Développement d'une chaîne de boot sécurisée

Rapport de stage à Prove & Run

Dorian Lesbre
Supervisé par Patrice Hameau

Mars - Juillet 2020

Plan

1. Description du bootloader
2. Algorithmes cryptographiques
3. Chaînes de confiance
4. Notes d'implémentation

Description du bootloader

Fonctionnalités souhaitées

Pour servir d'origine à la chaîne de confiance :

- Vérifier l'intégrité du processeur et de la mémoire
- Vérifier l'authenticité du noyau et le lancer
- Mettre à jour le noyau
- Être robuste

Les processeurs i.MX

Deux mémoires :

- OTP (one time programmable)
- flash

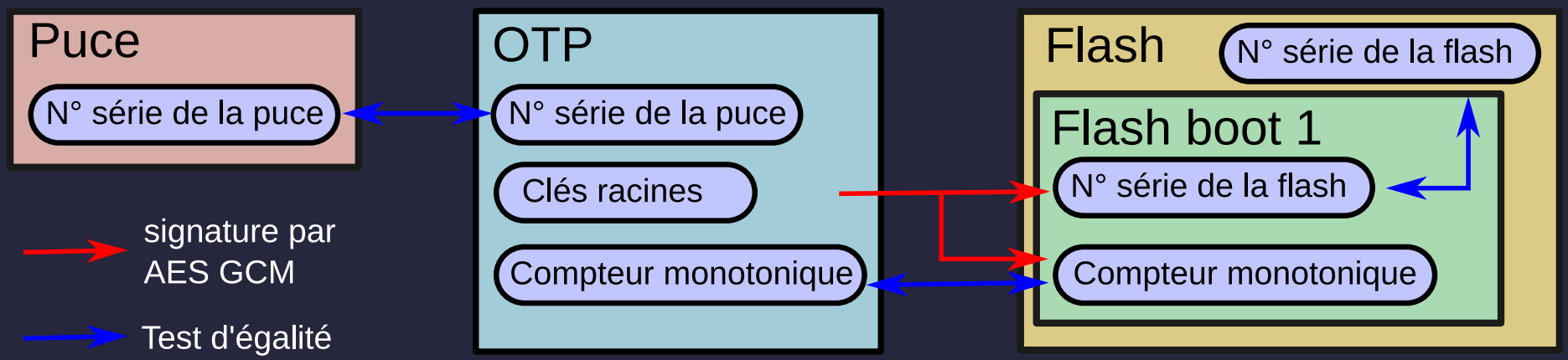
Des modules de sécurité :

- accélérateur cryptographique (CAAM)
- module de boot sécurisée (HAB)

Séquence de boot standard

1. Vérifier le hardware
2. Vérifier le code et le charger en mémoire
3. si échec, réinitialiser la puce
4. si échec persistant, installer une ancienne version du code

Séquence de boot standard



Vérification du hardware lors d'une séquence de boot

Séquence de mise à jour

Le code est stocké dans 3 emplacements mémoires :

- slot 1 - version courante
- slot 2 - nouvelle version
- slot 3 - ancienne version

