

Ready or not, here they come:

Are you prepared for the era of quantum computers?



utimaco®

www.utimaco.com



Contents

03
Introduction
The Arrival of Quantum Computers

04
Quantum Computers: Revolutionizing Computing and Challenging Cryptography

05
Why the Quantum Threat Is a Problem Now - Not Later

06
The Mosca Theorem – Consider Your Migration Time

07
The PQC Timeline - A Marathon and not a Sprint

08
How to address the Quantum Threat Strategies: PQC vs. QKD

11
The PQC Choice of Algorithms Keys, Encryption and Digital Signatures

12
Migration to Post Quantum Cryptography –The role of HSMs

13
Conclusion
Five Recommendations

14
Resources and Simulators
Technology and Partner Briefs, Free Demo Versions

utimaco®





Introduction

For cybersecurity teams everywhere, the clock is ticking. The arrival of quantum computers threatens to break today's cryptography, putting your organization's sensitive data at risk. But don't panic—Post Quantum Cryptography (PQC) offers a way out, and the time to start migration is now.

In this ebook, we'll break down the urgent need for PQC, the choice of algorithms, and how to make a successful transition before quantum computers become a reality. The future of your business depends on the actions you take today.

utimaco®

From eternity to seconds

Breaking a **2048-bit RSA** key would take 1 billion years with a classical computer.

A quantum computer could do it in **100 seconds**



Quantum Computers: Revolutionizing Computing and Challenging Cryptography

Traditional computers use bits to represent 1 or 0, while quantum computers use qubits, which can represent 1, 0, or both simultaneously through quantum superposition. This enables quantum computers to perform multiple calculations at once, making them far more efficient than traditional systems.

Modern digital security relies on symmetric and asymmetric cryptography. Symmetric methods use the same key for encryption and decryption, while asymmetric methods, like RSA and ECC, use public and private key pairs. These algorithms secure online communication through authentication, key agreement, and digital signatures.

While classical computers would take millions of years to break these methods, quantum computers, using superposition, could efficiently run algorithms like Shor's and Grover's, potentially breaking asymmetric and weakening symmetric cryptographic systems.

utimaco®



Q-Day in 20…30?

The German Federal Office for Information Security acts on the hypothesis that a cryptographically relevant quantum computers will be available in the early **2030s**.



Why the Quantum Threat Is a Problem Now - Not Later

You might think, “There’s no quantum computer powerful enough to break cryptography today, so why should I care now?” Well… here are two answers:

- **Harvest Now, Decrypt Later**

  Attackers could intercept and store encrypted data today, only to decrypt it once a quantum computer capable of breaking encryption becomes available.

