WOOKEY:
USB DEVICES STRIKE BACK

Ryad BENADJILA[1] Mathieu RENARD[1] Arnauld MICHELIZZA[1]
Philippe THIERRY[1] Philippe TREBUCHET[1] Jérémy LEFAURE[2]

[1] ANSSI, prenom.nom@ssi.gouv.fr [2] jeremy.lefaure@gmail.com

SSTIC SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

13 juin 2018

Le projet WooKey

Concevoir une clé USB chiffrante sécurisée

Le projet WooKey

Concevoir une clé USB chiffrante sécurisée

Répondre à la menace BadUSB

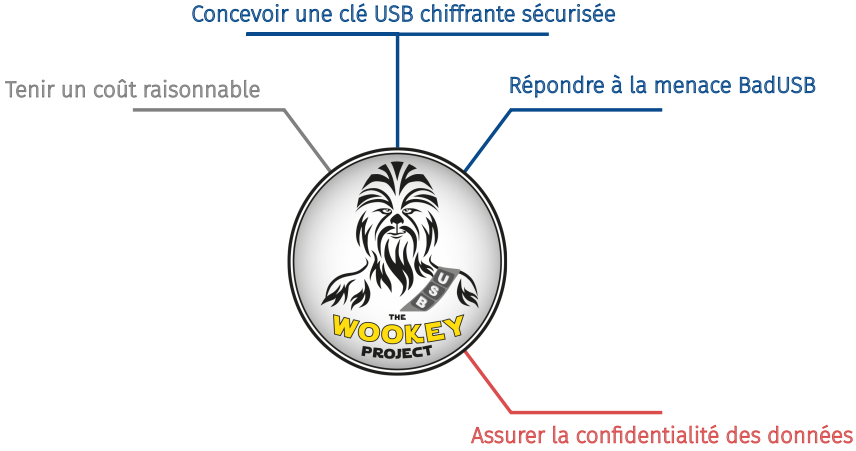
Le projet WooKey

Concevoir une clé USB chiffrante sécurisée

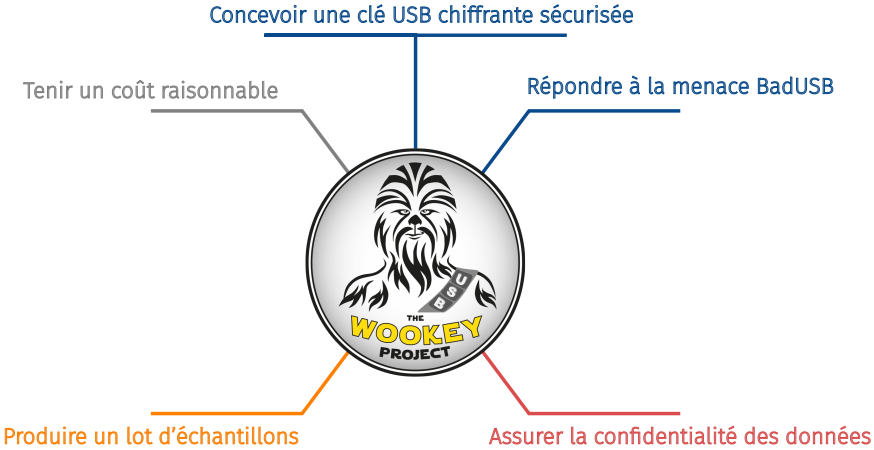
Répondre à la menace BadUSB

Assurer la confidentialité des données

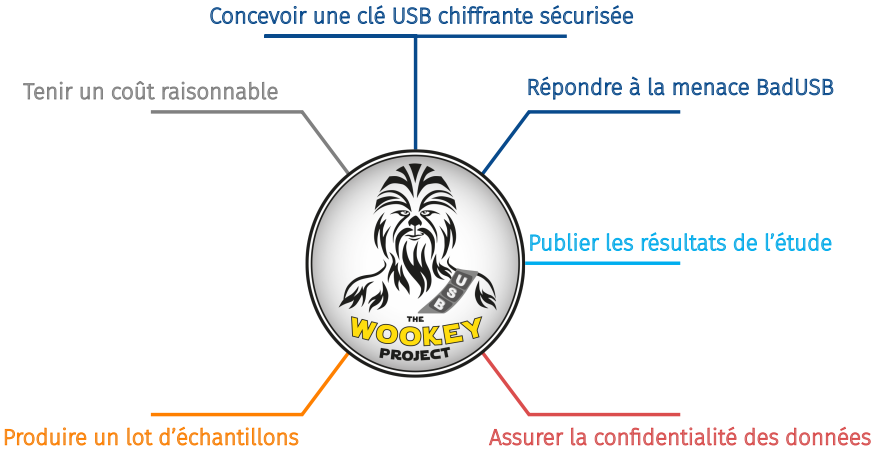
Le projet WooKey



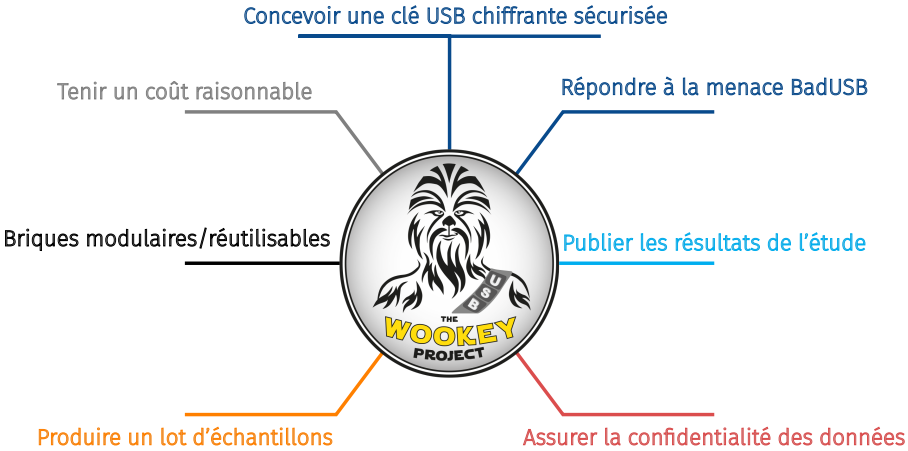
Le projet WooKey



Le projet WooKey



Le projet WooKey



Universal Serial Bus

Universal Serial Bus

Type de périphérique ?

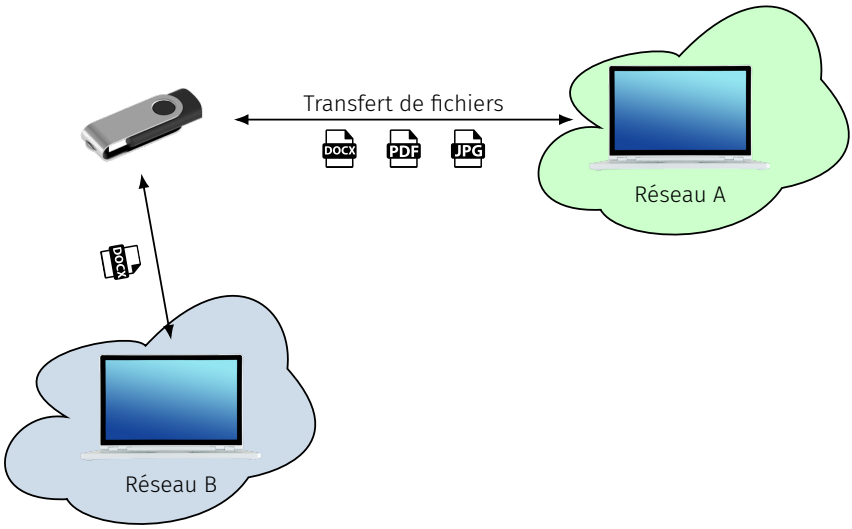
Périphérique « inoffensif »

