FTF 2016
TECHNOLOGY FORUM

TECHNIQUES FOR CRYPTO KEY MANAGEMENT USING i.MX

FTF-AUT-N1894

LAWRENCE CASE
SECURITY ARCHITECT
FTF-AUT-N1894
MAY 16, 2016

AGENDA

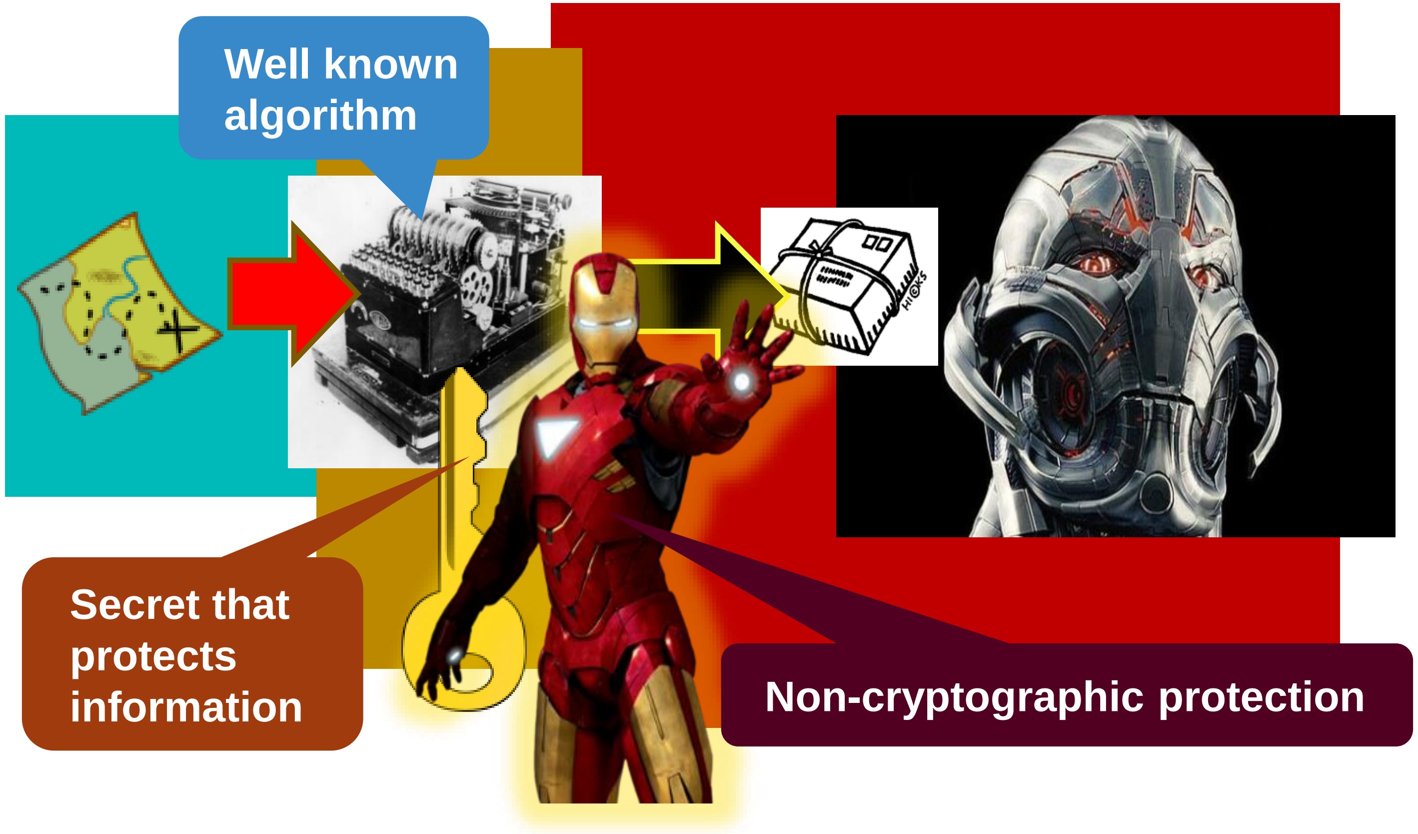
- Key Management Considerations
- Basic Key Life Cycle
- Types of Keys
- i.MX Key Management Support Features
  - Generation
  - Storage
  - Usage
  - Revocation
- Questions

Security Features on NXP Secure MCUs

- AES, RSA, ECC, SHA cryptographic hardware accelerators
- True Random Number Generators
- Pseudo Random Number Generators
- Security Life-cycle Management
- Password Protected Debug Access
- Password Protected Flash Prog.
- Permanently Secure Flash Regions
- Secret Key Storage
- Zeroised memory
- Tamper proof flash reprogramming audit trail
- Side Channel Attack Countermeasures
- Trust Zone

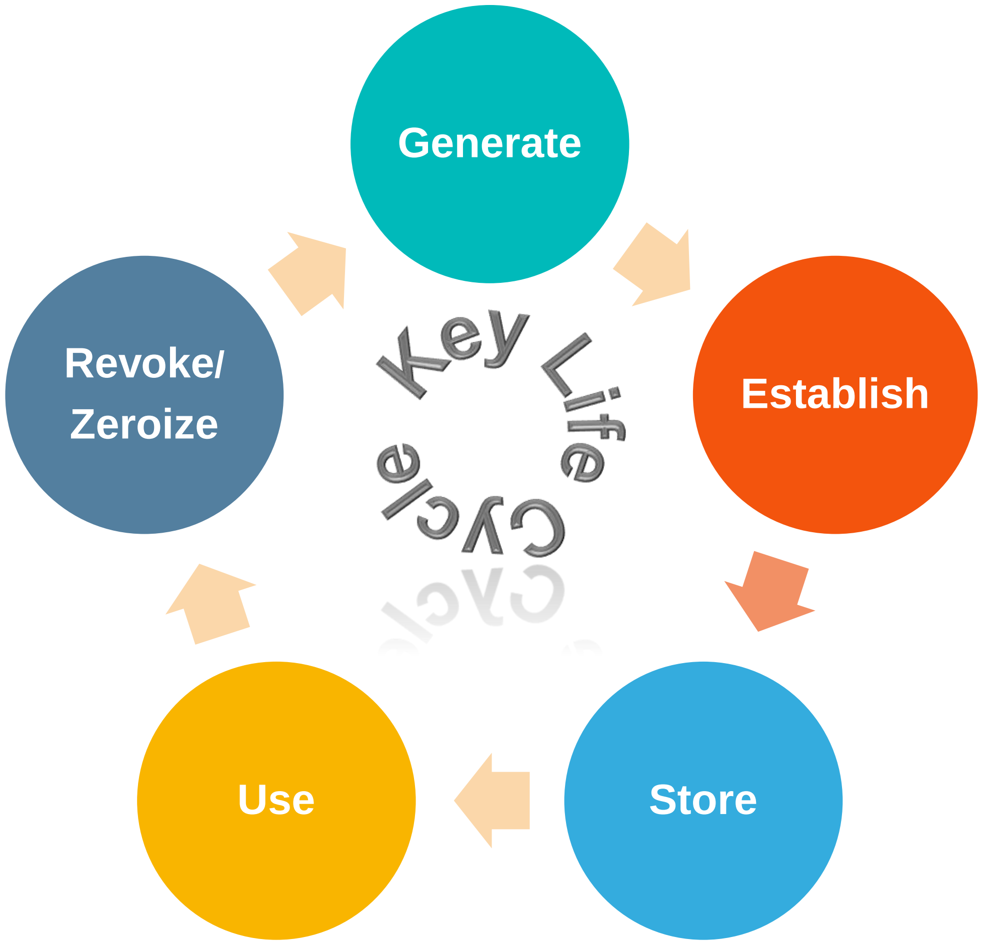
- Secure Boot
- Chain of Trust
- Symmetric Key Crypto Functions
- Asymmetric Key Crypto Functions
- EVITA 1, 2, 3 Compliance (HSM)
- SHE (CSE)
- FOTA

Key Management Considerations



- Most cryptographic functions are well-known, well-vetted algorithms
- A cryptographic key itself may not be encrypted
  - Relies on non-cryptographic protections
- Methods for protection and handling of keys can vary greatly, depending on implementation

Basic Crypto Key Life Cycle



Examples:

- Generation
  - Random value that can't easily be guessed
- Establishment
  - Sets up of keys between corresponding entities
- Storage
  - Protected location and/or encryption of key
- Usage
  - A single key has a dedicated purpose
- Revoke/Zeroize
  - Lifetime of key expires due to diminishing security

TYPES OF KEYS

Types of Cryptographic Keys

- Many types of cryptographic keys with different:
  - Uses
  - Sizes
  - Security property requirements (integrity vs confidentiality)
  - Lifespans

- While most keys are secrets, a public key can be known. Its integrity and binding to a source are typically strictly preserved

Common Types of Cryptographic Keys

- **Symmetric**
  - Shared secret among to corresponding parties
  - Same numerical value held by each party
- **Asymmetric**
  - Consists of a corresponding public and private key pair
  - Permits encryption between two parties without sharing the same secret
- **Signature Keys**
  - Signs a message by the source or verifies the source of the message
- **Ephemeral**
  - Keys of a single key agreement and not reused or backed up
- **Public**
  - Not Secret; requires trustworthy association to an identity (the keeper of the private key)
- **Key Wrapping Key (Key Encryption Key)**
  - Key to encrypt another key for storage or transport

i.MX-Specific Cryptographic Keys

- **Super Root Key**
  - Non-volatile, Public Asymmetric, Signature Verification Key
- **OTP Master Secret**
  - Symmetric Key Encryption Key
  - Statistically Chip Unique
- **Secure Boot Data Encryption Keys (DEK)**
- **Black Keys (two types)**
  - Wrapped Symmetric Key
- **Key Encryption Keys (JDKEK, TDKEK)**
  - Volatile key encryption keys for Black Keys
  - JDKEK (Unique per Job Descriptor)
  - TDKEK (Trusted Descriptor)
- **Manufacturing Protection Key Pair**
  - Recreates private ECC key only in secure conditions
  - Used for signing by genuine NXP part

i.MX KEY MANAGEMENT SUPPORT FEATURES

Key Generation - Hardware Support for Symmetric Keys

- **Random Number Generator (RNG)**
  - Entropy source & DRBG
  - Initializes storage key encryption keys
  - Initializes Trusted Descriptor signing keys
  - Direct interface to Zeroizable Master Key register
  - Initializes OTPMK (i.MX7 and later)

