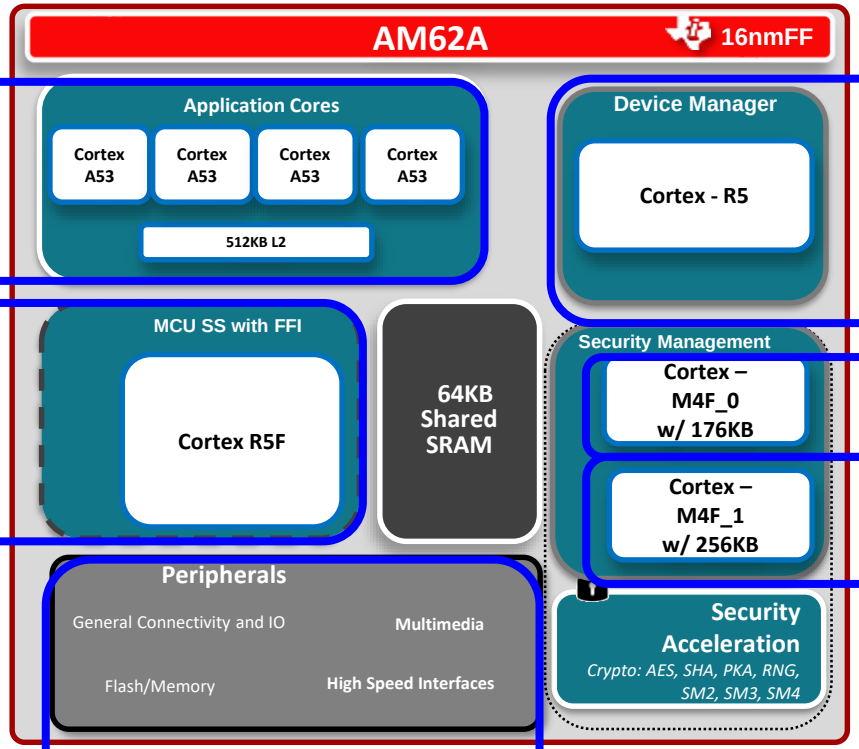
AM62P Boot Overview

2023

TI Confidential – NDA Restrictions

Texas Instruments

AM62P Boot Architecture



- OS Boot
- Apps processor

- Bootloader starts R5F
- Supports CAN response ~50ms (HS: ~70ms)
- Runs AutoSAR

- Boot Peripherals/Media

- Public Boot ROM
- Secondary Bootloader(SBL) –EMIF Config
- R5F BIST (optional) / code execution
- Device Management Firmware
- VPAC/Display driver

- Secure ROM
- TI Foundational Security(TIFS)

- Security MCU running 3P HSM SHE/EVITA stack
- Booted by SMS M4F

Supported Boot modes

- Memory Boot Options:

Interface	Implementation Notes
I2C	Using I2C EEPROM in 16/24 bit modes
OSPI/QSPI	Supports booting in single/quad/octal mode Support NOR and serial NAND flash
MMCSD/eMMC	Using FAT32 filesystem and sectioned boot image
USB Host	Using HS speed and FAT32 filesystem.
GPMC	SLC NAND Support only

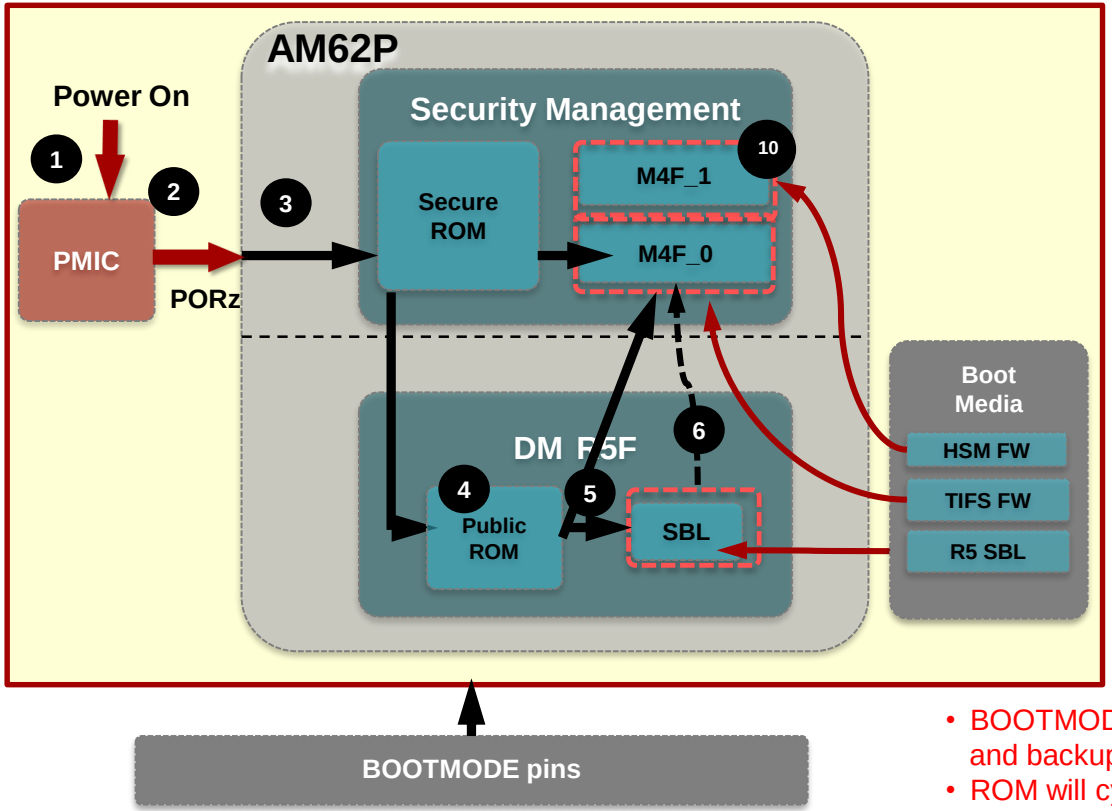
- Peripheral Boot Options:

