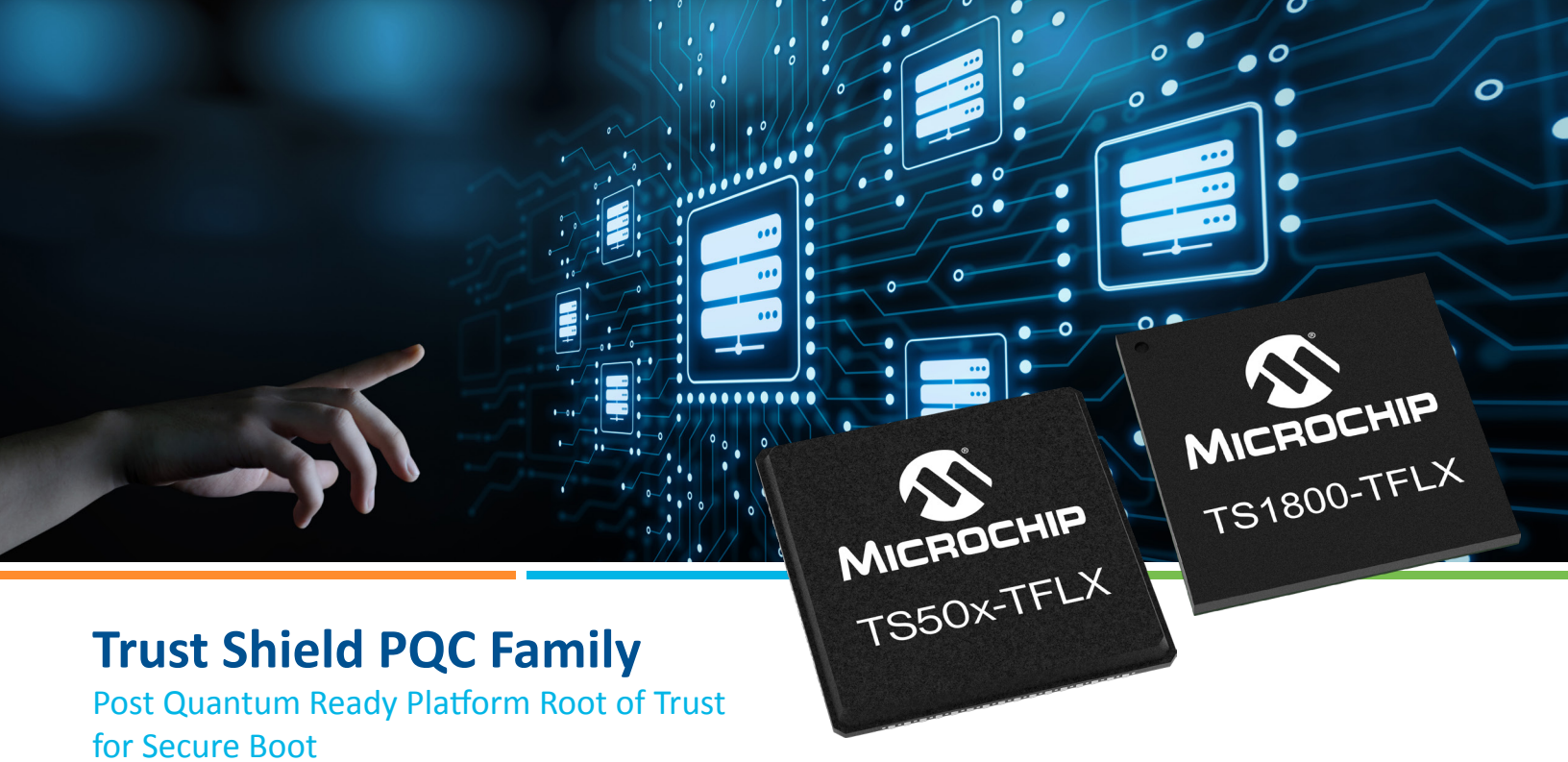

Trust Shield PQC Family

Post Quantum Ready Platform Root of Trust for Secure Boot

Future Ready Platform Security Starts in Hardware

As the industry prepares for the transition to Post Quantum Cryptography (PQC), system trust must be anchored in hardware and designed to evolve with emerging standards. The Microchip Trust Shield PQC Family delivers hardware based security solutions that protect firmware, establish a resilient chain of trust and align with modern platform security requirements.

Designed for data center, compute, defense, telecommunications and infrastructure systems, Trust Shield combines post quantum and classical cryptography, standards aligned resiliency, and scalable options—from full platform root of trust controllers to cost optimized root of trust Integrated Circuits (ICs).

Trust Shield PQC Family

TS1800 TrustFLEX — Platform Root of Trust

The TS1800 TrustFLEX—Platform Root of Trust includes the following features:

- High end external platform root of trust for complex, multi component systems
- Hybrid post quantum and classical cryptography
- Designed to meet NIST SP 800 193 and Open Compute Project (OCP) requirements
- High performance Arm® Cortex® M4F up to 192 MHz
- USB 2.0 for fast firmware updates
- Multi channel QSPI/SPI support
- Built in secure boot, secure updates, rollback protection, crisis recovery and lifecycle management

TS500 and TS501 TrustFLEX — Root of Trust ICs

The TS500 and TS501 TrustFLEX—Root of Trust ICs provide the following capabilities:

- Hardware based secure boot with post quantum ready authentication
- Inline between System on Chip (SoC) and Serial Peripheral Interface (SPI) Flash, holding the system in reset until verification succeeds
- Options for hybrid PQC and classical cryptography for secure boot migration
- Designed to support NIST SP 800 193 Platform Firmware Resiliency
- **TS500:** Firmware stored in external SPI flash
- **TS501:** Integrated internal SPI Flash for simplified designs
- Compatible with x86 and Arm® based systems

Designed for the Transition to PQC

The Trust Shield PQC Family helps system architects prepare for evolving security threats by combining hardware anchored trust, hybrid cryptography and standards aligned security to reduce risk and accelerate adoption across the platform lifecycle.

Learn More About the Trust Shield PQC Family

For more detailed information, including security features, compliance support, and target applications, visit https://www.microchip.com/en-us/products/security/prot

DS00006456A