WEBINAR

JEUDI 6 AVRIL 2023
11 H - DURÉE : 45 MIN

PHYTEC

NOUVEAU SOM STM32MP13x

- Efficience et sécurité
- Faible consommation d'énergie

RELEASE BSP STM32MP1

- Mises à jour sécurisées
- Sécurisation du STM32MP1

Denis Gilardin
Directeur Commercial
PHYTEC France

Christophe Parant
Ingénieur R & D
PHYTEC France

Kamel Kholti
Product Marketing Manager
STMicroelectronics

Nouveau SOM STM32MP13 et release BSP

Agenda

- PHYTEC en quelques mots
- Présentation STM32MP13
- SOM phyCORE-STM32MP13
- Nouveautés BSP
- Questions / réponses

PHYTEC en quelques mots

Innovations et Technologies pour les Systèmes Embarqués

34 années d'expertise

26 années en vision embarquée

370 Collaborateurs
40% d'ingénieurs et techniciens

"Made in Germany"

Maison mère et production :

- Mayence, Allemagne

Filliales:

- USA
- France
- Chine
- Inde

Product Line: SOMs, BSPs & SBCs

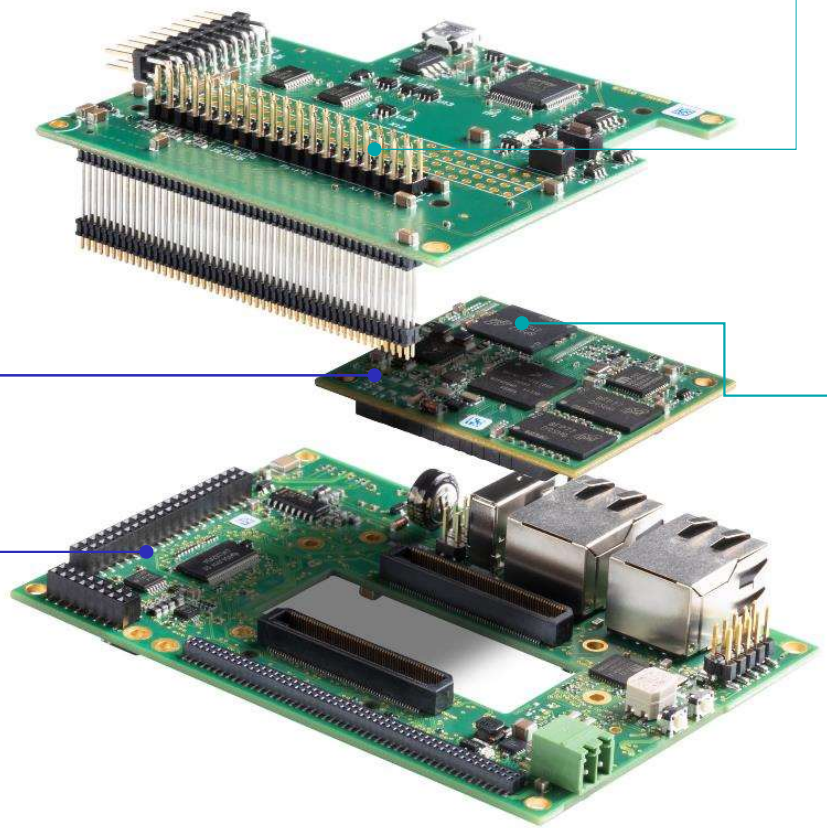
phyCORE®: solution SOM

System on Module (SOM)

- Solutions phyCORE ®
- RAM: DDR3, DDR4, LPDDR4
- Flash: eMMC, NAND, NOR
- Connectivité : Ethernet, WiFi / BT pré-certifié
- Conception robuste : PoH, EMI-resistant, PCBs multi-couches
- Interface connecteurs ou BGA

Single Board Computer (SBC)

- Solutions phyBOARD ®
- SOM + carte d'accueil = SBC
- Carte accueil propose les connectivités I/O et industrielles
- Solution prêt à l'emploi
- Plus de 15+ ans de pérennité



Technologies complémentaires

- Imagerie embarquée
- Cartes d'extension et compléments aux kits de développement (Vision, IA, Reconnaissance vocale)
- Modules RF phyWAVE
- Solutions écrans

Board Support Package (BSP)

- Linux, Android
- FreeRTOS
- QNX, VxWorks

Services & Expertise Logiciels

- Intégration Cloud (AWS, Azure)
- Machine Learning
- Mise à jour
- Sécurité (HAB, Secure Boot)

life.augmented

STM32MP135 on Phytec SoM

STM32 MPU roadmap

Positioning/price range

Sampling now

Next-gen MPU series

Big step-up in performance, networking, multimedia, AI & security

STM32MP15 in mass production

Dual Arm® Cortex®-A7 up to 800 MHz

Arm® Cortex®-M4 & GPU

NEW

STM32MP13 in mass production

Single Arm® Cortex®-A7 up to 1 GHz

Power- and cost-efficient with enhanced security

Timeline

life.augmented

STM32MP157 vs. STM32MP135 Main differences

	STM32MP157	STM32MP135
Cortex-A	2x Cortex-A7 @ 650/800MHz, 256kB L2 cache	1x Cortex-A7 @ 650/900MHz, 128kB L2 cache
Cortex-M	Cortex-M4 @ 209MHz	None
DRAM I/Fs	DDR3(L), LPDDR2, LPDDR3 32b @ 533MHz	DDR3(L), LPDDR2, LPDDR3 16b @ 533MHz
Flash I/Fs	eMMC v4.51, SD v3.01, 16b SLC NAND 8bit-ECC, Dual Quad-SPI NOR/NAND	eMMC v4.51, SD v3.01, 16b SLC NAND 8bit-ECC, Dual Quad-SPI NOR/NAND
GPU	3D GPU / OpenGL ES2.0	None
Display	Parallel 24b RGB, DSI 2x lanes	Parallel 24b RGB
Camera I/F	Parallel 14b	Parallel 16b, enhanced Camera pipe
Ethernet	1x Gbps GMAC	2x Gbps GMAC
Analog	2x 16b ADC + 2x 12b DAC	2x 12b ADC
Security	TrustZone, (T)DES, AES-256, SHA-256, MD5, HMAC, Secure Boot, 3x Tamper pins, Monitoring	TrustZone, (T)DES, AES-256 w/ SCA, SHA-256, SHA-512, SHA-3, HMAC, PKA ECC/RSA w/ SCA, OTF DDR Enc/Dec, Secure Boot, 12x Tamper pins, Monitoring

life.augmented

“

If only

I could optimize my MPU design while meeting the highest security standards!

