i.MX Security Seminar

Basics and Features

BERNHARD FINK

MAY 21, 2019

CONFIDENTIAL AND PROPRIETARY

SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURITY FUNDAMENTALS

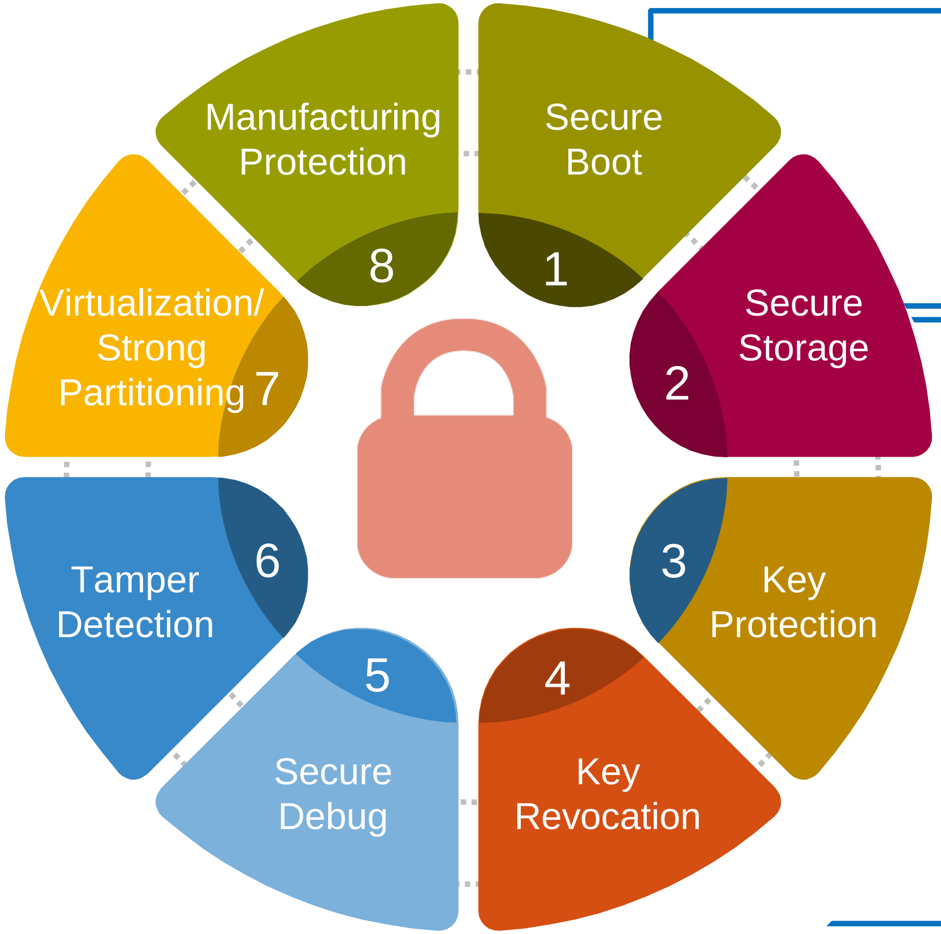
NXP Leverages Core Competence in End-to-End System Security

Mobile and stationary machines want full access to cloud-based knowledge

This requires faster, more reliable and secure connectivity

NXP is at the forefront of secure communications and tamper resistance

Leadership experience in security markets: over 10 Billion smart cards sold



Baseline Security
Secure Boot
Secure Debug
Secure Storage

Tamper Detection
Detect Tamper Events
Tamper Response

Advanced Security
Key Protection
Key Revocation
Strong Partitioning

Which kind of security needs to be implemented?

- Protection of user data
  - Storage of encrypted data
  - End-to-end encryption
- Protection against non-authorized use
  - Signed firmware
  - Secure boot
  - Disable debug port
- Protection of software and hardware IP
  - Encrypted firmware
  - Protection against re-engineering
- Protection against physical access
  - Housing
  - Moulding of the electronic components

Security on Silicon level

Where does security start? → On silicon design level.

