OmniTrust

DATA SHEET

FLEXHSM

Fully integrated security solution designed for modern MCUs

COMPLETE SECURITY

FlexHSM provides complete platform security solutions for all current security specifications:

- **AUTOSAR 4.3, 4.2, 4.x**
- **SHE 1.1, 1.0 integration**
- **EVITA**
- **MISRA 2014 compliance**
- **C2X/V2X verification**
- **Other automotive requirements**

FlexHSM is available for most multi-core/ multi-function processors available on the market, including:

- **NXP**
- **Infineon**
- **Renesas**
- **AMD**
- **Texas Instruments**
- **Intel**
- **Qualcomm**

The cryptographic algorithms in FlexHSM are the same implementation as our FIPS 140-2 Certified (NIST #1719 & #2290) and FIPS 140-3 level 1 cryptographic software.

THE OMNITRUST FLEX FAMILY

Today's connected products — from advanced automotive platforms to industrial and consumer devices — demand end-to-end lifecycle security. Increasing complexity in hardware and software supply chains makes this difficult to achieve without a robust, built-in solution.

The OminTrust Flex family delivers exactly that. By embedding cryptographic libraries, protocol stacks, and lifecycle management into devices from the start, the Flex solution makes products **secure by default**.

OMNITRUST FLEXHSM

The rapid development of complex computing systems using advanced internal networking, interfaces to WIFI/LTE/5G external networks, and remote software updates have significantly increased the surface area for attackers to exploit. As a result, the security and integrity of embedded systems have become a top priority for OEMs.

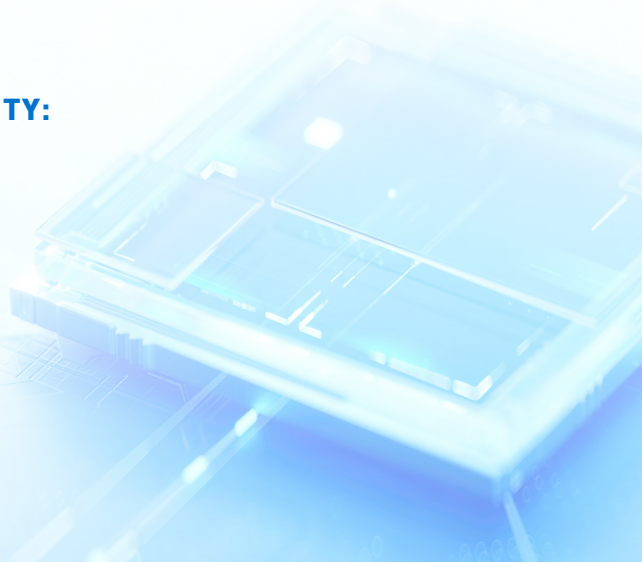
FlexHSM is a fully integrated security solution designed specifically for modern microcontroller units (MCUs).

FlexHSM is compatible with all modern 32-bit/64-bit processors including ARM® and Power Architecture® and is completely agnostic to any operating system and hypervisor type applications. OmniTrust integrates FlexHSM to your specific target processor to meet or exceed embedded security requirements in rapid development timeframes.

OmniTrust FlexHSM will ensure your products stay secure.