This is where we come in

life.augmented

The best of three worlds in a cost-effective MPU

Arm® Cortex®-A7 core running up to 1 GHz

LONGEVITY 10 YEARS COMMITMENT

Accessible

- Strong, user-friendly ecosystem for STM32 MPUs (OpenSTLinux, Linux-RT, RTOS)
- PCB layout reference designs

Secure

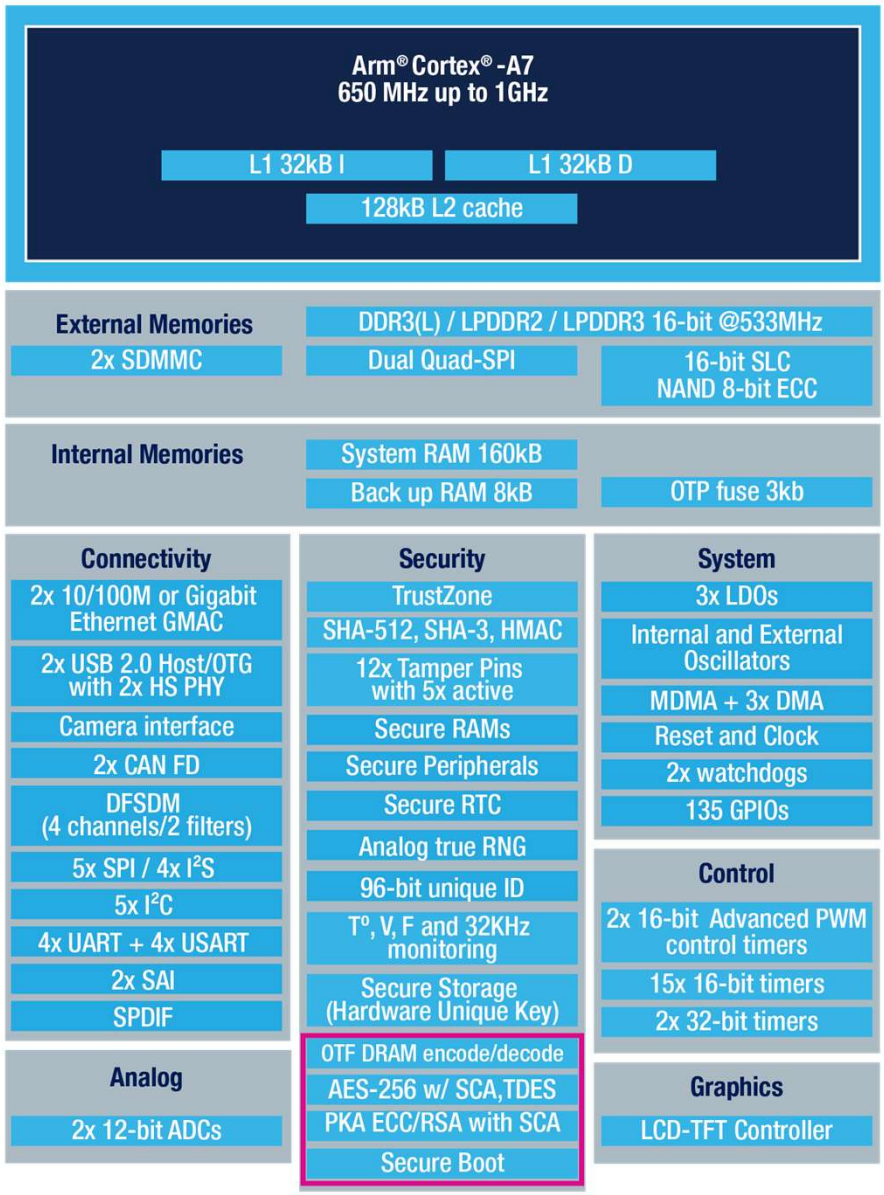
- Strong robustness
- Certified for faster time to market

Power efficient

- Best-in-class consumption in low power modes
- Over 90% energy savings in Standby and V_{BAT} modes

life.augmented

STM32MP135 block diagram



Arm® Cortex®-A7 @ 650MHz from -40°C < T_J < 125°C
Arm® Cortex®-A7 @ 1GHz from -40°C < T_J < 105°C

available for STM32MP135C and STM32MP135F only

Making your applications future proof

Industry 4.0

Factory automation

Payment terminals & secure applications

Smart metering

Smart homes

EV charging infrastructure

The right choice for your industrial applications

Industrial grade

Industrial qualification for demanding applications:

- 100% operating time for 10 years
- Junction temperature support from -40°C to +125°C

System performance

- Built on Arm® Cortex®-A7 core running from 650 MHz and up to 1 GHz
- System performances:
  - DRAM interface at 533 MHz
  - Optimized interconnect

STM32MP13 MPU offers certified security services

Memory protections
against illegal access control

Cryptographic accelerator
for hardware robustness

Platform authentication
during product lifecycle

Code isolation
for runtime protection

Security assurance level 3

Complete security ecosystem

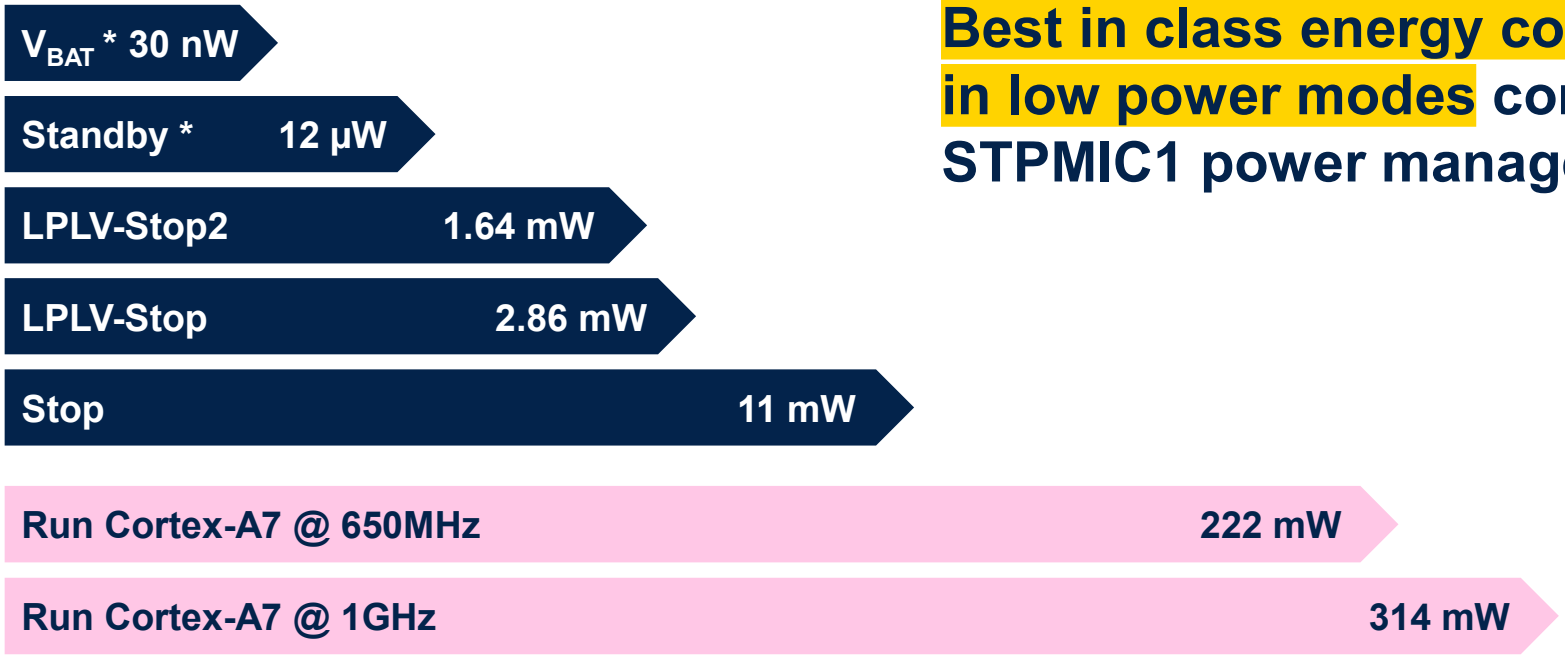
- Trusted execution with OP-TEE
- Trusted Firmware for Cortex A – TF-A
- Immutable Root of Trust
- STM32Cube framework for MPU
- Secure Secret Provisioning (SSP)
- Wide qualified partner solutions