Interface	Implementation Notes
UART	Using XMODEM protocol
USB Device	DFU boot from external host
CPSW(Ethernet)	RGMII and RMII Supported

TI Confidential – NDA Restrictions

Texas Instruments

AM62P Initial Boot Sequence



Initial Boot Flow (mandatory)

1. System Power On
2. PMIC releases SoC PoRz
3. Secure ROM Starts/Basic Init
4. Public ROM starts / Boot Periph Init
5. Public ROM on R5 (DM) loads and starts R5 SBL and TIFS. ROM also loads their board configuration data
6. R5 SBL completes TIFS initialization by sending it a command with pointer to board configuration.

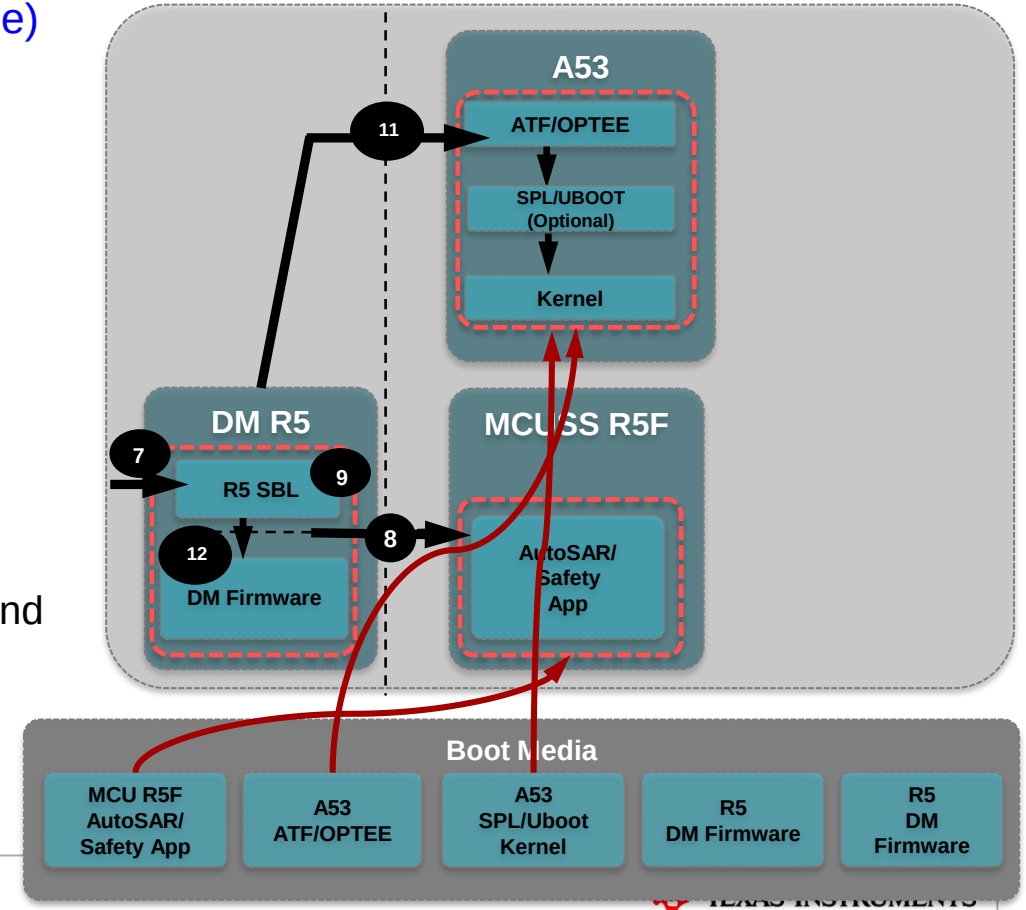
- BOOTMODE pins value is latched upon POR, and select primary and backup boot modes and peripheral configuration.
- ROM will cycle through primary and backup boot mode until security watchdog timer timeout occurs and resets the device

TI Confidential – NDA Restrictions

AM62A Sample Boot Continued

Continued Boot (core booting order flexible)

