QKEV7 – Quantum Crypto Chip

QKEV7

▣ Main Features

- Crypto Algorithm – HW Logic SoC Chip
- Progressing KCMVP certification (Highest grade, 2)
- Crypto Engine
  - ❖ Secure Boot
  - ❖ Secret Key Crypto (ARIA/AES engine)
  - ❖ Public Key Crypto (ECC256 engine)
  - ❖ SHA256 / HMAC verification
  - ❖ PUF (Physical Unclonable Function)
  - ❖ TRNG (True Random Number Generator)
  - ✓ NIST SP 800-22 statistical test
  - ✓ FIPS 140-2 compliant
- QRNG Engine
  - ❖ Photon unpredictable Random number
  - ❖ Intrinsically and provably Random
  - ❖ Instant full entropy from the first bit
  - ❖ Compliant to Standard NIST 800-90A/B/C
- Security Requirements
  - ❖ Data Confidentiality (Encryption, Key generation, Management)
  - ✓ ARIA/AES, QRNG, Token/Object/Section
  - ❖ Data Integrity (Hash function, Signature)
  - ✓ SHA256, HMAC, ECDSA
  - ❖ Certification (Signature, ID/PW)
  - ✓ ECDH, ECDSA, SHA256
  - ❖ Transmission Data Security (Secret key)
  - ✓ ARIA/AES-128/192/256

▣ Standard Specifications

CPU	ARM Cortex-M3 processor
IO	Ethernet 10/100 PHY IF SD2.0 Card IF SPI IF (Master/Slave) I2C IF (Master/Slave) UART IF GPIO IF
Memory	E-FLASH 512Kbyte C-SRAM 416Kbyte D-SRAM 128Kbyte
Voltage	IO 3.3V / Core 1.2V
Power	120mA@100Mhz
Temperature	-40℃ ~ 85℃
Package	121-pin FBGA 9mm x 9mm

▣ Application fields

- Quantum IoT Device
- Quantum Smart City
- Quantum Smart Factory
- Quantum IP Camera
- Quantum Home Network
- Quantum Military (Weapon/Drone)
- Quantum Connected CAR
- Quantum Smart AMI/PMU

6F. KCS B/D, 269, Dongmak-ro, Mapo-gu, Seoul, Korea
www.kcins.co.kr
+82-2-6377-5001