Clé USB et usages

Transfert de fichiers

Laptop Pro/Perso

Clé USB et usages



Clé USB et usages

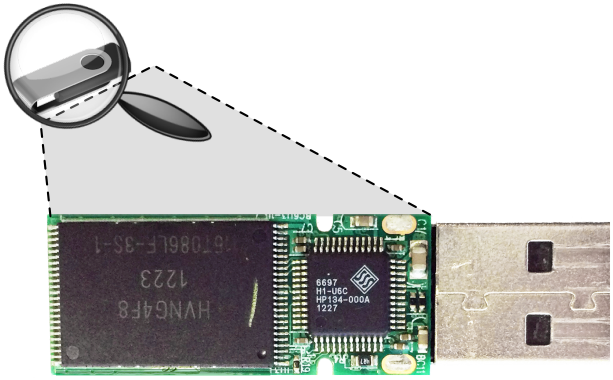
Transfert de mise à jour

Laptop Pro/Perso

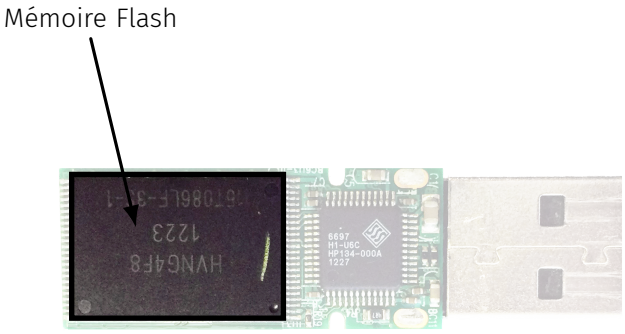
Automate, routeur, ...

Menaces

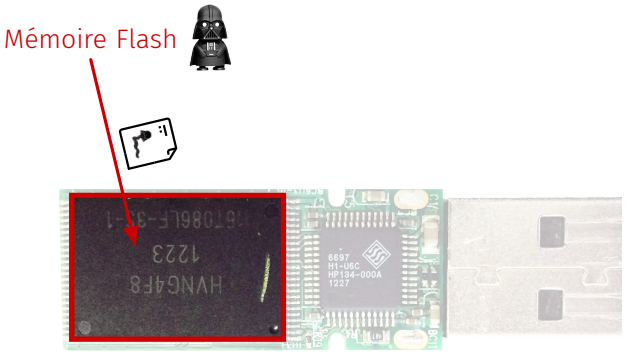
Menaces



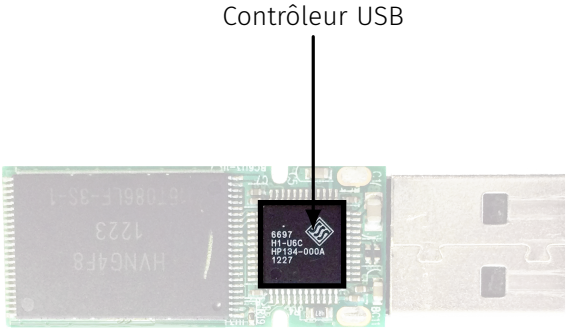
Menaces



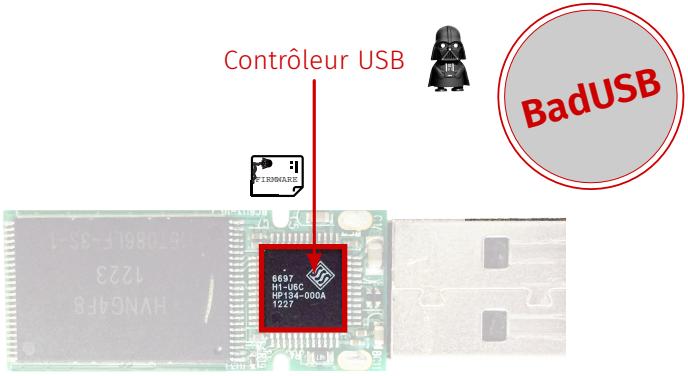
Menaces



Menaces



Menaces



ÉTAT DE L'ART DES SOLUTIONS LIBRES

USB Armory

- 2014
- Cortex-A = SoC smartphone
- Architecture complexe
- BootROM (non désactivable)
- Coûteux
- Plateforme de développement

ÉTAT DE L'ART DES SOLUTIONS LIBRES

USB Armory

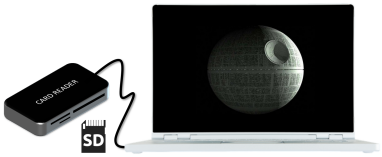
- 2014
- Cortex-A = SoC smartphone
- Architecture complexe
- BootROM (non désactivable)
- Coûteux
- Plateforme de développement

Nitrokey

- 2016
- AVR
- AES logiciel
- Pas de protection mémoire (MPU)
- Application sur l'hôte

Modèle de Menace

Vol de la carte SD et lecture des données

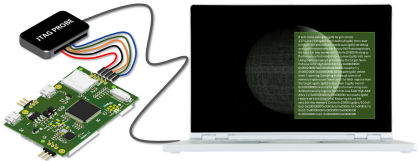


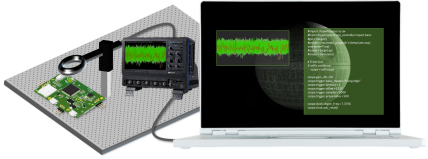
Modèle de Menace

Attaques logicielles sur la clé USB

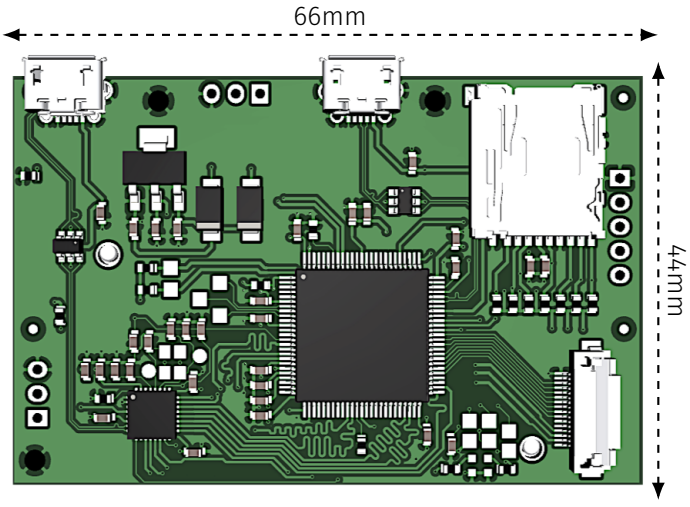
Modèle de Menace

Attaques matérielles





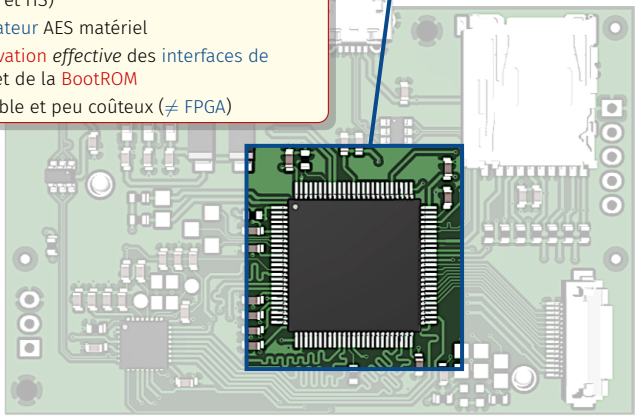
Architecture Matérielle



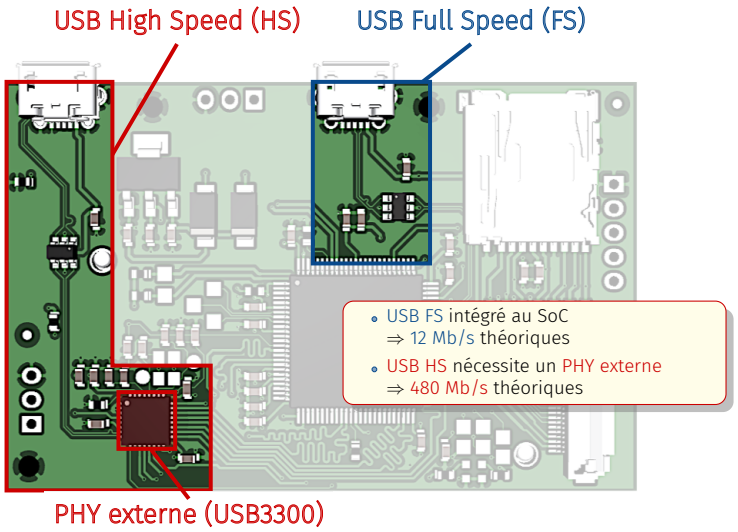
Architecture Matérielle

- 2 MB de flash, 256 kB de SRAM
- MPU : primitive de cloisonnement mémoire
- USB (FS et HS)
- Accélérateur AES matériel
- Désactivation *effective* des interfaces de *debug* et de la BootROM
- Disponible et peu coûteux ($\neq$ FPGA)

MCU = Cortex-M4 STM32F439

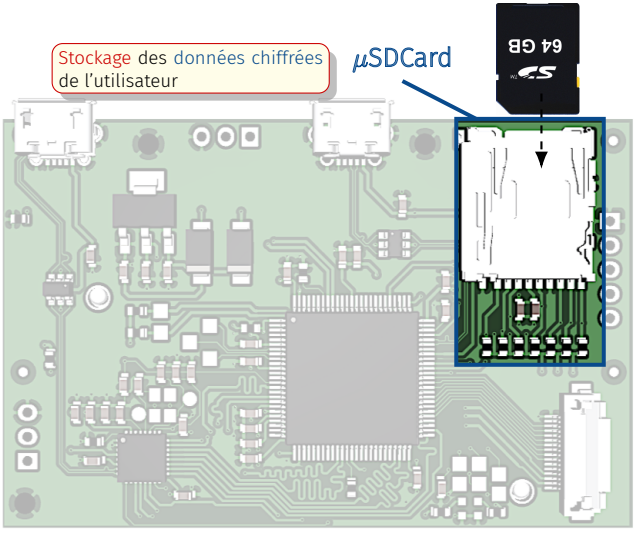


Architecture Matérielle

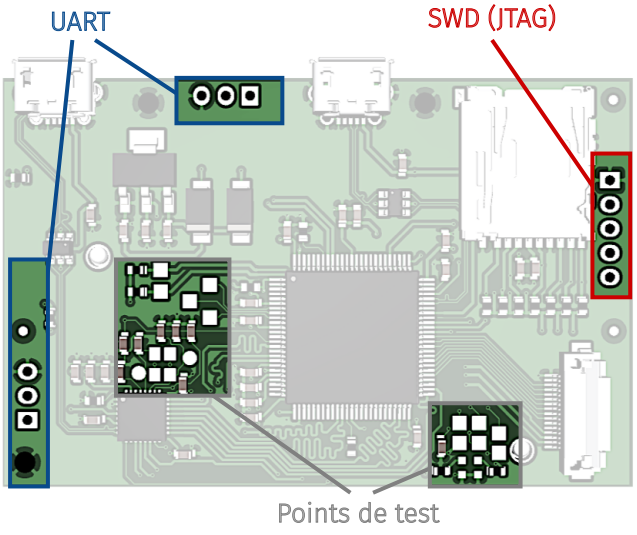


- USB FS intégré au SoC
  ⇒ 12 Mb/s théoriques
- USB HS nécessite un PHY externe
  ⇒ 480 Mb/s théoriques

Architecture Matérielle

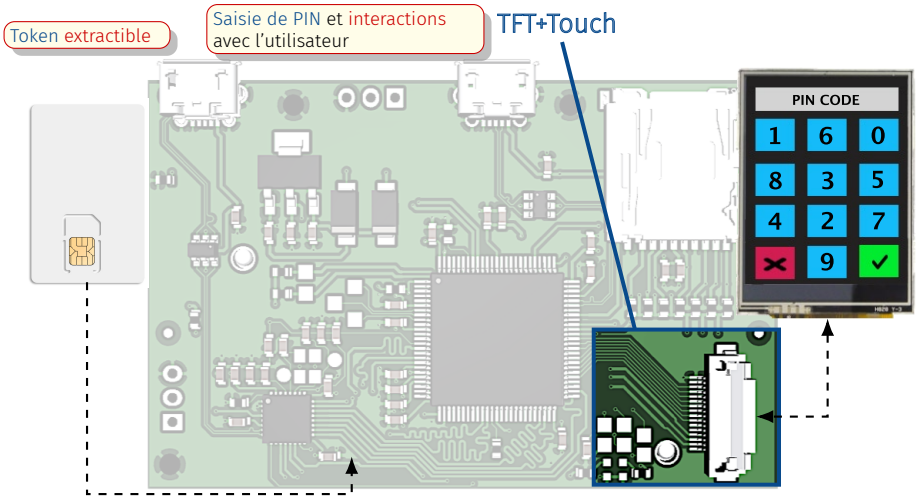


Architecture Matérielle

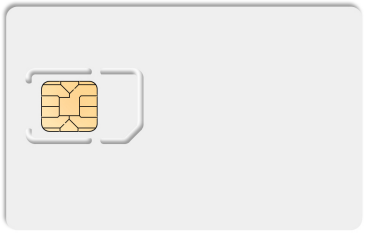


Interfaces de *debug* protégées en mode production (RDP)

Architecture Matérielle



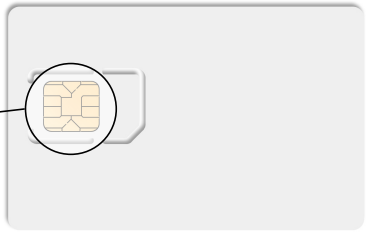
Token extractible : Javacard



Token extractible : Javacard

NXP JCOP JD081

- Javacard 3.0.1, Global Platform 2.2.1



Token extractible : Javacard

NXP JCOP JD081

- Javacard 3.0.1, Global Platform 2.2.1
- Évaluation CC EAL 4+ VAN5 :
  Protection contre les attaques par *canaux auxiliaires* et *attaques en fautes*
- Sujet abordé dans une autre présentation SSTIC 2018

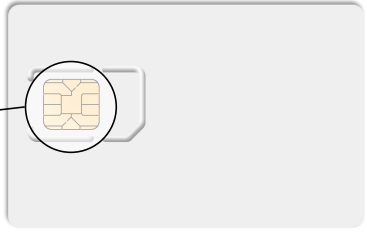
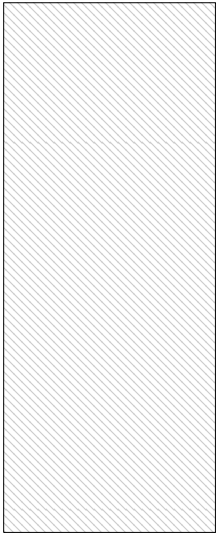


