U2F2 :
Prévenir la Menace Fantôme sur FIDO/U2F

SSTIC 2021

Ryad Benadjila, Philippe Thierry

ANSSI

<prenom.nom@ssi.gouv.fr>

Juin 2021

Pourquoi ?

- Mots de passe fragiles

Attaques en force brute

Mots de passe alphanumériques
Moyennes sur NVidia RTX 2070
Moyennes sur SHA-1

Longueur	Temps d'attaque 1 GPU	Temps d'attaque 100 GPUs
1	<1 seconde	<1 seconde
4	2 secondes	<1 seconde
6	6 secondes	<1 seconde
8	6 heures	216 secondes
10	1024 jours	10,24 jours

Source : article 2020 "Hash-Based Authentication Revisited in the Age of High-Performance Computers"

Pourquoi ?

- Mots de passe fragiles

Fuites massives de bases de données

COMB 2021 : 3,2 milliards d'entrées

Pourquoi ?

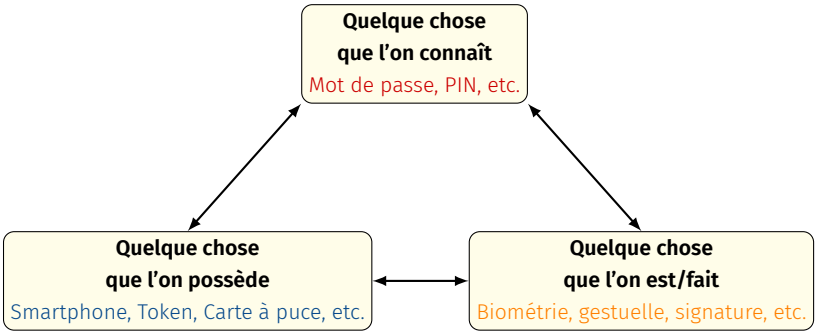
- Mots de passe fragiles

Vol par malware, phishing, etc.

Keylogger

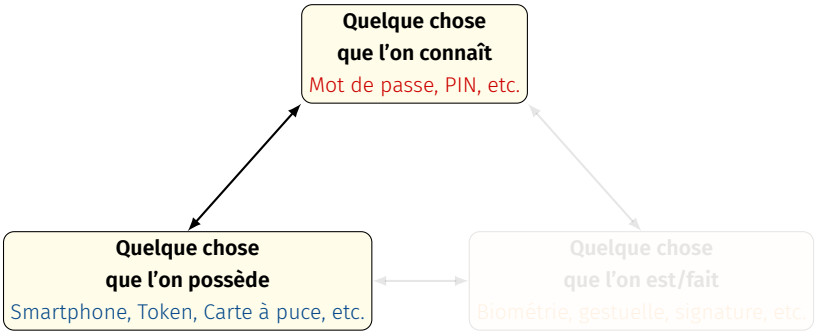
Définition

- Concaténation d'au moins deux facteurs d'authentification



Définition

- Concaténation d'au moins deux facteurs d'authentification



2FA : Des premières solutions limitées

- One Time Passwords (OTP)

2FA : Des premières solutions limitées

- One Time Passwords (OTP)

Phishing

Canal SMS attaquable

2FA : Des premières solutions limitées

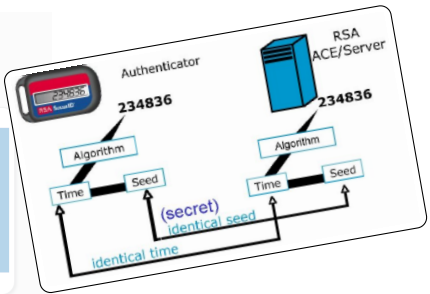
- One Time Passwords (OTP)

Phishing

Canal SMS attaquable

2FA : Des premières solutions limitées

- One Time Passwords (OTP)



Phishing

Canal SMS attaquable

Clé secrète partagée

2FA : un nouveau standard

- 2014 : le consortium FIDO standardise **U2F**
- Utilisation d'un **Token** (matériel) dédié

2FA : un nouveau standard

- 2014 : le consortium FIDO standardise **U2F**
- Utilisation d'un **Token** (matériel) dédié

Avantages

Cryptographie asymétrique ECDSA
(protection contre les attaques des services)
Protection contre le phishing + rejeu
Action physique de l'utilisateur
Protection de l'anonymat
(cloisonnement des services)
Simple + Standardisé $\Rightarrow$ large adoption

2FA : un nouveau standard

- 2014 : le consortium FIDO standardise **U2F**
- Utilisation d'un **Token** (matériel) dédié

Avantages

Cryptographie asymétrique ECDSA
(protection contre les attaques des services)
Protection contre le phishing + rejeu
Action physique de l'utilisateur
Protection de l'anonymat
(cloisonnement des services)
Simple + Standardisé ⇒ large adoption

Limitations

Vol (avec ou sans remise) du token
PC suppposé de confiance
Attaques physiques (SCA, fautes)
Autres limitations
(confusion, "désenregistrement")

2FA : un nouveau standard

- 2014 : le consortium FIDO standardise **U2F**
- Utilisation d'un **Token** (matériel) dédié

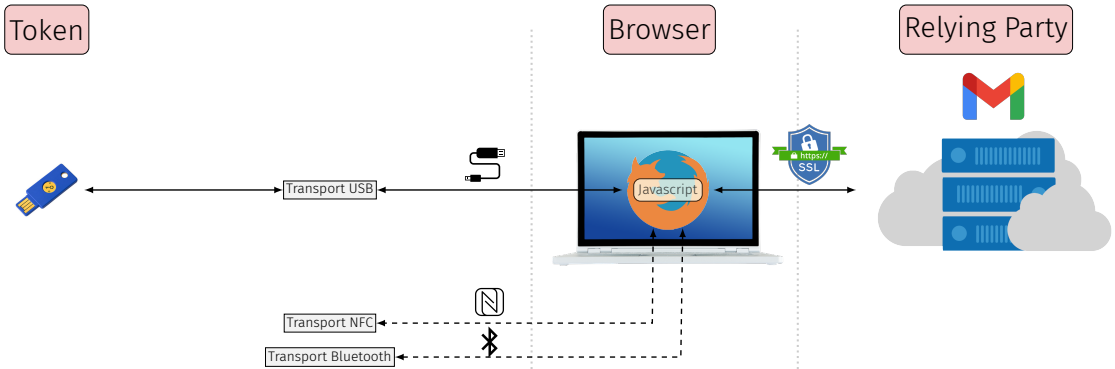
Limitations

du token
nance
ques physiques (SCA, fautes)
Autres limitations
(confusion, "désenregistrement")

Contexte de cette présentation

Fonctionnement de FIDO

Architecture à trois entités

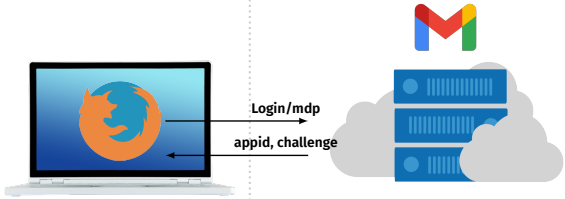


REGISTER : ENREGISTREMENT DU TOKEN

Token

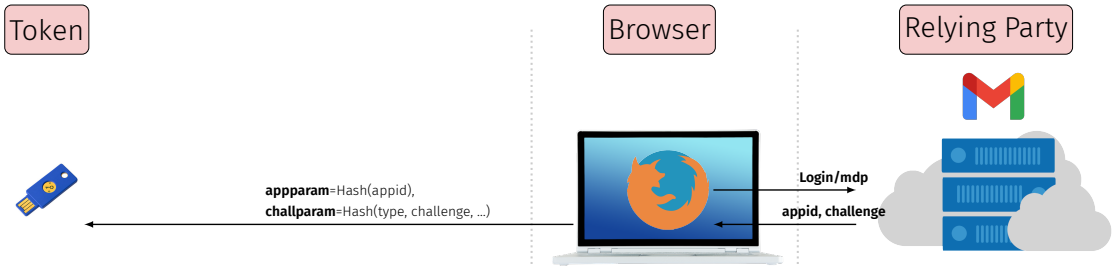
Browser

Relying Party

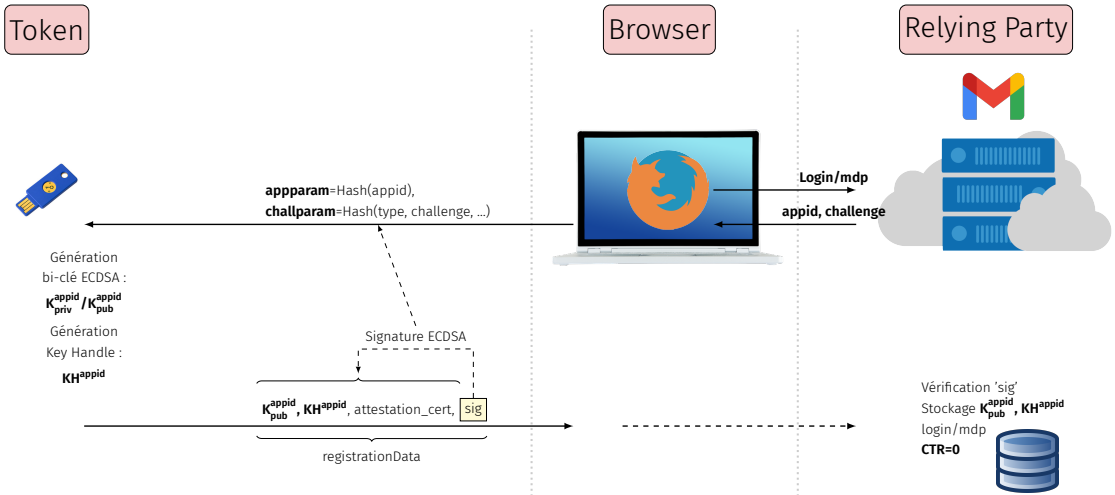


Fonctionnement de FIDO

REGISTER : enregistrement du token



REGISTER : ENREGISTREMENT DU TOKEN

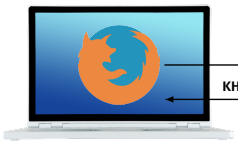


AUTHENTICATE : AUTHENTIFICATION DU TOKEN

Token

Browser

Relying Party



Login/mdp

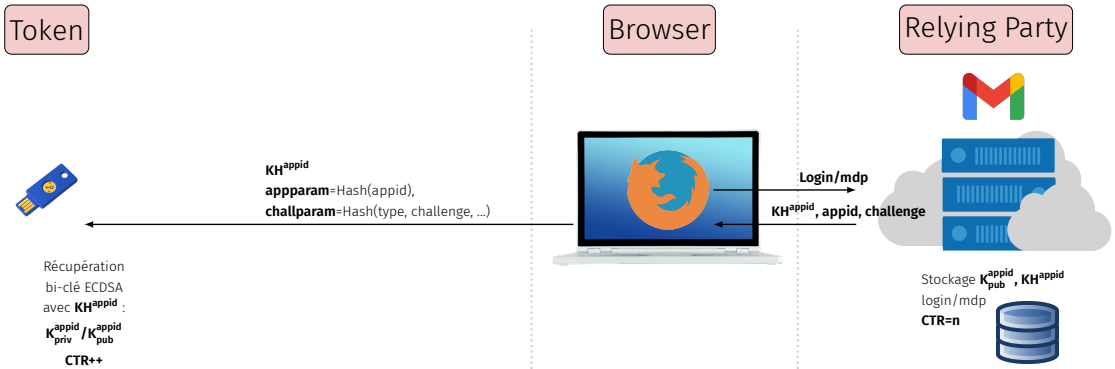
KH^{appid}, appid, challenge

Stockage K_{pub}^{appid}, KH^{appid}

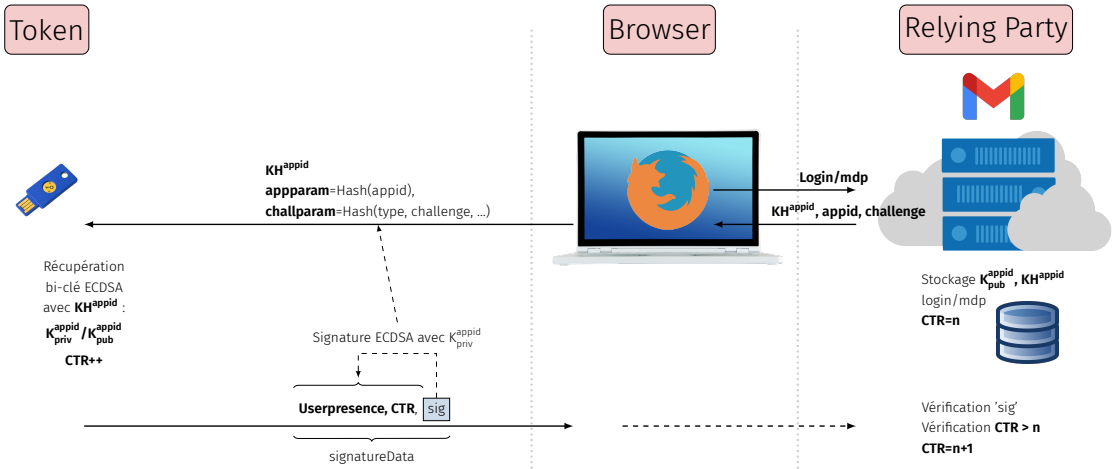
login/mdp

CTR=n

AUTHENTICATE : AUTHENTIFICATION DU TOKEN

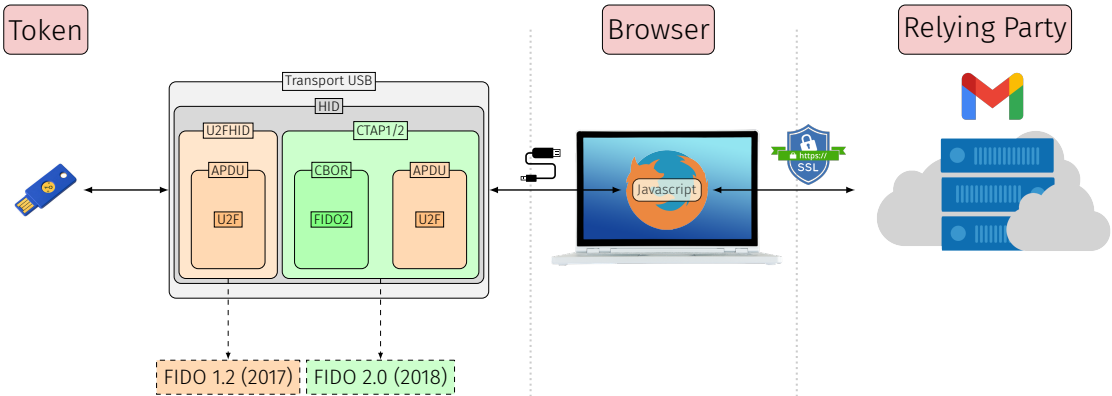


AUTHENTICATE : AUTHENTIFICATION DU TOKEN

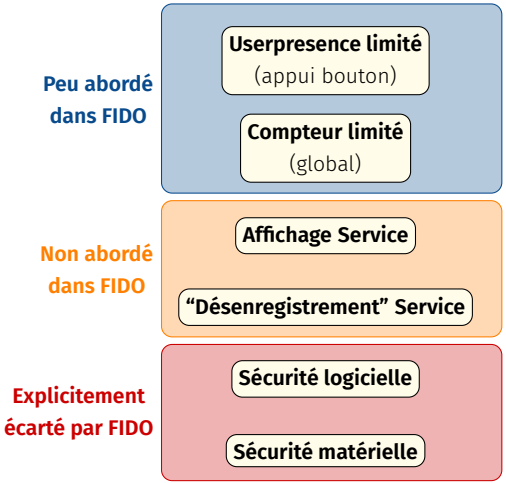


Fonctionnement de FIDO

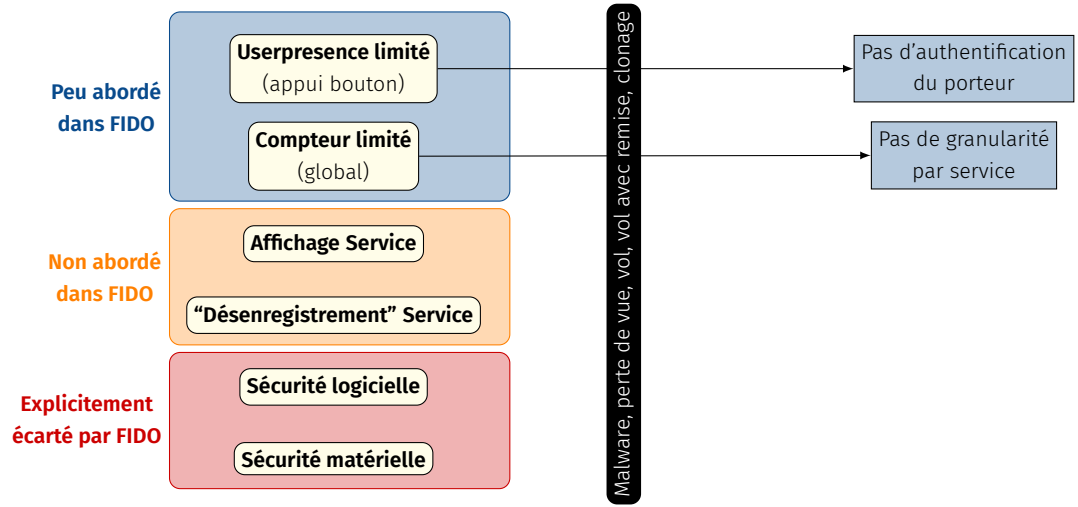
U2F et FIDO 2.0



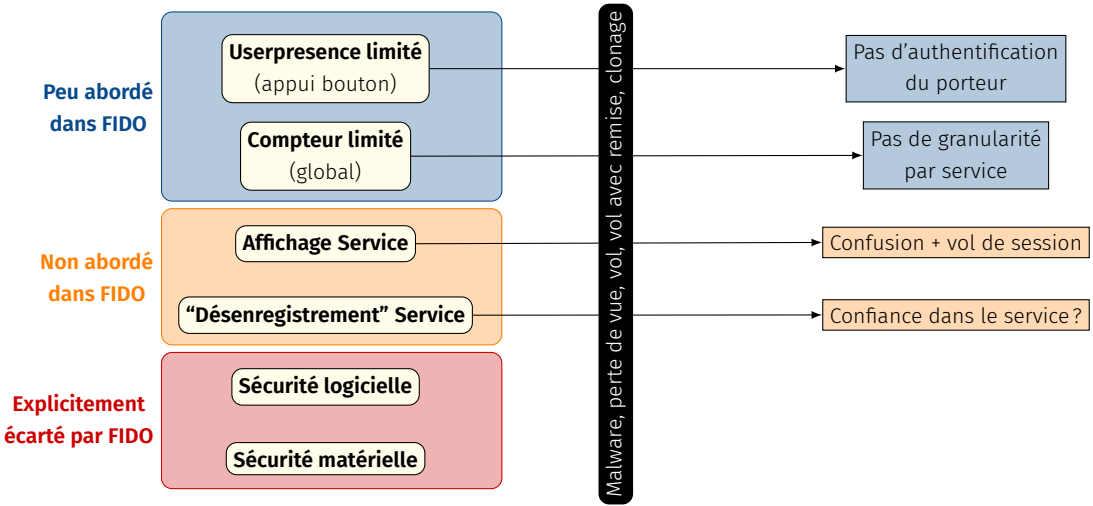
Un Token à la sécurité limitée



UN TOKEN À LA SÉCURITÉ LIMITÉE

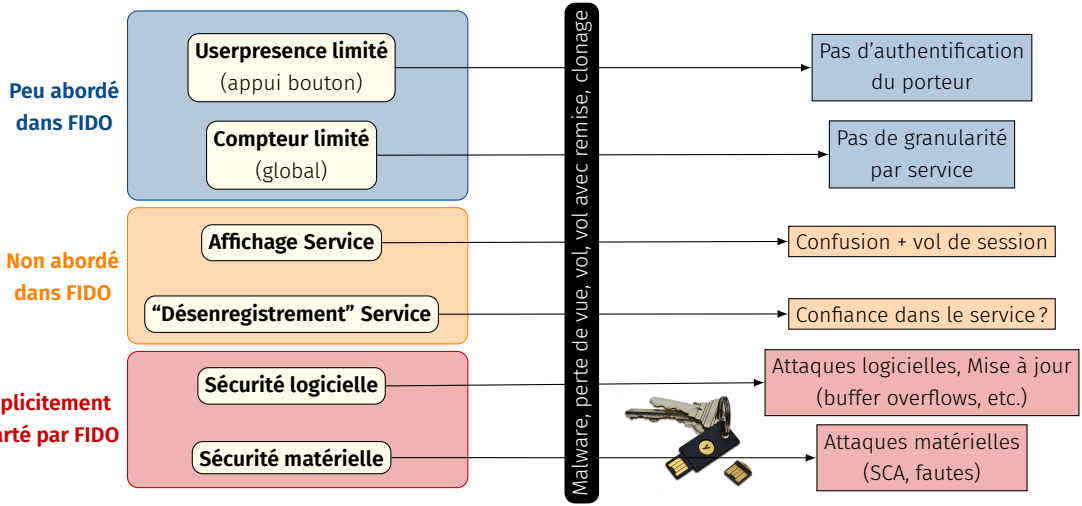


UN TOKEN À LA SÉCURITÉ LIMITÉE



FIDO : Limitations et modèle de menace