When does security start? → Right after reset.

- Without the right silicon design, you will not achieve real security

- As soon as a chip is powered up and a hard-coded or soft-coded machine starts to run, you need to protect the system against attacks and bricks

Security on Software level

What‘s the aim? → **Do not execute unauthorized software.**

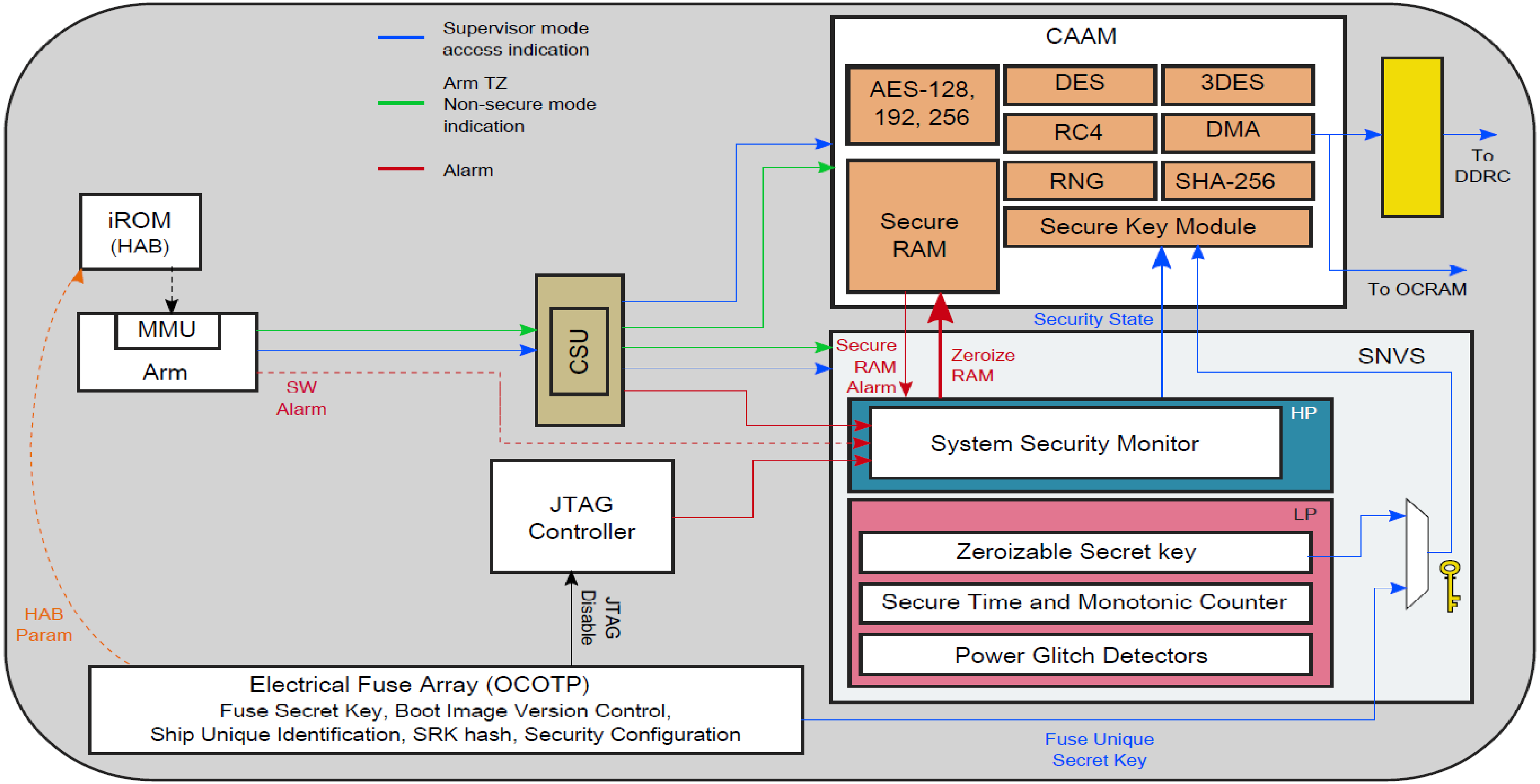
- Software (components) must be verified to be genuine, before they are allowed to be executed.
- For systems with external memory (for example Linux in DDR) some sort of protection against sniffing and content modification needs to be applied.

