2.0, OIDC) offers a cost-effective, low-threshold migration path that avoids dedicated quantum networks while securing critical infrastructure authentication.

Mandatory PQC roadmaps from the European Commission and NIST, coupled with migration commitments by major industry players like Google and Cloudflare, underscore the project's timeliness. Commercial momentum in Quantum Key Distribution (QKD) and QRNG security research (e.g., Gehring and Lupo) further

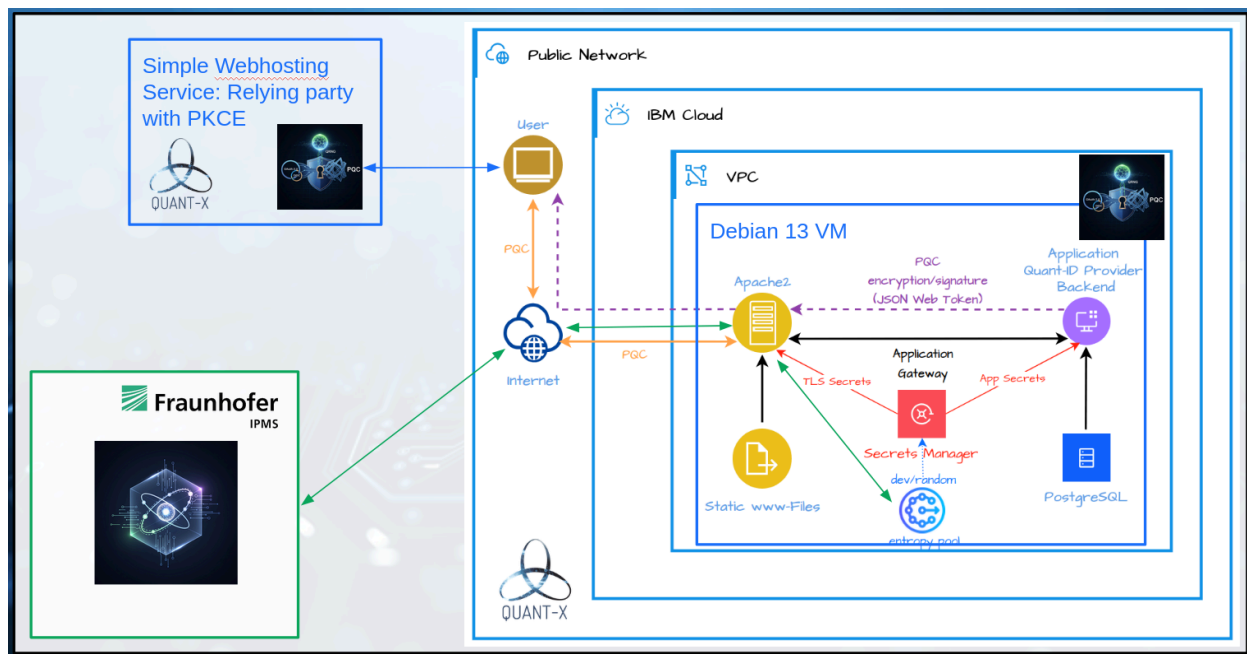
⁹ [cyberunity | quantum-proof random numbers: developments and challenges in the implementation of qrngs in modern cryptography](#)

validates our approach. Standard bodies like the OpenID Foundation actively drive PQC integration across identity protocols. Quant-X contributed significantly to specifying PQC in OAuth 2.0 and OIDC through its presentation at OSW 2026.