SESIP™3

PCI ready

psacertified™ level one

STM32MP13 power consumption

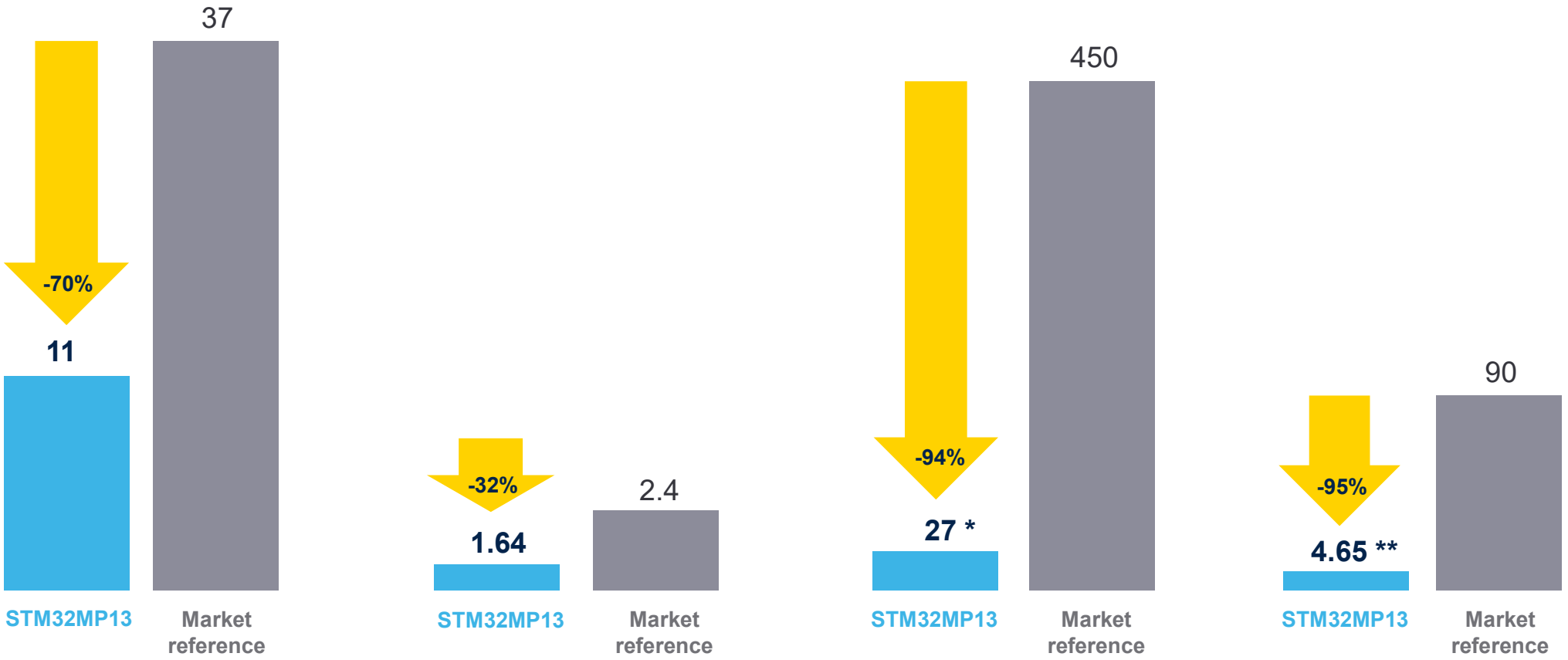


Best in class energy consumption in low power modes combined with STPMIC1 power management IC

Typ @ V_{DDCORE} = 1.25V, V_{DD} = 3.3V @ 25 °C, Peripherals OFF
* Backup SRAM, RTC, LSE/CSS, Tº monitoring OFF

life.augmented

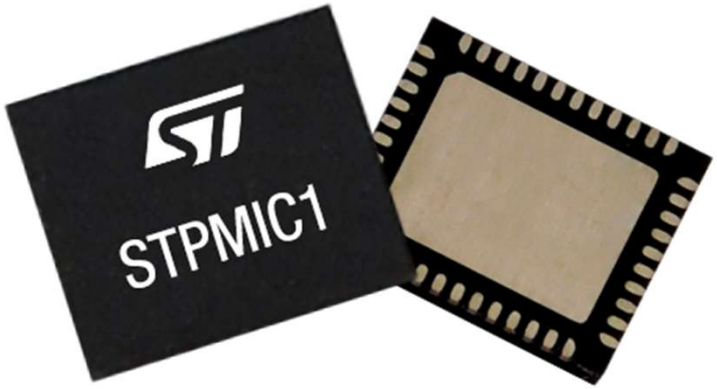
How the STM32MP13 compares to the market reference



Notes: * Backup SRAM, RTC & LSE ON // ** with RTC/Tampers & LSE ON

STPMIC1 power management IC dedicated to STM32MP1 series MPU

Simplify your design and optimize power consumption



DC/DCs & **LDOs** for
- STM32MP1 series
- Memories
- External devices

Optimized power consumption

BOM savings for typical applications

Small PCB footprint vs. full discrete solution

life.augmented

Our technology starts with You

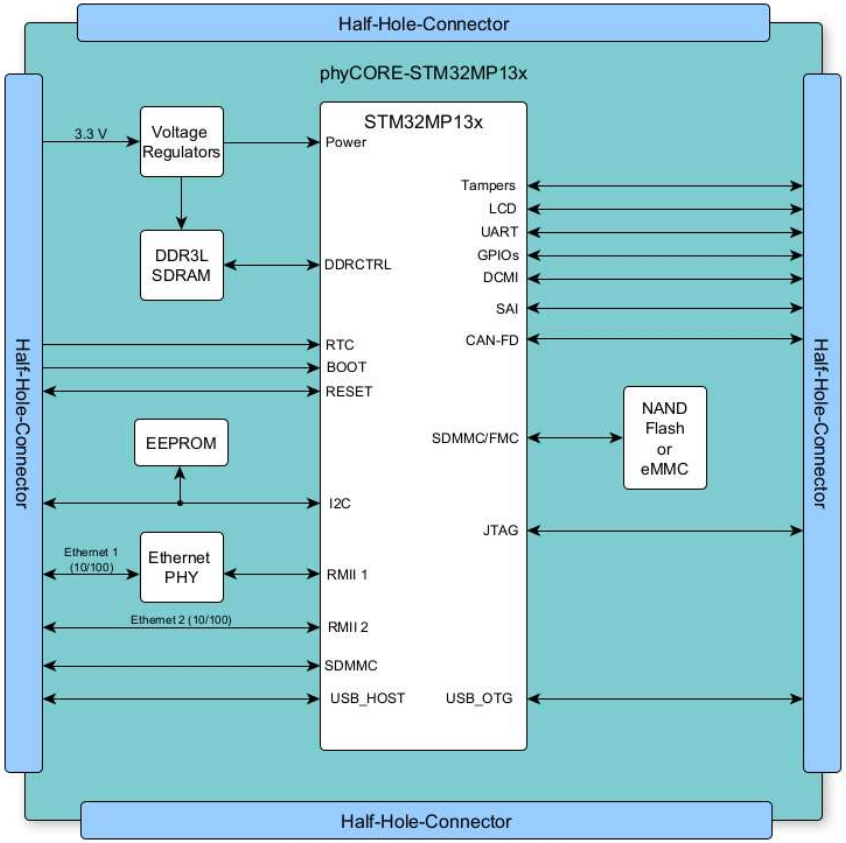
life.augmented

phyCORE ®-STM32MP135

System on Module (SoM)