Attack and brick methods

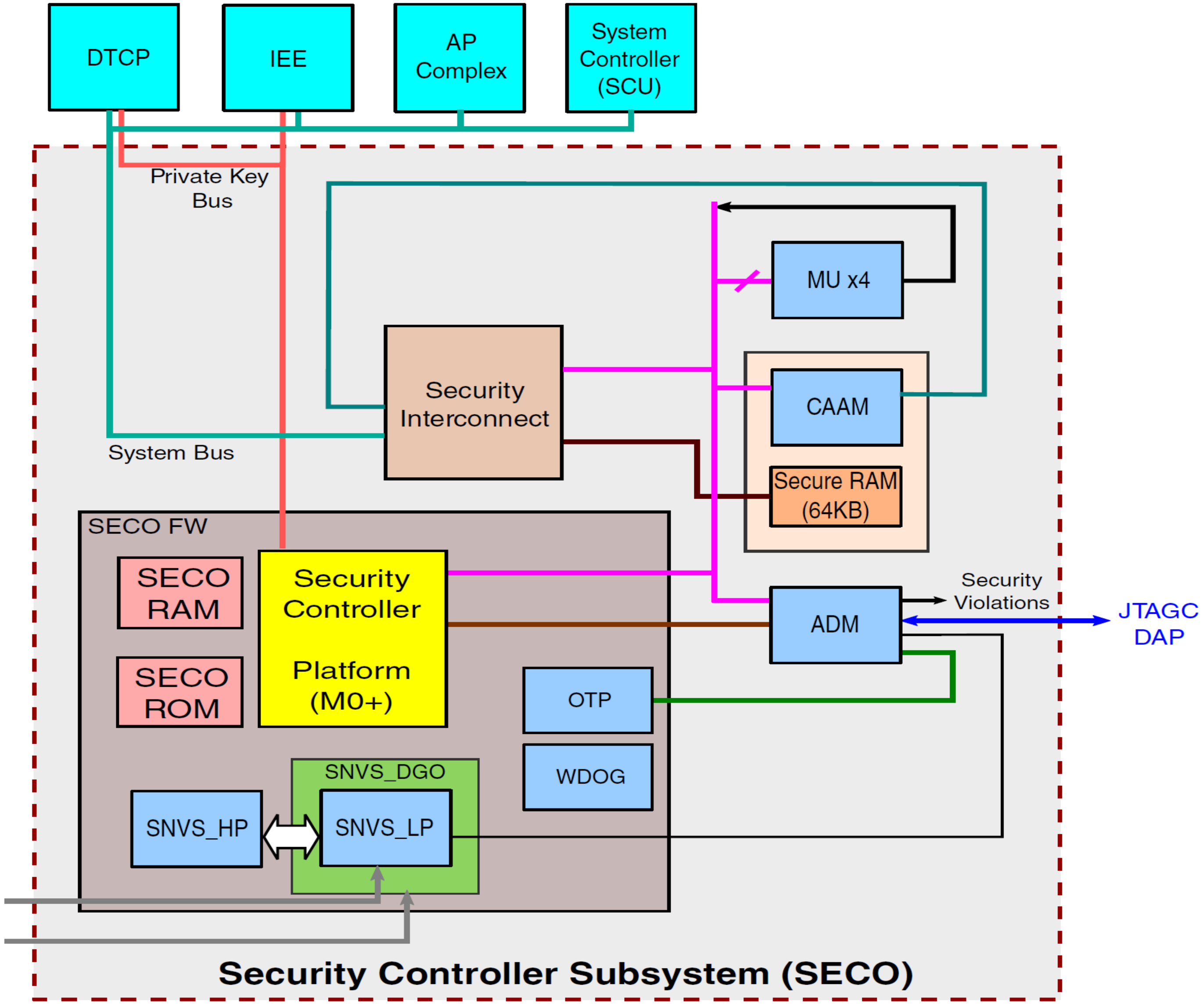
Attack Description	Attack Type
Circumvent the secure apps using the JTAG port	Physical access to debug port
Scan out secret keys and passwords	Physical access to debug port
Obtain keys from memory (on-board memory probing)	Physical access to PCB
Replace OS image in memory	Access to memory on the target (physical probing or remote)
Obtain system keys using “key sniffing” SW running in user mode	SW + profiler
Obtain system keys using “key sniffing” SW running in kernel mode	SW + profiler
Attack the OS kernel to obtain privilege mode	SW