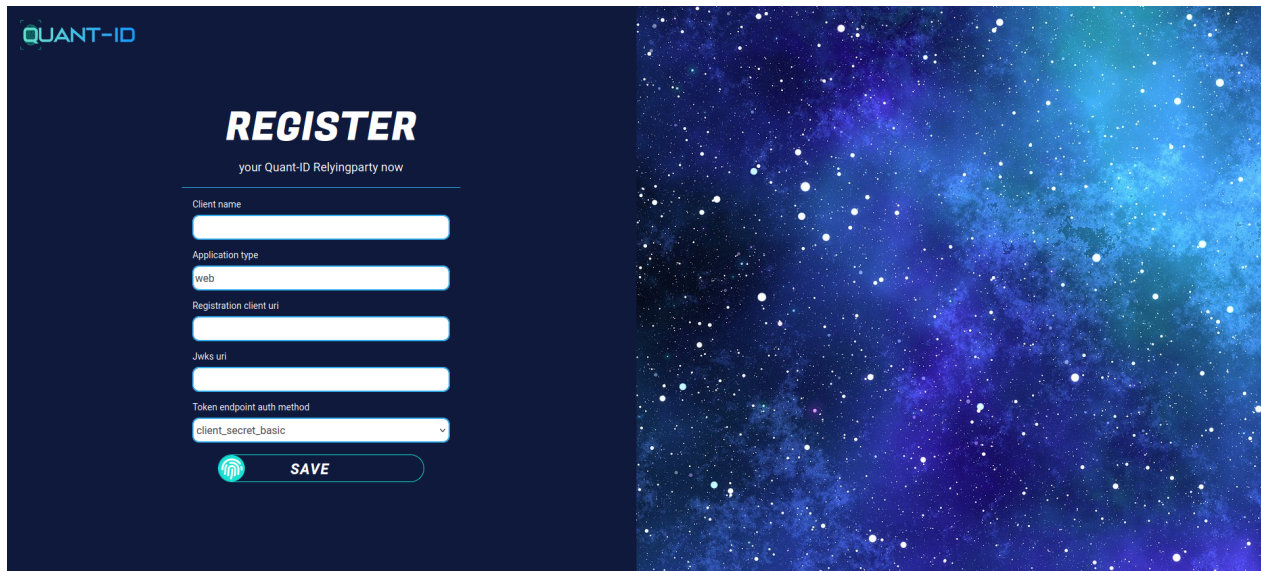
Quant-ID delivers an immediate practical benefit by providing a functional, quantum-secure end-to-end IAM solution. It equips critical infrastructure operators, financial institutions, and fintechs with a ready-to-deploy migration strategy against post-quantum decryption and forgery attacks.

Commercial and scientific exploitation of project results entered active execution following project completion on March 31, 2026. Since July 2026, Quant-X offers consultancy services leveraging expertise in PQC and quantum-secure IAM, helping clients fulfill regulatory compliance requirements. Commercial rollout of the developed authorization server as a service model is scheduled for mid-2027, with pilot evaluations currently underway alongside IAM platform vendors. Custom software development integrating quantum-secure libraries will launch in 2027. Furthermore, QRNG security proof methodologies will inform future device certification processes as standards finalize. Academic collaboration, thesis supervision, and standardization work with the OpenID Foundation continue actively following Quant-X's presentation at OSW 2026 in Leipzig.

In summary, Quant-ID provides a seamless transformation path for IAM systems into the post-quantum era. Early positioning, open-source contributions, and international standardization efforts establish a strong foundation for sustained market adoption across the DACH region from 2026 onward.