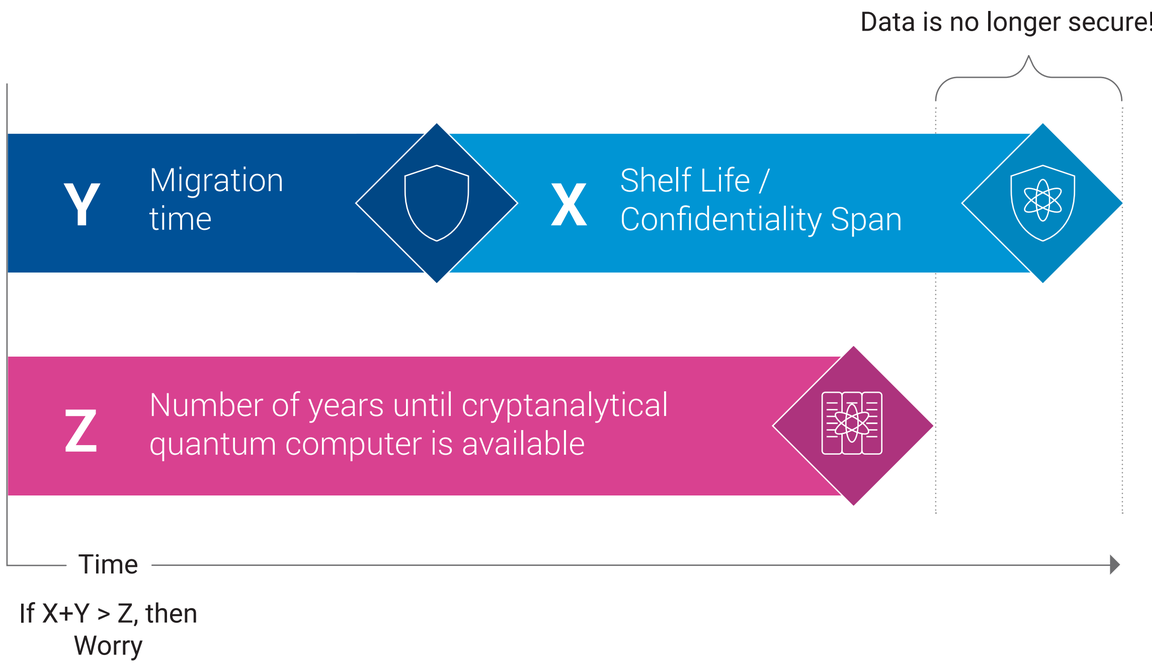
- **Breaking Digital Signatures**

  Attackers could reverse-engineer credentials from public information - even retrospectively. This could lead to an attacker approving fraudulent requests, signing documents, or issuing counterfeit firmware.

utimaco®



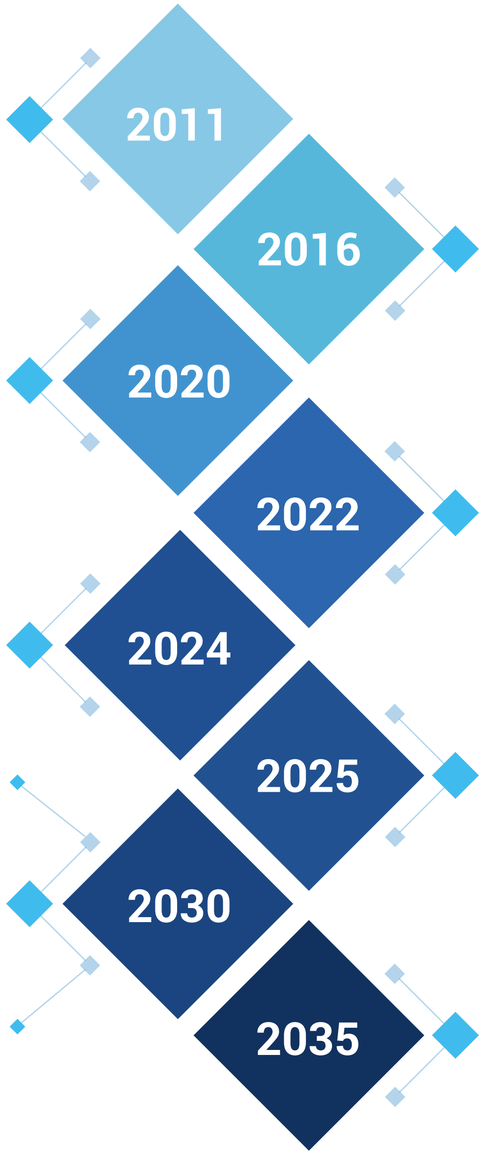
The Mosca Theorem – Consider Your Migration Time



If X+Y > Z, then Worry

utimaco®

The PQC Timeline – A Marathon and not a Sprint



2011
First commercial quantum computer released

2016
NIST announces its PQC standardization efforts

2020
NIST recommends stateful hash-based signature schemes for quantum-security

2022
NSA published CNSA 2.0 including: LMS, XMSS, ML-KEM, ML-DSA, AES, SHA

2024
PQC standards released:
- FIPS-203: ML-KEM
- FIPS-204: ML-DSA
- FIPS-205: SLH-DSA

2025
CNSA 2.0 to be used by default and preferred for first use cases

2030
Exclusive use of CNSA 2.0 for certain use cases

Q-Day: Industry expectance that a cryptanalytical-relevant quantum computer will be available

2035
NIST IR 8547: First algorithms deprecated

NIST IR 8547: Common public key algorithms disallowed

utimaco®

Hybrid cryptography is the use of both classical and post quantum cryptography. Since PQC algorithms are not (yet) that mature regarding implementation and practical experience, we recommend hybrid cryptography for most use cases.

How to address the Quantum Threat – Strategies

Post Quantum Cryptography (PQC)

Post Quantum Cryptography refers to cryptographic algorithms relying on "hard mathematical problems" that are believed to be resistant to quantum attacks. Since public key cryptography is particularly vulnerable, PQC algorithms primarily focus on use cases like key agreement and digital signatures.