SECURITY IMPLEMENTATION

Security Controller Implementation in i.MX 8M-Mini



Security Controller Implementation in i.MX 8X

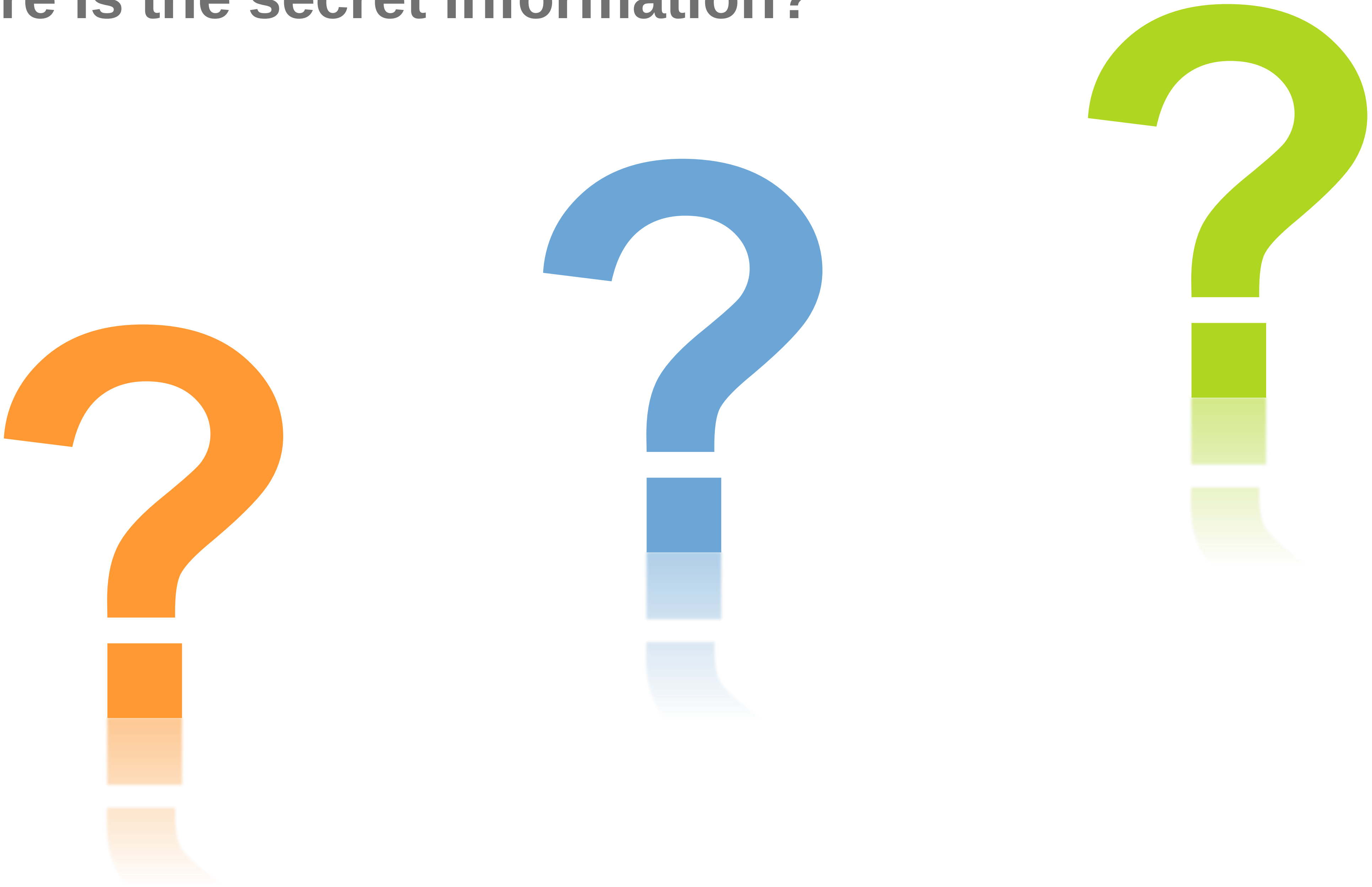


- Isolated Security Microcontroller:
  - Dedicated ROM and RAM
  - Dedicated OTP keys
- Shared Peripherals:
  - 4x Messaging Units in HW
  - RTC and Secure RTC timers
- Private Key Bus interface to outside blocks
- Cryptographic Acceleration and Assurance Module (CAAM) with secure RAM and RNG
- Authenticated Debug Support (ADM)

i.MX Security Features

Feature	i.MX6Q/D/S	i.MX6SX	i.MX6UL	i.MX7S/D	i.MX8QM	i.MX8QXP
Security Controller (SECO)	x	x	x	x	✓	✓
AES128/192/256, SHA1/256, DES/3DES	✓	✓	✓	✓	✓ + SHA 384/512	✓ + SHA 384/512
Elliptic Curve DSA (up to P521/B571) RSA (up to 4096)	x	x	✓	✓	✓ High performance	✓ High performance