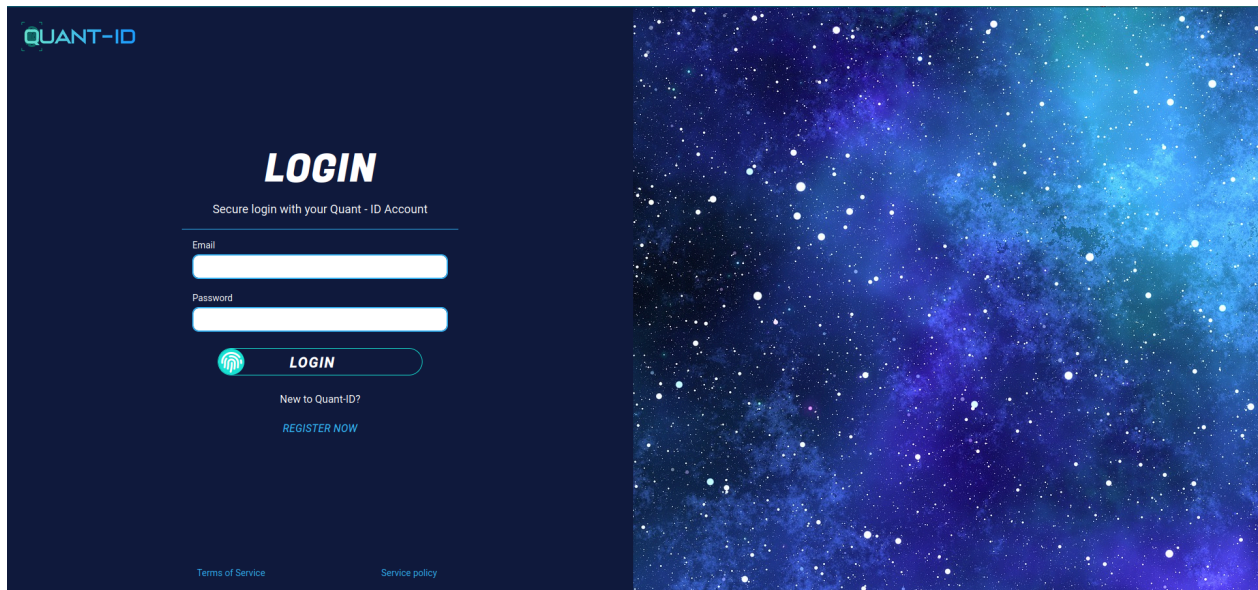
Pic. 2: Diagramm of Quant-ID Demonstrator Architecture by Quant-X Security & Coding GmbH.



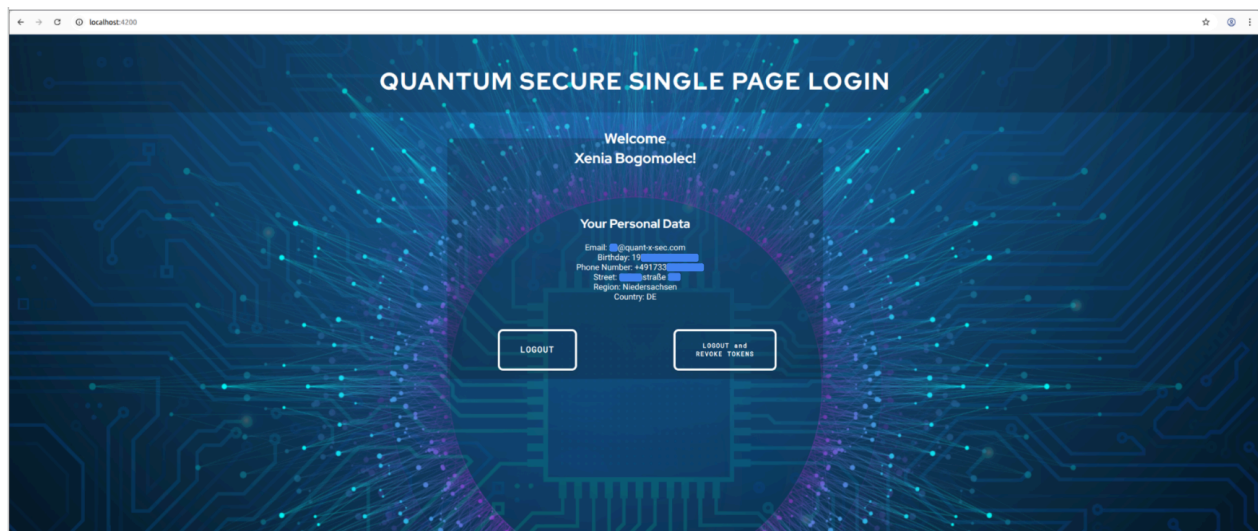
Pic. 3: Screenshot of the Quant-ID Provider Relying Party Registration Interface by Quant-X Security & Coding GmbH.



Pic. 4: Screenshot of the Relying Party Login Interface by Quant-X Security & Coding GmbH.



Pic. 5: Screenshot of the Quant-ID Provider Login Interface by Quant-X Security & Coding GmbH.



Pic. 6: Screenshot of the Relying Party Interface with user data after successful Quant-ID authorization by Quant-X Security & Coding GmbH.