ST SECURITY

Solution for Internet of Things

EBV ELEKTRONIK presents news on the authentication market which is currently expanding from largely deployed brand protection, IT security and TPM solutions to now include the Internet of Things market. Data issued from Objects involved in smart grids, smart cities, smart homes, smart industry, with Industry 4.0 initiative, must be trusted, and more and more connected devices are now adopting solutions based on secure elements similar to those used in printers, PCs, game controllers, phone accessories, batteries, and luxury goods.”

ST offers a full ecosystem with ready-to-use turnkey solutions to ensure device identity, systems and network integrity, for customers cautious about their brand, or willing to rely on a safe and secure IoT. These solutions may be used as standalone chips in consumables like ink cartridges or in conjunction with a application MCU - like STM32 - or MPU.

ST secure element family ranges from optimized STSAFE-A, to flexible Java based KERKEY™ and TCG compliant TPM

Relying on CC EAL5+ certified chips on top of which runs an ST developed secure operating system, ST’s solutions ensure state-of-the-art, security for the protection of objects and IoT networks against:

- Device counterfeiting
- User data corruption
- Device malfunction
- Service & network access corruption

KEY FEATURES

- **Security features - STSAFE-A100**
- Latest generation of highly secure MCUs
- CC EAL5+ AVA_VAN5 Common Criteria certified
- Active shield
- Monitoring of environmental parameters
- Protection mechanism against faults
- Unique serial number on each die
- Protection against side-channel attacks
- Advanced asymmetric cryptography
- Elliptic curve cryptography (ECC) with NIST or Brainpool 256-bit and 384-bit curves
- Elliptic curve digital signature algorithm (ECDSA) with SHA-256 and SHA-384 for digital signature generation and verification
- Elliptic curve Diffie-Hellman (ECDH) for key establishment
- Advanced symmetric cryptography
- Key wrapping and unwrapping using AES- 128/AES-256
- Secure channel protocols using AES-128
- Secure operating system
- Secure STSAFE-A100 kernel for authentication and data management
- Protection against logical and physical attacks

Security features - KERKEY™

- Platform: Java Card™, GlobalPlatform, ISO/IEC 7816 & Common Personalization Compliant
- AIS-31 class P2 compliant true random number generator (TRNG)
- Enhanced cryptographic algorithms:
- DES/3DES, RSA, ECC and AES
- SEED, SHA-1, SHA-256, MD5 and CRC16
- Password Authenticated Connection
- Establishment (PACE) protocol

ST SECURITY

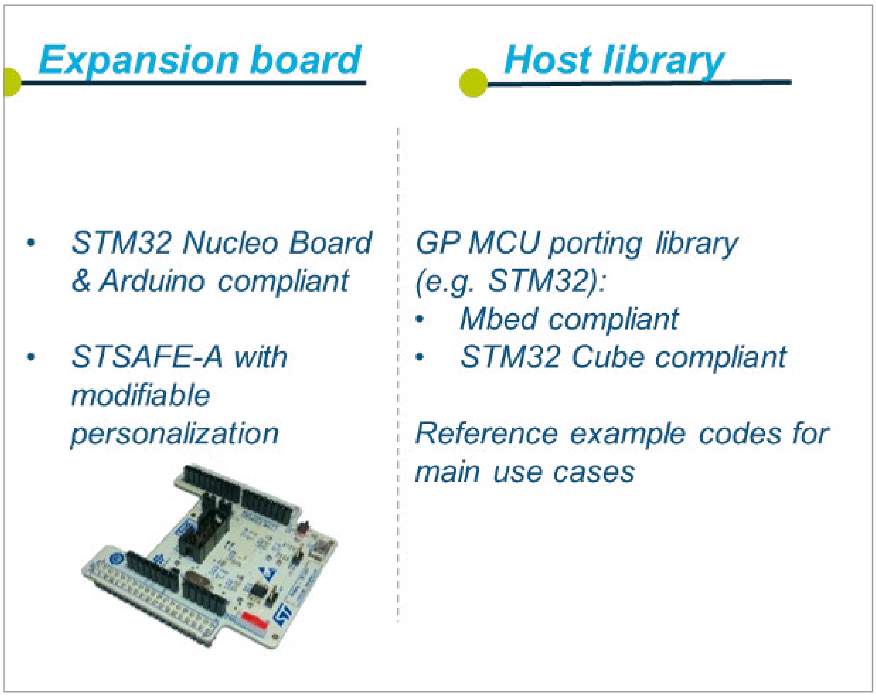
Solution for Internet of Things

Security features - STSAFE-TPM

- Active shield and environmental sensors
- Memory protection unit (MPU) used to segregate TPM assets between TPM1.2 and TPM2.0 modes
- Monitoring of environmental parameters (power and clock)
- Hardware and software protection against fault injection
- FIPS compliant RNG built on an SP800-90A compliant SHA256 DRBG and an AIS-31 Class PTG2 compliant true random number generator (TRNG)
- Cryptographic algorithms: – RSA key generation (1024 or 2048 bits)
  - RSA signature and encryption
  - HMAC SHA-1 & SHA-256
  - AES-128-192-256
  - ECC 224 & 256 bits

APPLICATION EXAMPLES

- Authentication & Secure IoT
- Smart Home & Smart Grid
- PCs & Game controllers
- Brand Protection (accessories, batteries, PCBs...)
- TPM



Expansion board

- *STM32 Nucleo Board & Arduino compliant*
- *STSAFE-A with modifiable personalization*

Host library

GP MCU porting library (e.g. STM32):

- *Mbed compliant*
- *STM32 Cube compliant*

Reference example codes for main use cases

Tools