7. R5 SBL initialization sequence
8. R5 SBL load/start MCU R5F core
   - AutoSAR/Safety App runs
9. R5 SBL relocates to DDR (this step is needed to free HSM RAM)
10. R5 SBL starts HSM core (M4F_1) (see previous slide)
11. R5 SBL load/start A53 (optional for A53)
    - ATF/OPTEE runs
    - SPL/u-boot runs (skip optional)
    - Kernel runs
12. R5 SBL loads and starts DM Firmware and exits

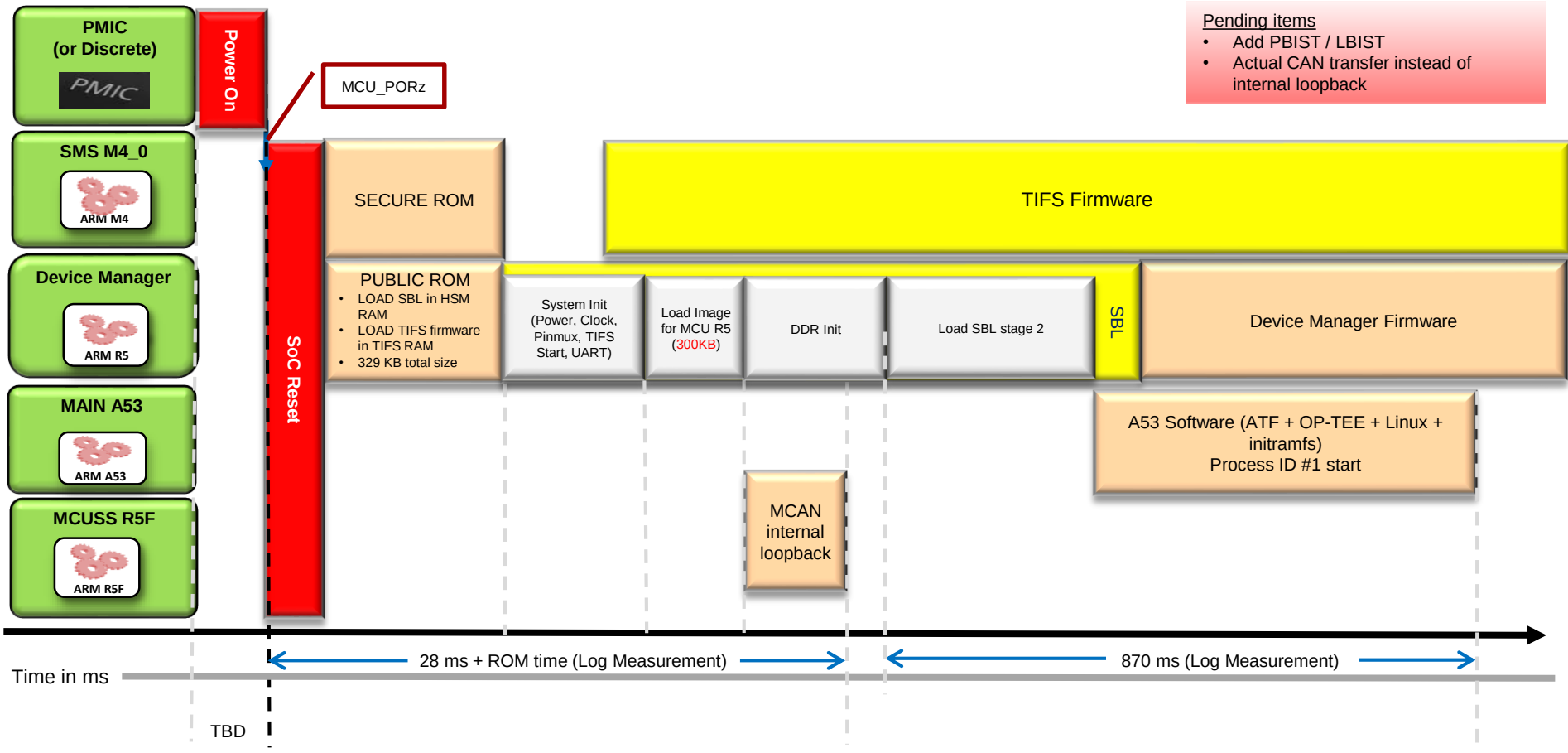


Boot timing on AM62A