Séquence de mise à jour

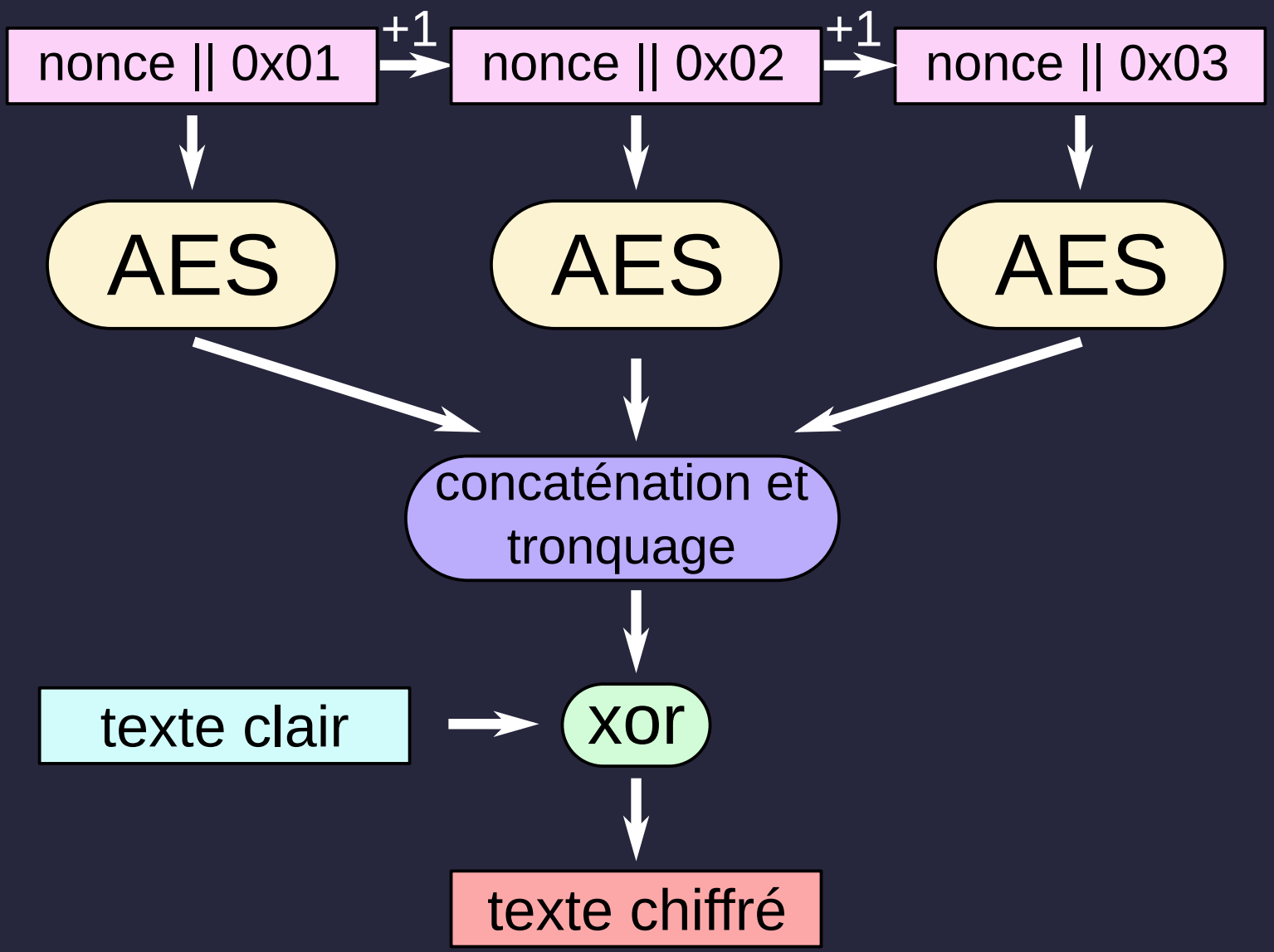
1. vérifier le code des slot 1 et 2
2. enregistrer l'état "backup"
3. copier $1 \rightarrow 3$
4. enregistrer l'état "install"
5. copier $2 \rightarrow 1$
6. enregistrer l'état "done"