Caractéristiques

- Mono-CoeurA7 650MHz à 1GHz
- Version à souder
- Graphisme : Neon + FPU
- Interface 32-Bit RAM 128MB - 1 GB (DDR3L)
- Tous les signaux processeurs disponibles sur le connecteur (sauf l'interface DDR)
- Stockage NAND Flash (jusqu'à 1GB SLC) ou EMMC (4 GB - 128 GB)
- SDMMC
- 2x10/100M/1GBits Ethernet, dont 1 PHY sur la carte
- USB HOST et OTG 2.0
- UART x4, SUARTx4
- I²C , SPII
- LCD 24 Bits
- Caméra parallèle 16 Bits
- SAI
- CAN-FD
- Sécurité :
  - ***TrustZone,*** *(T)DES, AES-256w/ SCA, SHA-256, SHA-512, SHA-3, HMAC,PKA ECC/RSA w/ SCA,OTF DDR, Enc/Dec, Secure Boot,12x Tamper pins, Monitoring*
- Autres :
  - Ultra Low Power RTC moins de 100nA
  - I²C EEPROM (4k à 32k)



phyCORE ®-STM32MP135

System on Module (SoM)

Caractéristiques (suite) :

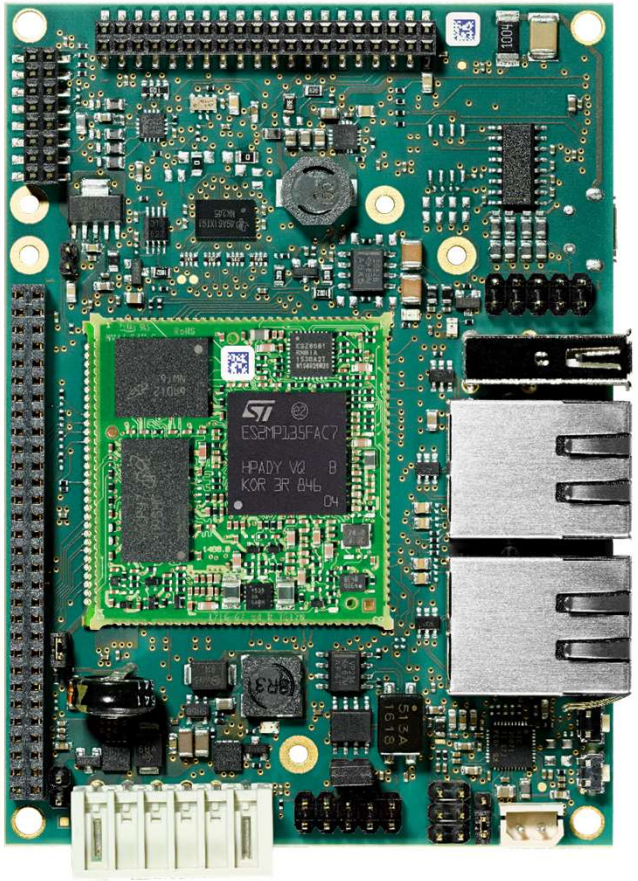
- PCL-076 STM32MP13-phyCORE-Module, soldering pin.
- Taille : 36mm x 36mm x 1,5mm
- Disponible en version étendue : -40°C/+85°C
- Poids du module : 6g
- Alimentation : 3,3 V
- Consommation : faible

- Version standard :

  phyCORE STM32MP13 Core A73 650MHz
  512MB RAM
  4GB SLC eMMC
  4kEEPROM I²C
  10/100 Mbit Ethernet PHY
  10/100/1GB Ethernet RMII
  ADC, LCD, FD-CAN

phyCORE ®-STM32MP135

phyBOARD-SEGIN - Single Board Computer (SBC)



Caractéristiques

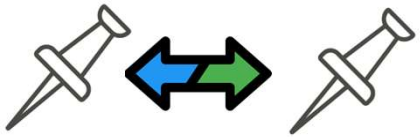
- Solution prête à l'emploi :
  - ***Pour votre évaluation***
  - ***Comme design de référence pour le développement de votre carte d'accueil spécifique***
- Interfaces reseau
- Interface **écran** : *Parallèle, écran capacitif 7''*
- Interfaces USB Host et OTG
- **Interfaces industrielles** RS232, RS485 et CAN FD (5MBit) avec leurs transceivers
- Format Pico-ITX et conçue pour les environnements industriels

phyCORE ®-STM32MP135

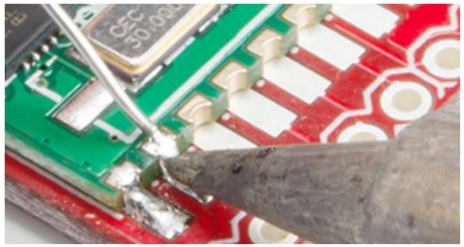
System on Module (SoM)

Compatibilité PIN-PIN avec d'autres solutions SOM PHYTEC

phyCORE-i.MX 6UL et phyCORE-i.MX 93



Possibilité de développer avec une solution cost-effective et évoluer vers une solution plus performante.



Solder On Module: Simple Castellated Edge solder Technology

- Solution à coût optimisé
- Hauteur minimale (3mm)
- Pose facilitée
- Carte d'accueil optimisée en complexité et coût : PCB 4 couches

Solution complète en réponse aux attentes des applications du domaine de la sécurité et de la cybersécurité

phyKNOX-Distro

phyCORE ®-STM32MP135

System on Module (SoM)

Roadmap :

Présentation Embedded World 2023

Finalisation PIN-MUXING en cours

BSP : fin Q2/2023

Disponibilité : Q3/2023

BSP STM32MP1

Caractéristiques

- **OpenSTLinux v4.1.0**:
  - Yocto Kirkstone (4.0) (**LTS**)
    - Sécurité renforcée dans Weston (utilisateur spécifique autorisé)
    - STM32MP1:
      - Gestion du **F**irmware **U**pdate (**FWU**)
      - **F**irmware **I**mage **P**ackage (**FIP**): Secure Monitor, u-boot
      - Support du STM32MP13
  - TF-A 2.6
    - Firmware update
    - Paramétrage de la “Chaîne de Confiance” via le “**F**irmware **C**onfiguration **F**ramework” (FCONF)
  - U-boot 2021.10
  - Linux 5.15 (**LTS**) : compatible **RT-Linux** (**X-LINUX-RT** OpenSTLinux Expansion Package)