Building trust and achieving maturity in these algorithms is a key challenge. To address this, the U.S. National Institute of Standards and Technology (NIST) is leading a PQC Standardization Process. As of now, three algorithms have achieved standardization:

- ML-KEM (FIPS-203)
- ML-DSA (FIPS-204)
- SLH-DSA (FIPS-205)





Quantum Key Distribution (QKD)

Quantum Key Distribution is a technique for securely exchanging keys using quantum mechanics.

The unique advantage of QKD lies in its “built-in eavesdropping detection.” By utilizing entangled quantum states, any interception attempt is immediately detectable, making the compromised key invalid.

Unlike traditional methods, QKD’s security does not depend on the computational difficulty of mathematical problems, making it resistant to attacks by both classical and quantum computers. For this reason, QKD is often promoted as a secure alternative to post-quantum cryptography.

utimaco®



PQC vs. QKD – What's the best approach?

While both PQC and QKD have their strengths, PQC currently stands out as the more practical and reliable option. PQC serves as an all-around solution designed to replace quantum-vulnerable cryptography in systems we already use today. The algorithms have been rigorously tested through an open standardization process led by NIST, ensuring they are ready for real-world deployment.

QKD has a much narrower scope, focusing solely on key distribution and has other limitations to consider:

- Solutions have not been evaluated in a formal standardization process
- It is not yet 100%-proven to be secure
- It has distance limitations
- Requires significant infrastructure investments

While research into improving QKD is ongoing, most experts agree that it is not yet mature enough to meet today's security needs. So, for now, PQC is the safer bet.

utimaco®

The PQC Choice of Algorithms

Key Encapsulation / Encryption

Algorithm	Method	Status	Recommendation
ML-KEM	Lattice-based	NIST Standard published: FIPS-203	ML-KEM-1024 for all classification levels
HQC	Code-based	NIST Selected Algorithm to be Standardized	N/A
Classic McEliece	Code-based	NIST PQC Standardization Round 4	N/A
Bike	Code-based	NIST PQC Standardization Round 4	N/A
Frodo-KEM	Lattice-based	Not standardized Recommended by German Federal Office for Information Security	N/A

Digital Signatures

Algorithm	Method	Status	Recommendation
ML-DSA	Lattice-based	NIST Standard published: FIPS-204	ML-DSA-87 for all classification levels
SLH-DSA	Hash-based	NIST Standard published: FIPS-205	N/A
FALCON	Lattice-based	NIST Selected Algorithm to be standardized	N/A
LMS / HSS	Stateful Hash-based	Standardized NIST SP 800-208	All parameters approved for all classification levels. LMS SHA256/192 is recommended
XMSS / XMSS-MT	Stateful Hash-based	Standardized NIST SP 800-208	All parameters approved for all classification levels
SHA family	Hash function	Standardized FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels

utimaco®

u.trust General Purpose HSM Se-Series





ML-KEM

XMSS

ML-DSA

LMS

Migration to Post Quantum Cryptography – The role of HSMs

Transitioning to PQC is vital, but protecting cryptographic keys during the process is equally critical. Even with PQC algorithms, unprotected keys - whether stored in applications, the cloud, or software – pose a security threat.

Hardware Security Modules (HSMs) provide a tamper-resistant, secure environment for cryptographic keys. These trusted physical devices generate, manage, and store keys, supporting encryption, digital signatures, and authentication for applications, identities, and databases.