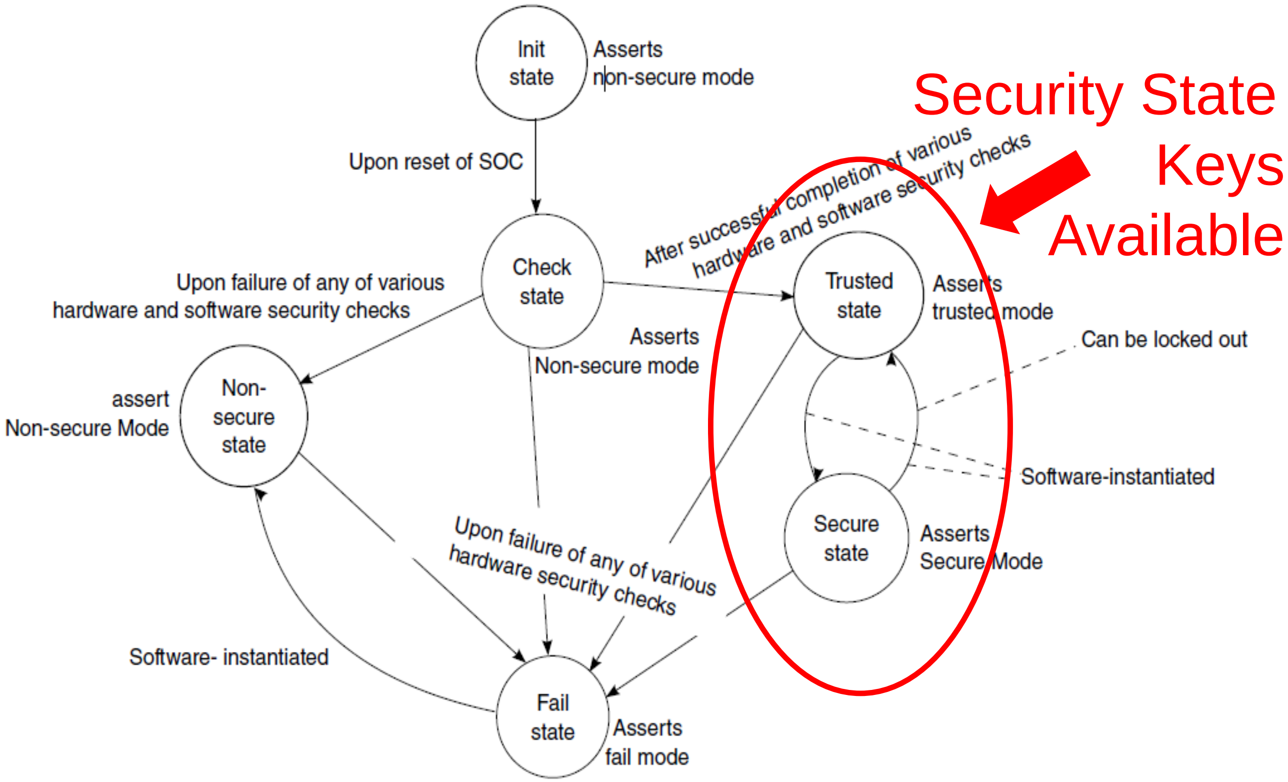
- **Manufacturing Protection**
  - Generates a key pair and keeps private key within hardware

- **Discrete Log Key Pair Generation**
  - Prime Field or Binary Field
  - DSA or ECDSA

- **Finalization of RSA Key Generation**
  - Computations after primes and exponent are given

- **Diffie Hellman and ECDH**
  - Shared secret output

Key Establishment

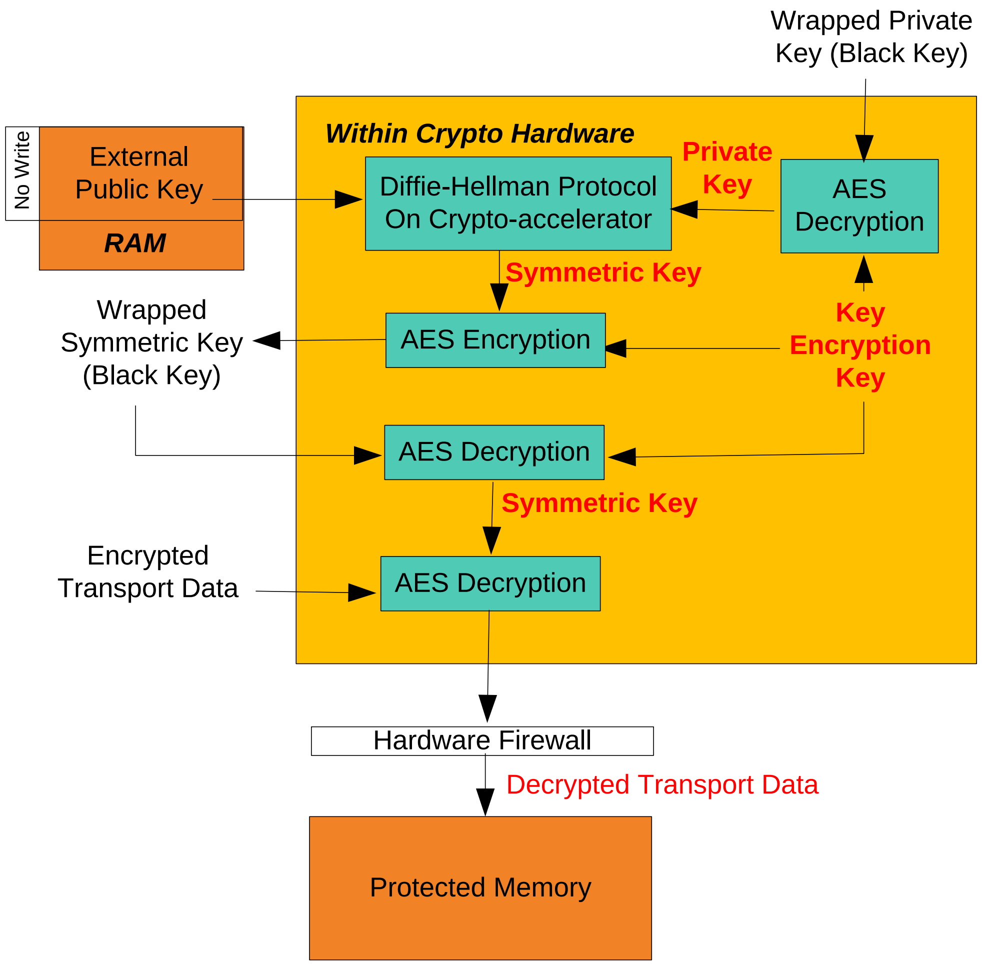


- **Hardware detection logic**
  - Determines if operating conditions are trustworthy for secure boot (tamper or test pins asserted)
- **Secure Boot**
  - Immutable process that loads keys and sets up security state which gives access to many keys
  - Binds SRK to the Manufacturing Protection ECDSA key pair
- **Some keys are only available in certain security states**
  - OTP Master Key
  - Zeroizable Master Key
  - Trusted State Key for Blobs

