TESIC RISC-V
CC EAL5+ ready Secure Element IP

Applications
TESIC RISC-V is a CC EAL5+ PP0084/PP0117 certification-ready secure element IP that is delivered as hard or soft macro for easy SoC integration.

Targeted designs are SoCs that require a security enclave highly protected against side-channel attacks and perturbation/fault attacks, and that execute secure software such as:
- Secured/certified iSIM/iUICC, EMVCo payment, FIDO2 Web authentication, V2X HSM protocols, Smart-Car-Access
- Secured boot, secure OTA firmware update, secure debug

Highlights
- Proprietary IP (no third-party IP rights/royalties)
- CPU based on 32-bit RISC-V core (RV32IMC instruction set)
- Available on various processes (GF55, TSMC40, GF22 FDX, TSMC16)
- Compliant with/ready for CC EAL5+ and/or EMVCo certifications
- Delivered with CC EAL5+/EMVCo CryptoLibrary and Secure Boot Loader

Features
CC EAL5+ secure microcontroller system
- Secure microcontroller core (32-bit RISC-V core)
- Memory Protection Unit (MPU)
- Timers (3)

CC EAL5+ secure cryptography
- FIPS 197 compliant AES up to 256 bits
- FIPS 46-3 compliant DES/3DES with hardware CBC mode
- Public Key Accelerator: RSA up to 4096 bits, ECC up to 521 bits
- SHA2 and SHA3 hardware accelerators
- CRC 16-bit, compliant with ISO/IEC 13239
- TRNG compliant with AIS-31 and FIPS140-2
- PRNG

CC EAL5+ security sensors
- Glitch detectors
- Temperature sensor
- Active shield
- 4 phases hand-shake protocol

Interfaces
- Slave interface: standard APB slave
- Master interface: standard AHB master
- Secure GPIOs
- Secured standard JTAG TAP for test
- Slave ISO 7816 for integration of SoC test framework
- NFC ISO 14443 for admin interface or payment (option)

Secure software:
- Crypto library
  - AES: ECB, CBC, CMAC, CTR
  - DES/TDES: ECB, CBC
  - SHA1, SHA2, SHA3
  - RSA, ECDSA, ECDH, ECIES
  - NIST approved TRNG, DRNG
- Bootloader for OTA updates
- Javacard 3.0.5 OS (third-party)
TESIC Software Environment

- **Software Development Kit (SDK)**
  - Compiler, linker and debugger based on GNU GCC/GDB with compilation chain optimized for TESIC MCU, or
  - Third-party RISC-V software development environments (RV32IMC instruction set)
- **CC EAL5+ and EMVCo certified CryptoLibrary**
- **CC EAL5+ and EMVCo certified Boot Loader**
  - Protection profile PP0084b package 2 (allowing secure OTA updates)
- **TESIC Security API**
  - Device identification/authentication
  - Secure boot, secure firmware update
  - Secure storage, secure debug
- **Third-party operating systems and applets**
  - JavaCard 3.0.5 OS
  - Network authentication stacks (iSIM/iUICC)
  - EMVCo payment applications (VISA, MasterCard)
  - Web authentication (FIDO2)
  - V2X HSM applications (requires specific TESIC version)