Charter of Trust

Our Post-Quantum Cryptography Ambition

Allianz · Atos · BOSCH · Danfoss

elastic · IBM · Infineon · Microsoft

MITSUBISHI HEAVY INDUSTRIES · SIEMENS · TÜV SÜD · zscaler

Charter of Trust

A Quantum Leap for Cybersecurity

The Urgency of Post-Quantum Encryption

The digital era is accelerating at an unprecedented pace. With AI shaping decisions, massive data flows powering innovation, and billions of devices connected, the foundations of our global economy and society are being transformed.

But just as these technological advances promise immense benefits, they also expose us to new and more complex risks. Cyberattacks are no longer limited to conventional digital systems, they now threaten critical infrastructure, healthcare, transportation, and the integrity of democratic institutions. Moreover, the advent of quantum computing adds another layer of risk that must be carefully addressed.

Quantum computers might eventually be able to break many of the cryptographic systems that currently protect our digital world. This looming shift poses a significant threat to long-term data confidentiality and digital trust. What's secure today may become vulnerable tomorrow.

While the EU's aspiration for a full quantum transition by 2035 is in line with global efforts it's important to acknowledge that the path to quantum readiness will vary significantly across sectors and criticality of infrastructures within respective environments. The ongoing discussions among Partners of the Charter of Trust highlight the value of a flexible, context-aware approach.

That's why the Charter of Trust has established a dedicated working group to explore, discuss, and raise awareness around Post-Quantum Cryptography (PQC), **with the goal of facilitating a coordinated and efficient transition when the time is right**.

Cybersecurity must evolve in step with the technologies it protects. It is not simply a technical feature; it is the foundation of trust in a digital society. And that trust must be preserved as we look ahead to the quantum era. **We aim to facilitate an efficient and well-informed transition, not by pushing premature change, but by supporting a concerted, thoughtful approach grounded in cybersecurity principles**.

Transitioning to quantum-resistant cryptography is not a task for any one organization alone. It requires broad collaboration across industries, governments, academia, and technology providers. **The Charter of Trust, together with its network of companies and experts help to shape this transformation responsibly**.

In alignment with our core mission, to build trust in a secure digital world, we support a proactive, well-coordinated, and risk-driven PQC transition. This includes:

- Raising awareness about quantum risks to current cryptography,
- Promoting standards-based approaches to PQC migration,
- Supporting interoperability and scalable solutions, and
- Encouraging public-private partnerships to accelerate readiness.

This document marks the beginning of our collective effort. It presents the PQC ambition of the Charter of Trust working group and sets the stage for continued dialogue, alignment, and strategic direction. As this working group continues its efforts, we will share further insights, guidance, and collaborative opportunities. Stay tuned, there is much more to come as we work together to secure the digital future in the quantum era.

Our PQC Ambition

1. Facilitating an Efficient and Secure PQC Transition

- **Promote Early Planning and Thoughtful Adoption**
  Advocate for and support a well-timed, priority-driven transition to quantum-resistant cryptographic algorithms across industries to safeguard long-term data confidentiality and system integrity in an efficient manner.

- **Strengthen Supply Chain Readiness**
  Promote quantum awareness among suppliers, integrators, and partners throughout the value chain and support coordinated implementation of PQC solutions.

- **Foster Cryptographic Agility**
  Encourage the adoption of agile cryptographic architectures that enable smooth transitions of algorithms as standards evolve, and threats emerge.

---

2. Advancing Technical Foundations for Quantum-Safe Security

- **Drive Standardization and Interoperability**
  Support and contribute to international standardization efforts (e.g., NIST, ETSI, ISO), advocating for secure, robust, and widely adoptable PQC algorithms and protocols.

- **Advance Quantum-Safe Digital Signatures**
  Promote research, testing, and deployment of quantum-resistant signature schemes to safeguard software, firmware, and communications, vital for securing digital identities and supply chains.

- **Develop Migration Pathways for Legacy Systems**
  Provide practical guidance for assessing existing cryptographic infrastructure and designing phased, low-risk migration plans tailored to diverse operational needs.

- **Champion Ethical Innovation and Inclusivity**
  Ensure that the development and deployment of PQC technologies align with ethical standards, privacy rights, and inclusive access to secure digital infrastructure.

- **Facilitate Early Adoption of Quantum-Safe Key Exchange**
  Encourage rapid deployment of post-quantum hybrid key exchange mechanisms to reduce exposure to “harvest now, decrypt later” risks and strengthen forward secrecy during the transition period.

---

3. Fostering Awareness and Collaboration Across Sectors

- **Raise Global Awareness of Quantum Threats**
  Lead education and outreach efforts to inform stakeholders, from executives and policymakers to engineers and IT professionals, about the urgency of PQC readiness, including the long-term risks of “harvest now, decrypt later” scenarios.

- **Facilitate Cross-Sector Collaboration and Knowledge Sharing**
  Establish a trustworthy, cross-industry forum for sharing research, implementation experiences, threat intelligence, and technical best practices related to PQC.

- **Encourage Government Engagement and Policy Alignment**
  Engage with governments, regulators, and public institutions to help shape coherent policy frameworks that support PQC adoption while ensuring accountability, transparency, and trust in the digital ecosystem.

Learn more on: www.charteroftrust.com

Follow us on LinkedIn: