OmniTrust

DATA SHEET

FLEXCC

Fully integrated security solution designed for modern MCUs

KEY BENEFITS

- **Full crypto portfolio** in one module (AES/SHA/RSA/ECC + ML-KEM/ML-DSA + LMS)
- **FIPS 140-3 certifiable design** with KATs for every algorithm
- **MISRA C:2023 & CERT C compliant** deterministic code
- **CPU + FPGA portability** (ARM/RISCV/x86 + Xilinx UltraScale+)
- **Open-source C, proprietary optimized C, and HDL** implementations
- **Designed for long-life devices** in regulated and safety-critical environments

The ISS FlexCC next-generation cryptographic core is a unified suite of conventional FIPS-aligned algorithms and NIST PQC finalists.

It is built for embedded and connected devices that must remain secure for decades across automotive, industrial, medical, aerospace, defense, and semiconductor environments. FlexCC delivers portable, certifiable, and quantum-ready cryptography with C and HDL implementations optimized for size, performance, and long-term maintainability.

AGING CRYPTO & NEW REQUIREMENTS CREATE RISK

Modern devices are deployed everywhere, and for longer than ever. This creates challenges:

- **Long product lifecycles (10–30+ years):** Legacy crypto libraries break, lose support, or fall behind compliance.
- **PQC transition deadlines are imminent:** Global regulators and OEM programs require adoption of ML-KEM / ML-DSA before 2030.
- **Resource-constrained devices need verified, deterministic crypto:** Safety-critical systems require MISRA/CERT C code quality, predictable execution, and auditability.
- **Multi-architecture supply chains need portable, certifiable primitives:** Automotive (R155), medical (FDA 524B), industrial (62443), and defense programs demand verifiable crypto behavior.

FlexCC solves these problems with a unified, maintainable, forward-compatible cryptographic engine.

Core Capabilities at a Glance

CONVENTIONAL CRYPTOGRAPHY (FIPS-ALIGNED)

- AES-128/192/256 (SP800-38A/B/C/D/E/F)
- SHA-2, SHA-3, SHAKE (FIPS 180-4, FIPS 202)
- RSA 2048/3072/4096 (PKCS#1 v1.5 / PSS – RFC 8017)
- DSA 2048/3072/4096
- ECDSA on NIST prime, binary, Edwards (25519/448) & Brainpool curves
- HMAC (FIPS 198-1) | ECIES (SEC1 v1.9) | RSA-OAEP
- SP800-90A DRBG, SP800-108 KDF
- Big-number math (add, multiply, divide, mod, inverse, compare)

POST-QUANTUM CRYPTOGRAPHY (PQC)

- **ML-KEM (Kyber family):** 512 / 768 / 1024
- **ML-DSA (Dilithium family):** 44 / 65 / 87
- **Stateful LMS:** SHA-256, SHA-256/192, SHAKE256/256, SHAKE256/192
- **SHA-3 / SHAKE XOF primitives**
- **TRNG (HDL):** Designed for FIPS 140-2/3 entropy requirements

IMPLEMENTATION OPTIONS

1. Open-source C implementation

- Full algorithm support
- Portable across CPUs
- Proven UltraScale+ port (ML-KEM benchmarked on ARM Cortex-M4)

2. Proprietary optimized C

- Tuned for constrained embedded targets
- Deterministic execution and reduced footprint
- Ideal for safety-critical and regulated devices

3. FPGA-agnostic HDL

- Vendor-neutral design
- Compiles on any FPGA
- Meets ≥150 MHz clock targets
- First FIPS 140-3 target: Xilinx UltraScale+

INDUSTRIES WHERE FLEXCC IS USED

Automotive: ECU secure boot, OTA, diagnostics, EV/charging, V2X, PQC transition

Industrial & IoT: PLC/RTUs, gateways, SCADA, energy systems

Medical: Implantables, pumps, clinical devices (FDA cybersecurity)

Aerospace & Defense: Mission-critical, certifiable crypto, supply-chain trust

Semiconductors: SoC RoT, secure boot, FPGA crypto IP

ASSURANCE, COMPLIANCE & TESTING

FIPS 140-3 readiness

- Known Answer Tests (KATs) for all algorithms
- CAVP test suite compliant
- PQC designs planned for full module validation

Code quality

- 100% function / branch / statement / condition coverage
- MISRA C:2023 "Mandatory" + "Required"
- SEI CERT C & ISO/IEC TS 17961 alignment
- Cyclomatic complexity controls

HDL criteria

- ≥150 MHz designs
- Customer-targeted area optimization
- TRNG suitable for certified key generation flows

Deliverables

- C or HDL source code
- API guide with function descriptions & error handling
- MISRA/CERT C analysis report
- FIPS KAT vectors
- Optional timing/performance report ("made to order")
- Integration support for FlexHSM, FlexTLS, FlexBoot, FlexOTA, FlexDB/CertDB

Part of the OmniTrust Device Lifecycle Management (DLM) system

OmniTrust brings 30+ years of embedded security leadership, securing billions of devices across automotive, industrial, medical, aerospace, and semiconductor markets. FlexCC extends this pedigree with a next-generation cryptographic engine designed for longevity, certification, and future-proof security.

ABOUT OMNITRUST

OmniTrust (formerly INTEGRITY Security Services) secures the connected world — from silicon to cloud systems and AI — by delivering verifiable, enforceable trust across the entire device and software lifecycle. As the leader in Trust Lifecycle Management, OmniTrust ensures security from design and provisioning through operation, update and retirement, protecting more than 2 billion devices and 3 billion software updates per year. OmniTrust enables full-lifecycle security across the chain of trust for companies in the automotive, aerospace and defense, finance, healthcare and other safety-critical, regulated sectors.

omnitrust.com

OmniTrust