Key Storage: Volatile

- **Zeroizable Master Key**
  - Immediately erasable 256-bit Register
  - Security violation drives the reset – no clock required
- **Black Keys**
  - Encrypted Keys, encrypted with a volatile KEK
  - Can only be decrypted into a crypto key register
  - Authenticating AES-CCM (MAC) option
- **Secure RAM**
  - Access blocked upon security violation and Auto-zeroized by hardware
- **Key Registers**
  - Scan protection; automatically cleared if scan is entered

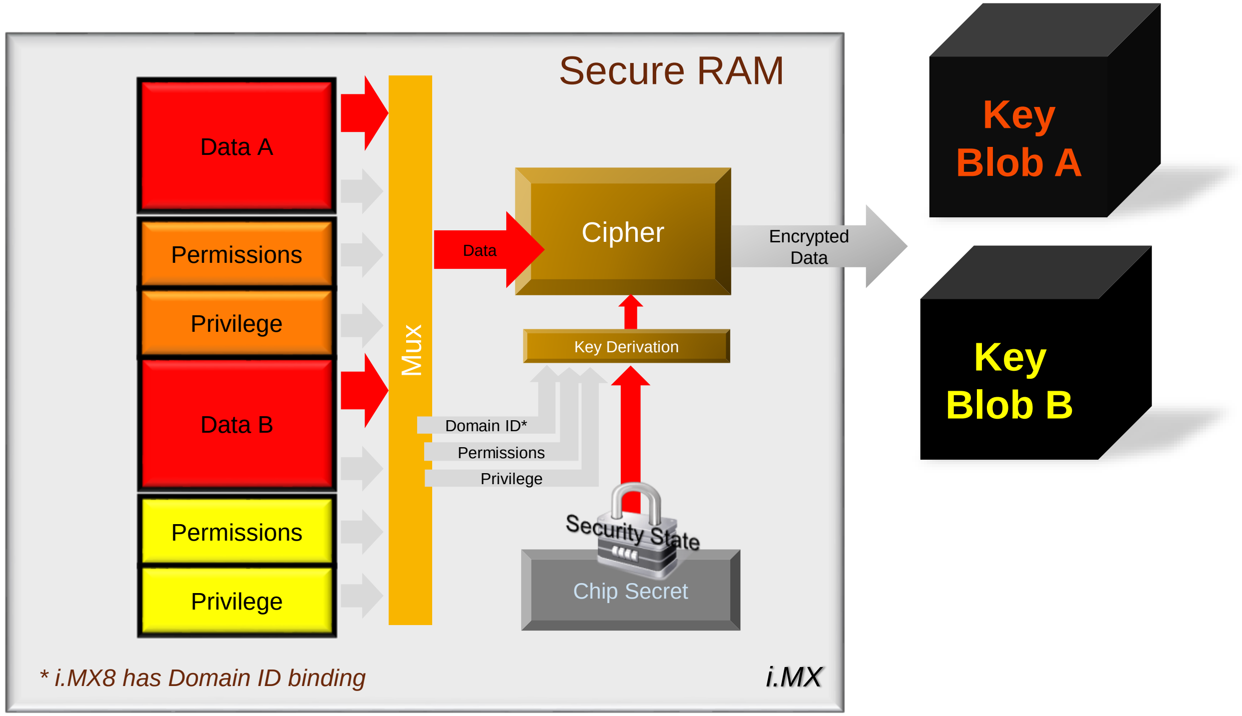
Key Storage: Black Keys



Black Keys:

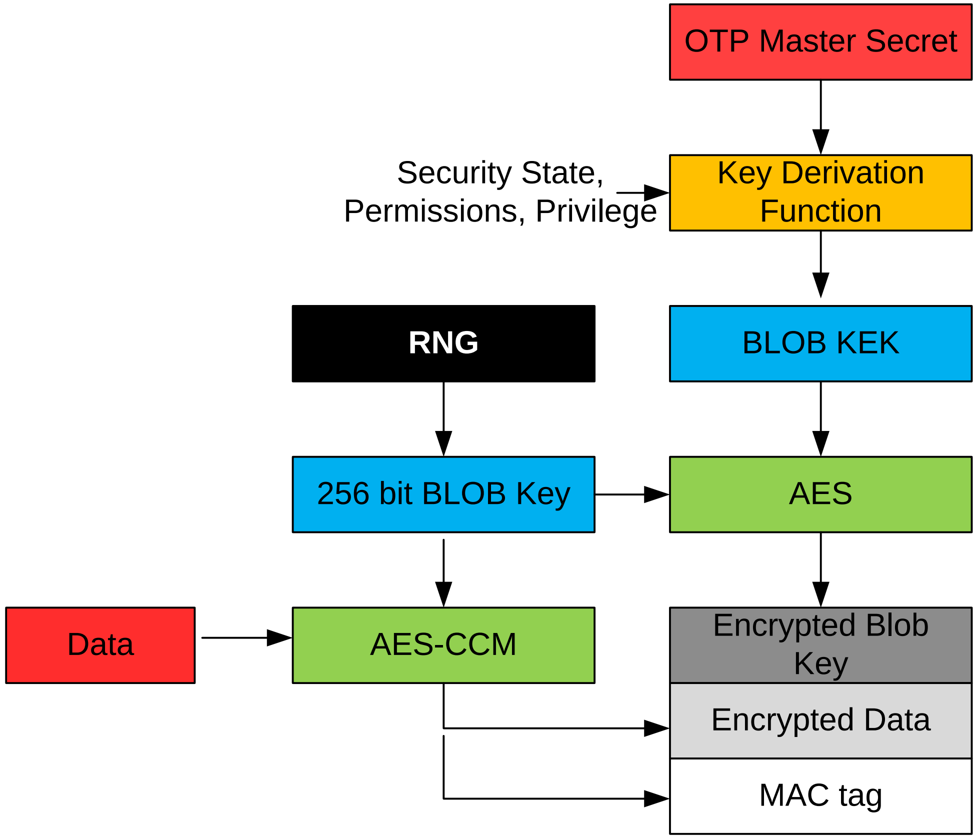
- Automatic encapsulation of cryptographic keys
- Bound to execution domain
- Crypto hardware automatically decrypts and installs Black Key before ciphering data