Image en flash : problématiques



Mises à jour

- Résilience
- Sécurisation

Image en flash : « Flip » et « Flop »

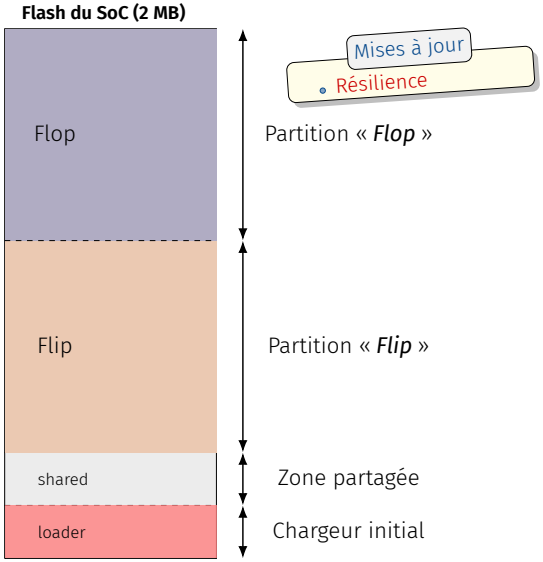


Image en flash : « Flip » et « Flop »

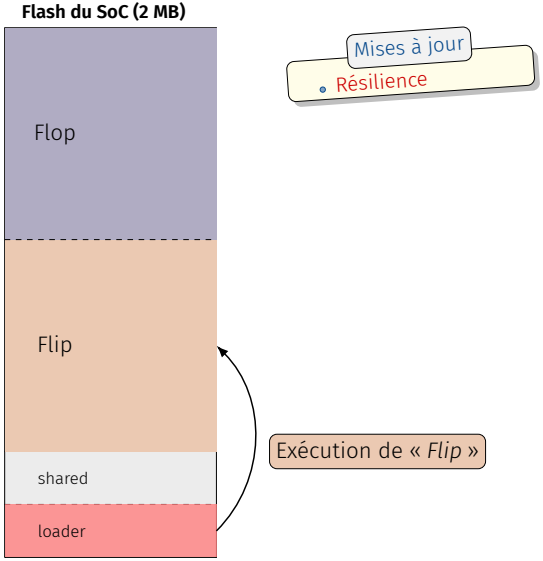
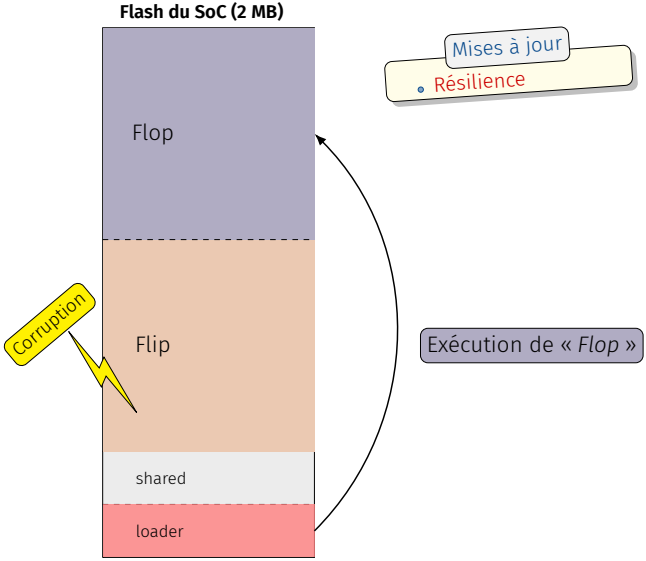
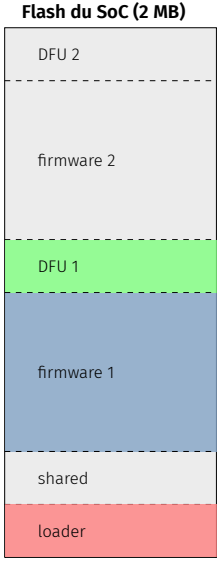


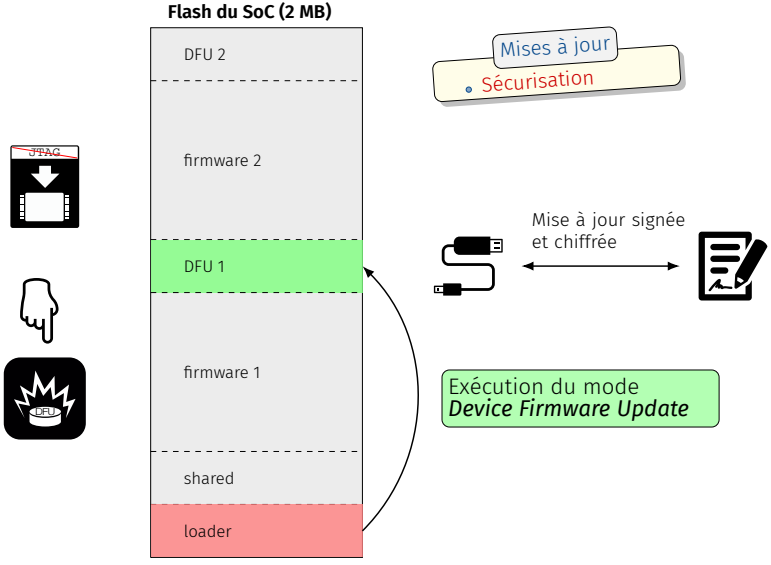
Image en flash : « Flip » et « Flop »



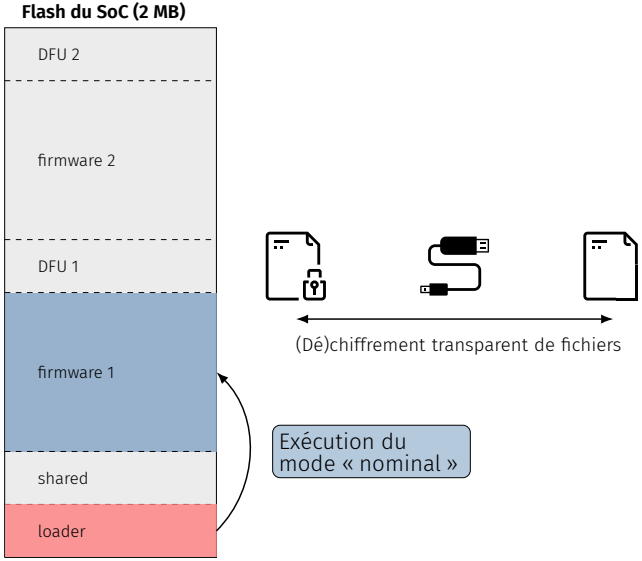
Détails du logiciel embarqué



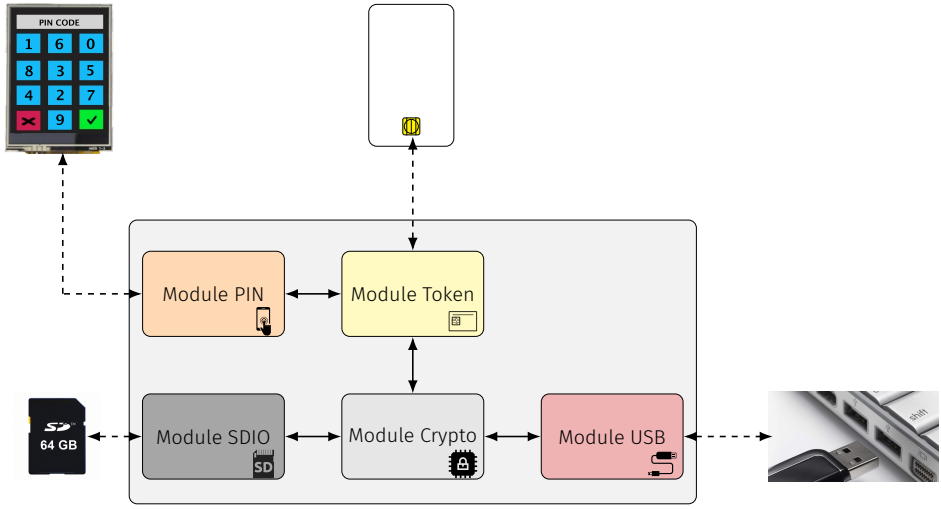
Mode « nominal »