Un Token à la sécurité limitée



FIDO : LIMITATIONS ET MODÈLE DE MENACE

UN TOKEN À LA SÉCURITÉ LIMITÉE

yubico Why Yubico Products Solutions Resources Company Support

Security advisory YSA-2019-02 – reduced initial randomness on FIPS keys

Published date: **2019-06-13**
Tracking ID: **YSA-2019-02**

Summary

Who should read this advisory? Customers, IT Managers, or FIPS Crypto Officers who use or manage YubiKey FIPS Series devices.

!

!

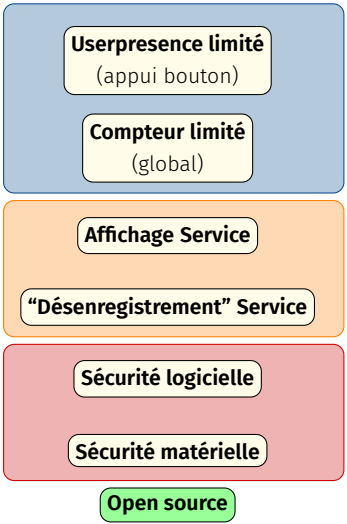
Contextes sensibles, attaques ciblées

Services sensibles

Rendre le contrôle à l'utilisateur

LeBrief du 11 janvier 2021

Des chercheurs ont réussi à cloner des clés Titan de Google, grâce à une attaque par canal auxiliaire


Userpresence limité
(appui bouton)
Compteur limité
(global)
Affichage Service
“Désenregistrement” Service
Sécurité logicielle
Sécurité matérielle
Open source

État de l'art

	SoloKeys Nitrokey3	OpenSK
Userpresence limité (appui bouton)	✗	✗
Compteur limité (global)	✗	✗
Affichage Service	✗	✗
“Désenregistrement” Service	✗	✗
Sécurité logicielle	~	~
Sécurité matérielle	~	✗
Open source	✓	✓

Rust/TockOS
Sécurité des mises à jour ?