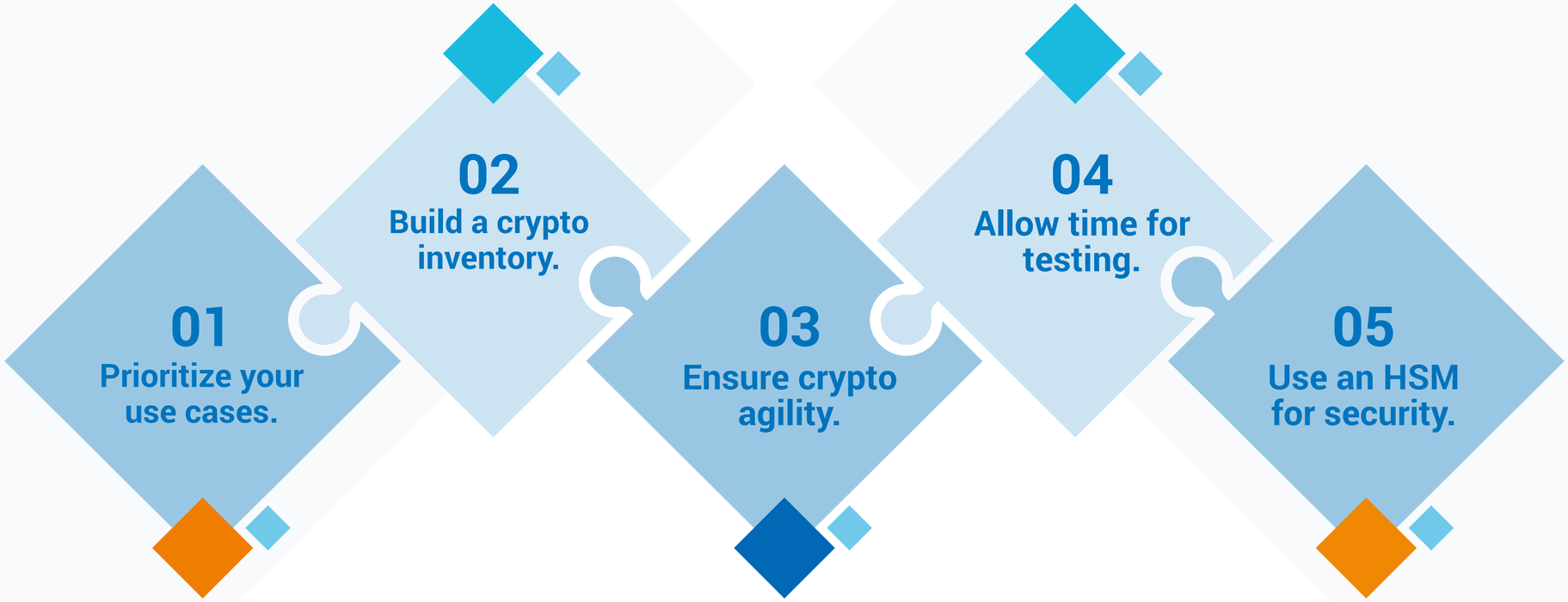
To be prepared for the quantum era, your HSM should be crypto-agile - meaning that it can adapt to new cryptographic developments. Utimaco's u.trust General Purpose HSMs are designed with crypto agility in mind and can be upgraded with PQC algorithms already today. With Utimaco, you ensure both high-security key management and readiness for PQC.

utimaco®

Conclusion - Don’t fall into PQC Paralysis

The time to prepare for the quantum era is now. While the implementation of PQC is individual to each organization and use case, here are five general recommendations to follow:

Stay crypto agile and start your migration today. Utimaco can help you with both.