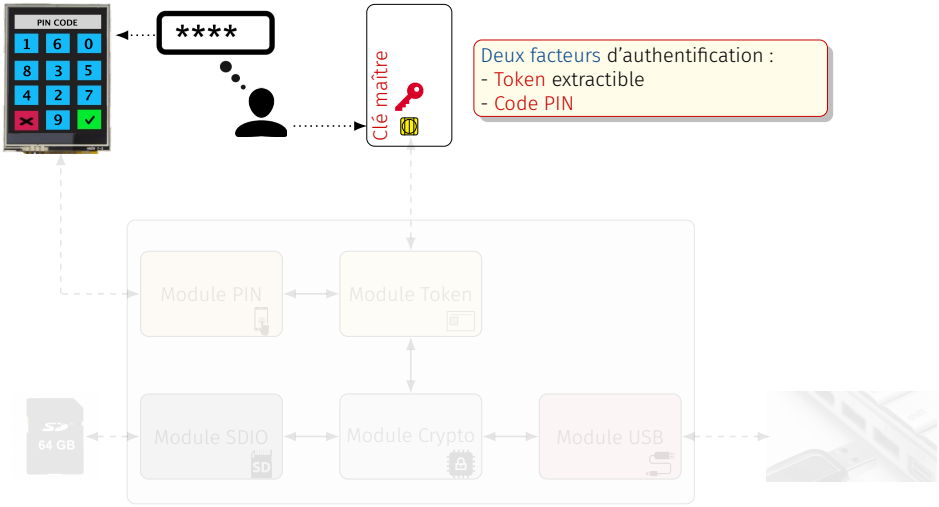
Mode « nominal »