Rust/Trussed
Peu d’éléments ouverts
(pour l’instant)

Seulement pour Nitrokey3 :
Secure Element “figé”

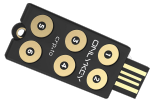
SoloKeys

OpenSK

État de l'art

	SoloKeys Nitrokey3	OpenSK	OnlyKeys
Userpresence limité (appui bouton)	✗	✗	✓
Compteur limité (global)	✗	✗	✗
Affichage Service	✗	✗	✗
“Désenregistrement” Service	✗	✗	✗
Sécurité logicielle	~	~	✗
Sécurité matérielle	~	✗	✗
Open source	✓	✓	✓

OnlyKeys



État de l'art

	SoloKeys Nitrokey3	OpenSK	OnlyKeys	Trezor
Userpresence limité (appui bouton)	✗	✗	✓	✓
Compteur limité (global)	✗	✗	✗	✗
Affichage Service	✗	✗	✗	✓
“Désenregistrement” Service	✗	✗	✗	✗
Sécurité logicielle	~	~	✗	~
Sécurité matérielle	~	✗	✗	✗
Open source	✓	✓	✓	✓

Trezor

Cloisonnement logiciel limité (usage MPU restreint)

État de l'art

	SoloKeys Nitrokey3	OpenSK	OnlyKeys	Trezor	Yubikeys	Ledger Nano
Userpresence limité (appui bouton)	✗	✗	✓	✓	~	✓
Compteur limité (global)	✗	✗	✗	✗	✗	✗
Affichage Service	✗	✗	✗	✓	✗	✓
“Désenregistrement” Service	✗	✗	✗	✗	✗	✗
Sécurité logicielle	~	~	✗	~	✗	✓
Sécurité matérielle	~	✗	✗	✗	✓	✓
Open source	✓	✓	✓	✓	✗	~

Yubikey “Bio”

Ledger Nano S

Biométrie (confiance ?)

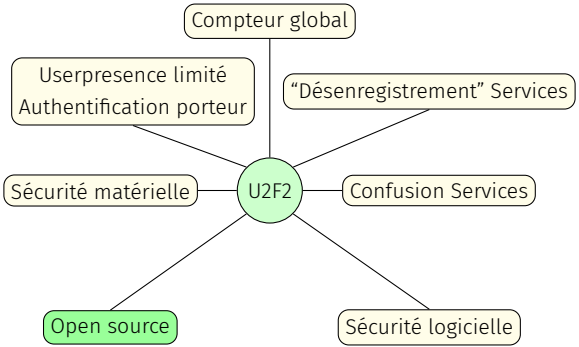
Pas de mises à jour

Application U2F open source (seulement)

État de l'art

	SoloKeys Nitrokey3	OpenSK	OnlyKeys	Trezor	Yubikeys	Ledger Nano	U2F2
Userpresence limité (appui bouton)	✗	✗	✓	✓	~	✓	✓
Compteur limité (global)	✗	✗	✗	✗	✗	✗	✓
Affichage Service	✗	✗	✗	✓	✗	✓	✓
“Désenregistrement” Service	✗	✗	✗	✗	✗	✗	✓
Sécurité logicielle	~	~	✗	~	✗	✓	✓
Sécurité matérielle	~	✗	✗	✗	✓	✓	✓
Open source	✓	✓	✓	✓	✗	~	✓

U2F2 : SOLUTIONS

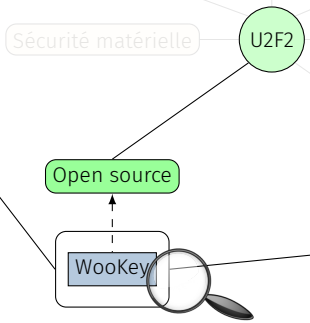


Carte à puce
Authentification forte
Applets open source
Certifiée $\geq$ EAL4+

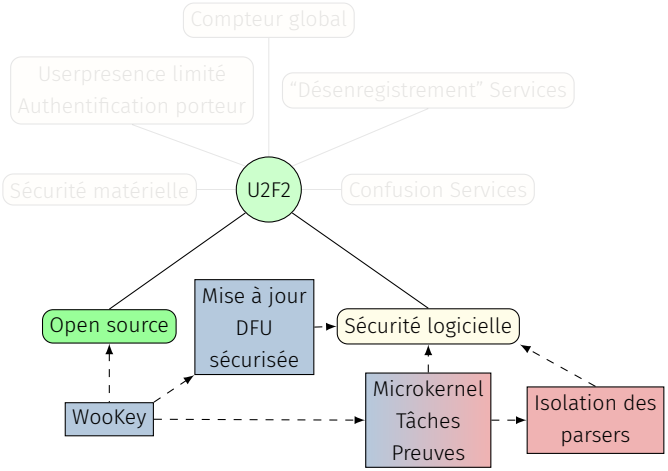
Disque USB chiffrant
Écran tactile
Device Firmware Upgrade (DFU) sécurisé
Défense en profondeur
(microkernel, tâches)