- **Outils:** STM32CubeMP1 v1.6.0 (Arm® Cortex®-M4), STM32CubeMX v6.7.0 , STM32CubeIDE v1.11.0
  - webinaire *"Mise en oeuvre de la solution MPU / MCU du STM32MP1"* https://www.phytec.fr/societe/videos-webinaires
- **Evolution Phytec:**
  - Renommage des device tree (pour conformité “upstream”)
  - u-boot : création d’une config PHYTEC “phycore-stm32mp1”

https://download.phytec.de/Software/Linux/BSP-Yocto-STM32MP1/BSP-Yocto-OpenSTLinux-STM32MP1-PD23.1.0/ReleaseNotes

BSP STM32MP1

Secure boot

- Garantie l'intégrité et la sécurité de la plateforme au moment de l'exécution

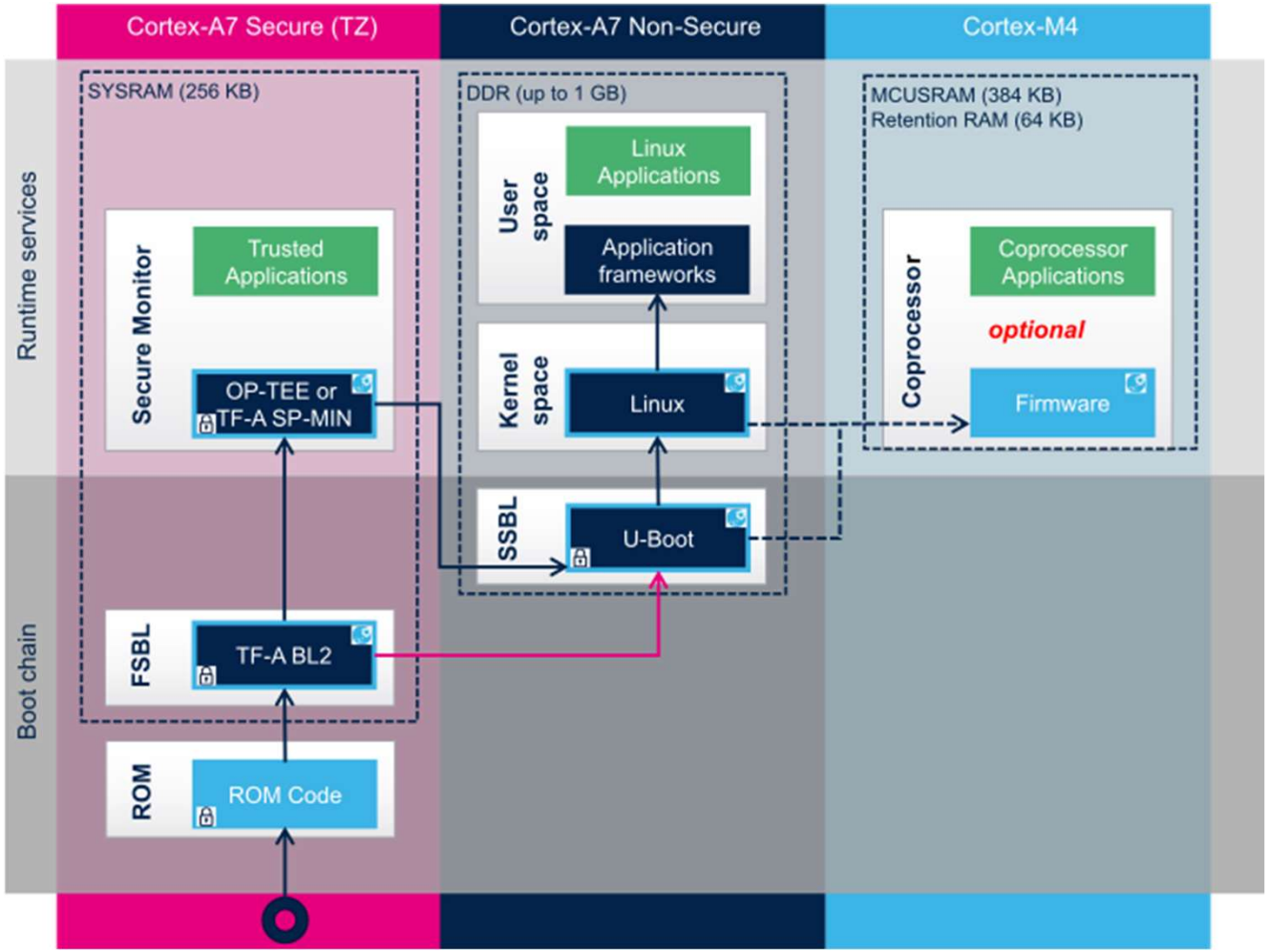
- **Trusted Boot chain: Code ROM** et fonctions de sécurité de **TF-A** (**Trusted Firmware-A**):
  - Vérification de l'**intégrité** (hachage) et **authentification** (cryptographie asymétrique) des composants logiciels => minimum pour le secure boot
  - **Décryptage** du binaire crypté chargé (optionnel avec **STM32MP13**)
  - Configuration de la plate-forme: périphériques sécurisés, capacité débogage (exécution sûre)

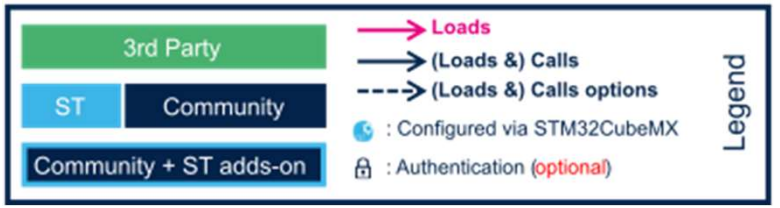
- Bloc de Hardware de cryptographie: HASH, AES, **SAES, PKA** (**STM32MP13**)
- **Arm® TrustZone**: isolation entre "**normal world**" (applications) et "**secure world**" (applications de confiance et services sécurisés). Pare-feu d'interdiction d'accès à des périphériques.

- **TF-A :**
  - Bootloader open source recommandé (**secure boot** et **contrôle d'accès aux périphériques**)
  - Implémentation de référence de logiciel "secure-world" fourni par Arm®
  - Conçu pour Armv8-A. Adapté par STMicroelectronics pour Armv7-A.