Modules et services de WooKey



Double facteur d'authentification



Manipulation des clés sensibles

Authentification mutuelle ECDH
Canal chiffré et intègre

Module PIN

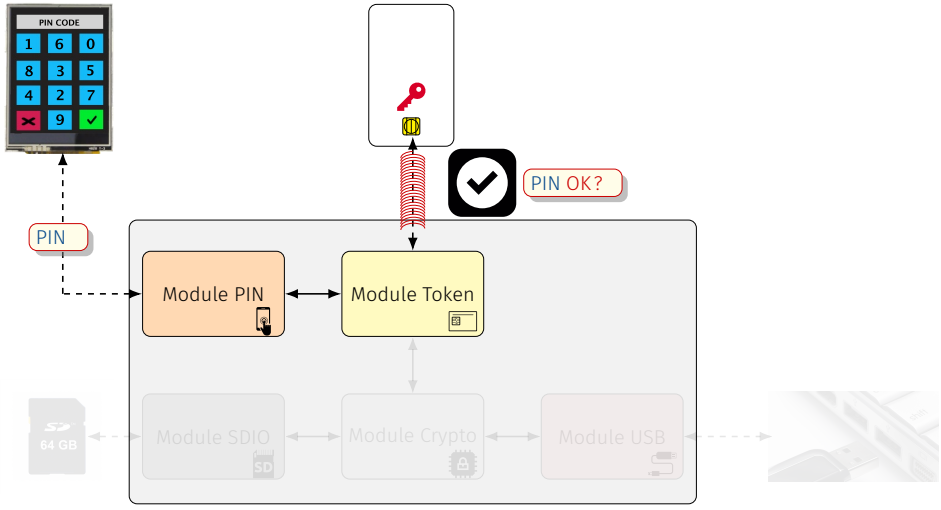
Module Token

Module SDIO

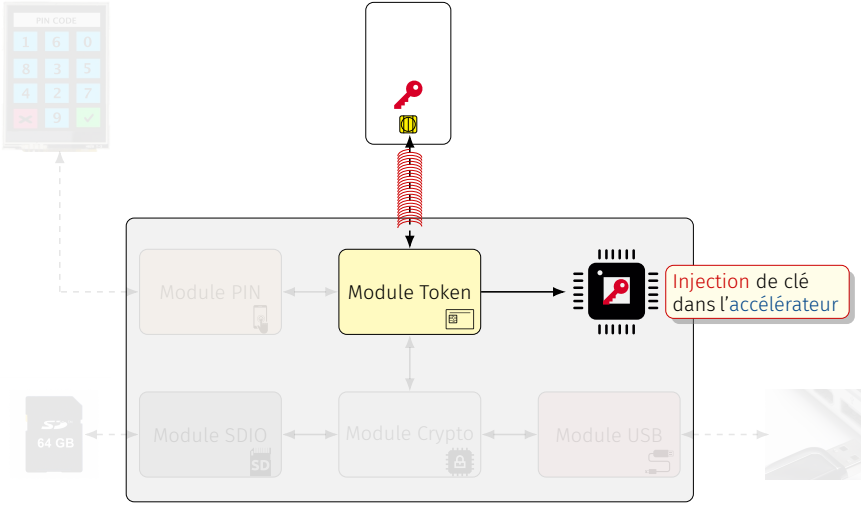
Module Crypto

Module USB

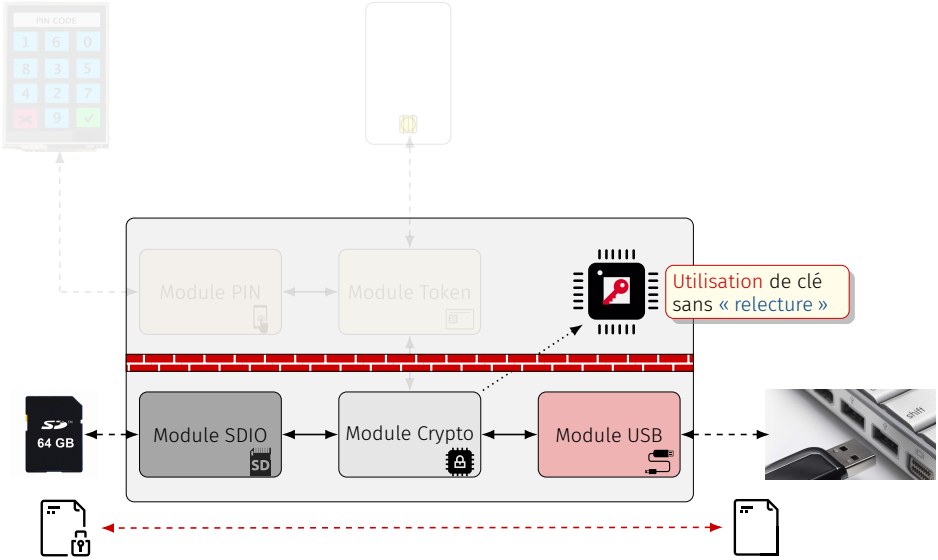
Manipulation des clés sensibles



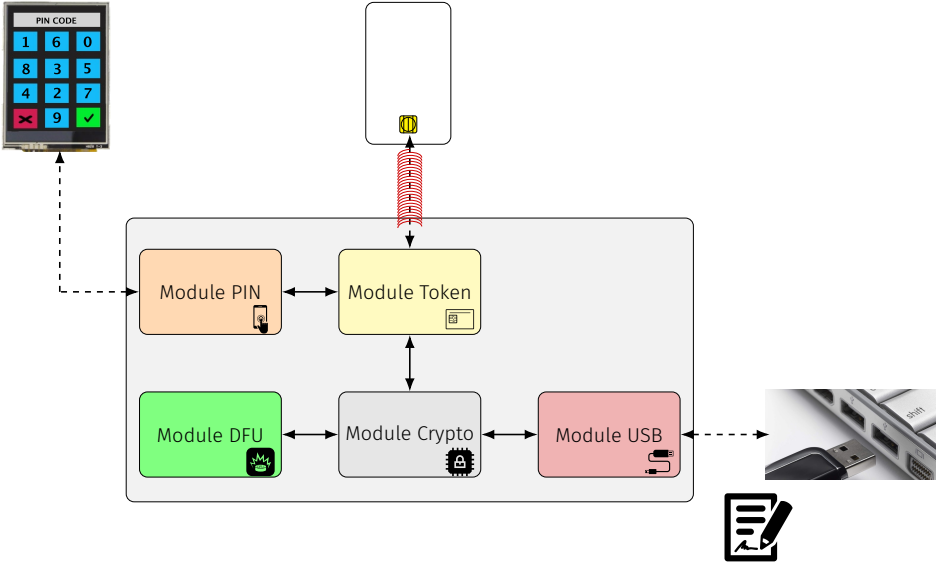
Manipulation des clés sensibles



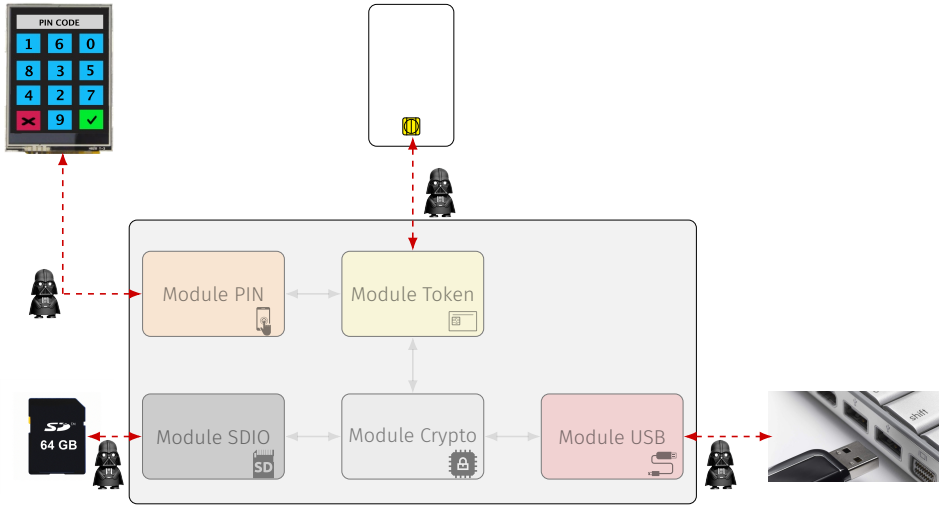
Chemin de données utilisateur



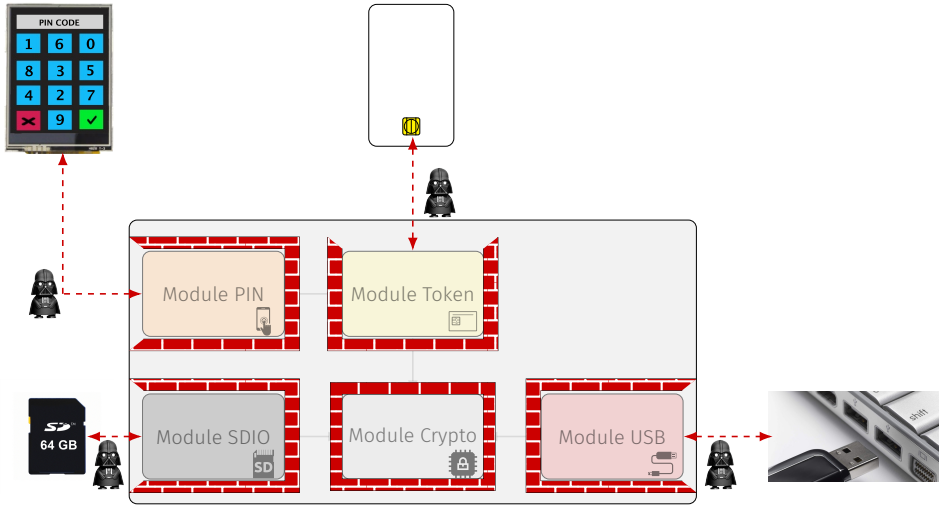
DFU ET TOKEN EXTERNE



Cloisonnement des modules

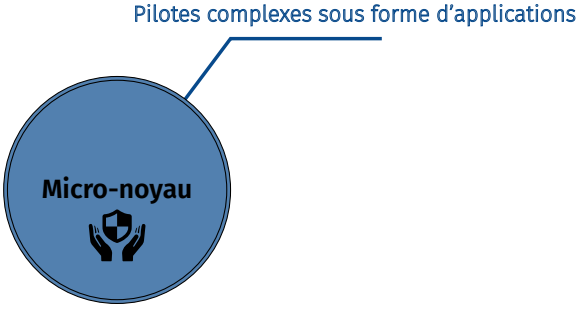


Cloisonnement des modules

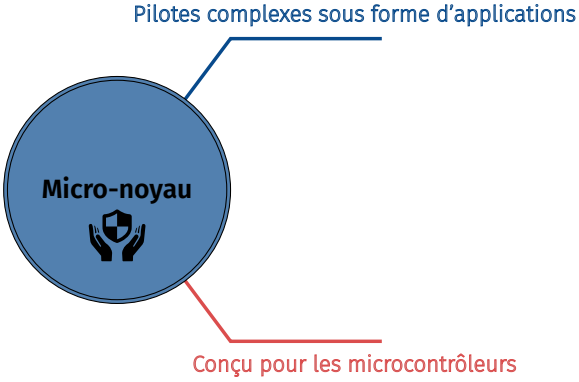


Micro-noyau : propriétés souhaitées

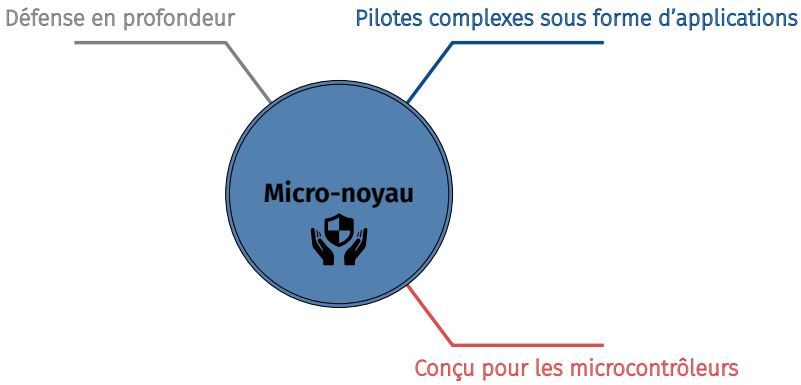
Micro-noyau : propriétés souhaitées



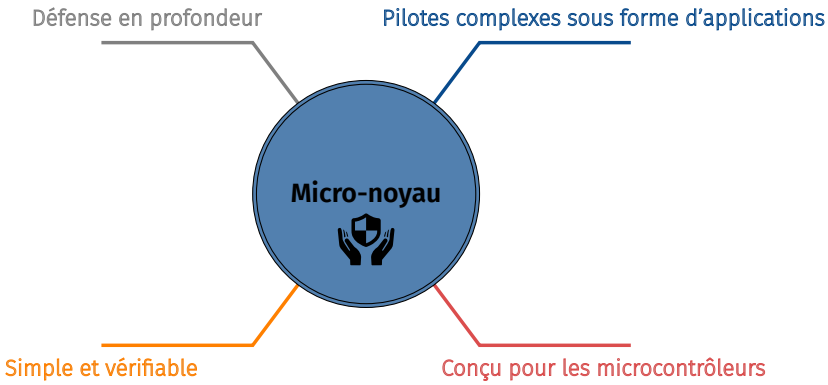
Micro-noyau : propriétés souhaitées



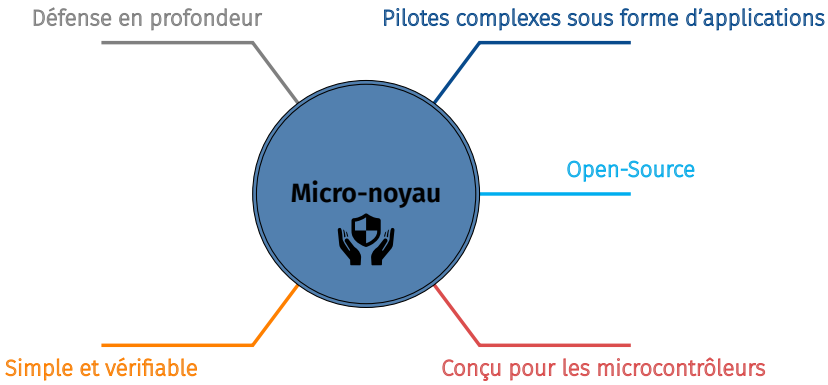
Micro-noyau : propriétés souhaitées