open source

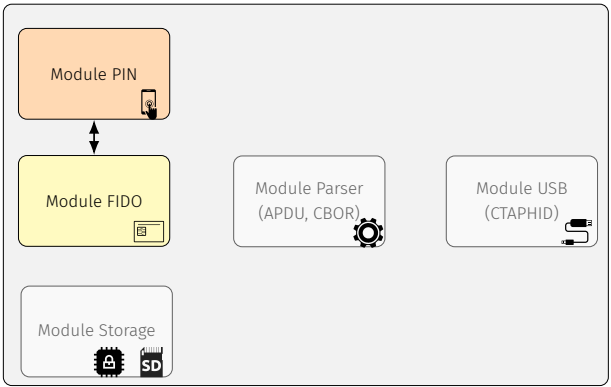
open hardware



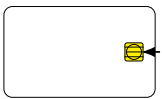
U2F2 : SÉCURITÉ LOGICIELLE

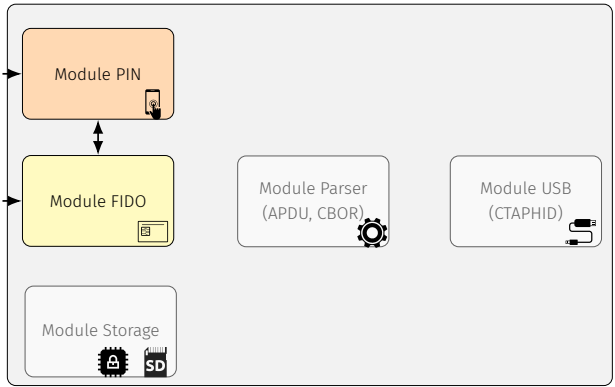


SÉPARATION EN TÂCHES

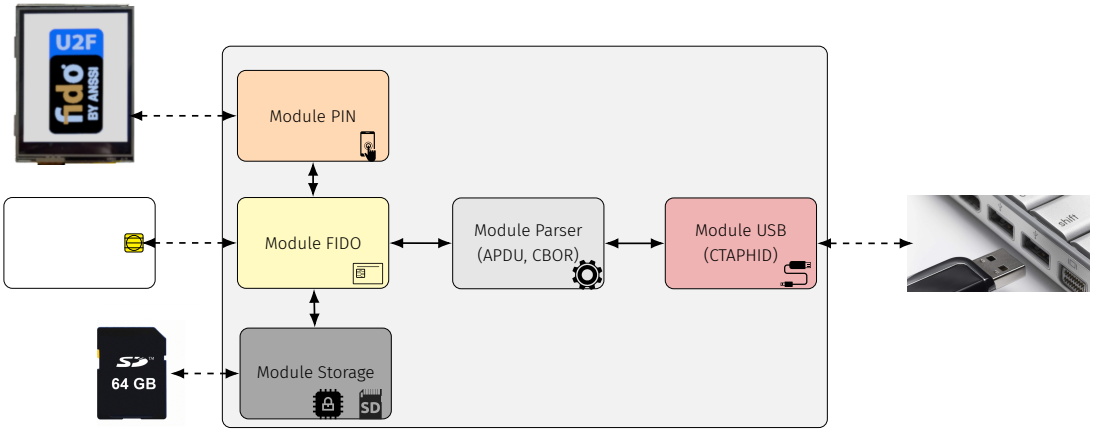


SÉPARATION EN TÂCHES

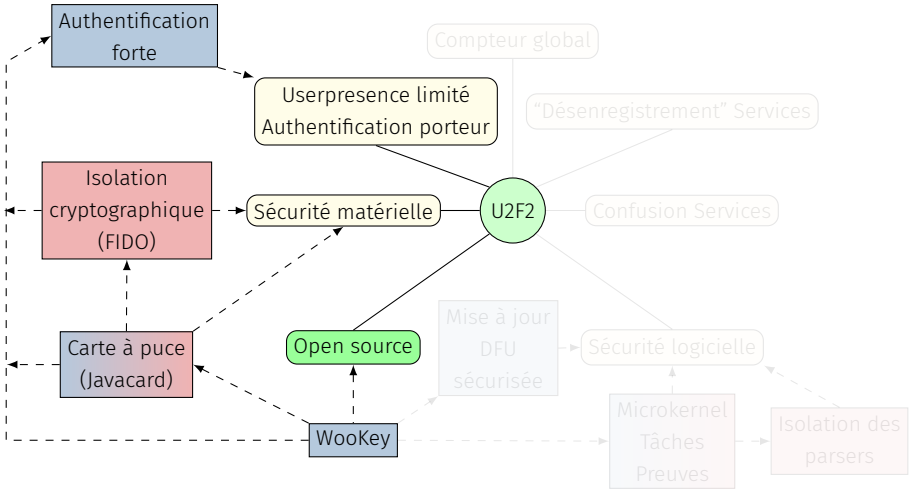




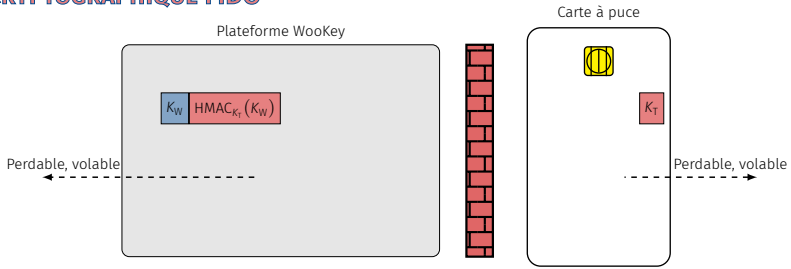
SÉPARATION EN TÂCHES



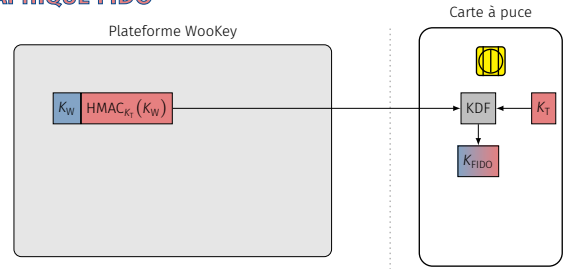
U2F2 : SÉCURITÉ MATÉRIELLE



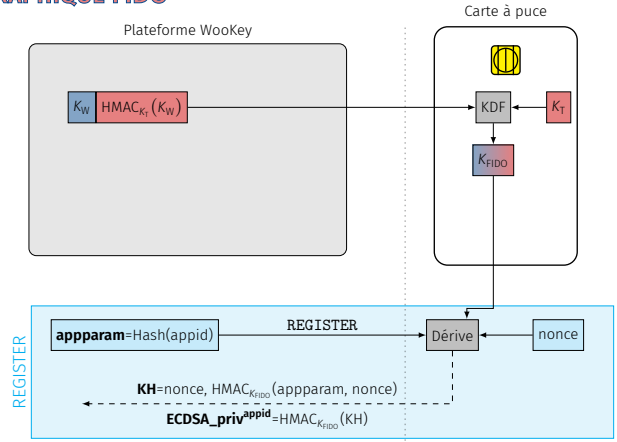
ISOLATION CRYPTOGRAPHIQUE FIDO



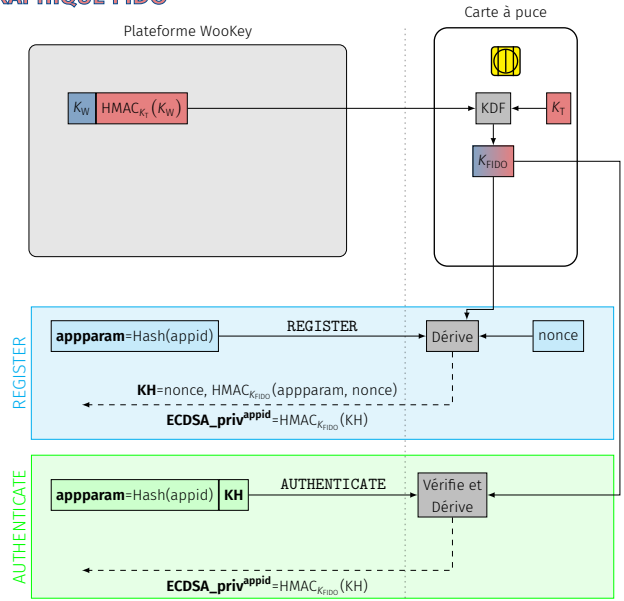
ISOLATION CRYPTOGRAPHIQUE FIDO



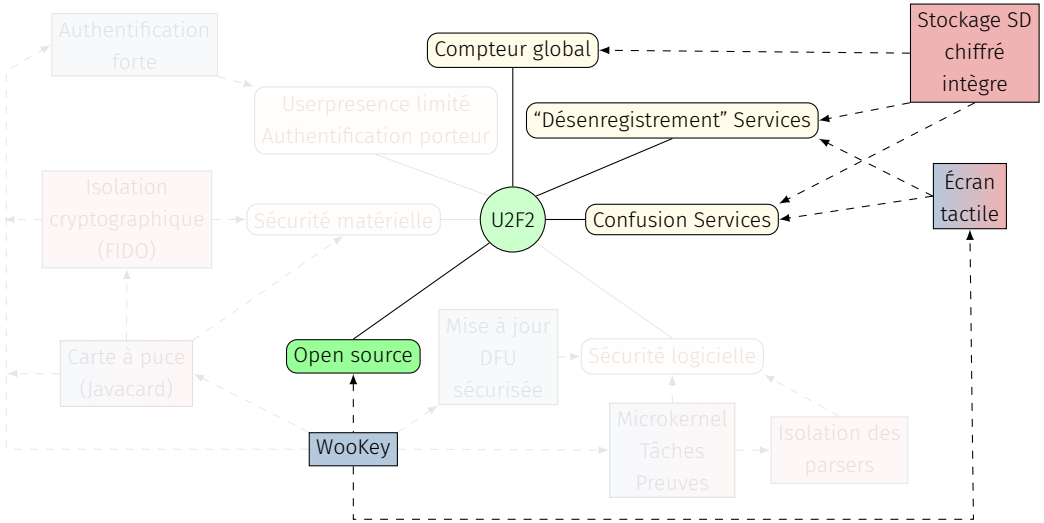
ISOLATION CRYPTOGRAPHIQUE FIDO



ISOLATION CRYPTOGRAPHIQUE FIDO



U2F2 : AIDES À L'UTILISATEUR



Identifier un compte

Identifier un compte

Service Gmail de Google

un service

Identifier un compte

Service Gmail de Google

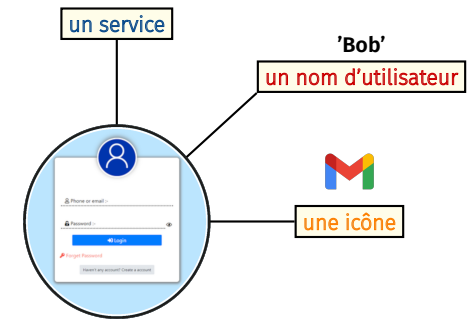
un service

'Bob'