Key Storage: Non-Volatile Blobs



- **Key Blobs**
  - Protects keys over power cycles
  - Keys are encrypted with Non-volatile Key Encryption Keys (KEK)
  - KEK is at least as strong as key it protects
- **Cryptographic Bindings Include**
  - Security State (Trusted, Secure, Other)
  - Access Permissions
  - Privilege (TZ or NS)
  - Resource Domain

Key Storage: Non-Volatile Blobs Cont.



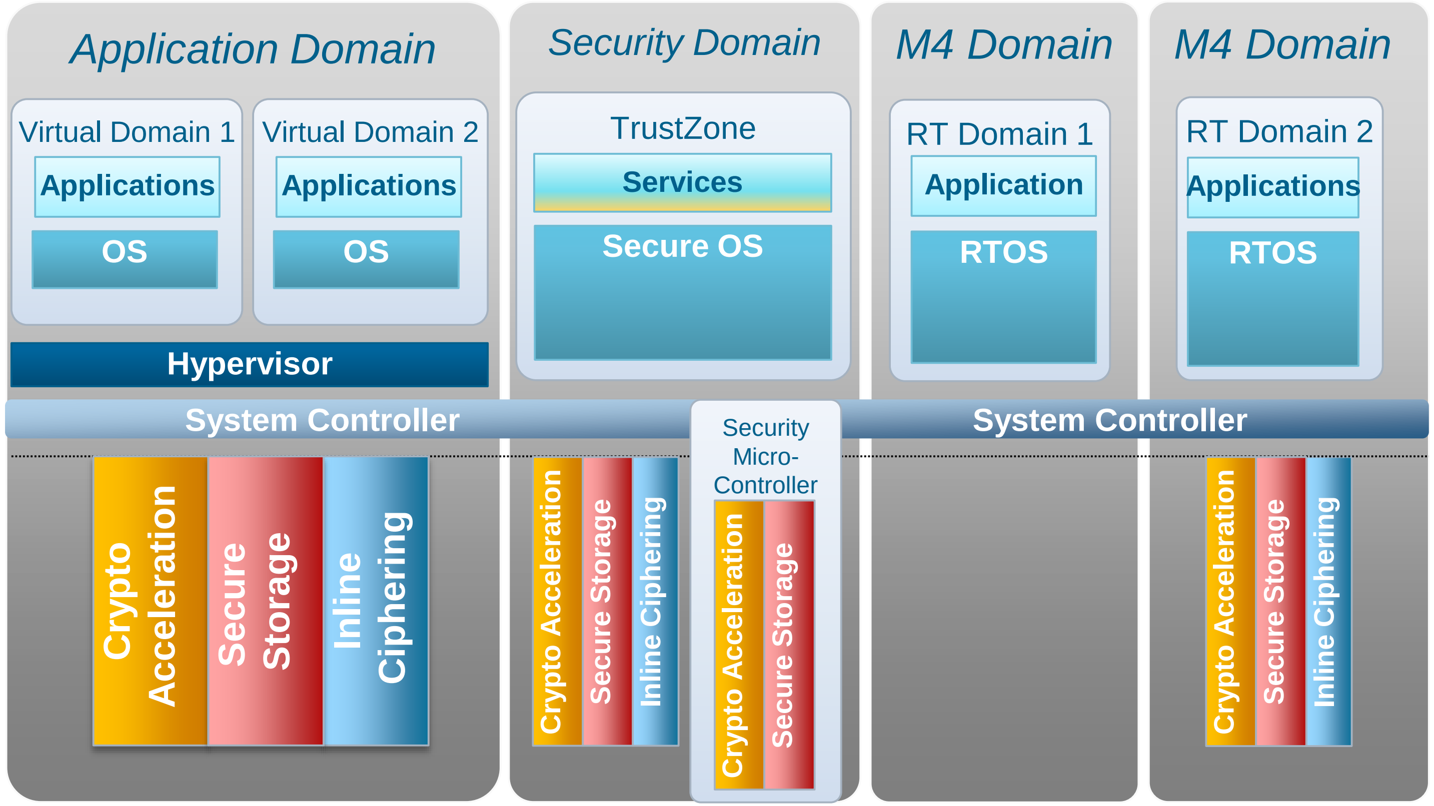
Blob Creation:

- Blobs normally consist of Encrypted Blob Key, Encrypted data, and a MAC tag
- Trusted State gives different Blob Key than Secure State
- Different Blob keys so one blob key cannot be used to decrypt another's data
- MAC tag ensures integrity
- Blob data is imported back to Secure RAM if State, permissions, privilege (TZ) and domain identifier match