Crypto Accelerator Unit (CAU) (DES, AES co-processor instruction)	x	x	x	x	✓	✓
Certifiable RNG	✓	✓	✓	✓	✓	✓
Run Time Integrity Protection	x	x	✓	✓	✓	✓
Isolated security applications (e.g. SHE)	x	x	x	x	✓	✓
High Assurance Boot (RSA, ECDSA)	✓RSA	✓RSA	✓RSA	✓RSA	✓	✓
Encrypted Boot	✓	✓	✓	✓	✓	✓
Secure Debug	✓	✓	✓	✓	✓ Domains	✓ Domains
Always ON domain	✓	✓	✓	✓	✓	✓
Secure Storage (non-volatile)	✓	✓	✓	✓	✓	✓
Tamper Detection Signal	✓	✓	✓ Active	✓ Active	✓ Active	✓ Active
Volt/Temp/Freq Detect	x	x	✓	✓	✓	✓
Inline Encryption	x	x	✓ **BEE**	x	✓ **IEE**	✓ **IEE**
Manufacturing Protection	x	x	x	✓	✓	✓
Resource Domain Isolation	x	✓	x	✓	✓	✓
Content Protection	✓ **6Q 1.x only**	x	x	x	✓ **HDCP 1.x/2.x, DTCP**	✓ **DTCP**

