

***FUTURE
PROOFING
IDENTITY
ACCESS
WITH PQC***



**ACCELERATE QUANTUM SAFE IDENTITY ACCESS & ACHIEVE
THE EU AND NIST TIMELINES FOR THE TRANSITION TO PQC**

ABOUT US



Family Owned Boutique Company (GmbH)

CEOs: Xenia Bogomolec, Alex Heß

Founded: 2019

In Hannover, Germany

Cybersecurity Consulting

Innovative Cybersecurity,
PQC,
PQC in identity access management (IAM),
Quantum-Security

RnD

Consortium lead of the successfully completed tech transfer project

QUANT-ID (funded by the BMFTR)

Partner of **QDD** (funded by the BMFTR)

OUR CUSTOMERS ARE CRITICAL INFRASTRUCTURE AND IT PROVIDERS

INNOVATION COMPETENCE

3 ½ YEARS SUCCESSFULLY COMPLETED CUTTING-EDGE RESEARCH ON QUANTUM SECURE IAM



THE QUANTUM THREAT TO IAM



Cryptographic Relevance

A quantum computer that breaks current cryptography
Identity access protocols heavily rely on cryptography
PQC is standardized since 2024, but hardly integrated in IAM

Transition Timelines for PQC

Quantum computer development is progressing continuously.
EU and NIST transition timelines for critical systems: 2030
Google even sets the timeline to 2029

Migration Risk

Classical cryptography is in use almost everywhere in IAM
Migrations to quantum-safe solutions are highly complex and can take an extremely long time
Many IAM systems are puzzled

Urgency and Warning

Data is currently being stored for future decryption
According to a BSI survey (2025), we should have begun the migration seven years ago

CUSTOMER NEEDS AND PAIN POINTS



SHORT TIMELINES - MISSING SOLUTIONS!!!

THREAT SCENARIOS



“Harvest Now, Decrypt Later” (HNDL)

Data encrypted using classical methods is being collected today in order to decrypt it later using a cryptographically relevant quantum computer.

“Trust Now, Forge Later” (TNFL)

Classically signed data can be forged with cryptographically relevant quantum computer. The integrity of a substantial volume of data must be preserved for many years—sometimes even decades.

Deploy Now, Exploit Later” (DNEL)

Devices and systems currently deployed with non-updatable classical cryptography (IoT, OT, satellites, medical devices) are becoming “insecure by design.”

THE HNDL AND TNFL SCENARIOS APPLY TO
IDENTITY ACCESS DATA

WE WANT TO INITIATE PROJECTS FOR QUANTUM SAFE IAM!



OUR OFFER

- Hands-on PQC tech transfer experience:
 - PQC / hybrid TLS
 - PQC in OAuth / OIDC
 - PQC algorithm suitability per use case
 - PQC / IAM security architecture
 - Crypto discovery (all tiers)
 - OpenSAML crypto assessments
- Hands-on QRNG integration to Linux

WE ARE LOOKING FOR

- Customers:
 - Companies that need quantum safe IAM
 - IAM providers to transition their systems
- Partners:
 - Cybersecurity companies which complement / support our expertise
 - IAM providers offering PQC secure IAM

**EXPERIENCE FROM 3 ½ YEARS CUTTING EDGE RnD (successfully completed 31.03.2026)
& SAP CRYPTO AGILITY / FIPS 140-3 PROJECTS**

SECURITY AGENCY STATEMENTS



"WE URGE PUBLIC ADMINISTRATION, CRITICAL INFRASTRUCTURE PROVIDERS, IT PROVIDERS, AS WELL AS ALL OF INDUSTRY, TO MAKE THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY A TOP PRIORITY.

FOR THE REASONS OUTLINED ABOVE, ORGANIZATIONS AND GOVERNMENTS SHOULD START THE TRANSITION NOW."

[Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography](#), a joint statement from partners from 18 EU member states 27.11.2024

***"Let's secure
the digital
future –
before
quantum
computers
arrive."***



CONTACT US:

- consulting@quant-x-sec.com
- +49 1733031816
(leave a message if we are busy)