Key Storage - Isolated Execution Environments

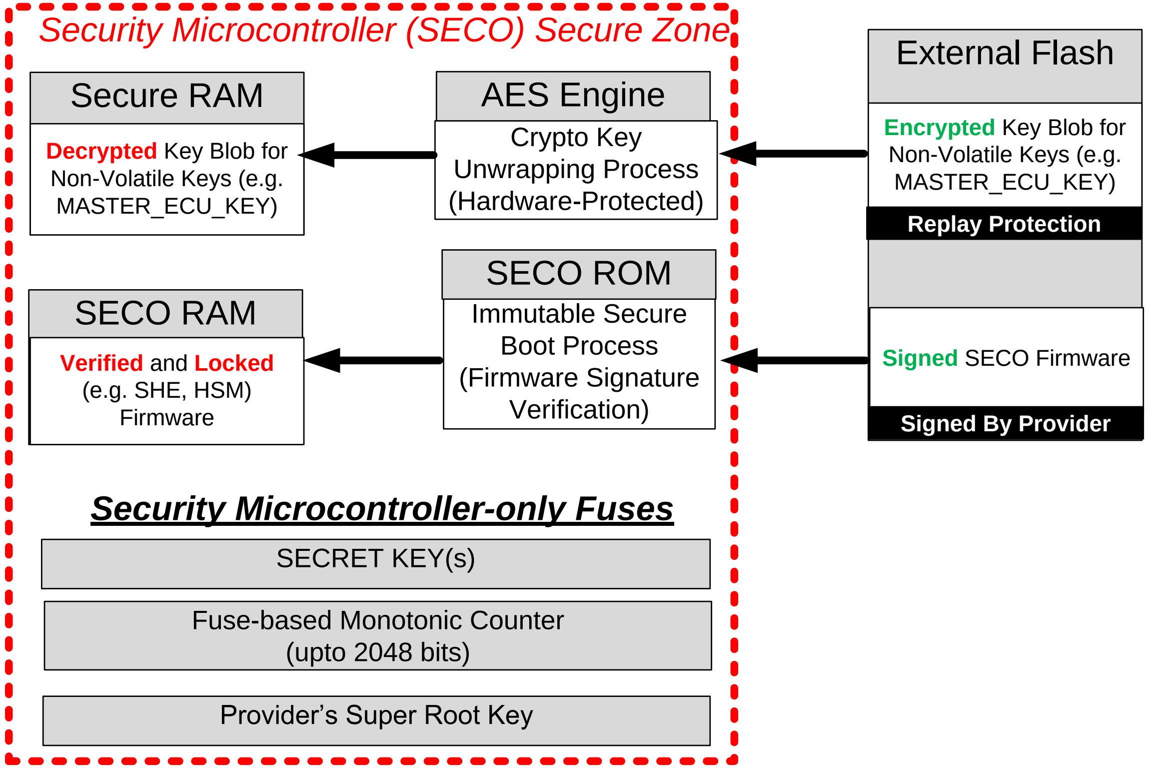
- **Domain Exclusive**
  - Trustzone
  - Resource Domain

- **Security Microcontroller (Multi-core chips)**
  - Logically Isolated
  - Allows fine grain control over key usage



Key Usage – Embedded Security Microcontroller

- Logically isolated security microcontroller
- Authenticated firmware implements high level key management functionality
  - Fine control over key use and life cycle
  - Adaptable to standards
  - Thousands of firmware updates permitted with replay protection
  - Controls access to security resources
- Queued messaging supports host command