TI Confidential – NDA Restrictions

Texas Instruments

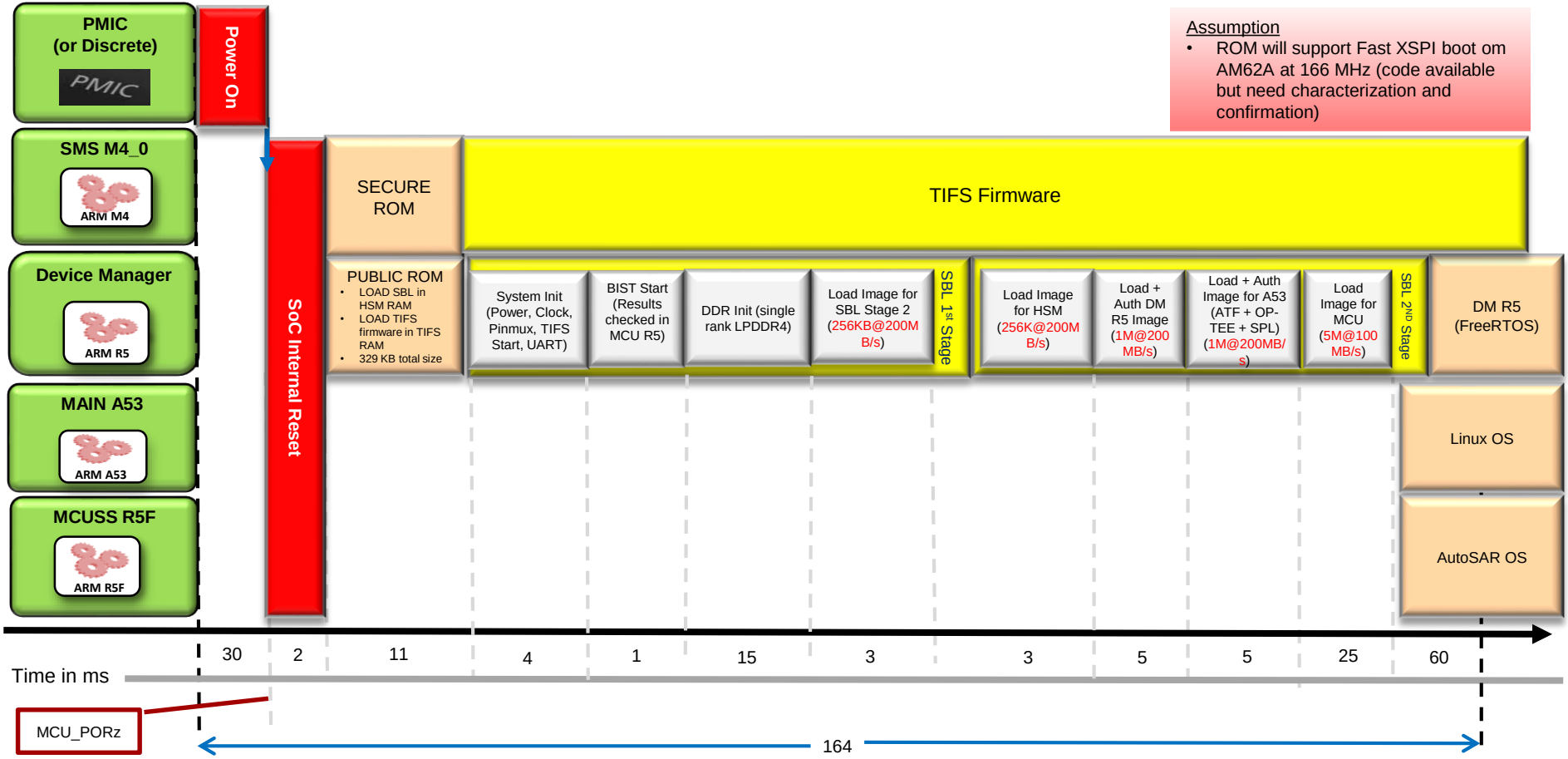
AM62A HSSE CAN response & Linux – (Measured, OSPI NOR, CAN from MCU RAM)



Pending items
- Add PBIST / LBIST
- Actual CAN transfer instead of internal loopback

TI Confidential – NDA Restrictions

AM62A CAN Response proposal (OSPI NOR, using AutoSAR in DDR)



Assumption

- ROM will support Fast XSPI boot om AM62A at 166 MHz (code available but need characterization and confirmation)