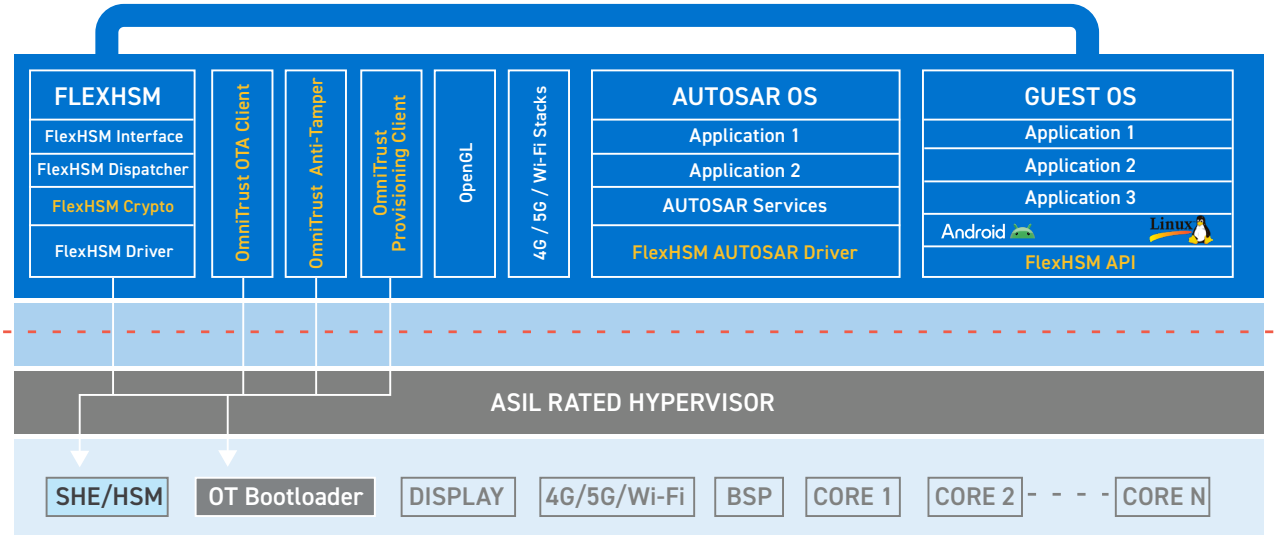
FLEXHSM CAPABILITIES DELIVERING THE HIGHEST SECURITY:

- → Separation controller
- → Configurable presentation layers
- → Comprehensive suite of algorithms
- → Hardware security integration
- → Secure key/certificate storage
- → Root of trust/secure boot process
- → Secure execution environment
- → Restrict access to any resource
- → Isolate and secure TCP/IP devices
- → Isolate and secure guest OS
- → Anti-tamper integration
- → Integrate multiple roots of trust
- → Integrate secure OTA software updates



FLEXIBLE DEPLOYMENT OF PLATFORM SECURITY SOLUTIONS

FlexHSM is designed to be modular utilizing underlying hardware resources to deliver the precise level of security specified for the target, whether the target is single function or multi-function. OmniTrust will integrate FlexHSM to fulfill your specific requirements in virtually all IoT applications.



TECHNICAL SPECIFICATIONS

Cryptographic Software

FIPS & CNSA Compliant Algorithms

- AES: 128, 192, 256
- NIST ECC Curves: P-224, P-256, P-384, P-521
- RSA 1024, 2048, 3072, 4096
- SHA2 256, 384, 512
- SHA3 256, 384, 512
- HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512
- Pseudo Random Number Generator (SP 800-90A R1)
- Key Derivation Function: KBKDF (SP 800-108)

Other Algorithms

- ECDSA - Curves: Brainpool256r1, 384r1 & 512r1; Koblitz-283; Edwards-25519
- ECDH - Curves: NIST P-224, P-256, P-384, P-521; Brainpool256r1, 384r1 & 512r1; Koblitz-283; Edwards-25519
- ECIES - Curves: NIST P-224, P-256, P-384, P-521; Brainpool256r1, 384r1 & 512r1; Koblitz-283; Edwards-25519
- DH 1024, 2048, 3072, 4096
- RSAES-OAEP 1024, 2048, 3072, 4096
- CMAC-AES 128
- [OPTIONAL] Quantum-Safe algorithms

AUTOSAR Software Modules

- Crypto stack
- Device drivers (platform specific)
- Complex driver (platform specific)

Hardware Integration (Platform Dependent)

- **TRNG**
  - Seed PRNG with minimum 128-bit entropy
- **Algorithm Acceleration**
  - Integrate AES, ECC, RSA or other hardware cores
- **Secure Key Storage**
  - Integrate secure storage for all provisioned keys, certificates, etc.
  - If no hardware storage, encrypted software key store implemented
- **Root of Trust & Secure Boot**
  - Integrate root-of-trust to authenticate device and signed code
  - Options for secure boot: 1-stage/2-stage/n-stage
- **Secure Execution Environment**
  - Integrate trusted execution functionality with protected memory (i.e. security operations separated from all other processing resources)
- **Secure Update of FlexHSM**
  - Integrate secure update of FlexHSM firmware (e.g. crypto-agility, etc.)

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