BSP STM32MP1

Trusted Boot Chain





Bootloaders:

FSBL: First-**S**tage **B**oot **L**oader

SSBL: Second-**S**tage **B**oot **L**oader

Moniteur de Sécurité :

TF-A SP-MIN: minimal secure monitor (services limités)

OP-TEE: Secure OS (recommandé) utilisé par défaut pour le STM32MP13

FIP:

SP-MIN / OP-TEE + U-Boot
+ FW CONFIG + HW CONFIG (device tree)

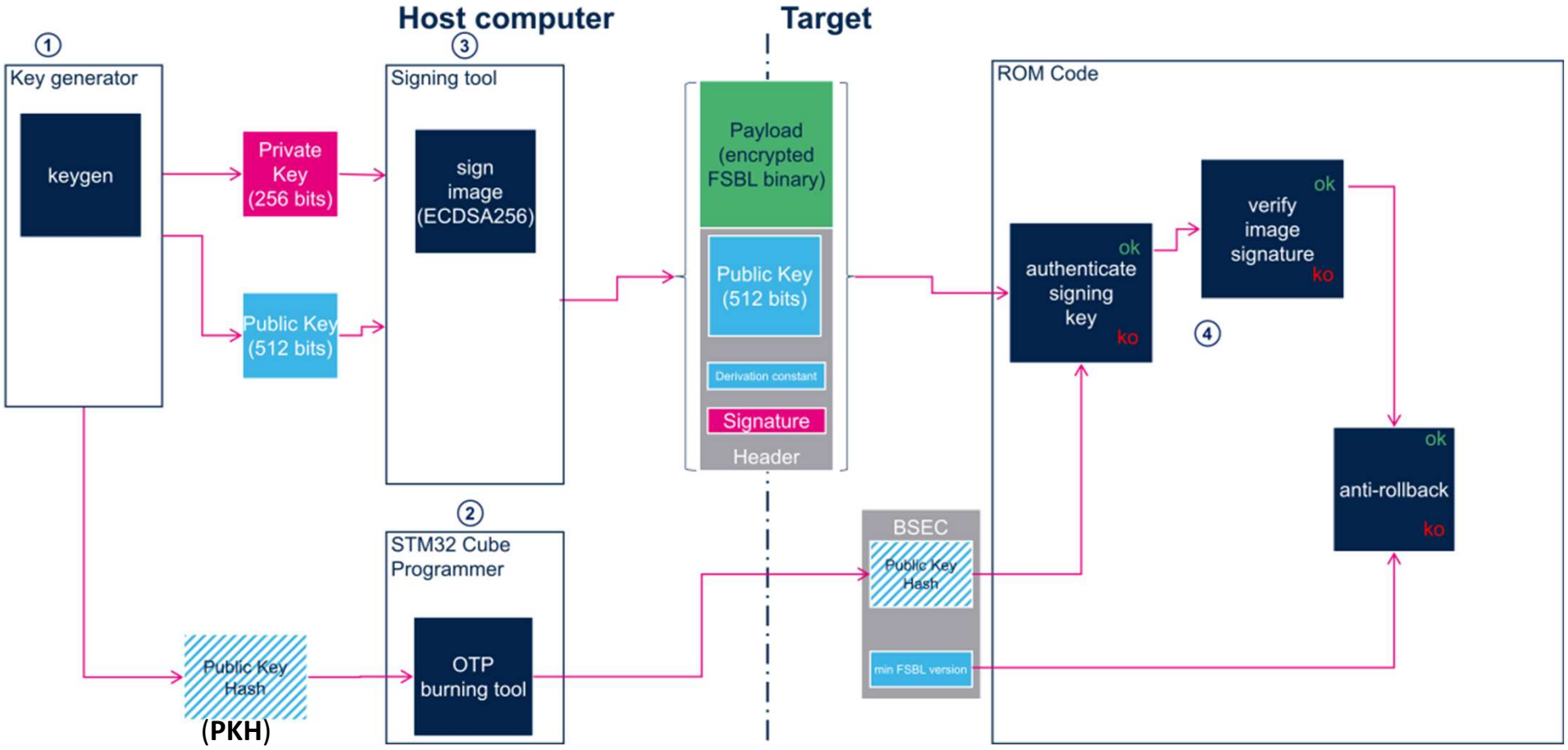
Nouveau STM32MP13 :

- Révocation de clés d'authentification (x8 clés)
- Cryptage FSBL
- Accélération Hardware (PKA, SAES)
- Zone DDR cryptée (“on the fly” crypt/decrypt)

BSP STM32MP1

code ROM - secure boot (STM32MP15)

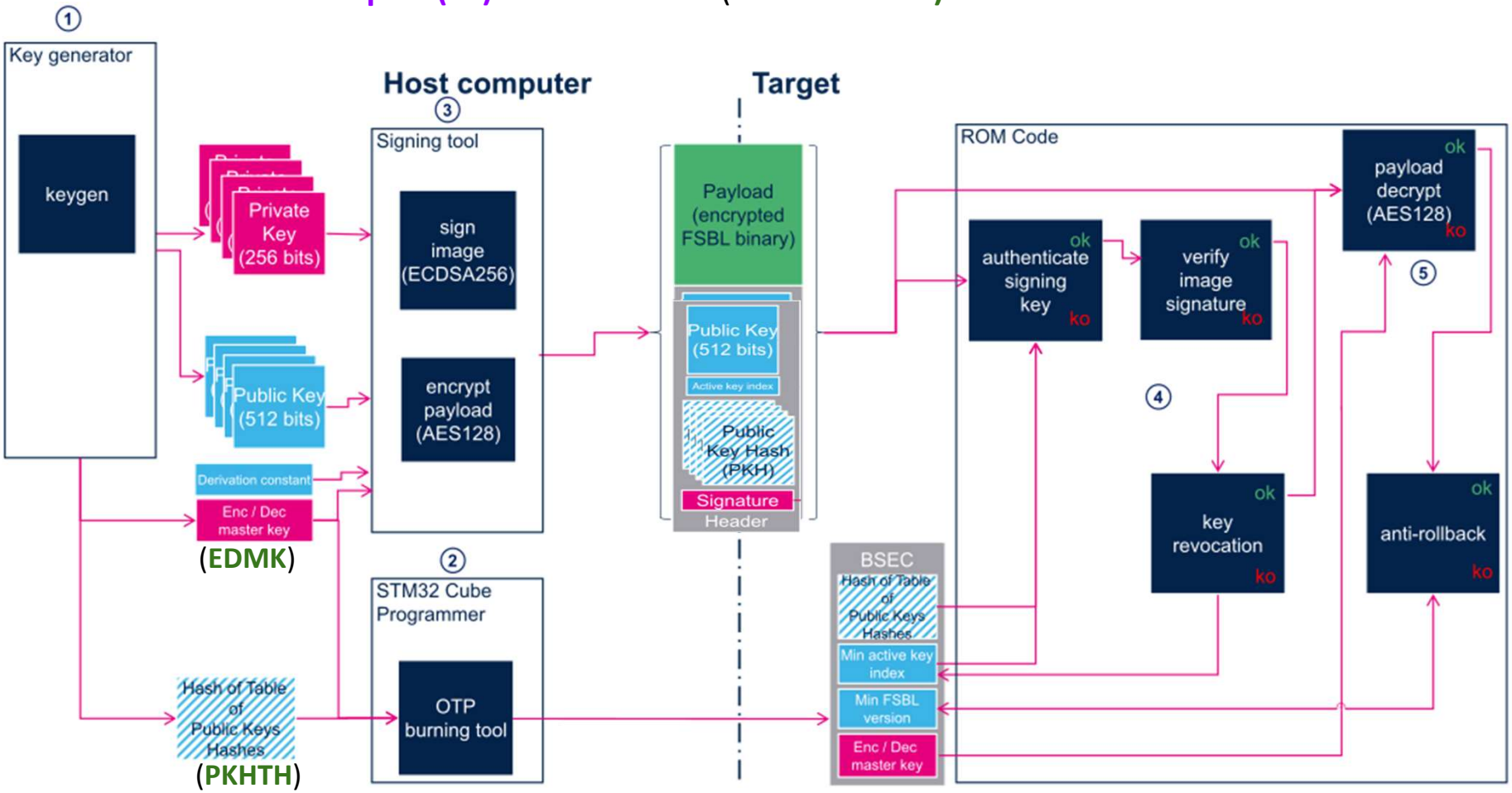
Algorithme de signature numérique (**ECSDA**)