Algorithmes cryptographiques

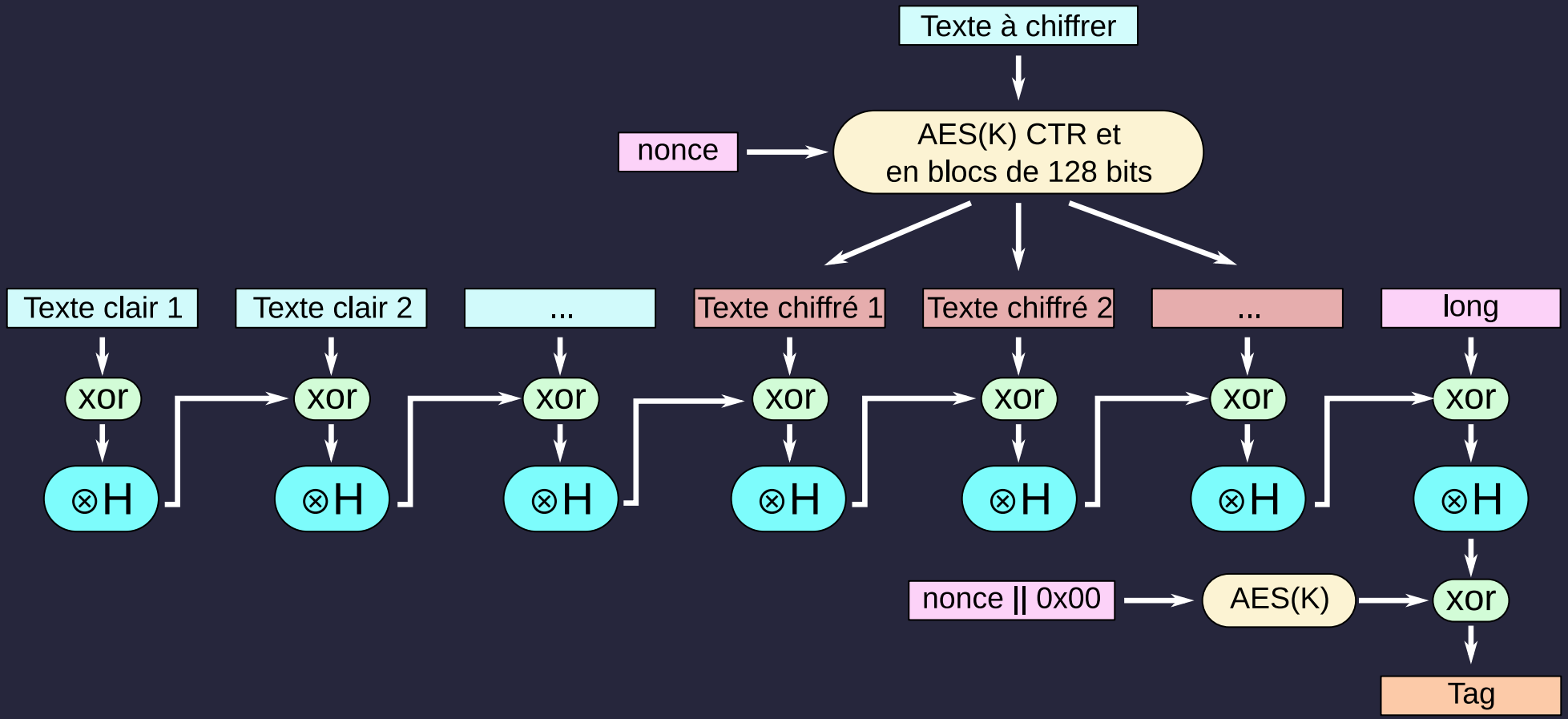
AES

- algorithme de chiffrement symétrique
- opère sur des blocs de 128 bits
- principal algorithme utilisé en interne

AES en mode CTR



AES en mode GCM

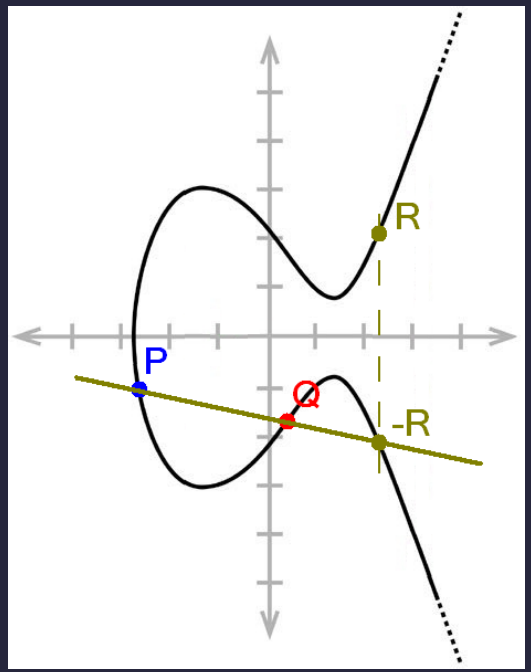


Cryptographie sur les courbes elliptiques

Courbes d'équation

$$y^2 = x^3 + ax + b$$

munies d'une loi additive



Cryptographie sur les courbes elliptiques

Cryptographie asymétrique : à clé publique et privée.