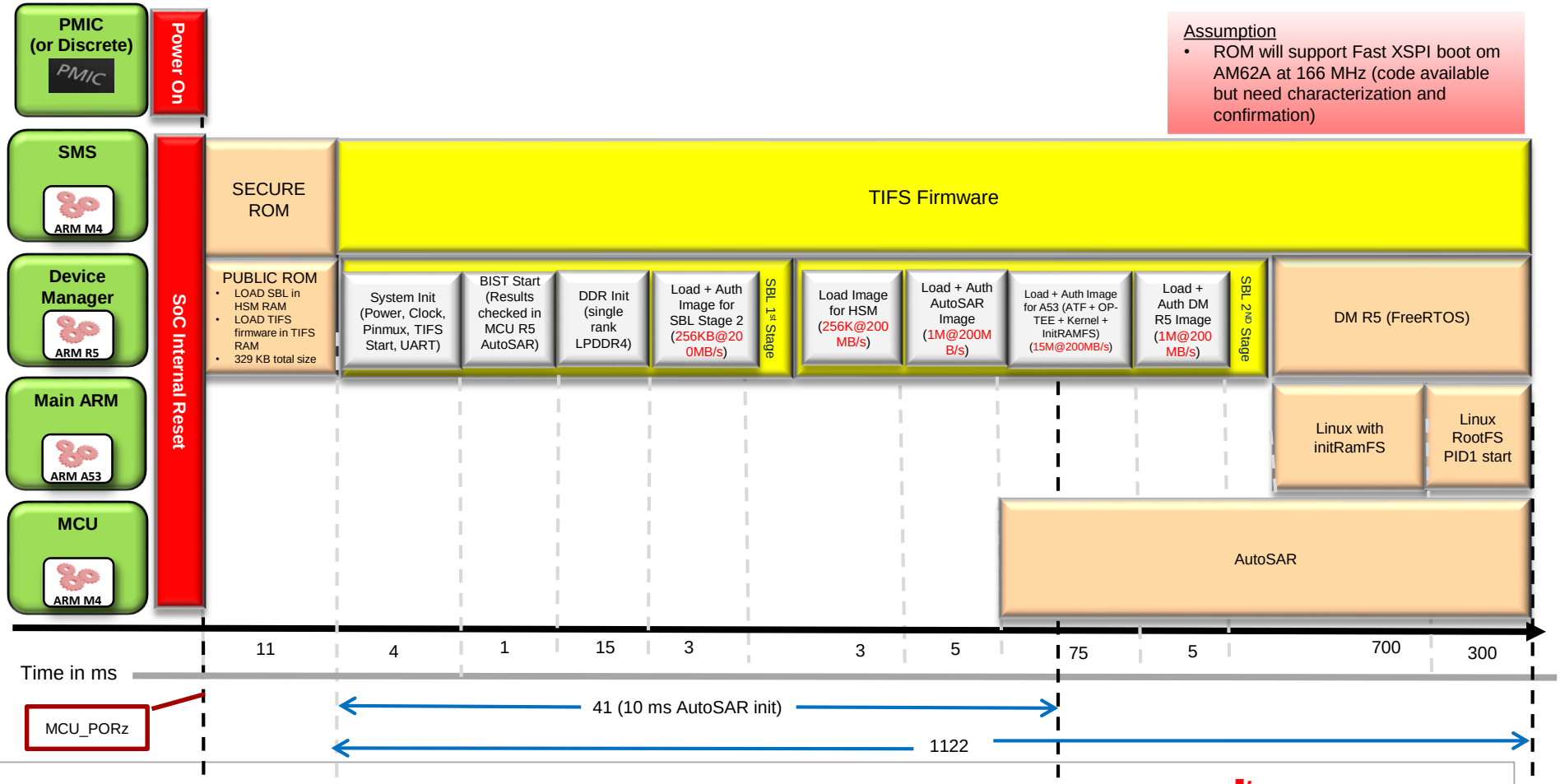
TI Confidential – NDA Restrictions

AM62A Boot Time Estimate – Breakup (using AutoSAR in DDR)

PMIC	30
SoC Reset	2
ROM (Load + Auth - 160KB TIFS + 256KB SBL, Fast XSPI boot	11
System Init	4
Start MCU LBIST/PBIST (no wait, check results in MCU R5)	1
DDR Init (single Rank, no ECC, one FSP)	15
Load + Auth SBL 2nd Stage (256K @ 200MB/s)	3
Load + Auth HSM (256K @ 200MB/s)	3
Load + Auth DM R5 (1M @ 200MB/s)	5
Load + Auth A53 (1M @ 200MB/s)	5
Load + MCU R5 (5M @ 200MB/s)	25
AutoSAR init and CAN response	60

TI Confidential – NDA Restrictions

AM62A CAN Response + Linux Boot (OSPI NOR, using AutoSAR in DDR)