BSP STM32MP1

code ROM - secure boot (STM32MP13)

Idem STM32MP15 + **clés multiples (x8) et révocation** (+ **chiffrement**)



BSP STM32MP1

TF-A Trusted Board Boot (TBB)

- Exigences TBB spécifiées par Arm® (suit Standard **X509.v3**)
- **P**ublic **K**ey **I**nfrastructure (**PKI**) : "**C**hain **O**f **T**rust" (**CoT)**

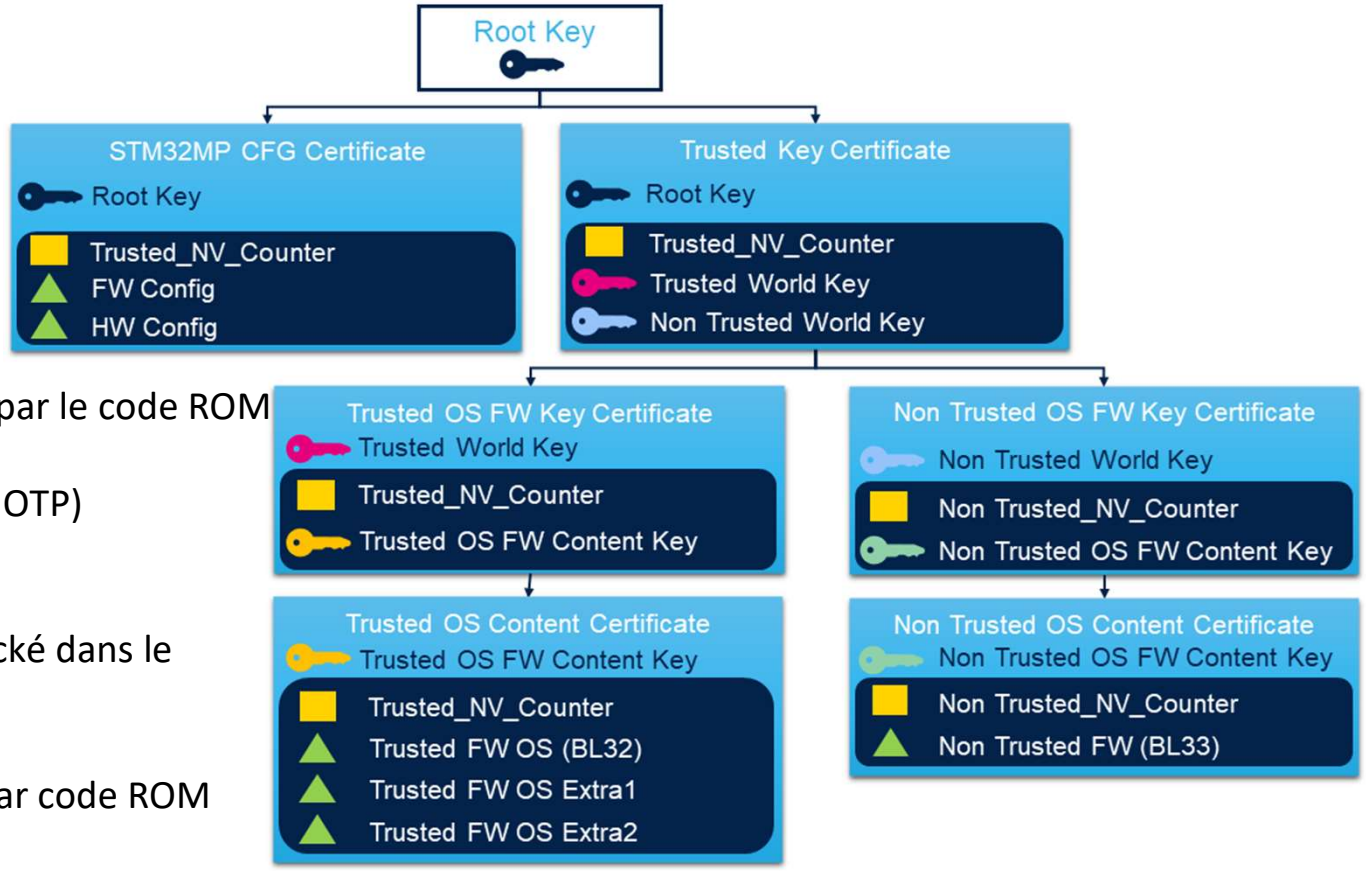
- Clés et Certificats embarqués dans le **FIP**
- avec compteur Non-Volatile: **anti-rollback** (dans Registre "Tamper")

- Chaîne de certificat définie par device tree du TF-A: fdts/stm32mp1-cot-descriptors.dtsi

- Défaut: même clé publique que celle utilisée par le code ROM
- STM32MP1**5**:
  - ROTPK vérifié par rapport à la **PKH** (en OTP)

- STM32MP1**3**:
  - ROTPK vérifié par rapport à la **PKH** stocké dans le TF-A BL2 Header.
  - Cryptage du FIP
    défaut: même clé de cryptage utilisé par code ROM (**EDMK** en OTP)

Root Of Trust Public Key (ROTPK)



BSP

Etapes pour activer le Secure Boot

1. Générer des clés d'authentification
   => **STM32 KeyGen tool**

2. Générer des clés de chiffrement (**optionnel STM32MP13**)
   => **STM32 KeyGen tool**

3. Enregistrer les clés dans les **OTP** (fusibles) du MPU (“**provisionning**”)
   => via **u-boot** ou STM32CubeProgrammer

4. Signer le TF-A et FIP
   => TF-A: **STM32 Signing tool**
   => FIP: **à la génération du FIP (yocto)**

5. Fermer le device (fusible spécifique de l’OTP)
   => exemple: commande **“stm32key close”** via **u-boot**

BSP

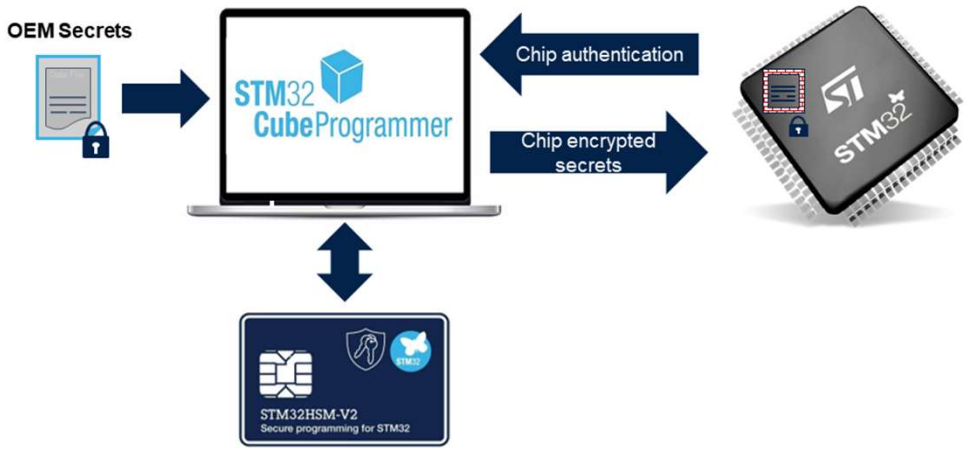
SSP (**S**ecure **S**ecrete **P**rovisionning) - STM32MP15 ou MP13