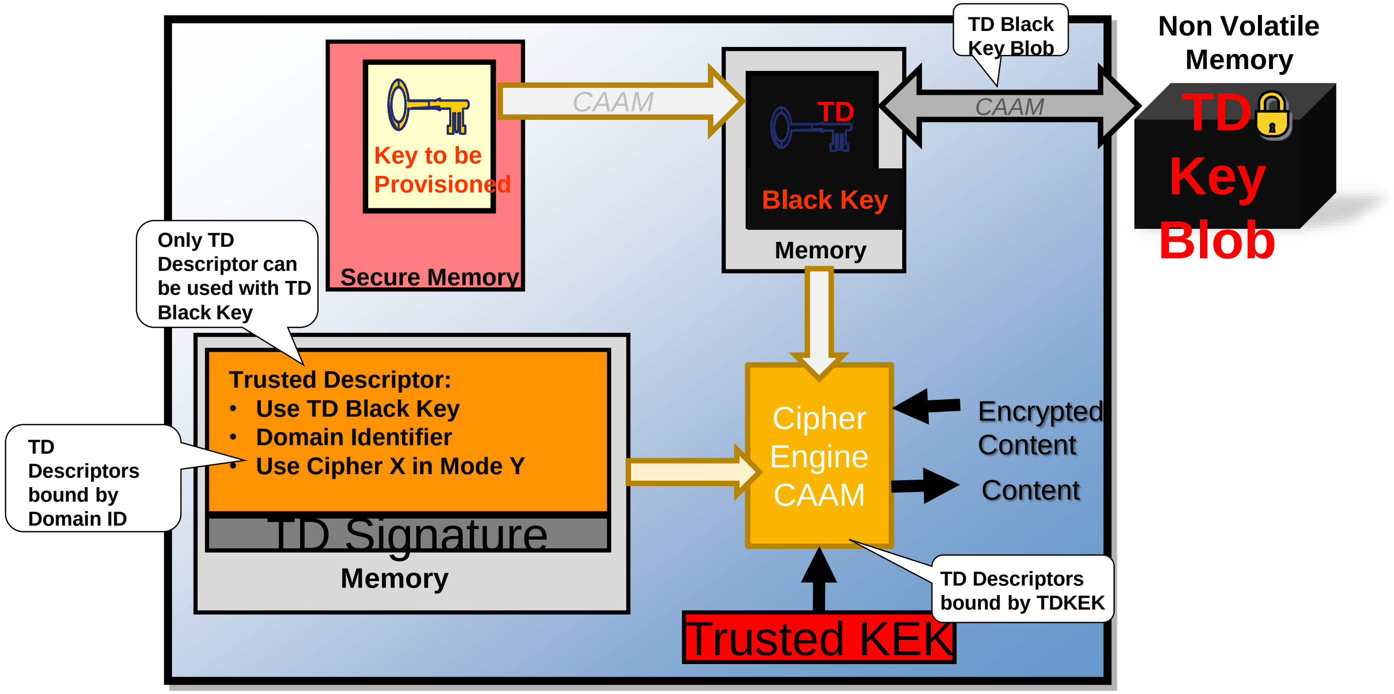


Key Usage - Trusted Descriptors

Trusted Descriptor integrity and source is protected by signed hash

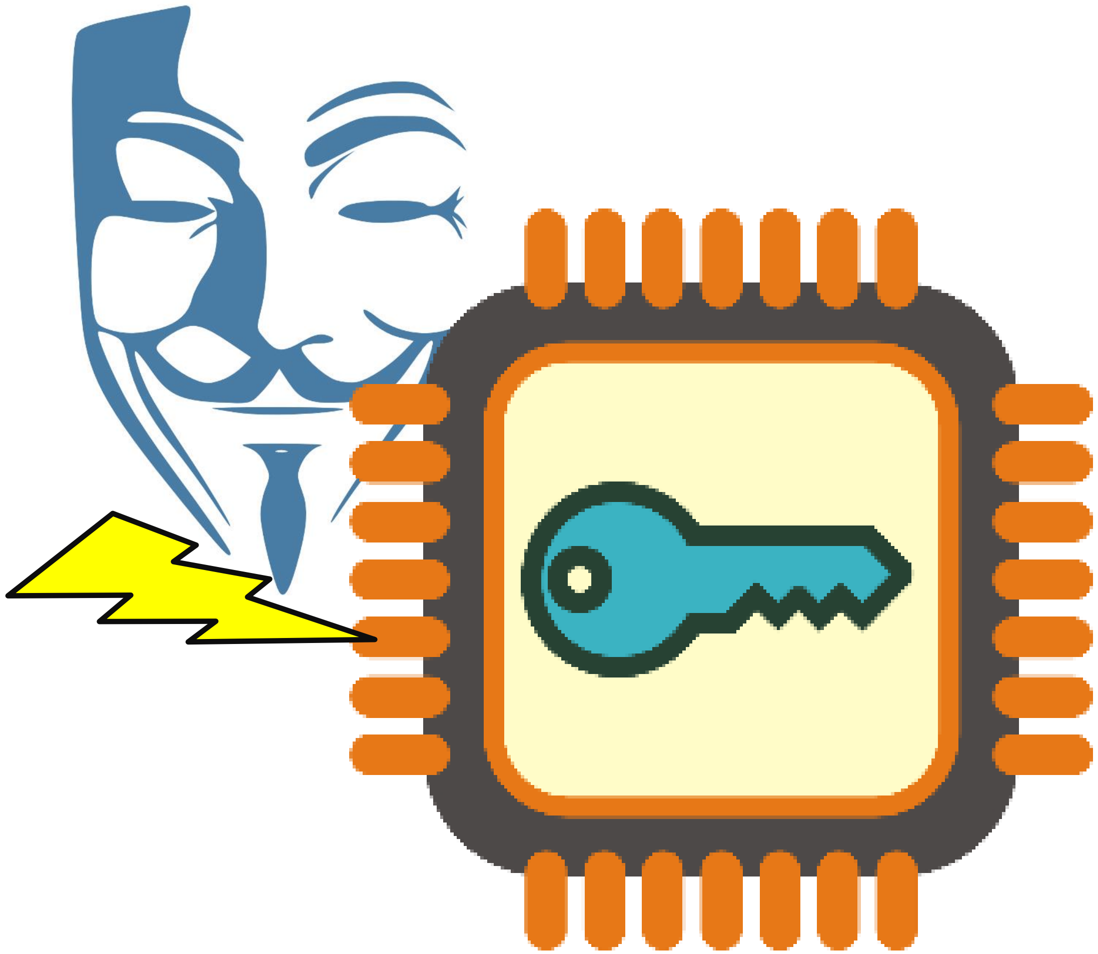
- Trusted Descriptors (TD) feature is means for trustworthy software to create a cipher descriptor that assuredly executes when run by less trustworthy software
- Only TDs are allowed to use TD Black Keys and TD Blobs
- Trusted Black Keys remain encrypted until utilized. Will not be decrypted if TD signature fails
- A TD is integrity checked at run-time and executed only if the check passes

Trusted Descriptors Cont.



- TD Black Keys cannot be used by normal descriptors
- TD Key Blobs cannot be decapsulated by normal descriptors
- TD can have an exclusive region in secure RAM that only it can access
- In i.MX8, TDs and associated context can be bound to the Domain Identity too

Key Zeroize



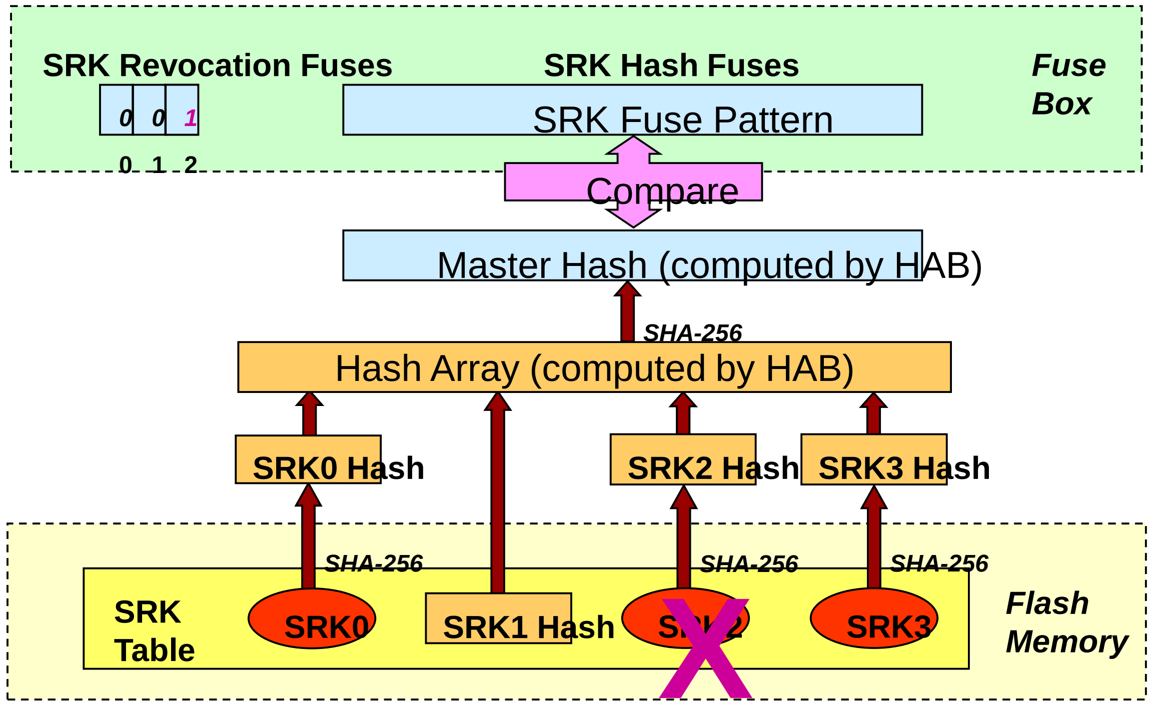
- **Tamper detection from sensors causes:**
  - Security State Change to Remove Storage Keys
  - Secure RAM Blocks Access and Zeroizes
  - Zeroizable Master Key immediately resets