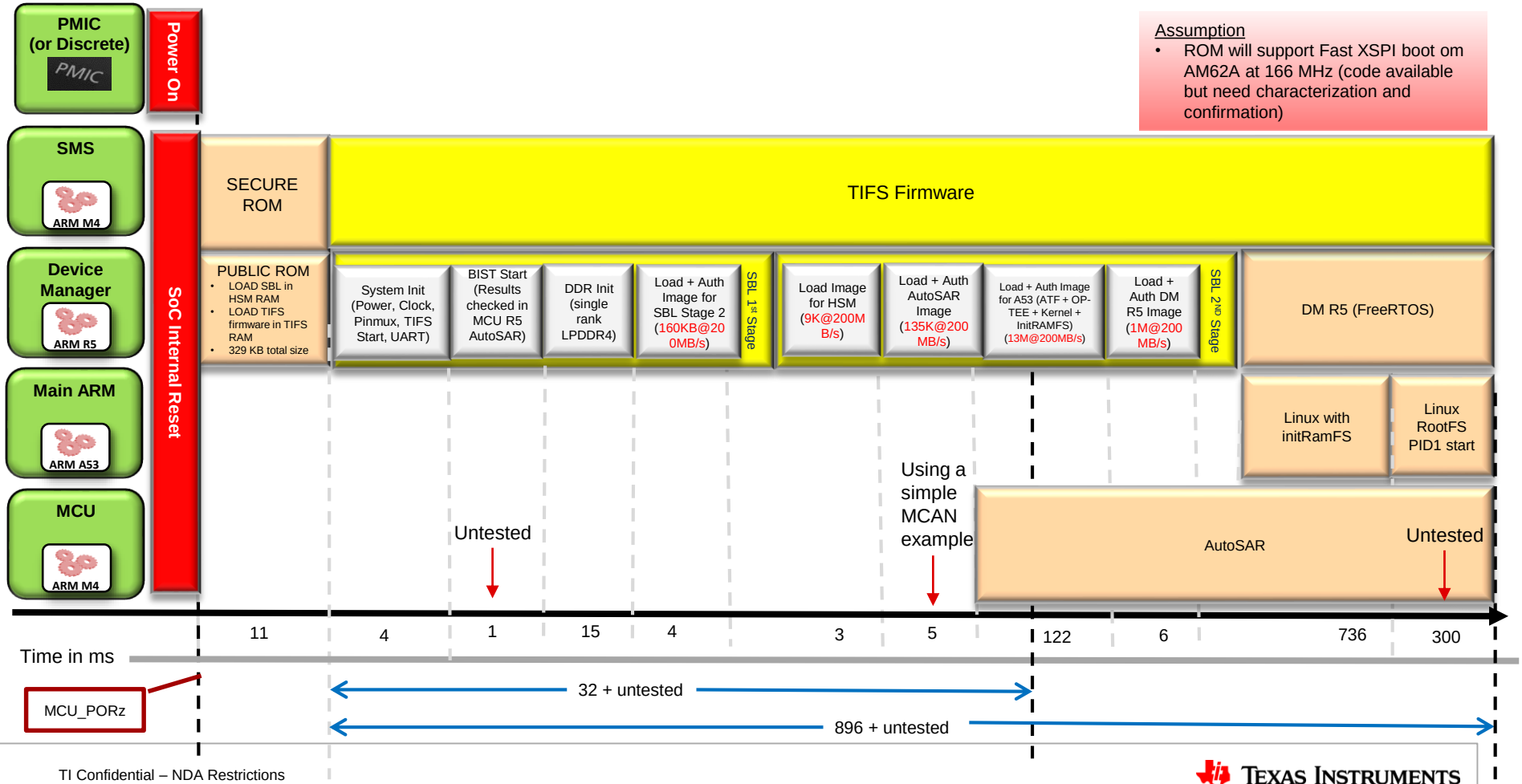


Assumption

- ROM will support Fast XSPI boot om AM62A at 166 MHz (code available but need characterization and confirmation)

TI Confidential – NDA Restrictions

AM62A CAN Response + Linux Boot (Measured, OSPI NOR, using AutoSAR in DDR)