un nom d'utilisateur

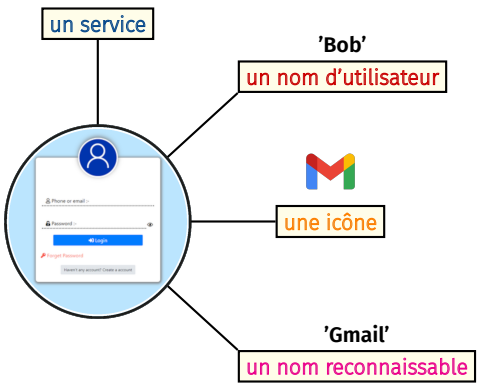
Identifier un compte

Service Gmail de Google

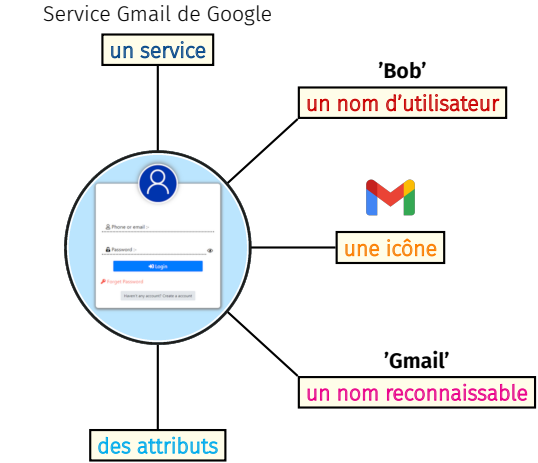


Identifier un compte

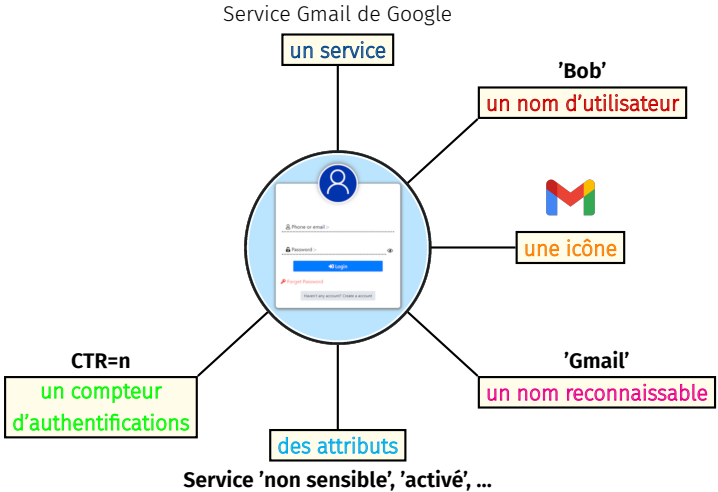
Service Gmail de Google



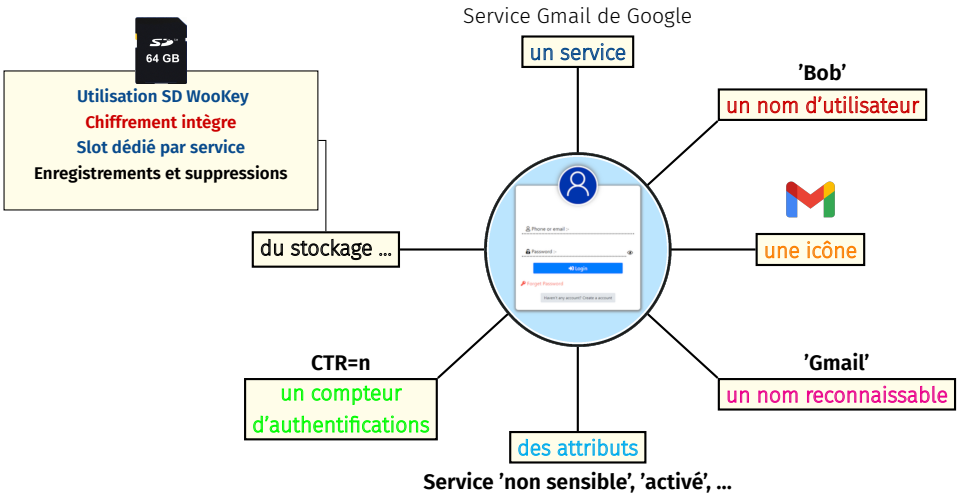
Identifier un compte



Identifier un compte



Identifier un compte



U2F2 : CINÉMATIQUE DU REGISTER

Module PIN

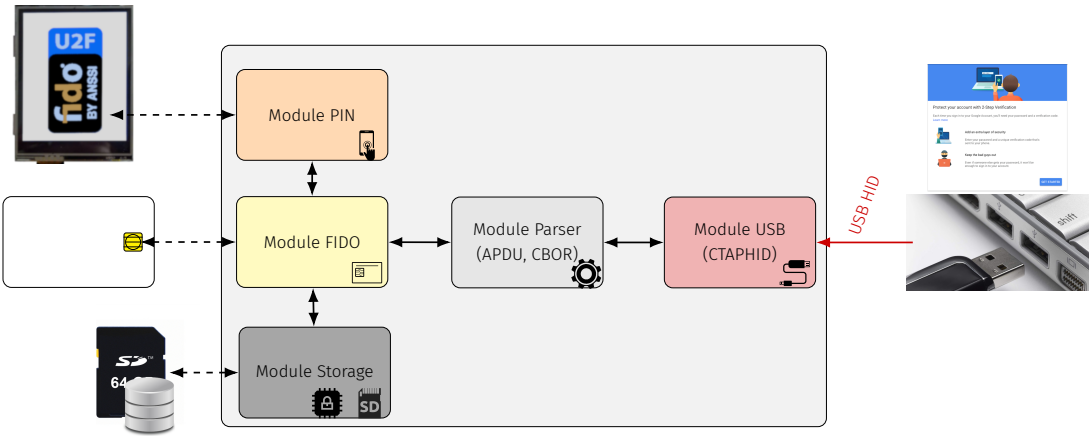
Module FIDO

Module Parser
(APDU, CBOR)

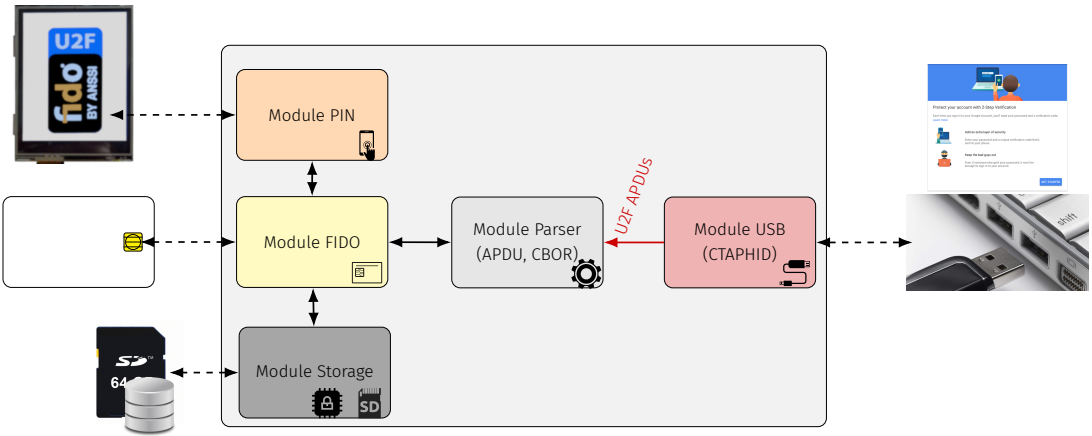
Module USB
(CTAPHID)

Module Storage

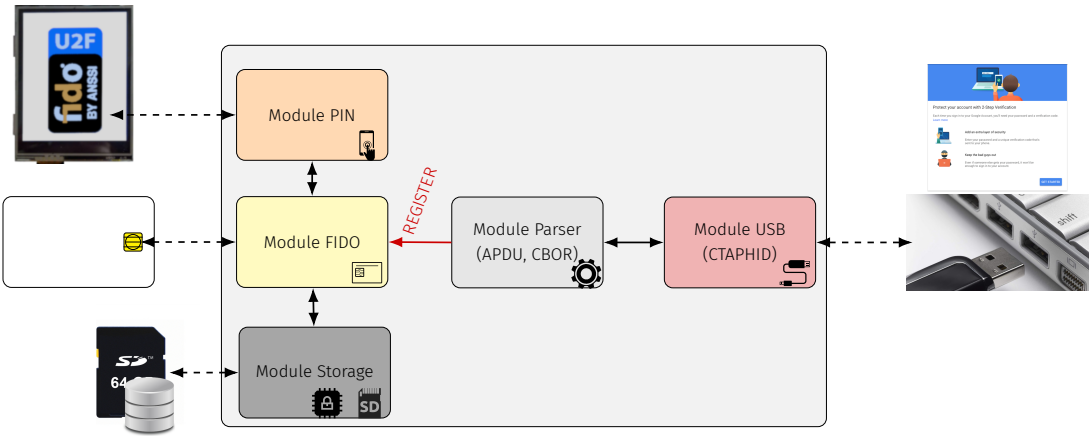
U2F2 : CINÉMATIQUE DU REGISTER



U2F2 : CINÉMATIQUE DU REGISTER



U2F2 : CINÉMATIQUE DU REGISTER



U2F2 : CINÉMATIQUE DU REGISTER

Module PIN

Module FIDO

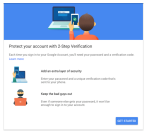
Module Parser
(APDU, CBOR)