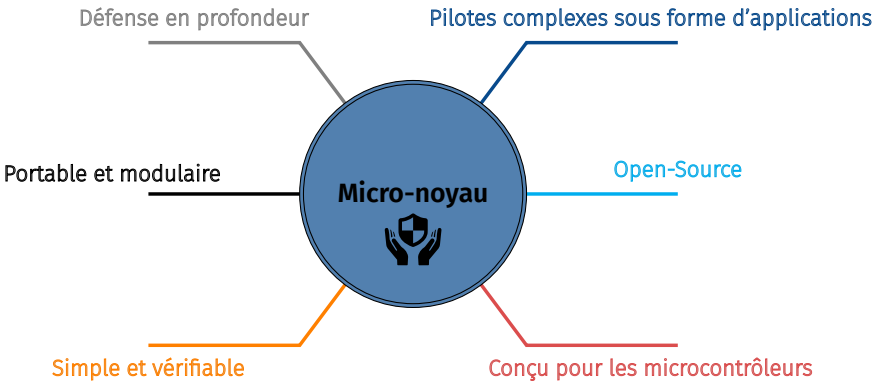
Micro-noyau : propriétés souhaitées



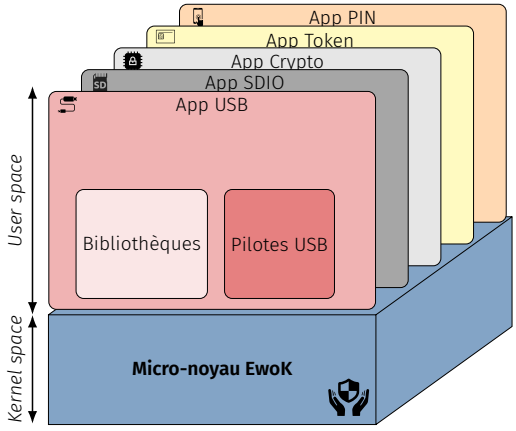
Micro-noyau : propriétés souhaitées



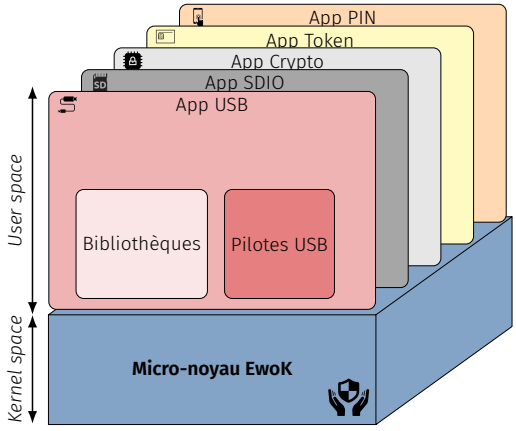
Micro-noyau : propriétés souhaitées

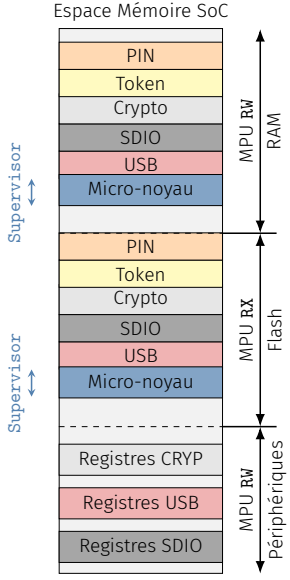


Micro-noyau : cloisonnement des applications

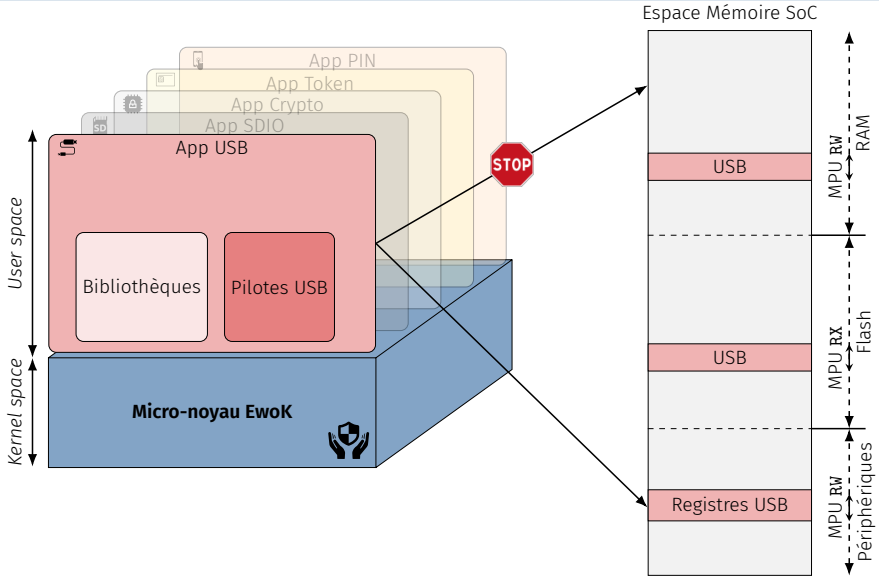


Micro-noyau : cloisonnement des applications

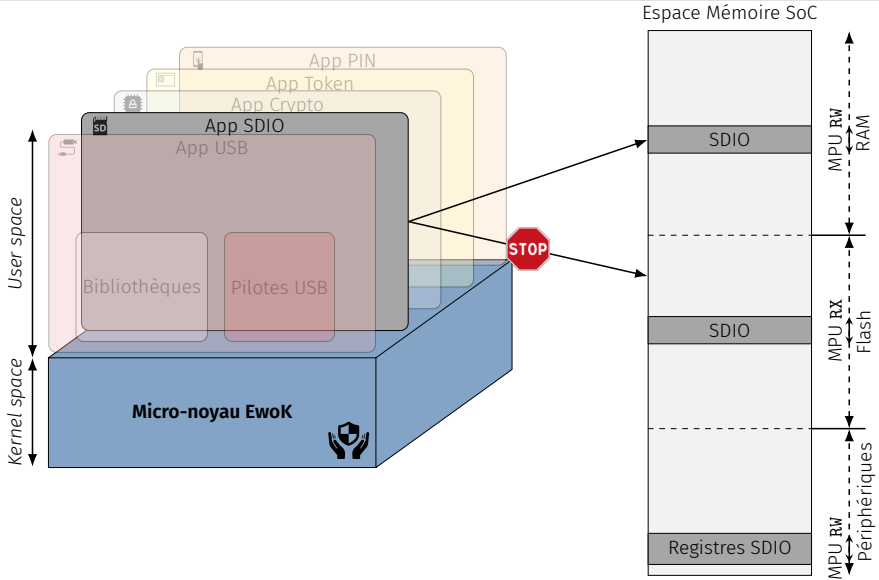




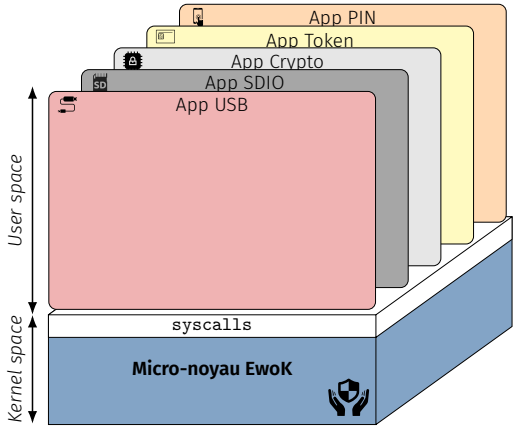
Micro-noyau : cloisonnement des applications



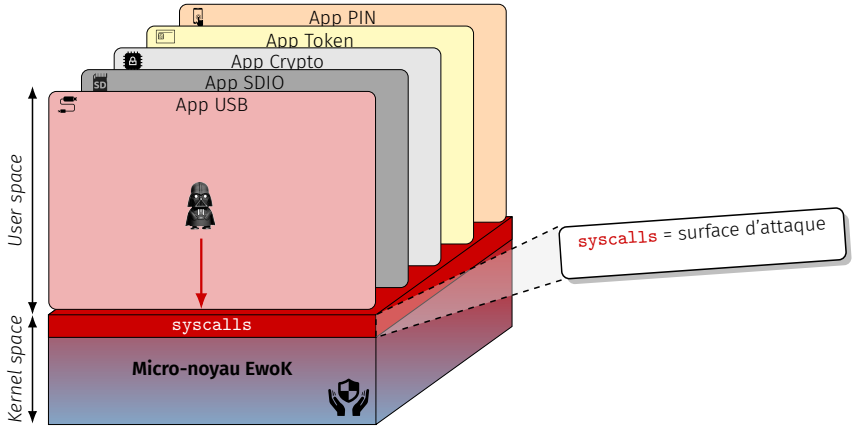
Micro-noyau : cloisonnement des applications



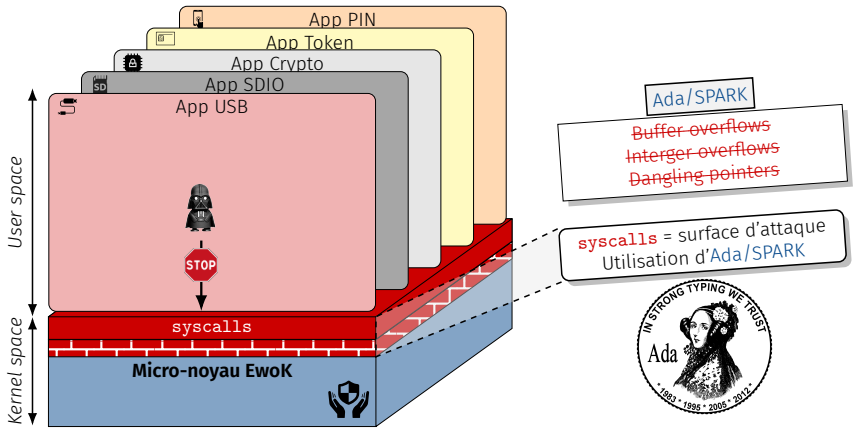
EwoK : défense en profondeur



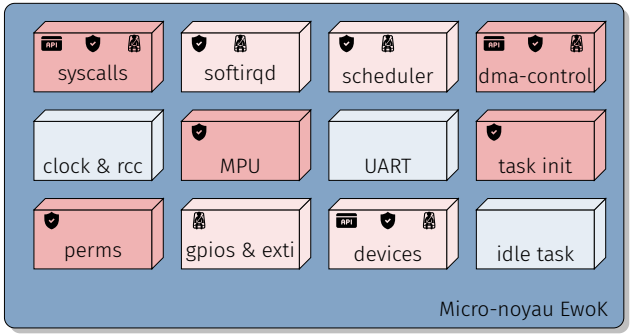
EwoK : défense en profondeur



EwoK : défense en profondeur



EwoK : ADA/SPARK



C | Ada | Ada+SPARK

API, impose une validation stricte des entrées/sorties

Composant critique pour la sécurité

Composant critique pour la sûreté de fonctionnement