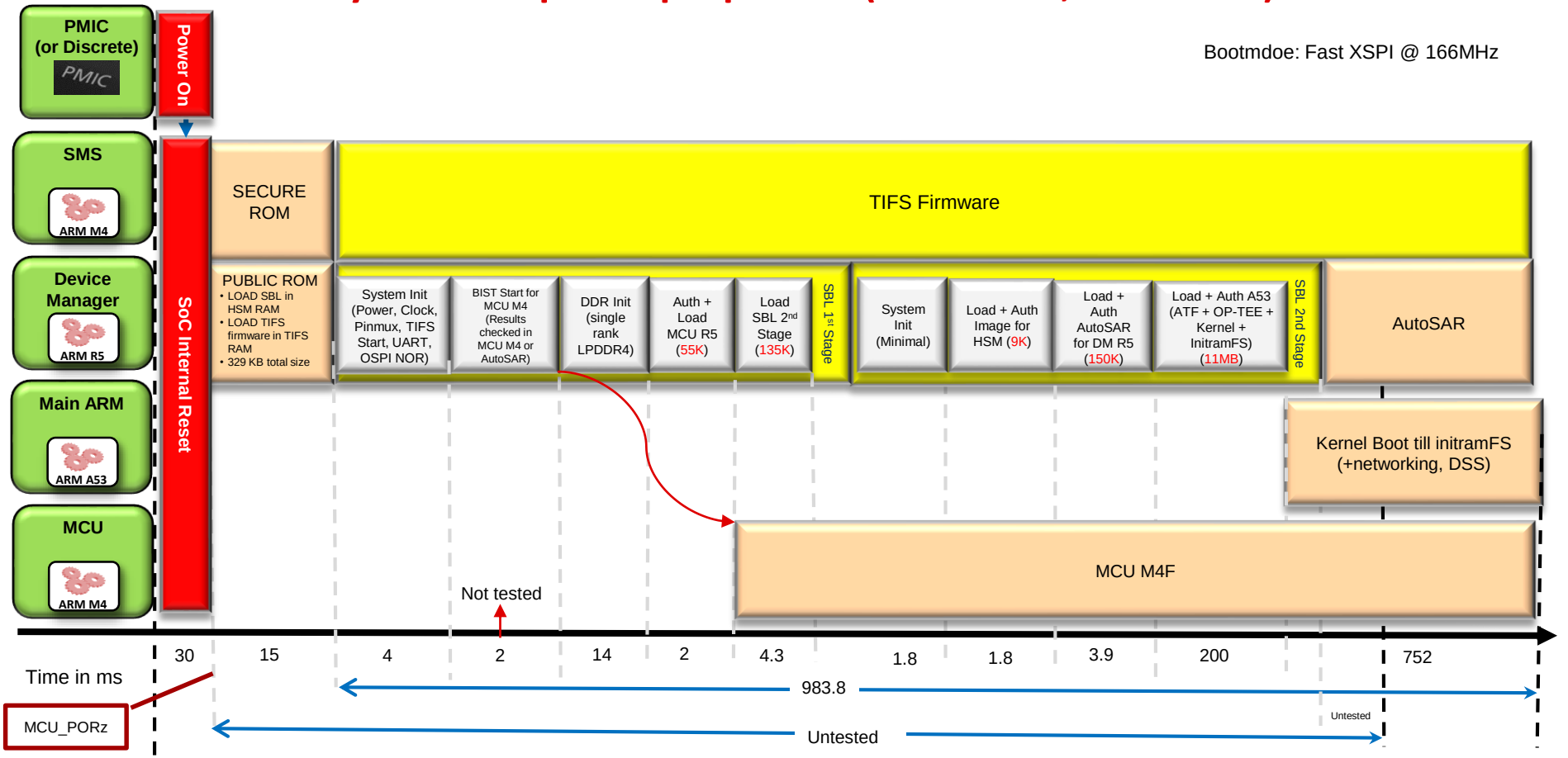


Assumption

- ROM will support Fast XSPI boot om AM62A at 166 MHz (code available but need characterization and confirmation)

TI Confidential – NDA Restrictions

AM62A HSSE Early boot Response proposal – (Measured, OSPI NOR)



TI Confidential – NDA Restrictions

AM62A Boot Time Estimate – Breakup (using MCU RAM)

PMIC	30
SoC Reset	2
ROM (Load + Auth - 160KB TIFS + 256KB SBL, Fast XSPI boot	11
System Init	4
Start MCU LBIST/PBIST (no wait, check results in MCU R5)	1
DDR Init (single Rank, no ECC, one FSP)	15
Load + Auth MCU R5 (512K @ 200MB/s)	4
Load + Auth SBL 2nd Stage (256K @ 100MB/s)	3
Application init and CAN response	10
Total	**80**

TI Confidential – NDA Restrictions

Texas Instruments

SBL Authentication Performance Improvements

Image Size	New ms (Authenticate and Move Image – aka Auth 2)
1 MB	5.5 (181 MB/sec)
2 MB	9.5 (210 MB/sec)
5 MB	22 (227 MB/sec)

SBL 1st Stage MCU R5 Authentication (Source DDR, Destination DDR)

TI Confidential – NDA Restrictions

Sitara AM6x Linux Boot time Benchmarks

Devices	eMMC Boot	OSPI Boot
AM62	1.9 seconds	1.11 seconds
AM62A	**0.96 seconds**	~ 0.8 seconds (est.)

Notes:

- Setup used AM62x SK EVM and AM62A SK LP EVM with eMMC flash (MTFC16GAPALBH)
- Quad A53 running at 1.2 GHz; OSPI : 166MHz DDR mode & eMMC at HS200 mode with 200 MHz clock with
  - **AM62** : 16 bit DDR4 at 1600M; Boot R5F : 400 MHz
  - **AM62A** : 32 bit LPDDR4 at 3200M ; boot R5F : 800 MHz **(Same as AM62P)**
- Boot scheme used was Falcon mode operation with (SPL loading the kernel directly)
- Uboot/SPL size: 335 KB Kernel size : 8MB and TinyFS (Size optimized filesystem)
- Major portion of the AM62A boot time is consumed with loading of Linux kernel image (0.6 seconds.)
- Benchmarking used non-secure silicon with boot image integrity check but with no authentication or decryption
- Boot time doesn`t account for time for PMIC settle down time and initialization before logging starts (<100ms)
- On AM62A eMMC boot, time taken from MCU_PORz going high to 1st user space GPIO toggle is 0.87 seconds. Login prompt is 1.12 seconds

Additional potential Boot time Improvement options:

- Optimized DDR HW Leveling timing
- Compression of kernel Image

3P Boot Time Optimization options

- **AOX**
- **Bootlin**
- **Lineo**

TI can provide Suspend to RAM HW reference sequence as an alternative to cold boot.