Module USB
(CTAPHID)

Accès stockage

Module Storage

Gmail
Unused



U2F2 : CINÉMATIQUE DU REGISTER

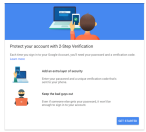
Module PIN

Information utilisateur

Module FIDO

Module Parser
(APDU, CBOR)

Module USB
(CTAPHID)



Gmail
Unused

Module Storage

U2F2 : CINÉMATIQUE DU REGISTER

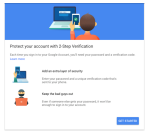
Module PIN

Module FIDO

Module Parser
(APDU, CBOR)

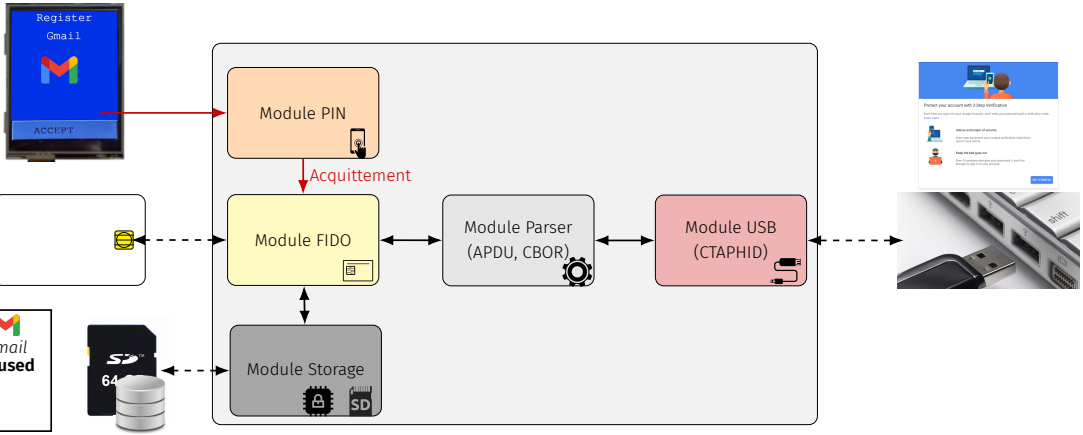
Module USB
(CTAPHID)