- Génération d'un fichier crypté **.ssp** ("OEM secrets"):
  - Clés d'authentification OEM (voir de chiffrement)
  - Mot de passe RMA
  - Secrets OEM

  => **STM32 Trusted Package Creator**

- Enregistrement des clés publiques dans les OTP (fusibles) du MPU (**"secret provisionning"**):

  => Sécurisé via firmware **TF-A SSP** (TF-A réduit) :
  => STM32CubeProgrammer
  + smartcard HSM (**H**ardware **S**ecurity **M**odule)



BSP STM32MP1

Secure Firmware Update: Partitionnement

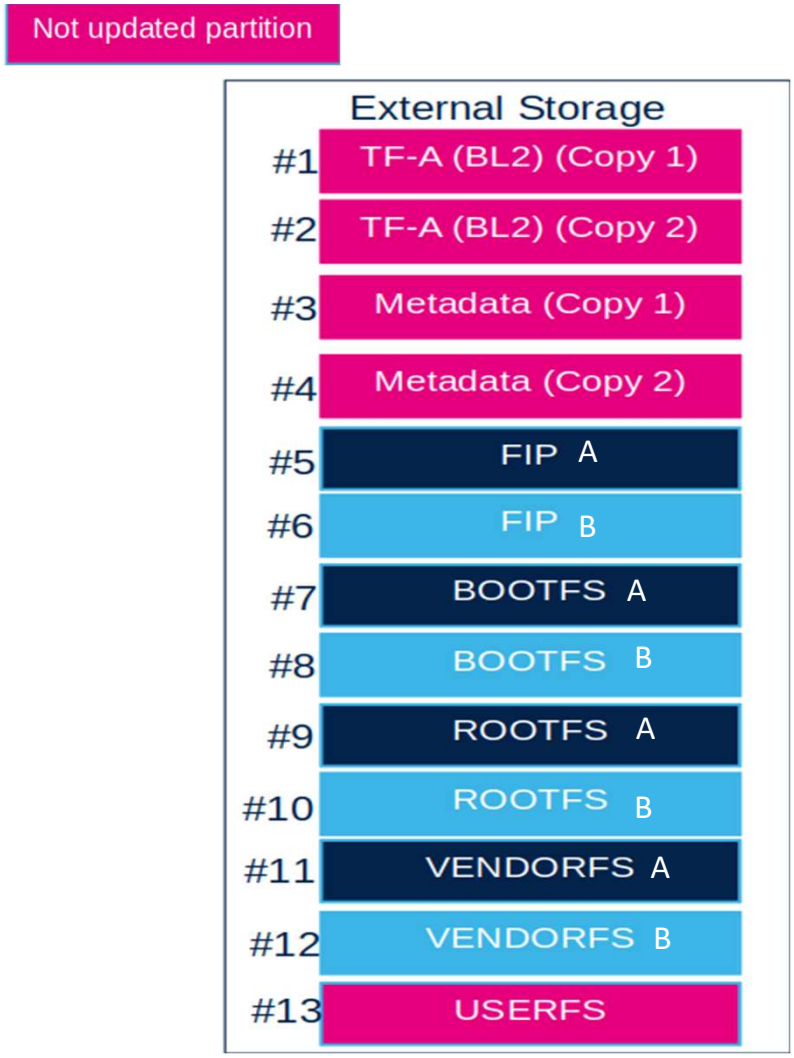
- Mise à jour du **bootloader FIP** (OP-TEE / TF-A SP-MIN, U-Boot,)
- Démarrage du dernier FIP fonctionnel après N tentatives (watchdog)

- **TF-A**:
  - Non mis à jour
  - Gère la mise à jour par lecture/écriture des metadata

- **Metadata**:
  - Non mis à jour
  - Variables partagées entre Linux et TF-A
    - **active_index** (A ou B)
    - **previous_index** (A ou B)

- **Système symétrique A/B**
  - Partitions dupliquées (“FIP A”, “FIP B”, “rootfs A”, “rootfs B”, …)
  - Partition FIP à charger identifiée par metadata
  - Autres: U-boot (scripts), Linux (gestionnaire de mise à jour)

- **Userfs:**
  - Données persistantes lors des mises à jour



BSP STM32MP1

Secure Firmware Update: Principe

1. La **partition A** est utilisée.
   Une demande de mise à jour est reçue (serveur FOTA, …)

2. Gestionnaire de mise à jour (sous **Linux**):
   a. télécharge l'image et programme **partitions B**.
   b. met à jour les metadata: **active_index =1**
   c. lance un redémarrage du système.

3. TF-A:
   a. active le compteur de boot (**BOOT_COUNT**)
   b. charge la partition FIP en fonction de l'index actif (**FIB B**)

4. Gestionnaire de mise à jour (si **démarrage avec succès** de Linux depuis la **partition B**):
   a. met à jour les metadata: **previous_active_index =1**

5. En cas d'**échec de démarrage**:
   a. TF-A incrémente le compteur de boot à chaque reboot (watchdog)
   b. Après **N échecs** de démarrage TF-A met à jours les metadata pour booter sur la **partition A**: **active_index = 0**

BSP STM32MP1

Secure Firmware Update: Mise en oeuvre (“FOTA”)

- Solutions existantes: RAUC, Mender, OSTree, …

- Solution proposée pour les BSP Yocto PHYTEC:
  - **RAUC** (**R**obust **A**uto-**U**pdate **C**ontroller)
  - Serveur de déploiement : Eclipse **Hawkbit** (open sources)
  - Solution clé en main: PHYTEC + Connagtive IoT Device Suite

- Webinaire *"Faire vivre sa solution embarquée, gestion à distance et mise à jour logicielle"* https://www.phytec.fr/societe/videos-webinaires

Roadmap BSP PHYTEC STM32MP1

- 7 mars 2023: PD23.1 (phyCORE-STM32MP15)
- **Juin 2023:** PD23.2
  - Support du **phyCORE-STM32MP13** et **phyBOARD-Segin**
  - Mise à jour avec **RAUC / Hawkbit**
  - **OP-TEE**
- **Q4**: PD23.3: OpenSTLinux **v5** (kernel 6.x , …)

Nouveau SOM STM32MP13 et Release BSP

Questions / Réponses

PHYTEC

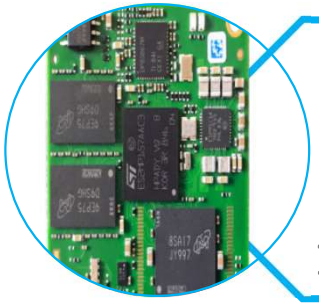
+33 (0)2 43 29 22 33

info@phytec.fr

sales@phytec.fr

support@phytec.fr

Nos prochains rendez-vous



Journée Technique

- Imagerie embarquée
- Sécurité

1er Juin 2023 Novotel -Massy