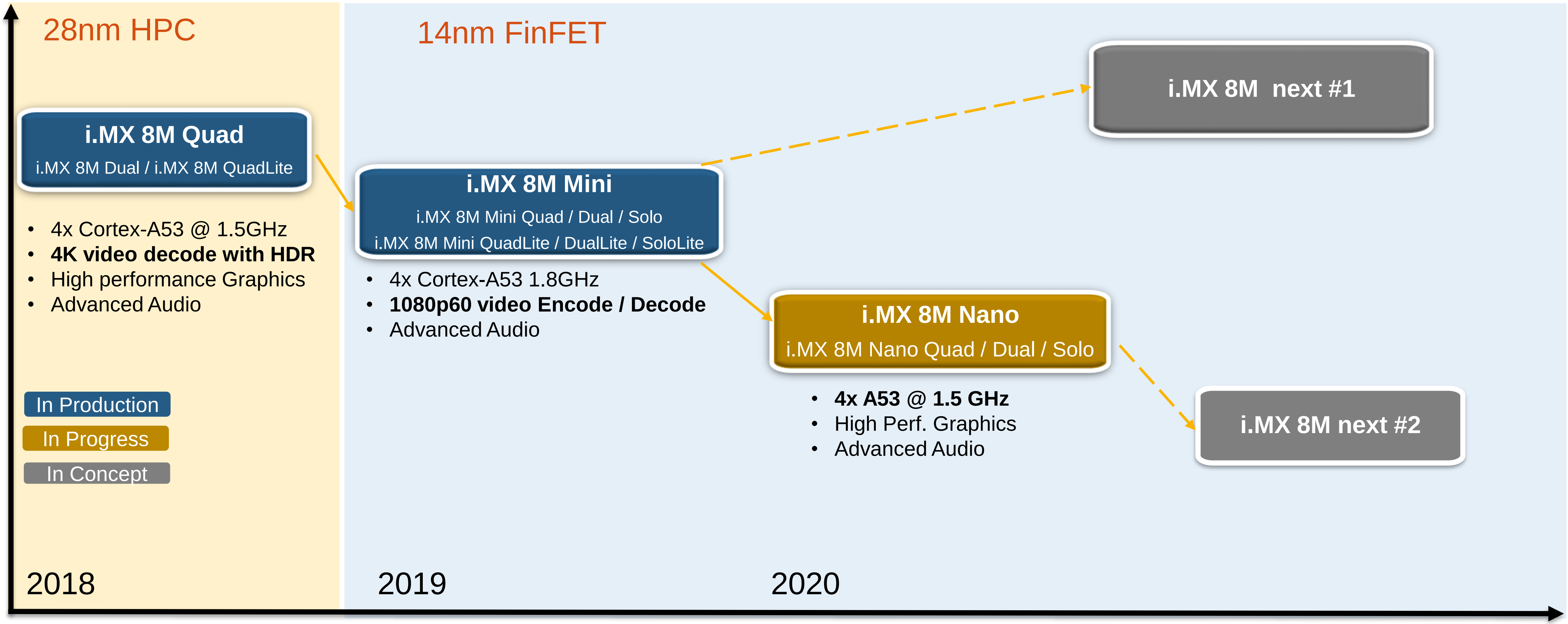
Where is the secret information?



I.MX PRODUCT ROADMAP

Roadmap for i.MX 8M Series

Preliminary – Subject to Change



28nm HPC

i.MX 8M Quad

i.MX 8M Dual / i.MX 8M QuadLite

- 4x Cortex-A53 @ 1.5GHz
- **4K video decode with HDR**
- High performance Graphics
- Advanced Audio