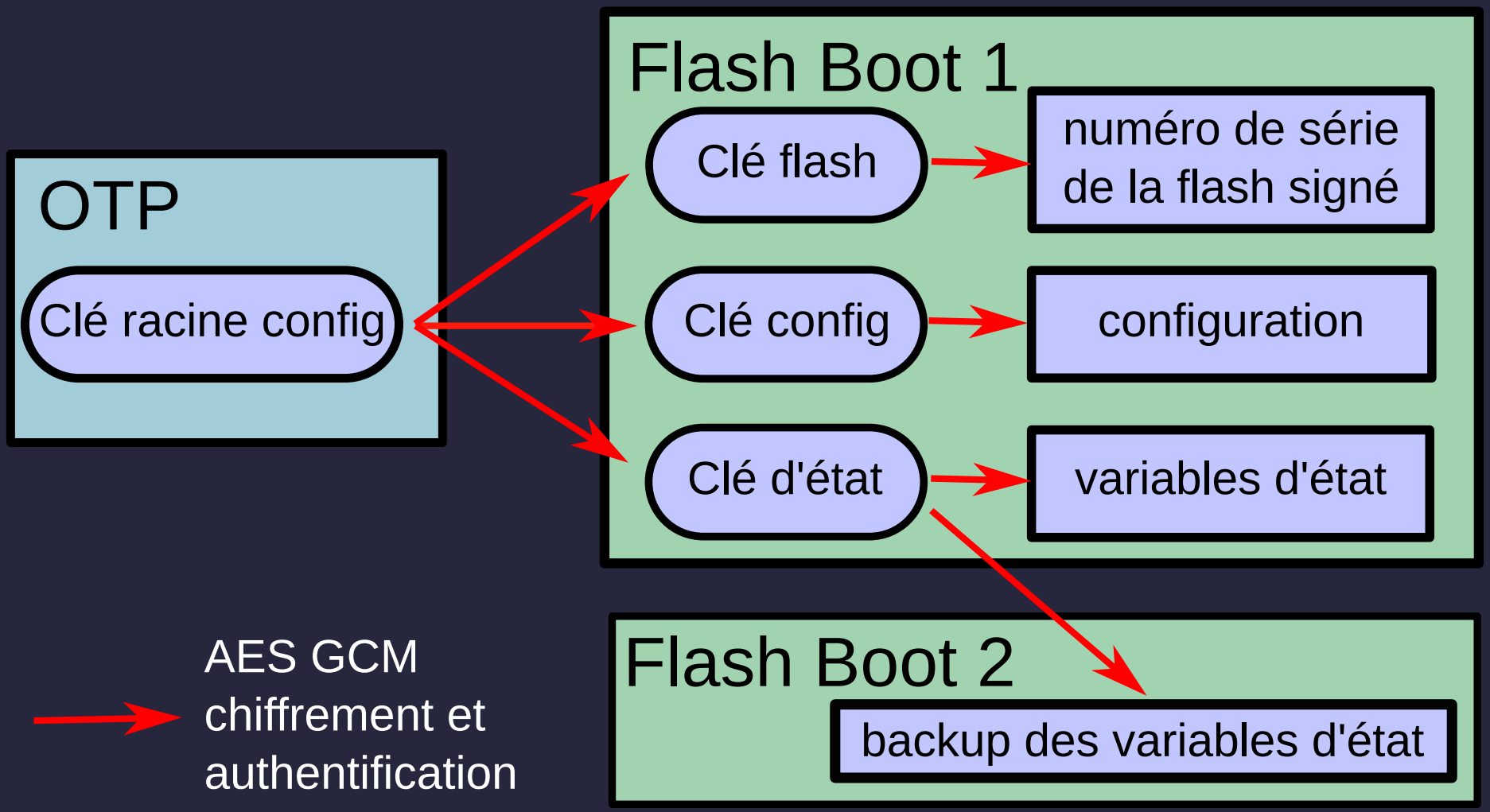
- la puce diffuse sa clé publique au 1er boot
- la puce a une liste des clés autorisées.

Deux algorithmes :

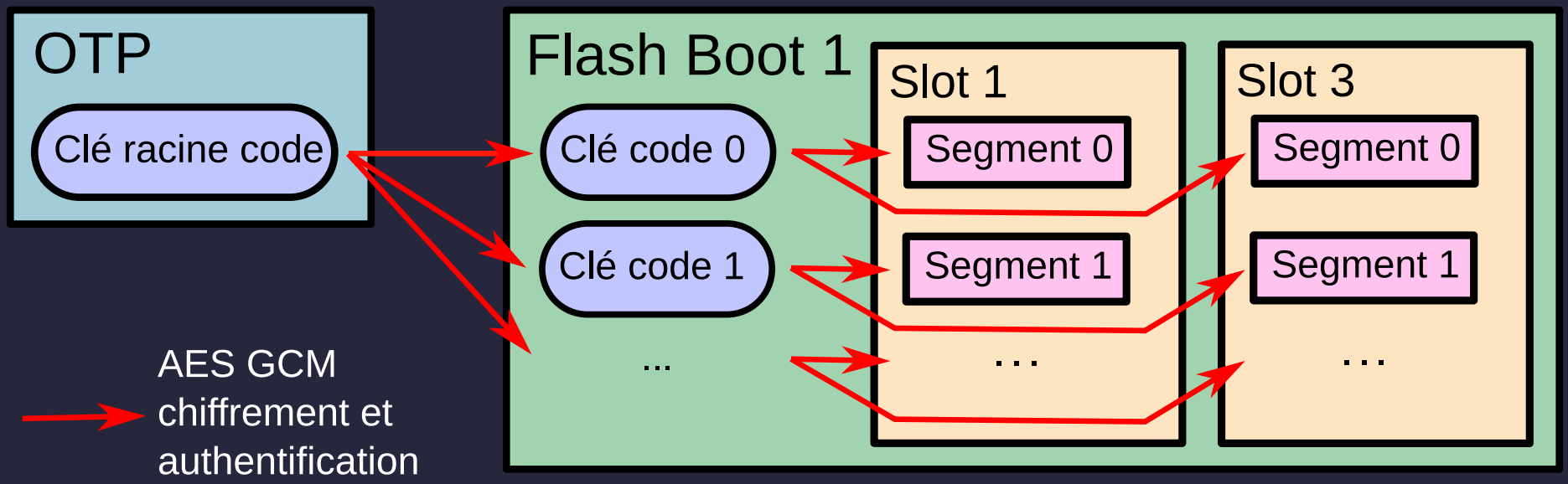
- signature (ECDSA)
- secret partagé (ECDH)

