# Module 1.2
# Hardware Security Module and Zymkey 4i

**CompuThings *Technology;**

# Function of HSM

- Secure on board key generation
- Secure on board key storage
- Key management
- Encryption and Digital Signature Function
- Offloading application server for complete asymmetric and symmetric cryptography.

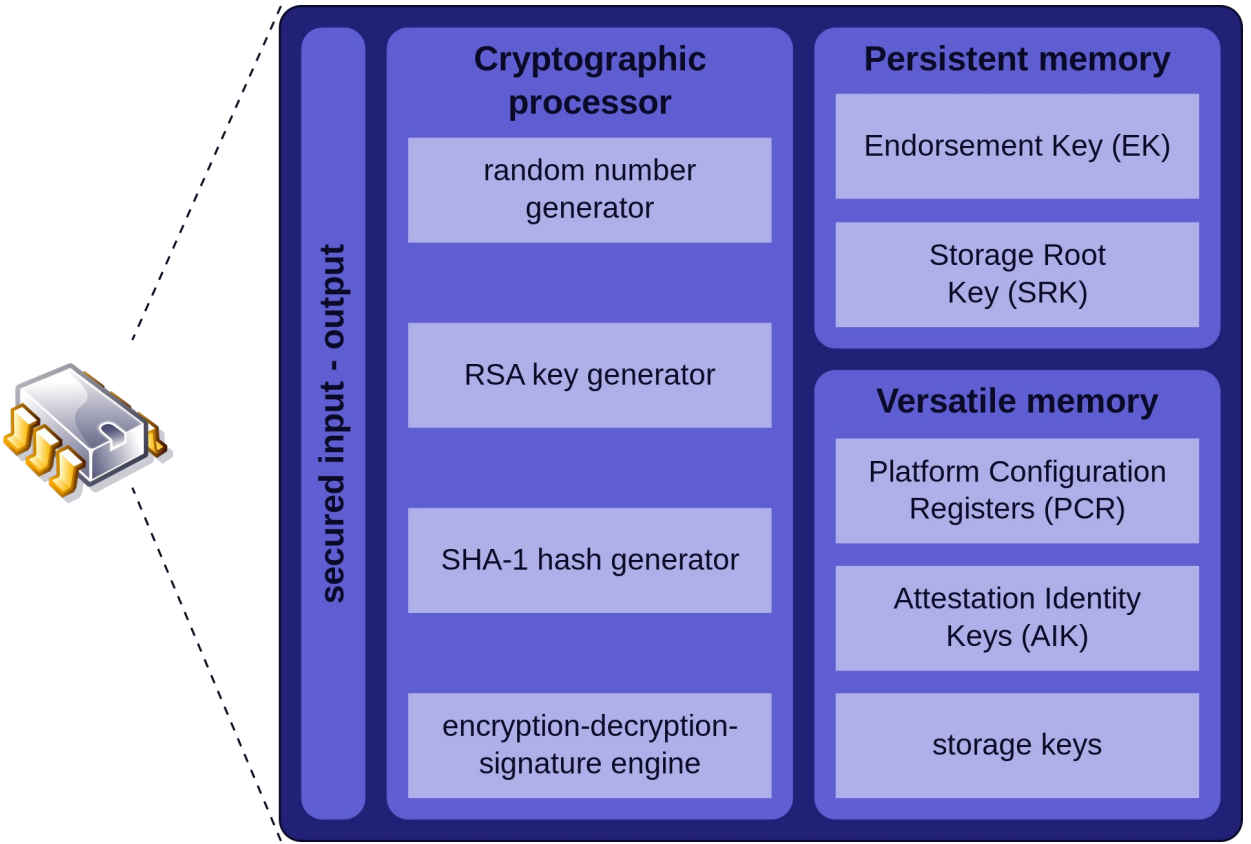
# IBM3845 Channel Attached DES,1977

- Can access more than 70 quadrillion possible keys.
- Temper resistance, random number generator, secure key storage.
- Based on DES and TDES
- Refer official IBM slides on HSM

# HSM Certification – FIPS 140

- Provide user independent assurance that the design and implementation of the product and cryptography algorithms are sound.
- Only one HSM get the highest FIPS 140 security certification (security level 4 – overall) - https://www.ultra.group/
- When use in finance system, HSM is validated by Payment card industry security standard council.
- Version 140-3 approved on March 22,2019 and will be effective on September 22,2020.