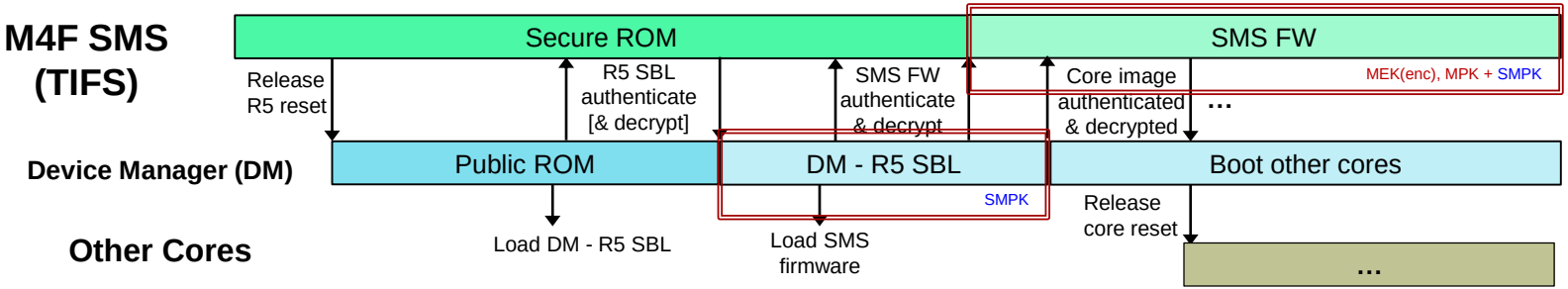
TI Confidential – NDA Restrictions

Backup slides

TI Confidential – NDA Restrictions

Texas Instruments

Secure Booting Sequence



- DM Cortex-R5 is SoC boot master
- SMS M4 Boot security / authentication
- R5 boot loader authenticated by SMS ROM
- R5 boot loader then loads/authenticates SMS runtime firmware
- R5 boot loader then continues booting other cores

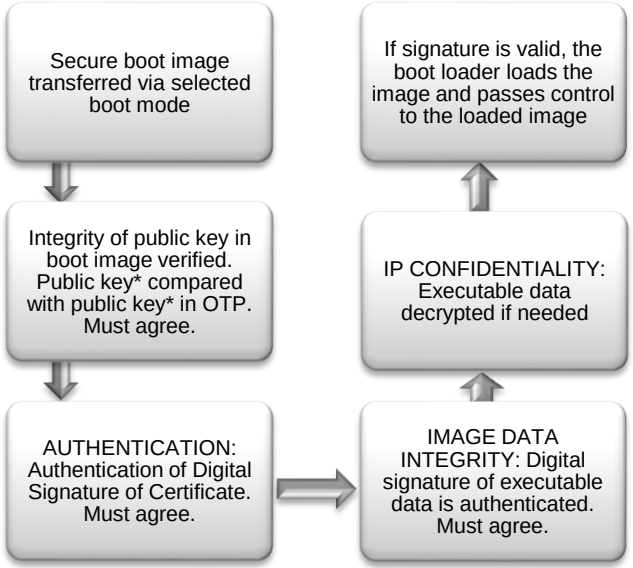
BootROM Key Features

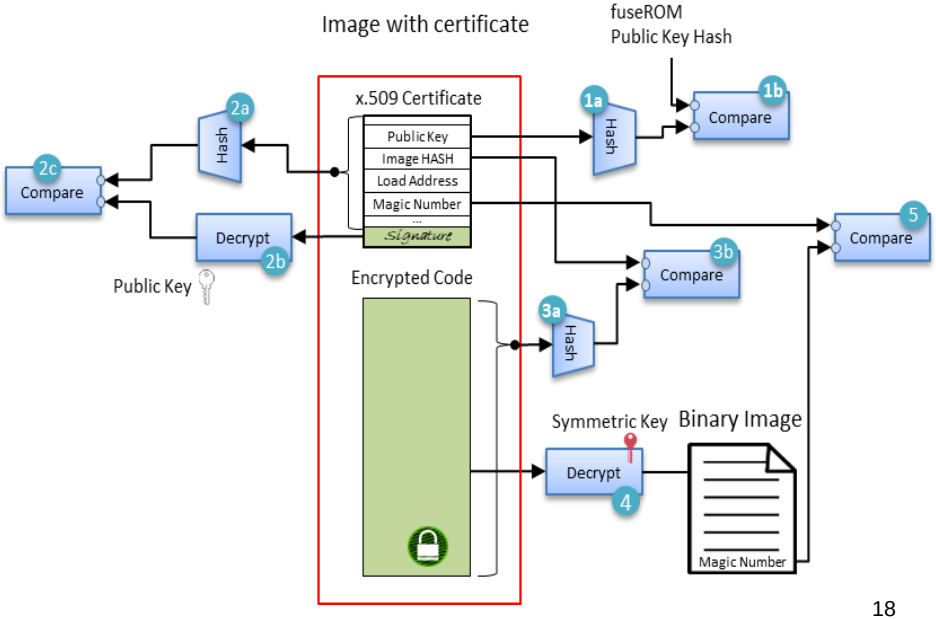
- Authentication: ECDSA (secp256, secp521), RSA(2K, 4K)
- Decryption: AES-256
- Image integrity check (SHA-512) for GP and HS device
- Back-up Customer Key Set based root of trust (when Customer Primary Key Set compromised)
- Debug flows

- Hide Secure ROM once boot is over
- Support for Customer Return Debug. Ability to hide customer assets
- Consistent Image format across all device types GP/HS-FS/HS-SE
- Image format based on open source X509 certificate

Root-of-Trust / Secure Boot / Authentication

- Asymmetric PKI – RSA-2K,3K,4K or ECC-256,384,521
  - With SHA2-512 hash and (optional) AES-256 encryption
  - SHA2-512 hash of Public Key fused into OTP bits
  - AES-256-bit key fused into OTP bits





TI Confidential – NDA Restrictions

Texas Instruments