utimaco®



Resources & Simulators

Quantum Protect Simulator

Quantum Protect Technology Brief

Crypto Discovery:
Joint Solution Brief InfoSec Global

GP HSM Simulator

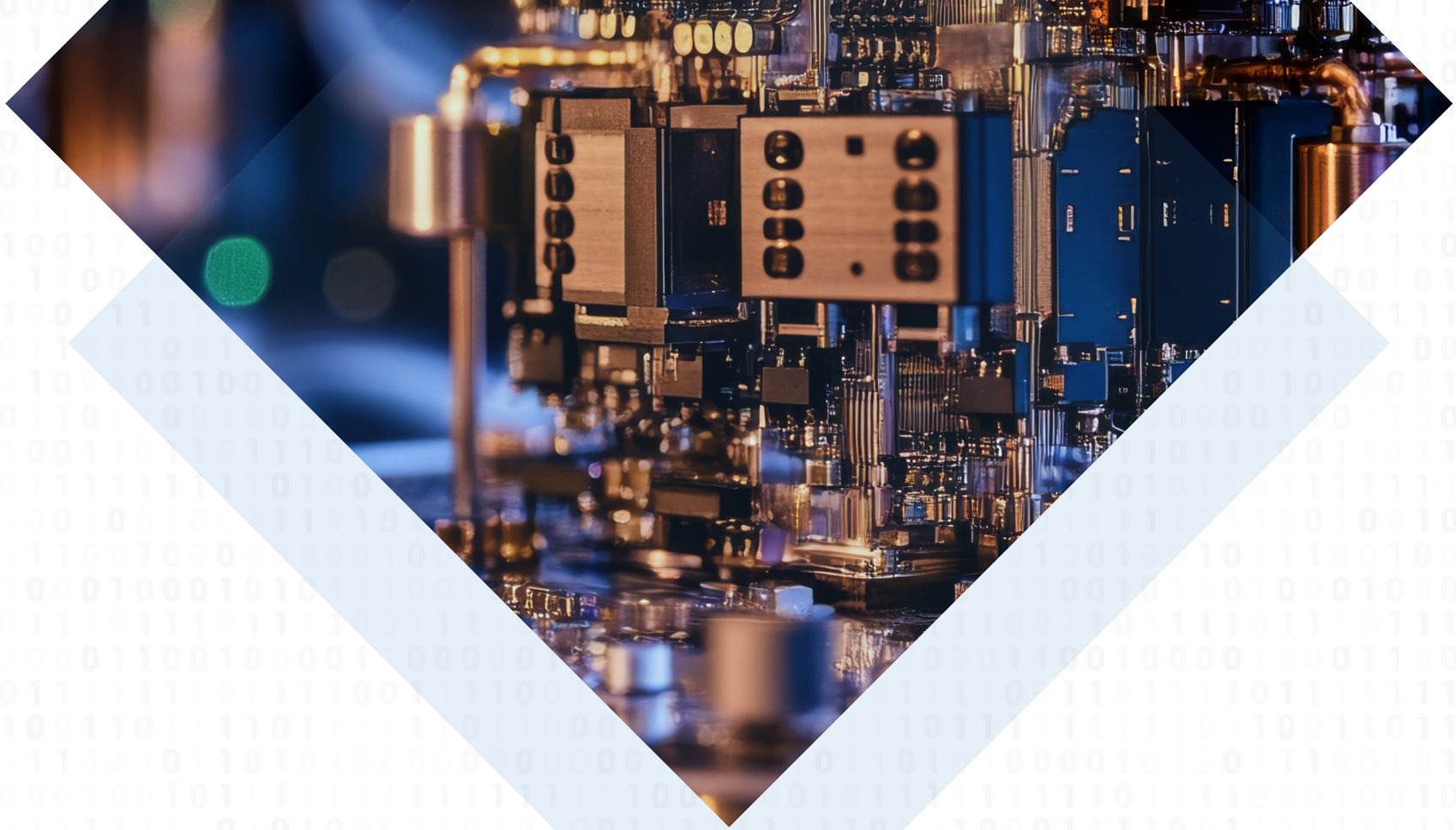
u.trust General Purpose
HSM Se-Series Datasheet

Frost & Sullivan Report

utimaco®

Contact Us

info@utimaco.com
+49 (0) 2411696-0
utimaco.com



Imprint
Author/Publisher: Utimaco Management Services GmbH
Address: Germanusstrasse 4, 52070 Aachen, Germany
Contact: info@utimaco.com
VAT ID: DE347442338

Copyright Notice
© 2025 Utimaco Management Services GmbH. All rights reserved. This eBook is protected by copyright law. No part of this publication may be copied, reproduced, distributed, or transmitted in any form or by any means without the prior written permission of the author or publisher, except for brief quotations in reviews. Unauthorized use may result in legal consequences.

Disclaimer
The contents of this eBook are for informational purposes only. While every effort has been made to ensure accuracy, the author assumes no responsibility for errors or omissions. The information is provided "as is" without any express or implied warranties. If this eBook contains legal, medical, financial, or other professional advice, it should not be considered a substitute for consultation with a qualified professional.

Privacy Policy
This eBook does not collect personal data. However, if links to external websites are provided, the author is not responsible for the privacy policies or content of those third-party sites. Please refer to their respective privacy policies for more details.

Sources & Image Credits
If this eBook includes third-party content, proper attribution is given. Images used in this eBook are either owned by the author, licensed, or used under appropriate Creative Commons licenses.

Usage Rights & Licensing
This eBook is for personal use only. It may not be resold, redistributed, or modified without permission. If you have received this eBook from an unauthorized source, please contact the author.

utimaco®

© Copyright 2025