



Secure your Infrastructure with Quantum-Resistant Cryptography

Apply Post-Quantum Cryptography today with UTIMACO Q-safe 1.0.



With the UTIMACO Q-safe firmware module running on SecurityServer, you can **apply PQC algorithms, evaluate performance, usability and quantum resistance** to your crypto infrastructure now.

Use Cases

- Document Signing
- Code Signing
- PKI
- Key Injection (in IoT)
- Hybrid Certificate

UTIMACO is proud to launch the 1st HSM firmware extension for UTIMACO's industry proven SecurityServer general purpose HSM that allows for the use of quantum safe algorithms in your IT security infrastructure.

Quantum computing will decimate the security infrastructure of the digital economy, because quantum computing is a threat to traditional cryptographic algorithms that have proven to be secure for decades in the past.

Q-Safe allows you to face the challenge with Post-Quantum Cryptography today – apply PQC algorithms, evaluate performance, usability and security today within the secure hardware boundaries of UTIMACO's SecurityServer general purpose HSMs. Starting today, Q-Safe enables you to secure your IT infrastructure by using quantum-safe crypto algorithms for digital signatures and key agreement. These algorithms are in full compliance with the ongoing NIST standardization process and recommended by BSI (Federal Office for Information Security, Germany). You can use these crypto primitives as building blocks to establish hybrid crypto schemes to prepare for the risk related to weakened non-PQC algorithms in the future.

UTIMACO provides you with:

- the tools and knowledge for a future-proof, state-of-the-art security infrastructure
- hardware backed PQC algorithm support
- PQC consultancy for the right choice of algorithms and roadmap towards quantum-safe IT security infrastructures

Product Description

UTIMACO Q-safe is a loadable firmware module for the UTIMACO SecurityServer that provides support for Post-Quantum Cryptography.

The Q-safe firmware module is an extension for your SecurityServer Se Gen2/CSe-Series and simulators and as such retro-fittable to your installed base (Minimum Requirement SecurityServer 4.31.0).



Product Features

- PQC support for the UTIMACO SecurityServer as a loadable firmware module
- Quantum computing resistant algorithms for signing/verifying, as well as key encapsulation
- based on the field-proven ISARA Radiate™ Quantum-Safe library
- PKCS#11 support by the use of "Vendor Defined Mechanisms"
- Secure backup and restore functionality – even for stateful schemes

Cryptographic Algorithms

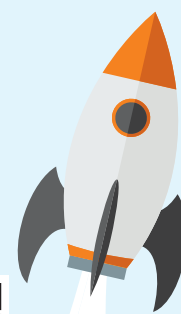
- Digital Signatures
- Dilithium
- HSS
- XMSS
- XMSSMT
- Key Agreement
- Kyber

Application Programming Interfaces (APIs)

- PKCS#11

Free Simulator

The best way to get started with PQC is to try our [free simulator](#) today.



About UTIMACO

UTIMACO is an international provider of IT security solutions with headquarters in Aachen (Germany) and Campbell, CA (USA). UTIMACO develops hardware security modules and compliance solutions for telecommunication providers in the field of regulation. UTIMACO is one of the world's leading manufacturers in both of these market segments.

Over 260 employees have committed to the company's goal to protect people, ideas and data. Customers and partners value the reliability and long-term investment security of UTIMACO's high-security products and solutions. UTIMACO stands for recognized product quality, user-friendly software, excellent support and products that effectively meet market requirements.

EMEA

UTIMACO IS GmbH

Germanusstraße 4
52080 Aachen,
Germany

+49 241 1696 200
hsm@utimaco.com

Americas

UTIMACO Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

+1 844 UTIMACO
hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

50 Raffles Place,
Level 19, Singapore Land Tower,
Singapore 048623

+65 6631 2758
hsm@utimaco.com

For more information
about UTIMACO HSM products,
please visit:

hsm.utimaco.com

© UTIMACO IS GmbH 07/20

UTIMACO® is a trademark of UTIMACO GmbH. All other named Trademarks are Trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

utimaco®