# Trusted Platform Module



# Zymkey 4i – Key Features

- Multifactor Device Identity and authentication
- Data Encryption and Signing Engine
- Key Generation and Secure Storage
- Physical Tamper Detection Sensors
- Secure Elements as root of trust

# Zymkey 4i

# Available Application Using Zymbit API

- SD card file system encryption for protection of IP, data and credentials.
- Secure device registration with AWS IoT
- Autonomous security for unattended IoT devices, no cloud dependence

# Multifactor Device ID and Authentication

- Zymkey 4i enables remote attestation of host device hardware configuration:
  - Unique ID token created using multiple device specific measurement.
  - Cryptographically derived ID token never exposed.
  - Custom input factors available to OEMs.
  - ID token bound to host permenantly for production or temporary for development.
  - Changes in host configuration trigger local hardware & API responses, policy dependent.

# Data Integrity, Encryption and Signing

- Zymkey 4i enables remote attestation of host device hardware configuration:
  - Strong cipher suite includes ECDSA, ECDH,AES-256,SHA256.
  - AES-256 encrypt/decrypt data service.
  - Integrates with TLS client side certificates.
  - TRNG – suitable seed for FIPS PUB 140-2,140-3 DRNG.

# Key Security,Generation and Storage

- Zymkey 4i generates and stores key pairs in temper resistant silicon to support a variety of secure services:
  - Multiple key slots,pre-defined and user defined.
  - Private keys never exposed outside of silicon.
  - Keys destruction available, user selectable.

# Physical Temper Detection

- Zymkey 4i monitor the physical environment for symptoms for physical tampering:
  - Power quality monitor detects anomolies like brown-out events.
  - Optional accelerometer detects shock and orientation change events.
  - Optional perimeter integrity circuits detect breaks in user defined wire loops/mesh.
  - Event reporting and response according to pre-defined policies.

# Real Time Clock

- Zymkey 4i includes a battery-backed real time clock to support off grid application:
  - 18-36 month operation,application dependent.
  - RTC clock service,available to client application.
  - RTC/UTC anamoly alerts available with zymbit security services.
  - 20ppm accuracy (standard). Optional 5ppm accuraty. (OEM features,MOQ apply)

# Secure Element : Hardware Root of Trust

- Zymkey provides multiple layers of hardware security:
  - Hard to penetrate dual secure-processor architecture.
  - Secure microcontroller supervises device multifactor identity / authentication and physical security.
  - Secure microcontroller isolates secure element from host.
  - Secure elements from Microchip -ATECC608, ATECC508.
  - Hardware based cryptoengine and keystore

# Ultra Low Power Operation

- Zymkey delivers long term autonomous security  from a battery:
  - ARM cortex-M0 microcontroller.
  - Years of secure operation from a coin cell – optional  larger battery.
  - Secure operation autonomous from host.

# Secure Element of Zymkey - ATECC508A

# ATECC508A

- Is a member of Microchip cryptoAuthentication family of crypto engine.
- The application of atecc508a include:
  - Network/IoT Node Protection
  - Anti-counterfeiting
  - Protection Firmware or Media
  - Storing Secure Data
  - Checking User Password

# ATECC508A - Features

- EEPROM array to store 16 keys,certificates,secret data and configuration data.
- Wide array of defense mechanism for physical and logical attack.
- Support i2c and swi. (single wire interface)
- Each ATECC508A ships with unique 72-bit serial number
- Generate FIPS high quality random number

# ATECC508A – Crypto Operation

- Implement complete ECC and ECDSA protocol.
- Features NIST standard P256 prime curve and support complete key life cycle from high quality  private key generation,to ECDSA signature generation,ECDH key agreement, and ECDSA public key signature verification.
- Support standard hash-based challenge-response protocol.

# ATEC508A

- Security Command (eg:GenDig)
- Cryptographic Command (eg: GenKey,Sign,ECDH,Verify)
- EEPROM Data Zone – 16 slots
- EEPROM Configuration Zone - 128Bytes
- EEPROM OTP Zone - 512bits

*(for detail, please refer to complete data sheet)*

# Conclusion

- ATECC508A is the secure element and root of trust inside Zymkey
- Understanding the hardware specifications inside a secure system is the important for hardware security engineers.
- However, zymbit ‘hide’ the accessibility to every function and command in ATECC508A using close source library.