Module Storage

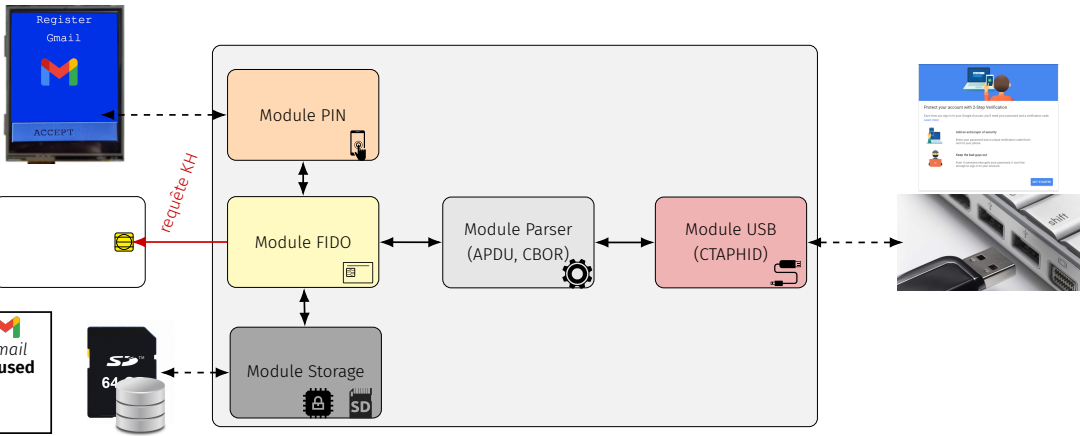


Gmail
Unused

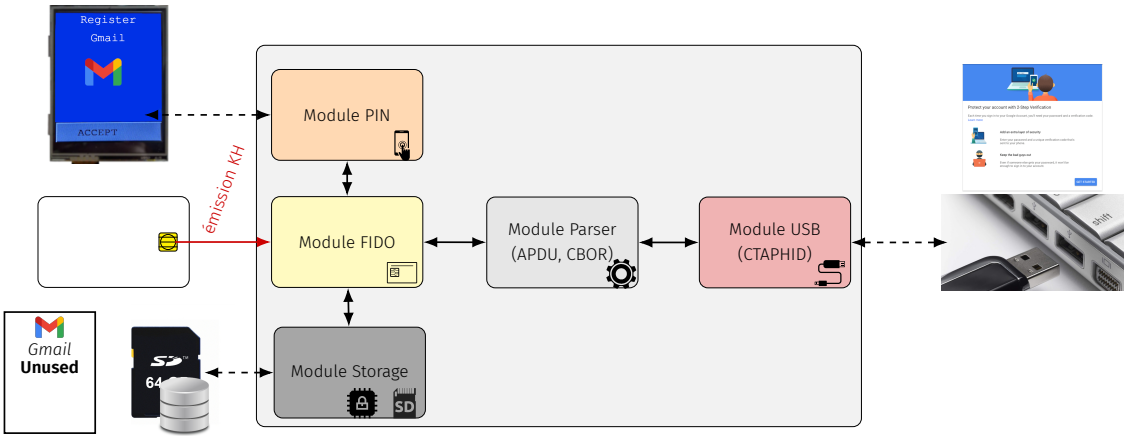
U2F2 : CINÉMATIQUE DU REGISTER



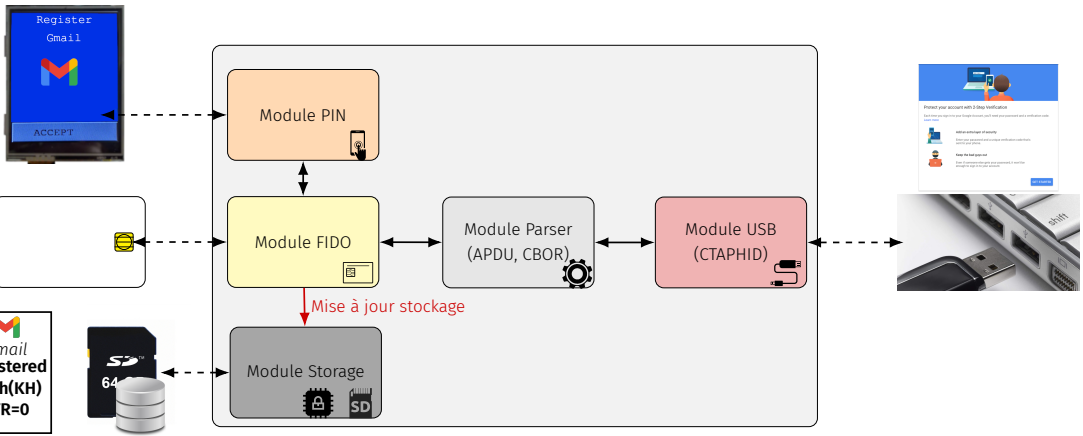
U2F2 : CINÉMATIQUE DU REGISTER



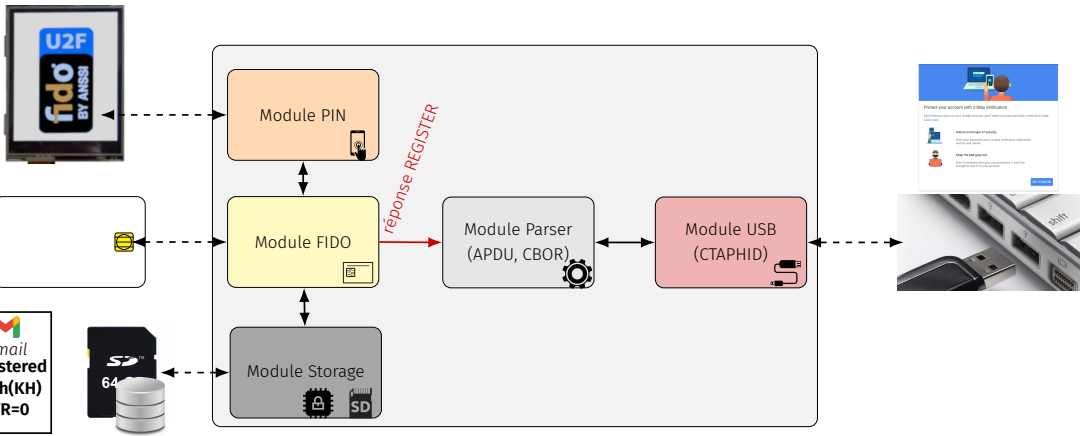
U2F2 : CINÉMATIQUE DU REGISTER



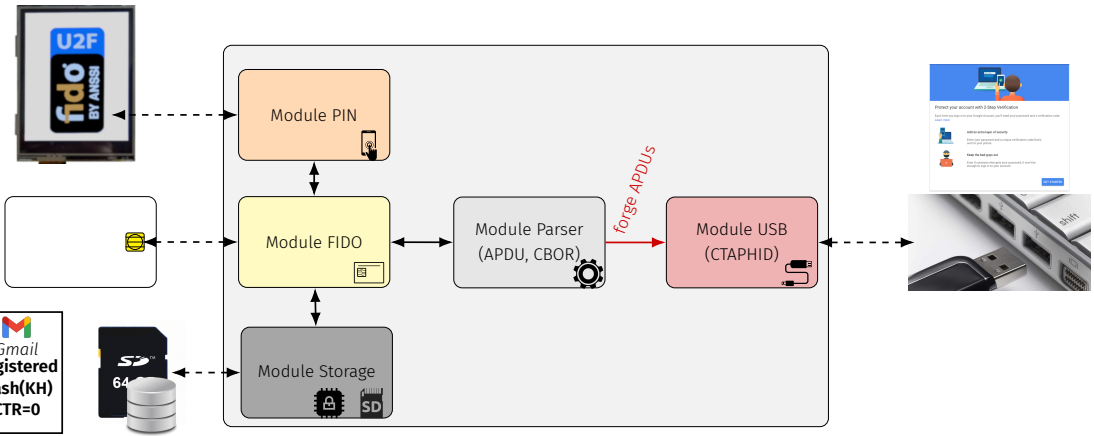
U2F2 : CINÉMATIQUE DU REGISTER



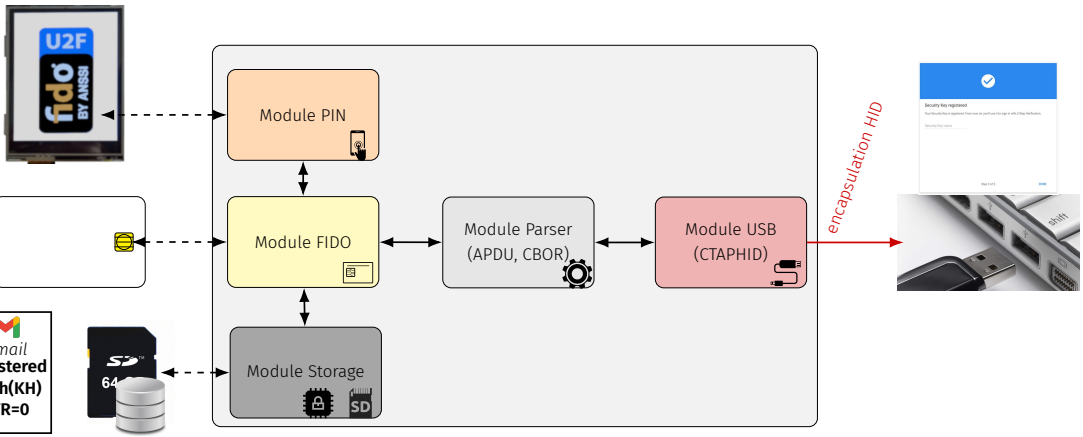
U2F2 : CINÉMATIQUE DU REGISTER



U2F2 : CINÉMATIQUE DU REGISTER



U2F2 : CINÉMATIQUE DU REGISTER



U2F2 : CINÉMATIQUE DU REGISTER

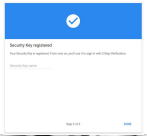
Module PIN

Module FIDO

Module Parser
(APDU, CBOR)

Module USB
(CTAPHID)

Module Storage



Gmail
Registered
Hash(KH)
CTR=0

U2F2 : APPLICATION DE GESTION DES SERVICES SUR PC

U2F2 FIDO configurator

```
Slot 0000, Slotid='@0x00002008', Appid='cdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcdcd', name='Mon service custom'
Slot 0001, Slotid='@0x00002010', Appid='53a15ba42a7c0325b8dbee289634a48f58aea3246645d5ff418f9bb8819885a9', name='Keeper'
Slot 0002, Slotid='@0x00002018', Appid='d65f005ef4dea9320c9973053c95ff6020115d5fec1b7fee41a578e18df9ca8c', name='Keeper'
Slot 0003, Slotid='@0x00002020', Appid='302fd5b4492a07b9febb30e73269eca501205ccfe0c20bf7b472fa2d31e21e63', name='Bitfinex'
Slot 0004, Slotid='@0x00002028', Appid='68201915d74cb42af5b3cc5c95b9553e3e3a83b4d2a93b45fbadaa8469ff8e6e', name='Dashlane'
Slot 0005, Slotid='@0x00002030', Appid='1b3c16dd2f7c46e2b4c289dc16746bcc60dfcf0fb818e13215526e1408e7f468', name='u2f.bin.coffee'
Slot 0006, Slotid='@0x00002038', Appid='fabeece3982fad9ddcc98f91bd2e75afc7d1f4ca544929b2d0d04212dffa30fa', name='Tutanota'
Slot 0007, Slotid='@0x00002040', Appid='70617dfed065863af47c15556c91798880828cc407fdf70ae85011569465a075', name='GitHub'
Slot 0008, Slotid='@0x00002048', Appid='968978a29953de52d3ef0f0c71b7b7b6b1af9f08e257896a8d8126918530293b', name='Amazon Web Services'
Slot 0009, Slotid='@0x00002050', Appid='6966abe3674ea2f53079eb710197848c9be6f363992fd029e9898447cb9f0084', name='FastMail'
Slot 0010, Slotid='@0x00002058', Appid='12743b921297b77f1135e41fdedd4a846afe82e1f36932a9912f3b0d8dfb7d0e', name='Bitbucket'
                                                                                                          me='Bitwarden'
                                                                                                          me='Duo'
                                                                                                          me='Stripe'
                                                                                                          me='Google'
                                                                                                          me='Gandi'
                                                                                                          me='Dropbox'
                                                                                                          me='Slush Pool'
                                                                                                          me='Slush Pool'
                                                                                                          me='GitLab'
                                                                                                          me='Fedora'
```

Application sur PC optionnelle

Permet la personnalisation de nouveaux comptes

Permet la suppression de comptes indésirables

Nécessite le séquestre de la clef chiffrée de plateforme WooKey

Edit Slot 14

appid:	f95e151ed8d4d3c767a6cc349435943794e884f3d023a8229fd
kh:	00000000000000000000000000000000000000000000000000000000
name:	Google
url:	google.com
ctr:	0
flags:	0
icon:	

Apply modifications | Delete slot | Cancel

Apport du projet

- Analyse poussée de la sécurité du Token
- Pour des contextes et services sensibles
- Prise en compte de risques écartés ou peu considérés par FIDO
  1. Sécurité logicielle et matérielle forte
  2. Anti-confusion
  3. “Désenregistrement”
  4. Compteur local à chaque compte
- Fourniture d’un prototype fonctionnel
  - Open source
  - Open hardware (base WooKey)
  - Tests de conformité U2F validés (de Yubico / Solokeys)

Limitations et roadmap

- Nombre de comptes actifs simultanés limité à 8192
- FIDO 2.0 (CBOR) en cours d'implémentation
- Personnalisation des slots sur Token (GUI embarquée) en cours de finalisation

U2F2 :
Prévenir la Menace Fantôme sur FIDO/U2F

SSTIC 2021

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

Question ?