- **Other security violation conditions include:**
  - Run-time integrity failure
  - DFT, debug activation detection

Key Revocation Cont.

- Revocation
- Monotonic Counter
  - Fuses or Battery Backed Counter
  - Synchronizes External Flash Blobs with Internal Counter

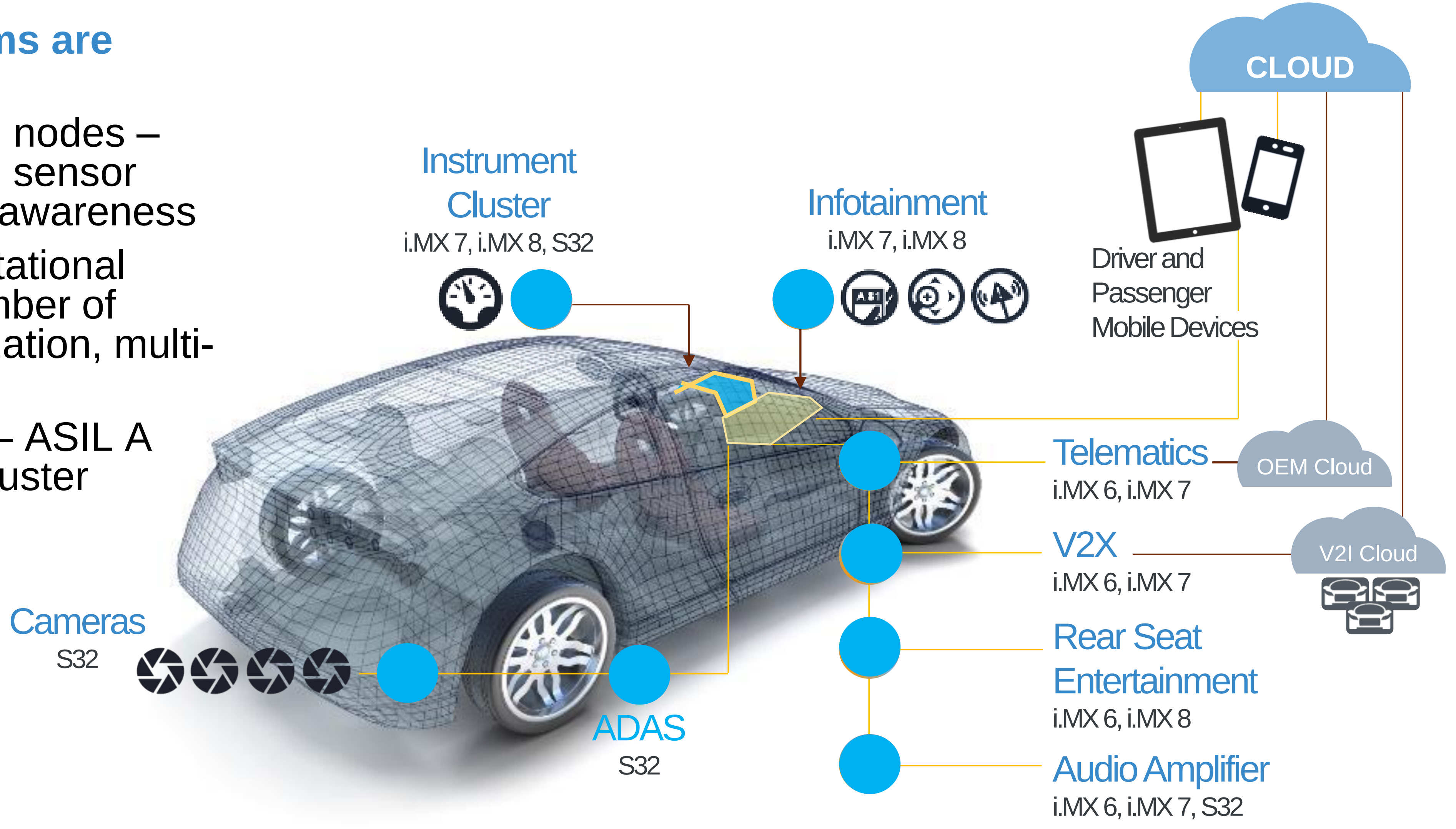
- SRKs
  - Up to four separate public keys with only one being selected at boot time by the “Install SRK” command



Secure MPU (i.MX)

Tomorrow's systems are focused on:

- Increased sensing nodes – multiple cameras , sensor fusion, situational awareness
- Increasing computational capability and number of displays – virtualization, multi-OS, HD displays
- Increasing safety – ASIL A camera, ASIL B cluster



QUESTIONS?

SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT