PQSHIELD

think openly, build securely.

Our expertise, clarity and care have enabled us to deliver new global standards alongside real-world, **post-quantum** hardware and software upgrades – modernizing the vital security systems and components of the world's technology supply chain.

Hardware IP

Modular hardware IP delivering **quantum-resistant security**, co-processing and side channel protection.

Software IP

FIPS 140-3 ready modular cryptographic libraries, APIs and SDKs for **quantum-safe** and hybrid transition.

Research IP

Setting the standards at NIST, RISC-V, IETF, World Economic Forum and many more platforms beyond. **19+ Patents**.

The Quantum Threat

It's no secret that quantum computing will soon have the power to break traditional cryptographic methods, and it is important to be ready for the impact.

Post-Quantum Cryptography (PQC) is a field of new algorithms that use advanced mathematical techniques to protect against quantum computers. In every single industry, the cryptography that keeps data, devices, connections, and components secure, needs to be modernized in order to align with new international PQC standards coming into effect in 2024.

PQShield is here to help. We're world leaders when it comes to these new PQC standards, and our team works to help organizations throughout the technology supply chain. We're a leading provider of PQC solutions, and we believe that by thinking openly and building securely, we can collectively drive the world towards quantum resilience.

For more on the Quantum Threat

See our comprehensive and acclaimed publications at **pqshield.com/publications**

Risk Assessment and Solution Design

Manufactured products often include hardware components that are built to last. However, those products can also include cryptography that could soon be obsolete.

This leaves systems vulnerable to attackers who could store or disperse data for more rapid decryption in the future. Additionally, products with long shelf-lives will be less protected in the years to come.

Our team is here to help. We've led multiple projects for the likes of RISC-V, and we've worked alongside many bodies contributing to the global PQC standards, including IETF, ETSI, GlobalPlatform, WEF, GSMA and the NCCoE. We lead the field on Side Channel Attack Resistance (SCA) and Hybrid FIPS 140-3 certification, as well as Advanced Protocols, with over 19 patents now in process. We make sure your security upgrade is done smoothly and professionally.

Discuss

Our team takes pride in being a voice of reason in a world of hype and jargon. We're here to guide you through every step of the way.

Evaluate

It's critical to know where your cryptography is at risk. We help evaluate existing infrastructure, determining the risk and agility of the underlying architecture.

Design

We can help design an end-to-end solution that is secure, quantum-resilient, and compliant with the international NIST standards.

Implement

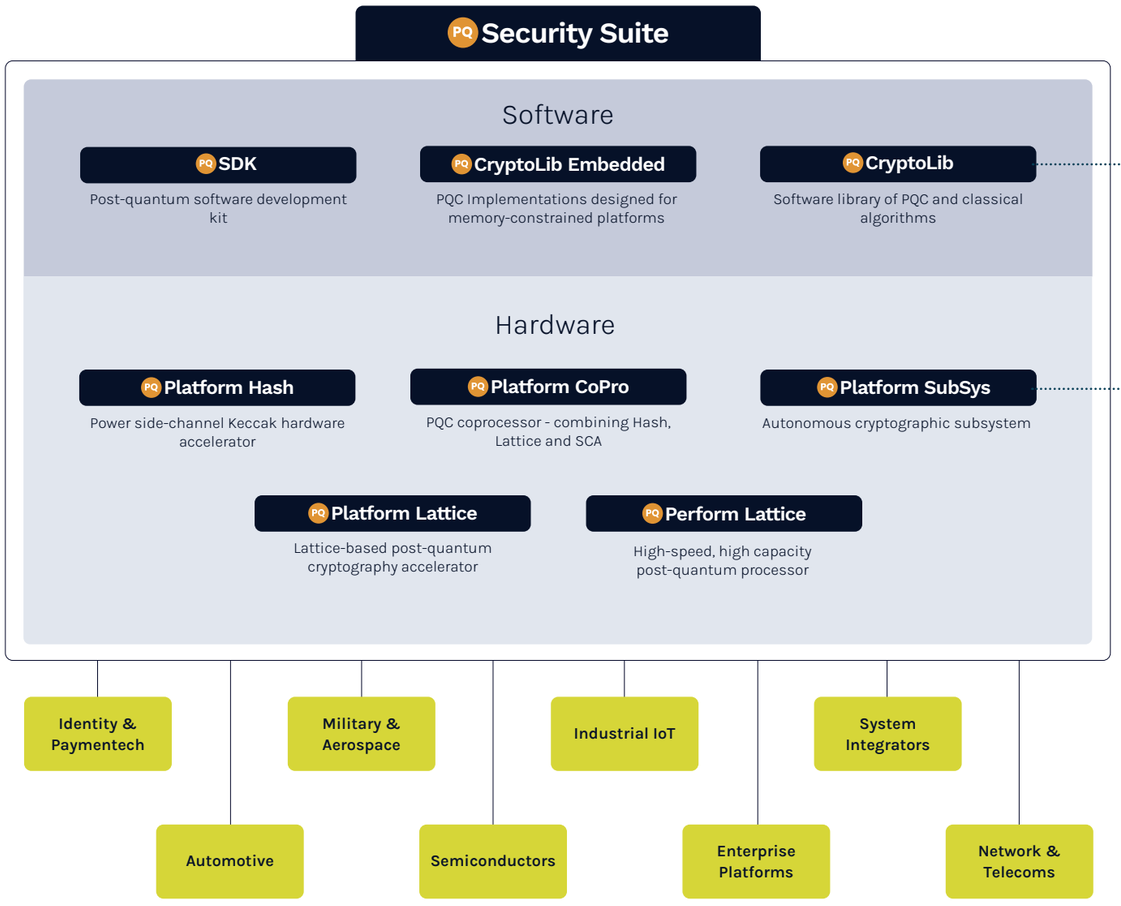
The PQShield team have the resources, experience and expertise to work alongside or as part of your wider team, securely deploying entire end-to-end solutions.

Shaping the way our digital world is protected today, against the threats of tomorrow.

Mature PQShield Security Suite

Our expertise, clarity and care have enabled us to deliver new global standards alongside real-world, post-quantum hardware and software upgrades – modernizing the vital security systems and components of the world's technology supply chain.

Our products are already being used by internationally-recognised organizations, industries and governments, and we're constantly researching and developing new ways to apply the very latest post-quantum technology to real-world systems and solutions.

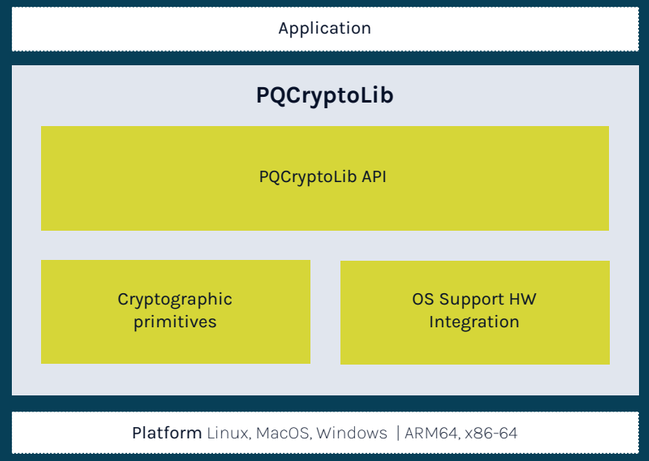


Example **FIPS 140-3 Ready Software IP**

PQ CryptoLib

Our hybrid cryptographic library, PQCryptoLib, consists of a library of modern cryptographic primitives designed with crypto-agility in mind to help companies transition smoothly and securely to the quantum-era.

It provides support for classical and hybrid key derivation, and for implementation within the TLS key schedule, supporting multiple PQC and classical algorithms.

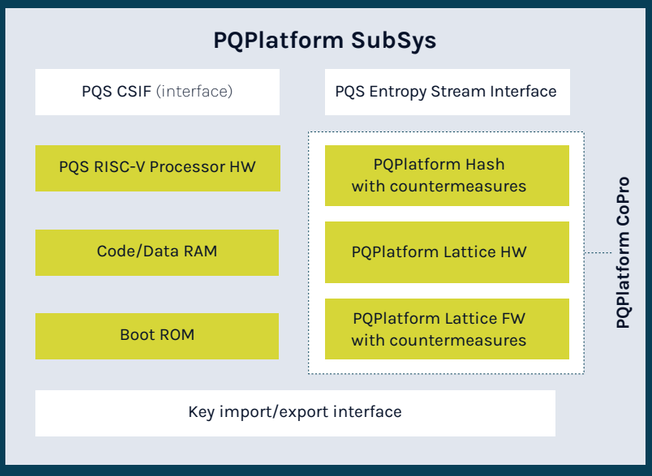


Example **Post-Quantum Hardware IP**

PQ Platform SubSys

PQPlatform SubSys is a cryptographic sub-system, designed to provide cryptographic services, including both post-quantum and classical signature generation, verification, and secure key establishment.

PQPlatform SubSys uses its built-in CPU to run autonomously from the surrounding system, allowing cryptographic services to be offloaded efficiently from the system processor.



PQShield's Expertise

The PQShield team is helping to shape the way our digital world is protected against the threats of tomorrow. At a time when quantum computers will soon be able to break current cryptography methods, we're focused on empowering organizations, industries, and nations, with the ultimate quantum-resistant cryptography solutions.

PQShield began as a spin-out from the University of Oxford, but now with a team of over 60 experts in Europe, Japan, the US, and the UK, PQShield is the largest commercial assembly of specialist PQC cryptographers anywhere in the world.

We are a source of truth for stakeholders at every level, and we're seen by both customers and competitors as a leading provider of PQC solutions in hardware and software.

Our think openly, build securely ethos has helped us deliver high-security quantum-safe cryptography, modernizing the vital security systems and components of the world's technology supply chain. Our PQC-ready products are already being used by the likes of Microchip, AMD, Mirise Technologies, Digicert, Unisys, Lockheed Martin, and many more.

PQShield's mission is to build products and solutions that help modernize the legacy cryptography in the world's technology supply chain, to deliver new global standards alongside real-world hardware and software upgrades, and to keep the world one step ahead of the attackers.

PQ SHIELD

Start a conversation today!
pqshield.com/contact us