Chaînes de confiance

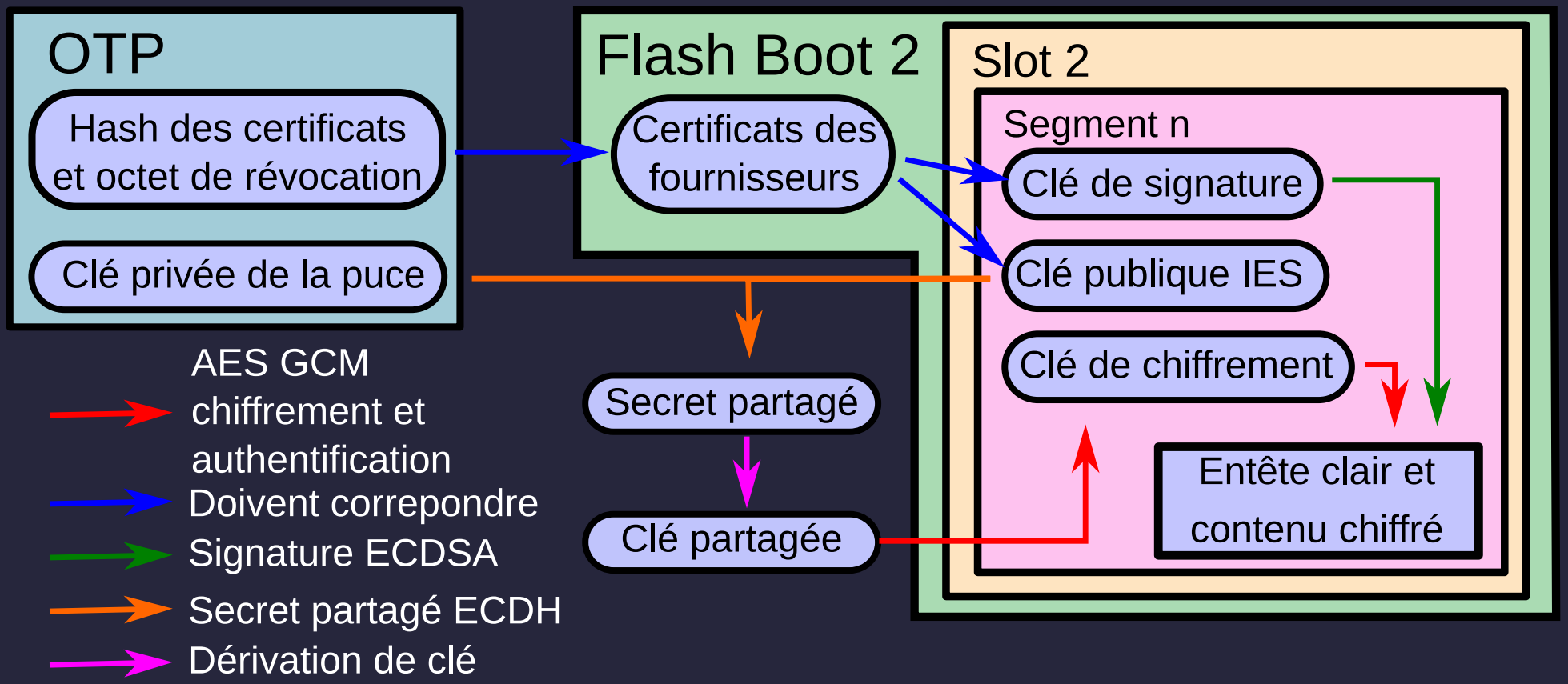
La chaîne interne



La chaîne de code



La chaîne de mise à jour



Notes d'implémentation

Merci de votre attention !