Primitives de sécurité versus menaces

DFU+signature

Chiffrement accéléré

EwoK+Ada/SPARK

Double facteur+
Authentification forte

Primitives de sécurité

Primitives de sécurité versus menaces

DFU+signature

Chiffrement accéléré

EwoK+Ada/SPARK

Double facteur+
Authentification forte

Primitives de sécurité

BadUSB+
Attaques logicielles

Attaques
matérielles basiques

Attaques
matérielles avancées

Menaces

Primitives de sécurité versus menaces

DFU+signature

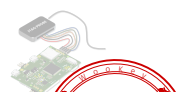
Chiffrement accéléré

EwoK+Ada/SPARK

Double facteur+
Authentification forte

Primitives de sécurité

Bad USB
Attaques logicielles



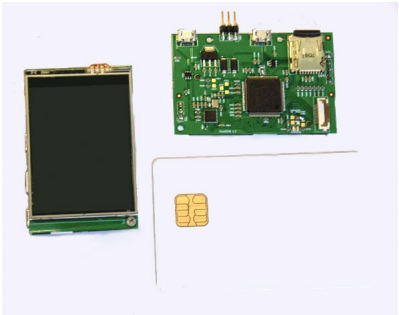
Attaques
matérielles basiques

Attaques
matérielles avancées

Menaces

Conclusion

- Exemple de clé USB sécurisée de confiance
  - `https://github.com/wookey-project` (Q3 2018)
- Plateforme matérielle Open Hardware
- Micro-noyau EwoK + SDK Open Source
- Double facteur d'authentification



QUESTIONS