In Production

In Progress

In Concept

14nm FinFET

i.MX 8M Mini

i.MX 8M Mini Quad / Dual / Solo

i.MX 8M Mini QuadLite / DualLite / SoloLite

- 4x Cortex-A53 1.8GHz
- **1080p60 video Encode / Decode**
- Advanced Audio

i.MX 8M Nano

i.MX 8M Nano Quad / Dual / Solo

- **4x A53 @ 1.5 GHz**
- High Perf. Graphics
- Advanced Audio

i.MX 8M next #1

i.MX 8M next #2

2018

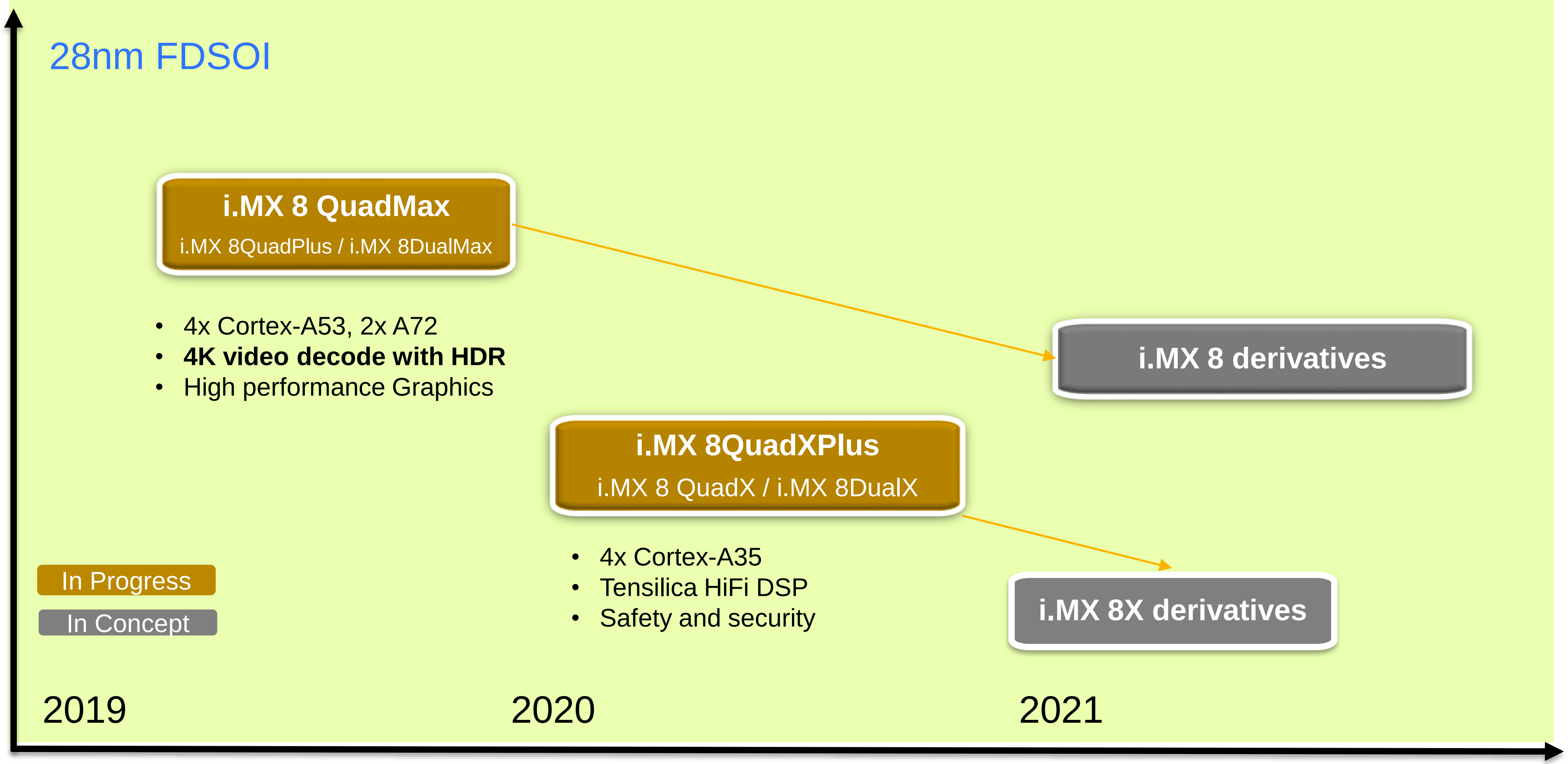
2019

2020

28nm HPC and 14nm FinFET technology can cover Consumer and Industrial platforms

Preliminary – Subject to Change

Roadmap for i.MX 8 / 8X Series



28nm FDSOI

i.MX 8 QuadMax

i.MX 8QuadPlus / i.MX 8DualMax

- 4x Cortex-A53, 2x A72
- **4K video decode with HDR**
- High performance Graphics

i.MX 8 derivatives

i.MX 8QuadXPlus

i.MX 8 QuadX / i.MX 8DualX

- 4x Cortex-A35
- Tensilica HiFi DSP
- Safety and security

i.MX 8X derivatives

In Progress

In Concept

2019

2020

2021

28nm FDSOI technology covers Automotive, Industrial and Consumer platforms

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD