

L'humanité vient de subir la pire fuite de données de l'histoire

NOUVELLES

Il est temps de mettre à jour votre mot de passe : 26 milliards de données personnelles viennent de fuir

L'ensemble de données atteint 12 To

Cybersécurité : des chercheurs découvrent une base de données de 26 milliards d'entrées piratées

Cette immense base renferme de nombreuses données personnelles compilées et réindexées. Un record.

“MOAB” (Mother Of All Breaches), Janvier 2024



Touraine Tech

Comment rendre possible (et sécurisée) l'authentification sans mot de passe



Julien Jimenez

Expert sécurité
Worldline



Kévin Héraud

Architecte Logiciel
Worldline

WORLDLINE 





Authentication

vs

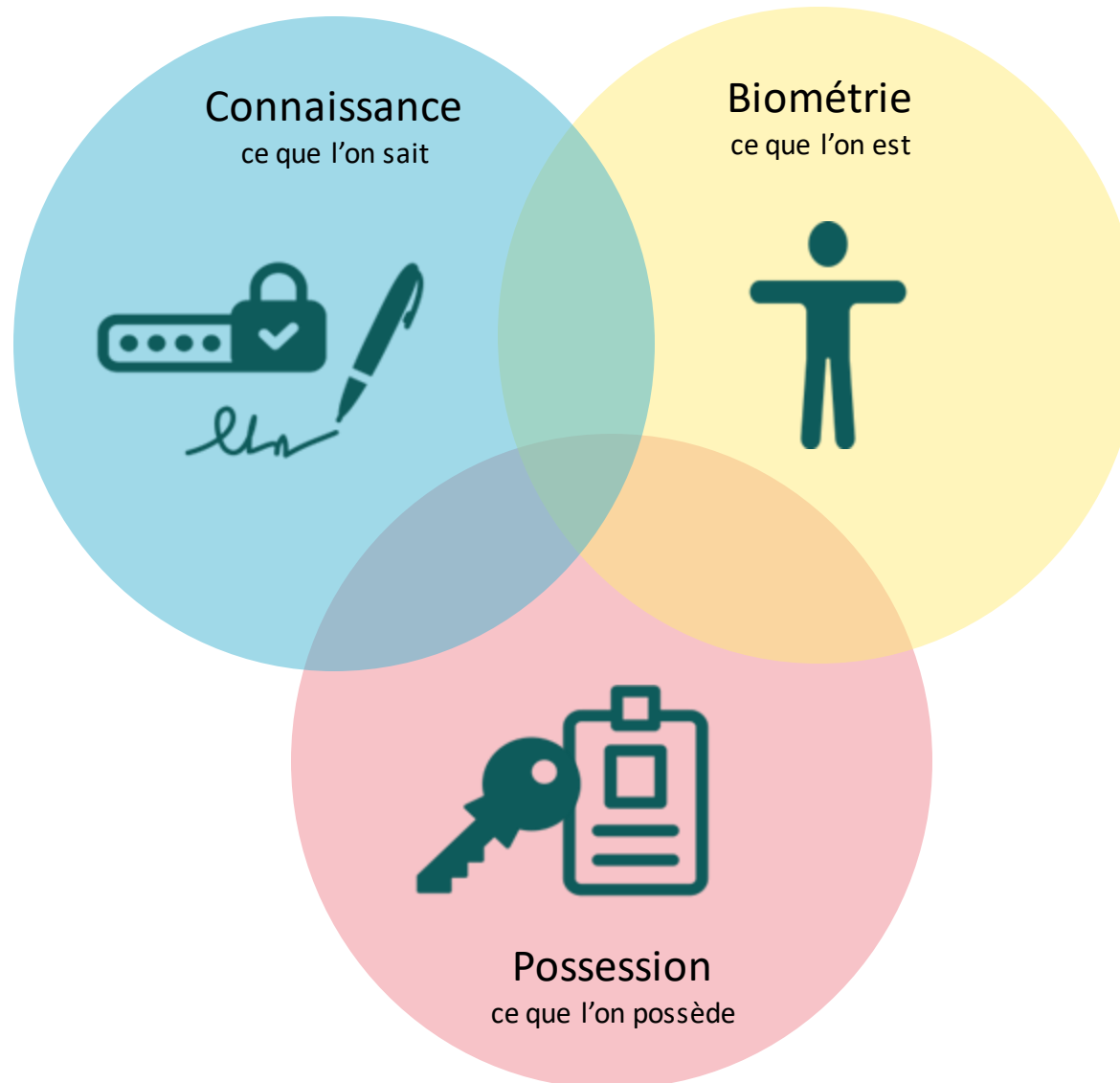
Identification

PASSWORD RAGE FATIGUE FRUSTRATION

123456789 ?
123456 ?
azerty ??
@#!?\$47# ?



Les facteurs d'authentification



Ce que je connais

- PIN
- Mot de passe
- Question secrète
- Shéma (déblocage par forme)

Principe de sécurité des mots de passe

- Format complexe
- Uniques par application
- Sécurisation du stockage
- Limiter le nombre d'essais
- Forcer le changement régulièrement
- ...

Expérience utilisateur 😞😞

- Authentification statique :

Au moment de l'authentification :

- le mot de passe est « haché »
- Le résultat est comparé à la valeur stockée

MITM Attaque



Phishing

Keylogger



Ce que je possède

- Clef RSA
- Carte PKI



=> Matériel et Logiciel propriétaire

Expérience utilisateur 😞

Peu d'interopérabilité

Sécurité 😊



Ce que je possède

- Clef RSA
- Carte PKI

=> Matériel et Logiciel propriétaire

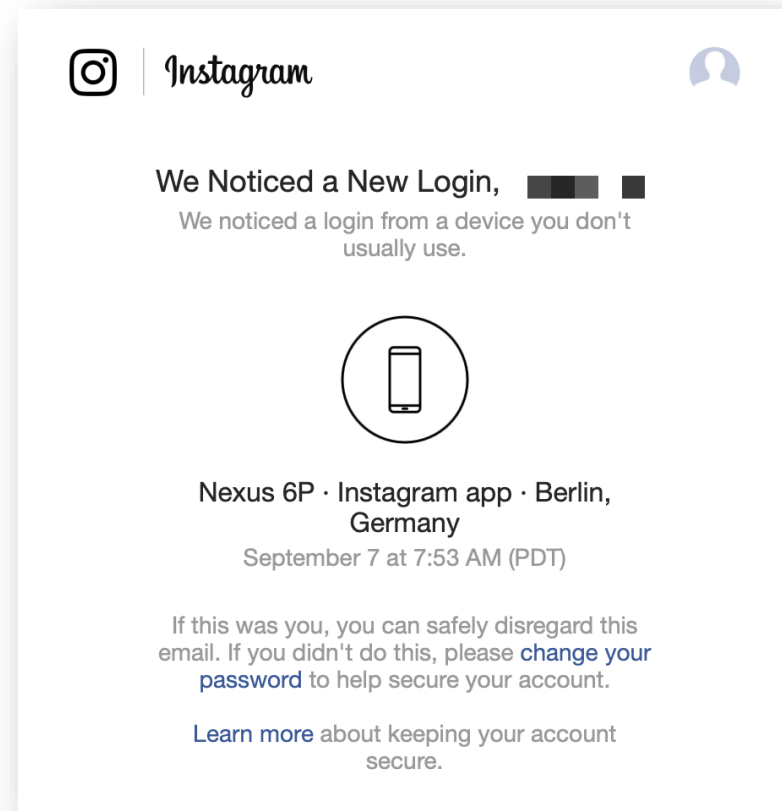


Expérience utilisateur 😞

Peu d'interopérabilité

Sécurité 😊

Device Fingerprinting



Niveau de sécurité variable



Ce que je possède

- Clef RSA
- Carte PKI



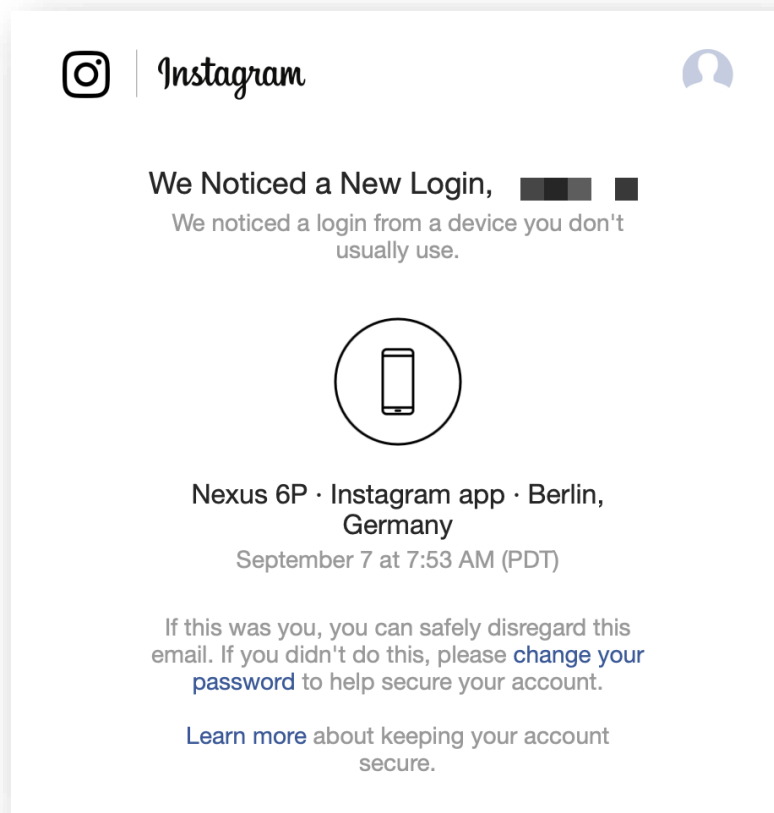
=> Hardware et Logiciel propriétaire

Sécurité 😊

Expérience utilisateur 😞

Peu d'interopérabilité

Device Fingerprinting



Niveau de sécurité 😞

SMS OTP



Smishing, Vishing

SIM Swapping



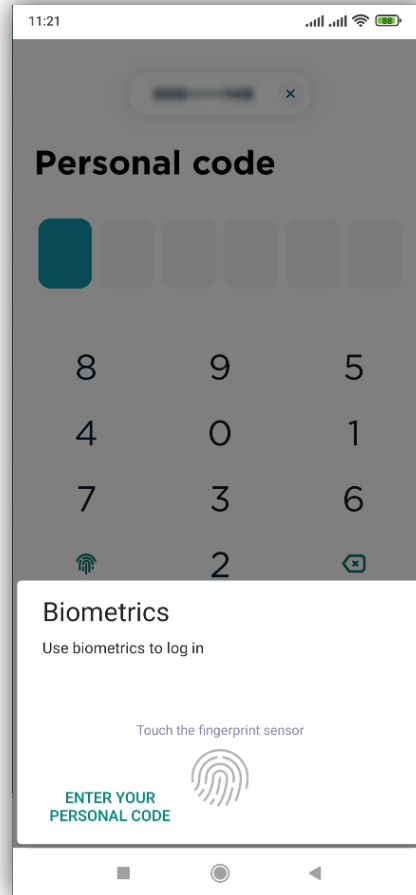
Ce que je suis

80% des smartphone équipés

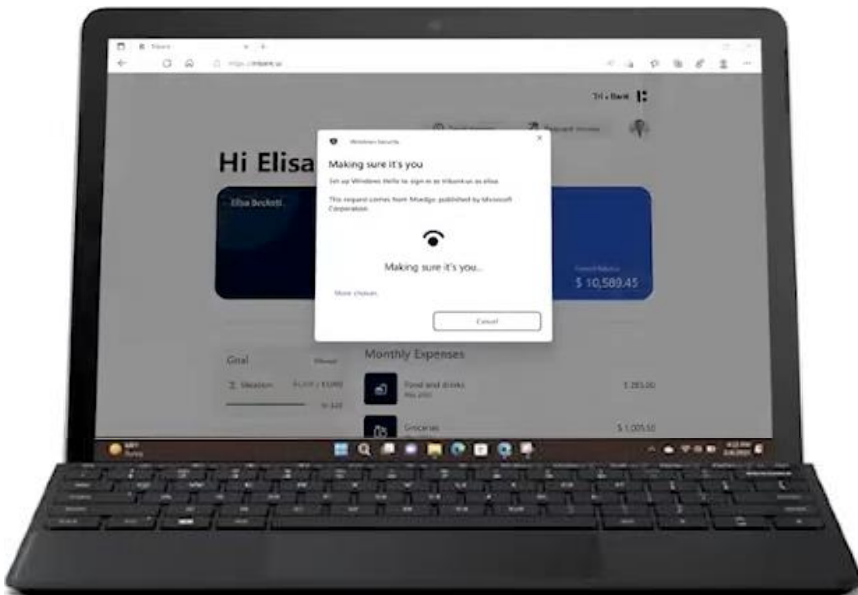
Les applis smartphone
peuvent facilement utiliser les librairies
biométriques iOS/Android



- Empreinte digitale
- Reconnaissance faciale
- Iris
- Forme de la main
- Veines de la main
- Etc.



Disponible également sur PC



Ce que je suis



- Voix
- Démarche
- Frappe au clavier
- Gestuelle
- Etc.

Comportementale

- Empreinte digitale
- Reconnaissance faciale
- Iris
- Forme de la main
- Veines de la main
- Etc.

Physiologique



**Niveau de sécurité dépend
de l'implémentation**

Vérification sur le serveur ?

Données sur le serveur ?

Vie privée ?

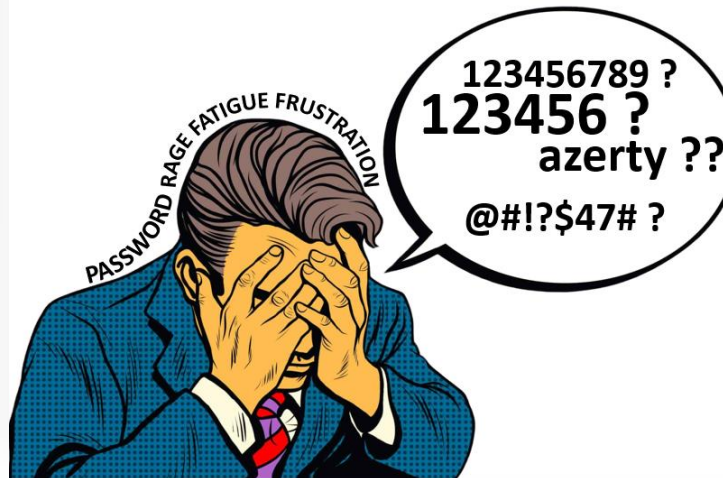


Les challenges

Interopérabilité



Expérience utilisateur



Sécurité & vie privée

Phishing

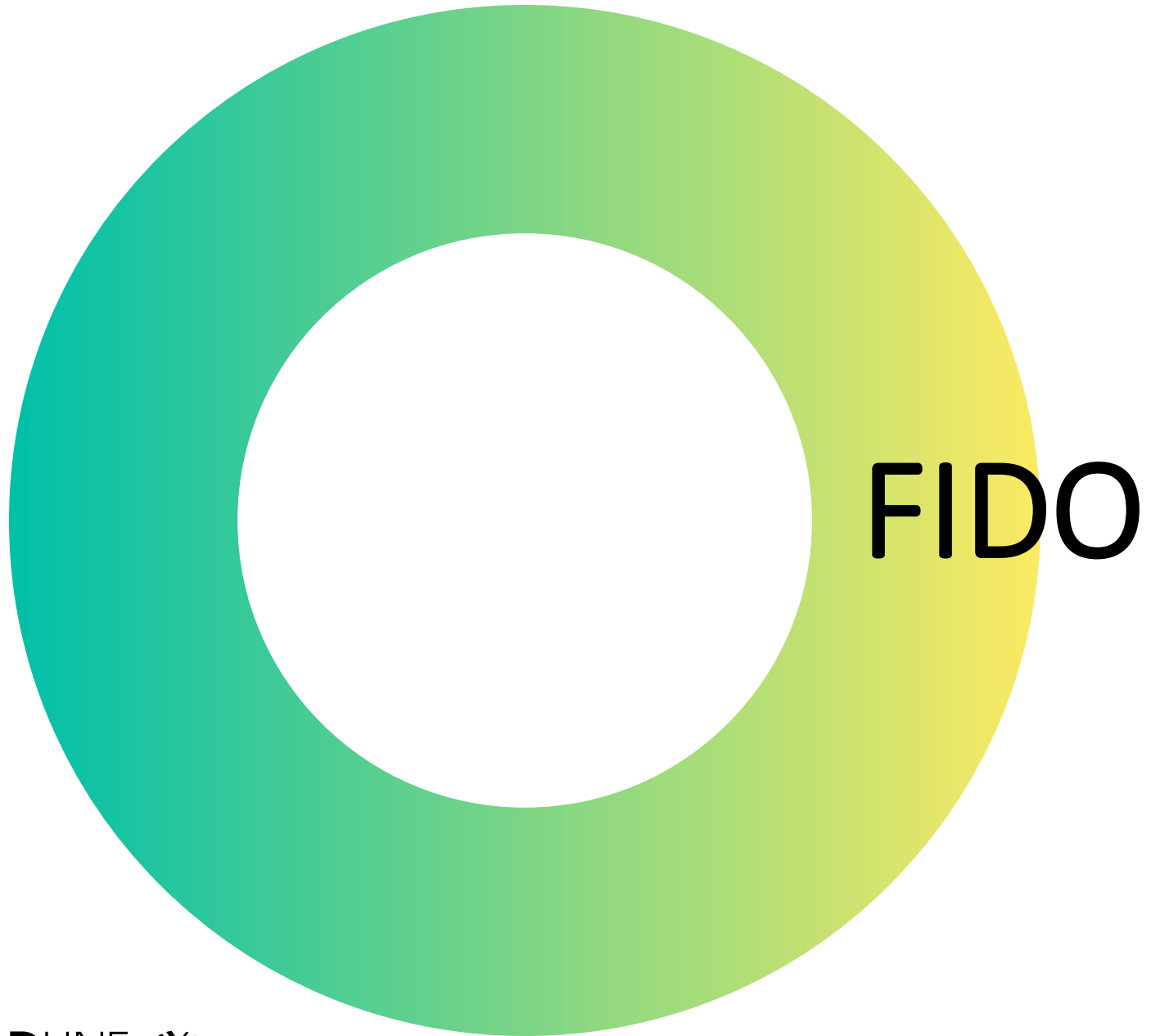
Smishing, Vishing

Evaluation du niveau de sécu

Données sur le serveur ?

Vie privée ?





FIDO



®





simpler
stronger
authentication



Qu'est-ce que FIDO ?

secure

standard passwordless

user device

Fast IDentity Online

asymmetric cryptography

2013

authentication



L'interopérabilité



FIDO2

WebAuthn

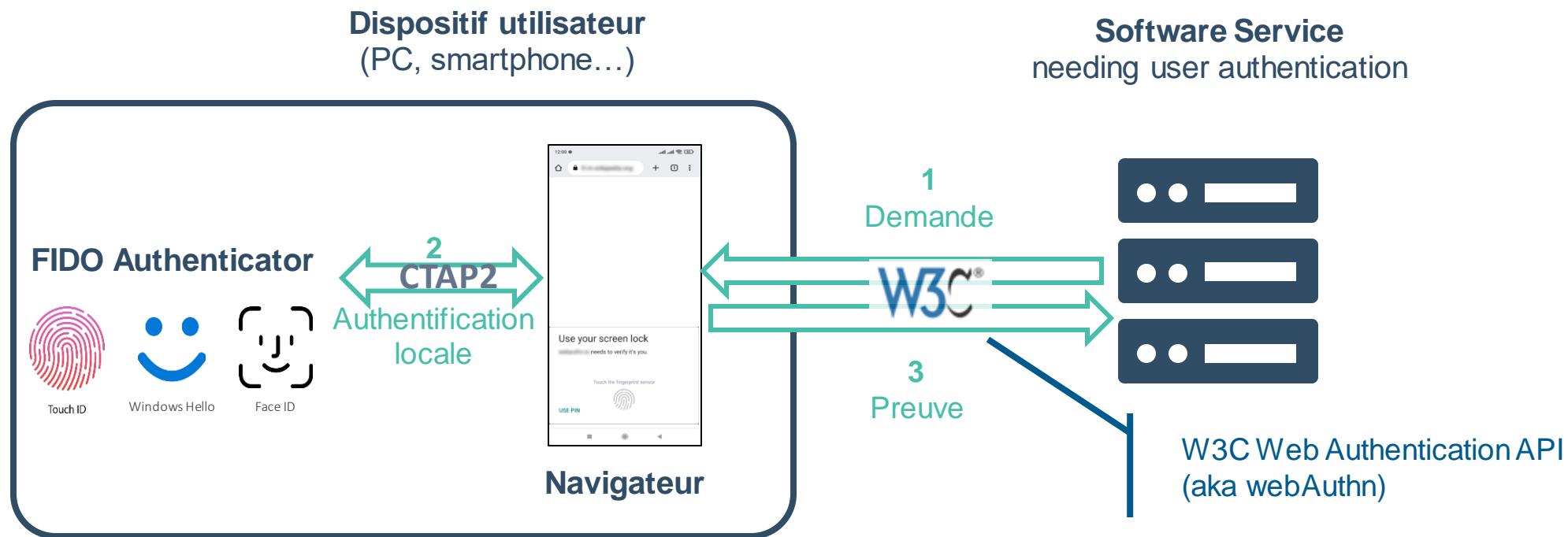
- Spécification du W3C développée en collaboration avec la FIDO Alliance
- API standard directement intégrée aux navigateurs
- Permet de créer et gérer des clés publiques

CTAP2

- « Client to Authenticator Protocol »
- Protocole facilitant l'interaction entre l'authenticator et le client
- Fonctionne en tandem avec WebAuthn



FIDO2 : Principe



Les authenticators

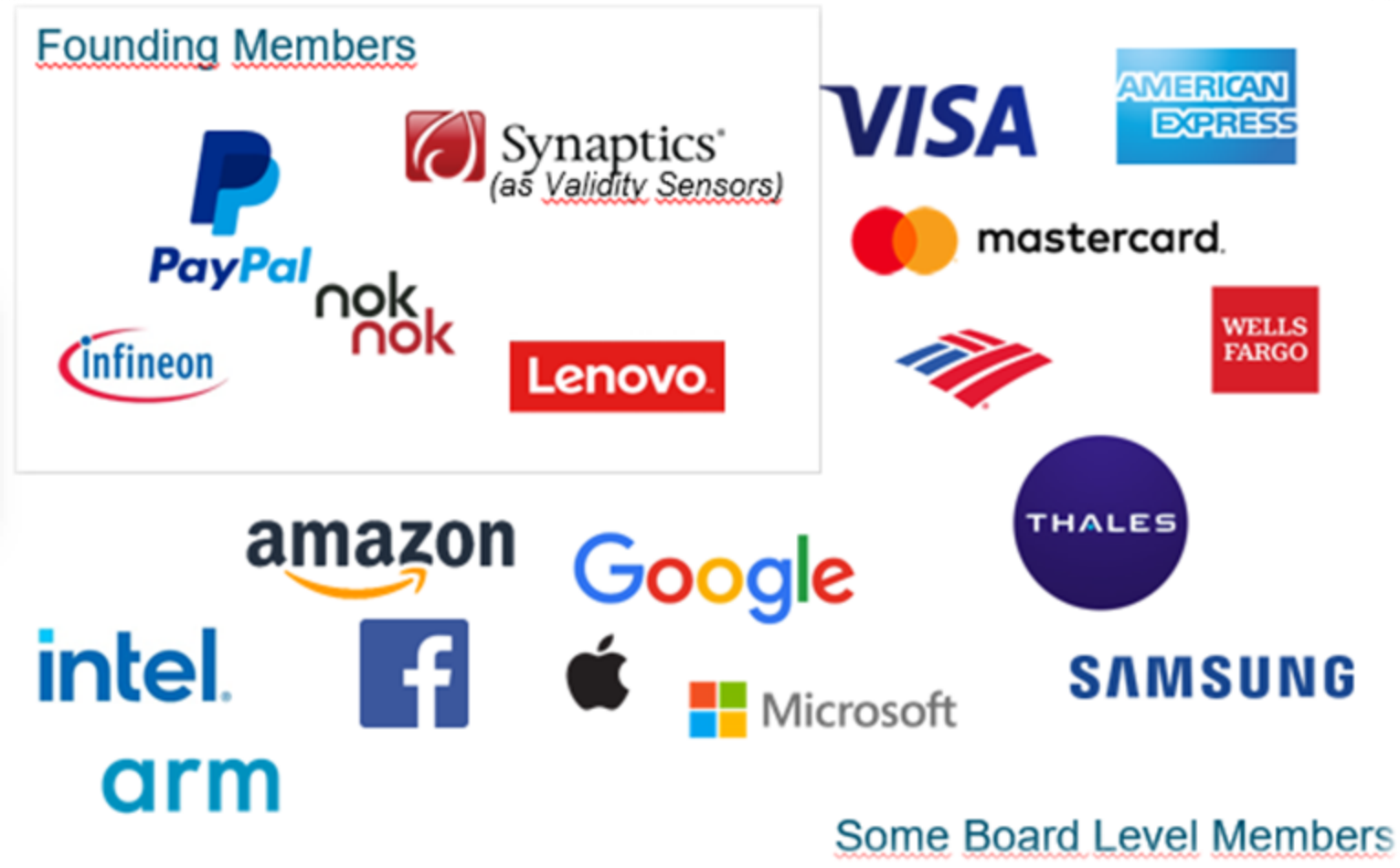


Les authenticators

- Dispositif matériel (ou logiciel) capable d'effectuer une authentification FIDO
- Platform / Cross-platform
- Doivent répondre aux exigences suivantes :
 - Génération d'une bi-clé (clé privée/clé publique)
 - Signature
 - Les clés privées restent sur le dispositif utilisateur
 - Test de présence d'un utilisateur (zone capacitive, ...)
- Peuvent également fournir une vérification de l'utilisateur (biométrie, ...)

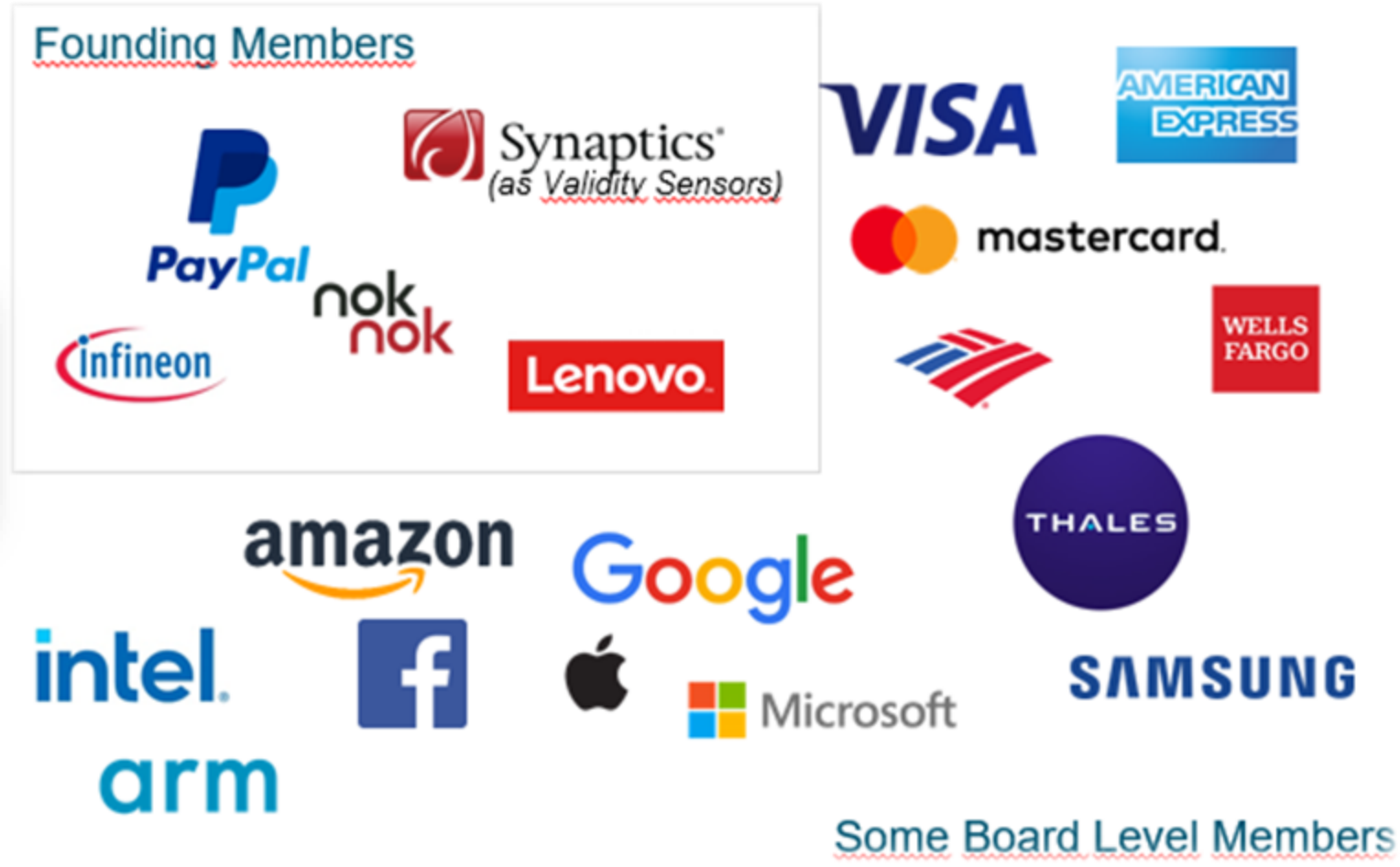


Standard reconnu





Standard reconnu



L'expérience utilisateur



Connectez-vous sans mot de passe !

Découvrez comment vous connecter en quelques secondes



J'utilise un périphérique

J'utilise la connexion de mon ordinateur

« This is a Revolution »

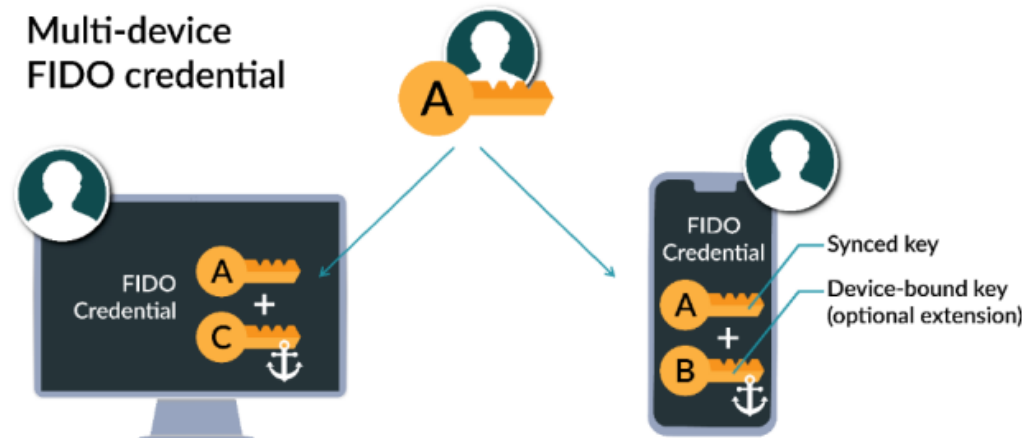
— WWDC 2022



Multi-device FIDO credentials aka Passkey



- Lancé en Mai 2022 par Apple, Google et Microsoft pour améliorer l'adoption de FIDO
- Passkey est un crédentiel FIDO, il est conçu pour fonctionner avec le protocol
- Passkey peut être sauvegardé et répliqué entre différent dispositifs, à travers les services cloud :
 - Apple KeyChain
 - Compte Google



Les clefs sont sauvegardées
via le cloud
par défaut



Multi-device FIDO credentials aka Passkey



- Fonctionnement identique à un gestionnaire de mot de passe avec un niveau de sécurité plus élevé
- Résistant au phishing (automatisation)
- Préservation de la confidentialité (uniquement côté client)



La sécurité



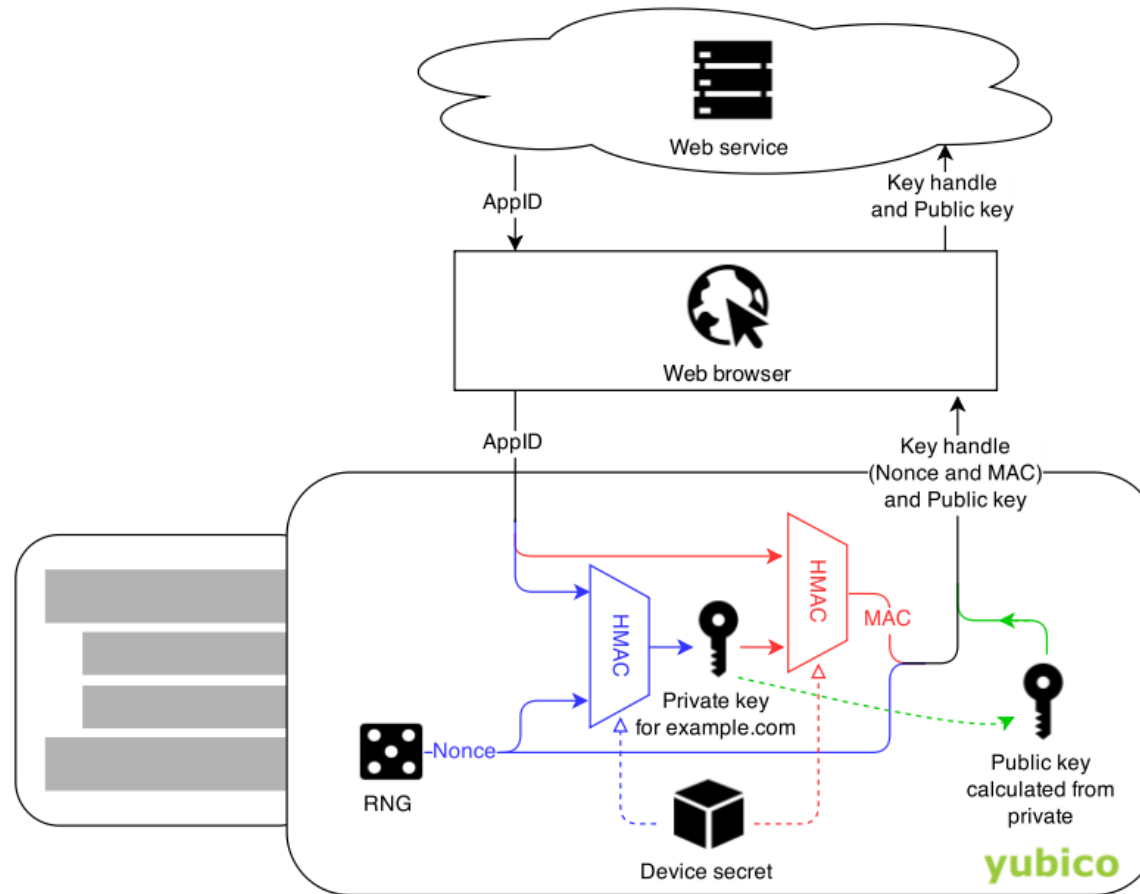


La sécurité

- FIDO ne modifie pas la sécurité intrinsèque des authenticators
- 2 facteurs plutôt qu'un seul (obligation dans le domaine bancaire)
- Cryptographie à clef publique :
 - La plateforme va générer les deux clés (publique et privée), qui fonctionnent ensemble.



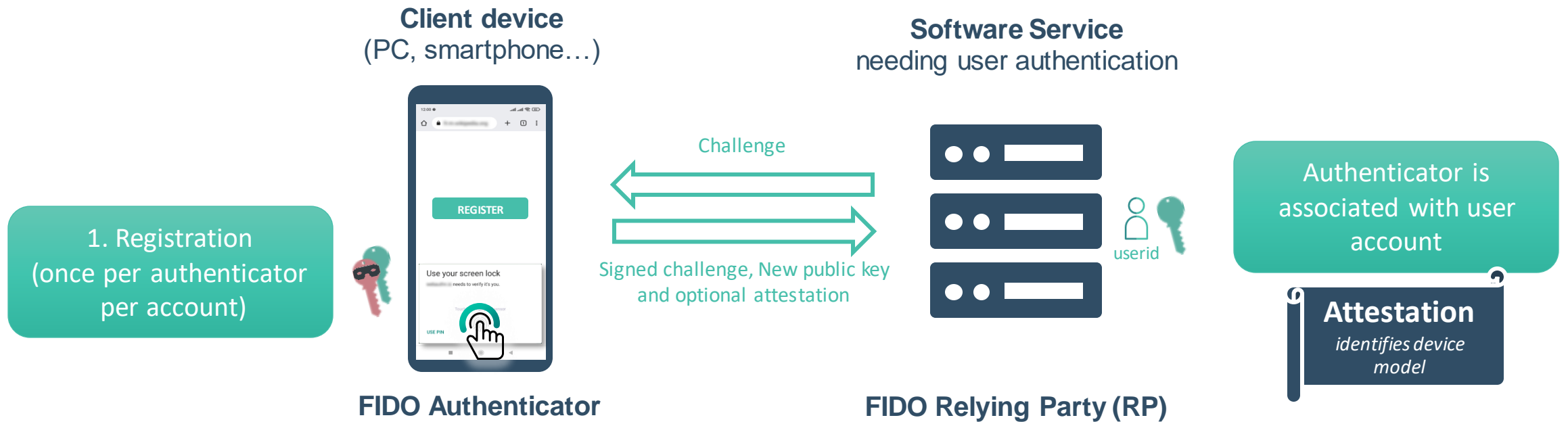
La gestion de la vie privée



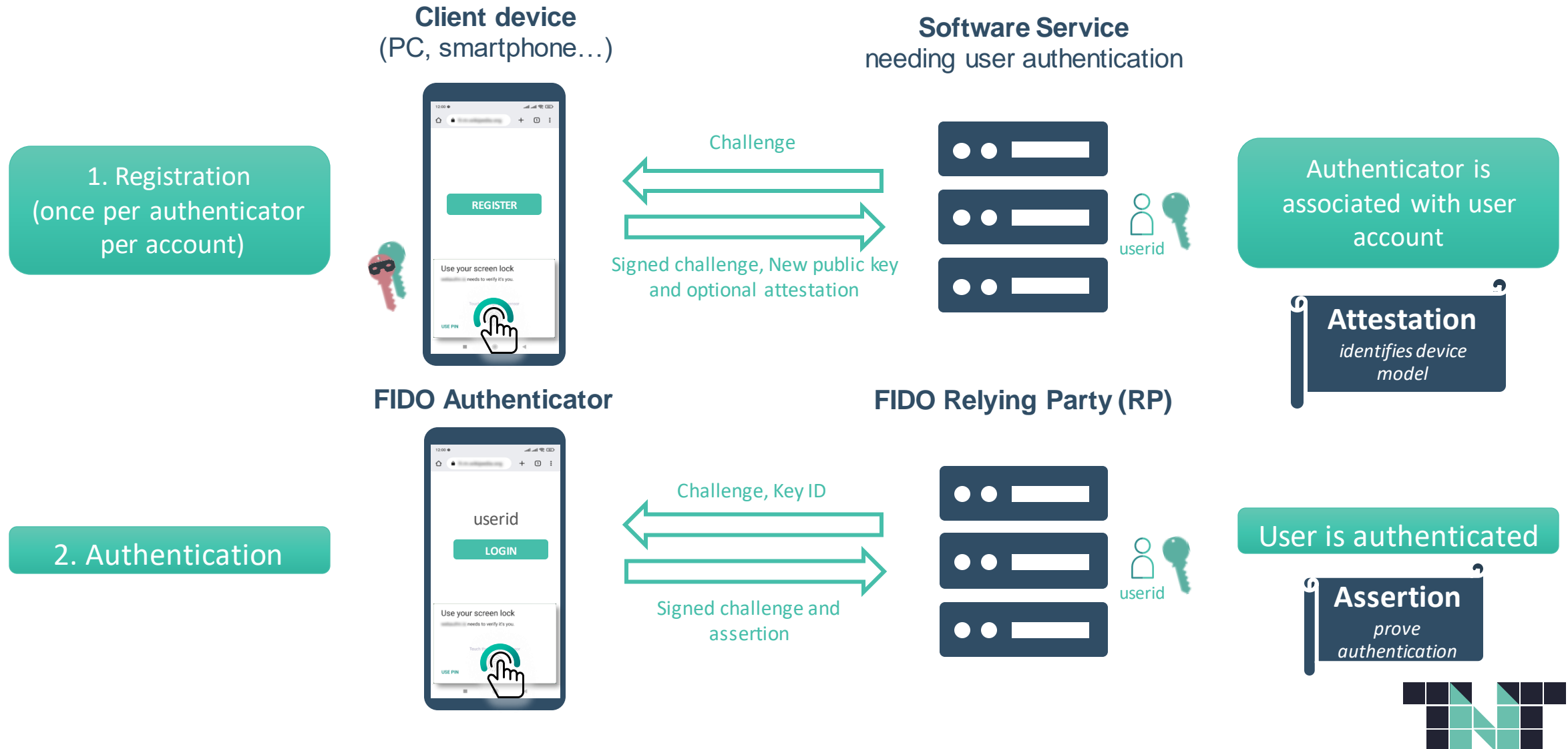
Local storage & verification of biometrics or PIN



La cryptographie à clé publique



La cryptographie à clé publique












FIDO Alliance Metadata Service (MDS)

- Informations :
 - aaguid (**A**uthenticator **A**ttestation **G**lobal **U**nique **I**Dentifier)
 - Description
 - UP (eyeprint, fingerprint, faceprint, ...)
 - Statut (FIDO_CERTIFIED_L1, FIDO_CERTIFIED_L1plus, REVOKED, FIDO_CERTIFIED_L2, ...)
 - ...
- Certificats (permet de prouver l'authenticité de l'authenticator)
- Autre cas d'utilisation :
 - Filtrer les authenticateurs → politiques de sécurité



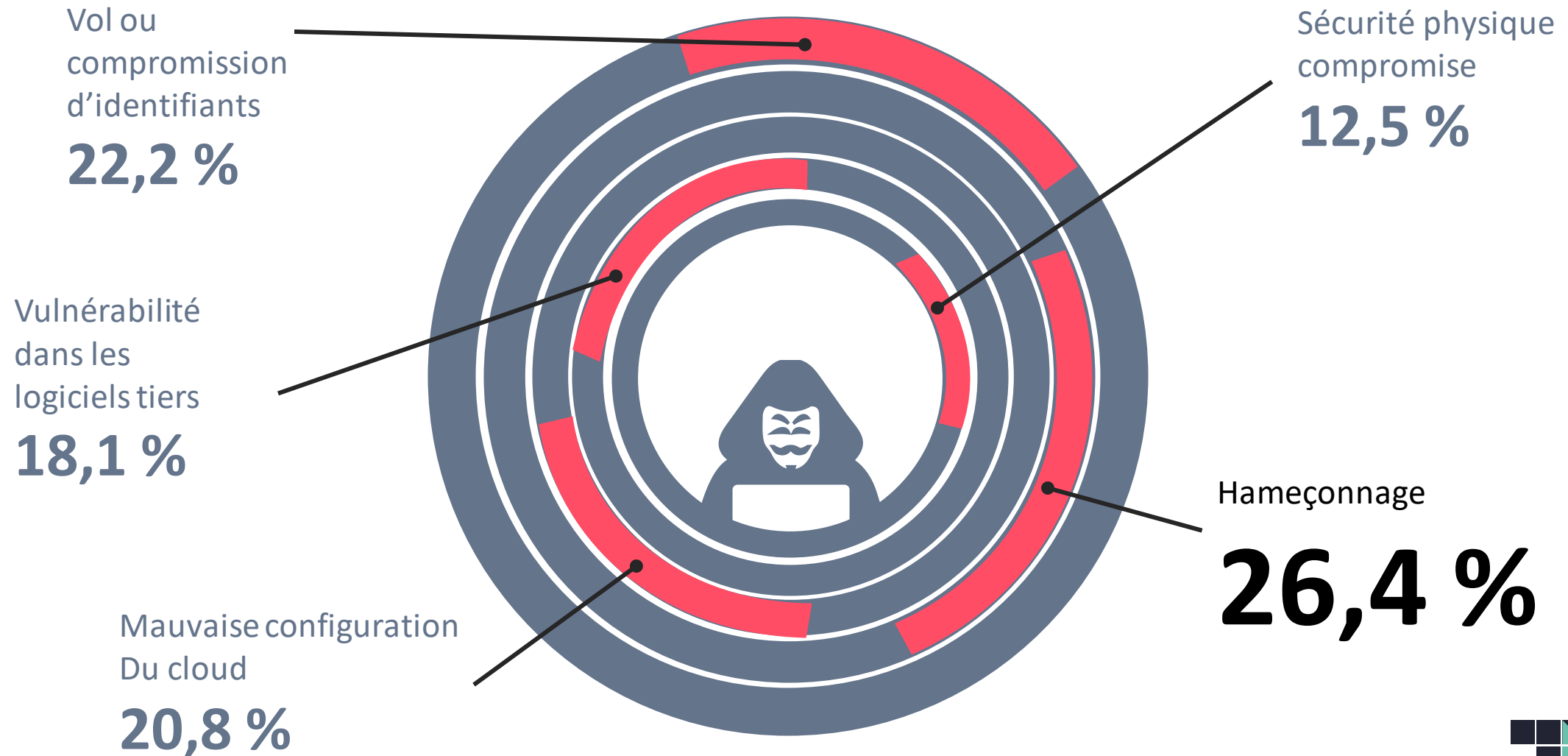
Les authenticators / certification

| | | | |
|-----|---|--|---|
| L3+ |  | USB U2F Token built on a CC-certified Secure Element Certification: L3+ | |
| L3 |  | USB U2F Token built on a basic simple CPU, OS is certified. Good physical anti-tampering enclosure Certification: L3 |  UAF implemented in a TA running on a certified TEE with POP memory Certification: L3 |
| L2+ | |  FIDO2 making use of the Android keystore. Keystore runs in a TEE that is certified at L2+ Certification: L2+ | |
| L2 | |  L2: UAF implemented as a TA in an uncertified TEE Certification: L2 | |
| L1+ | |  L1+: U2F in downloadable app using white box and other techniques Certification: L1+ | |
| L1 |  | Downloaded app making use of Touch ID on iOS Certification: L1 |  FIDO2 making use of the Android keystore. Keystore is not certified Certification: L1  FIDO2 built into a downloadable web browser app Certification: L1 |



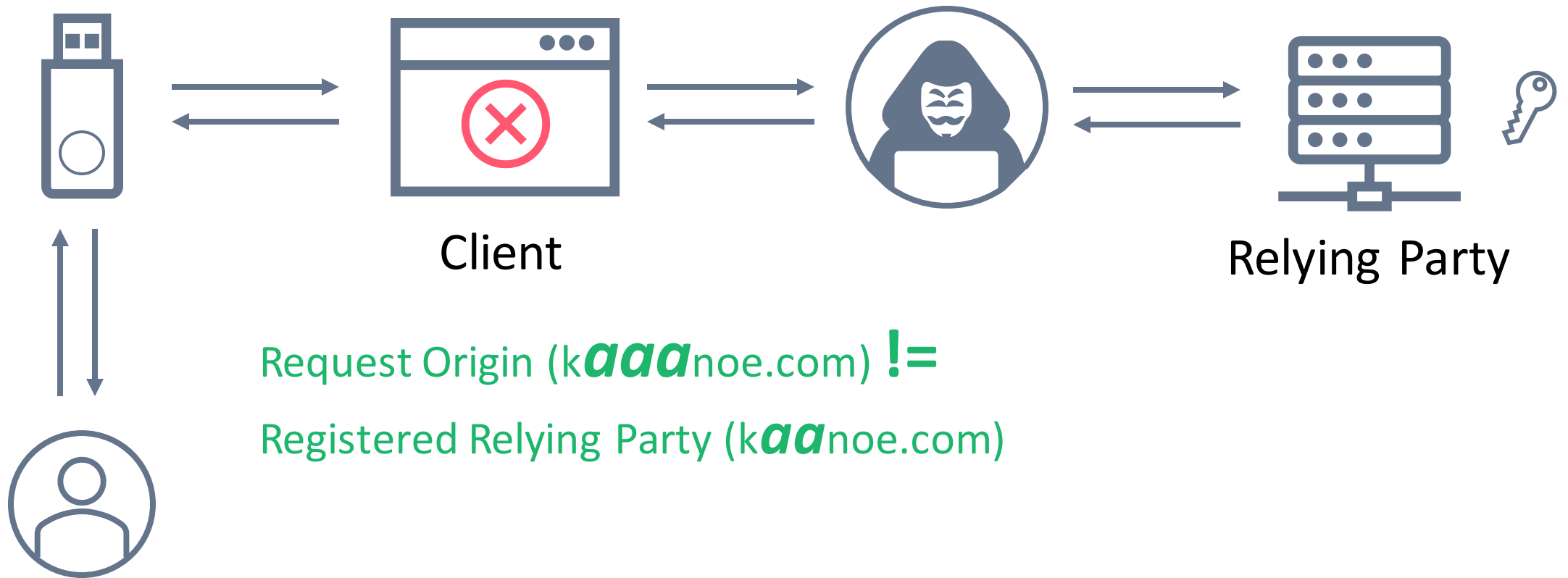


Le phishing, ennemi public numéro 1 !

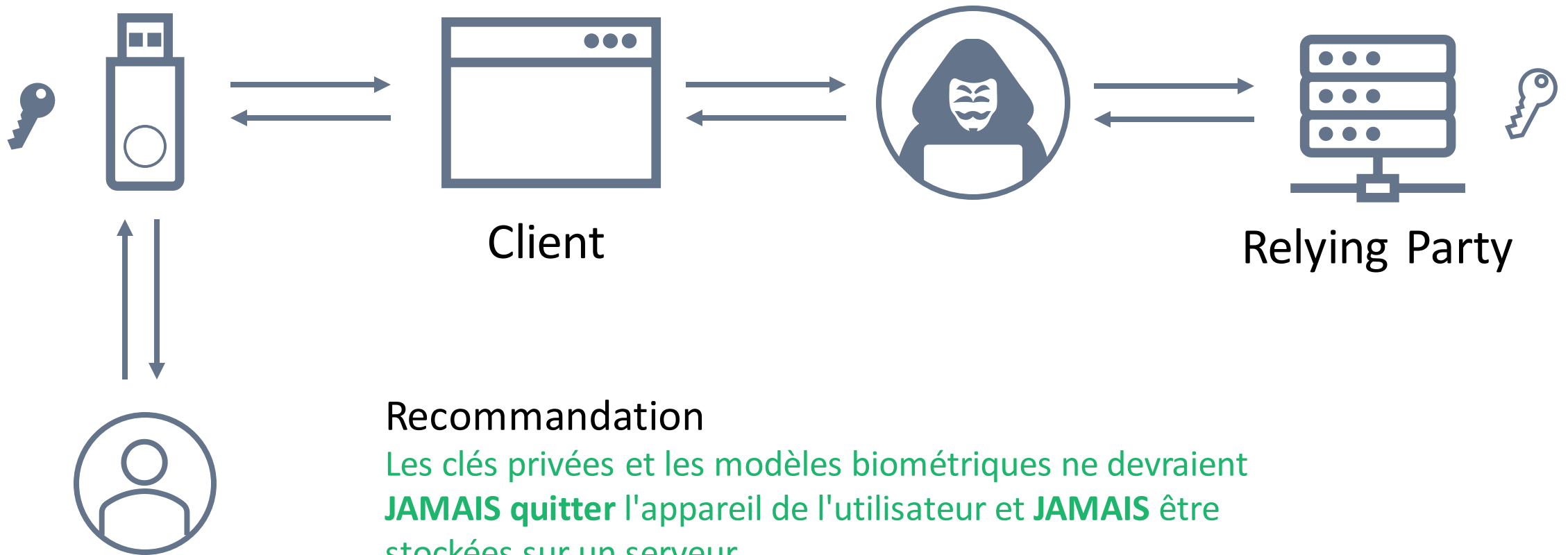


Phishing

key icon → kaanoe.com



Man In The Middle



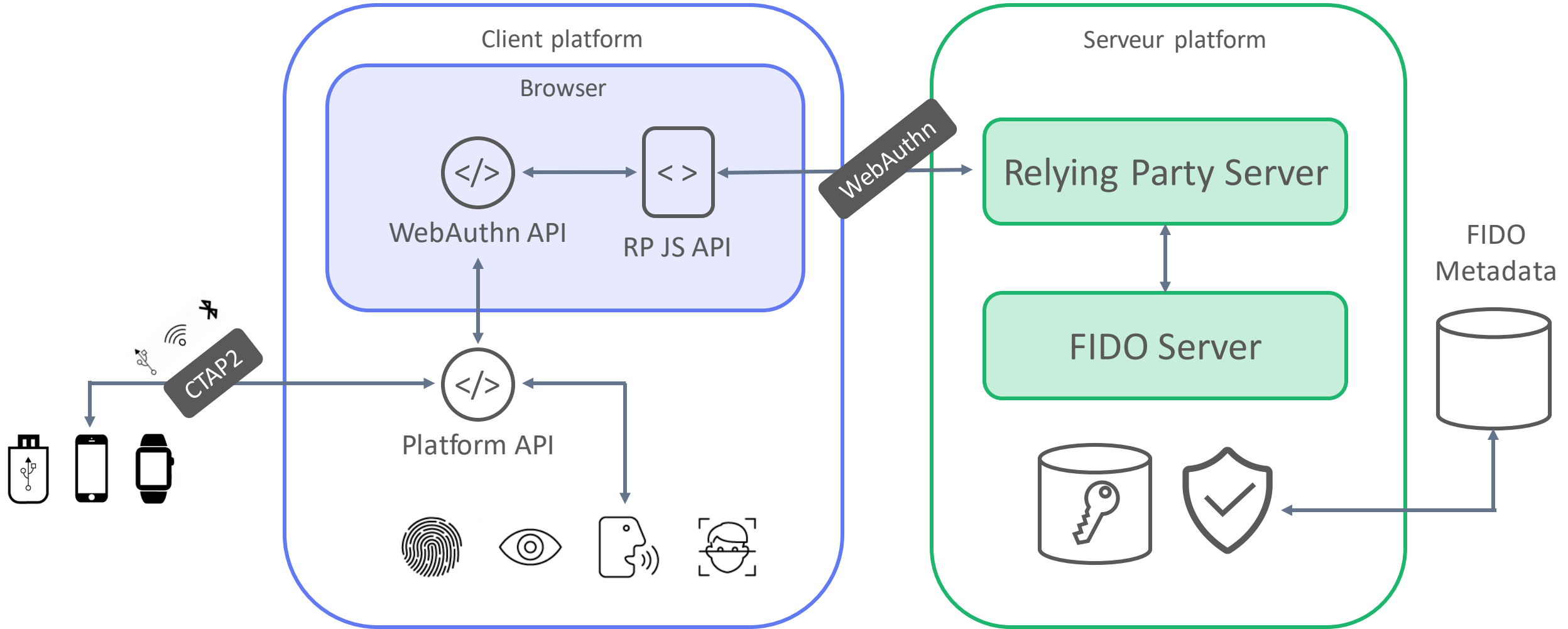
L'expérience développeur



DEMO



Vue d'ensemble de l'architecture FIDO



W3C WebAuthn API



```
navigator.credentials.create()
```

```
navigator.credentials.get()
```

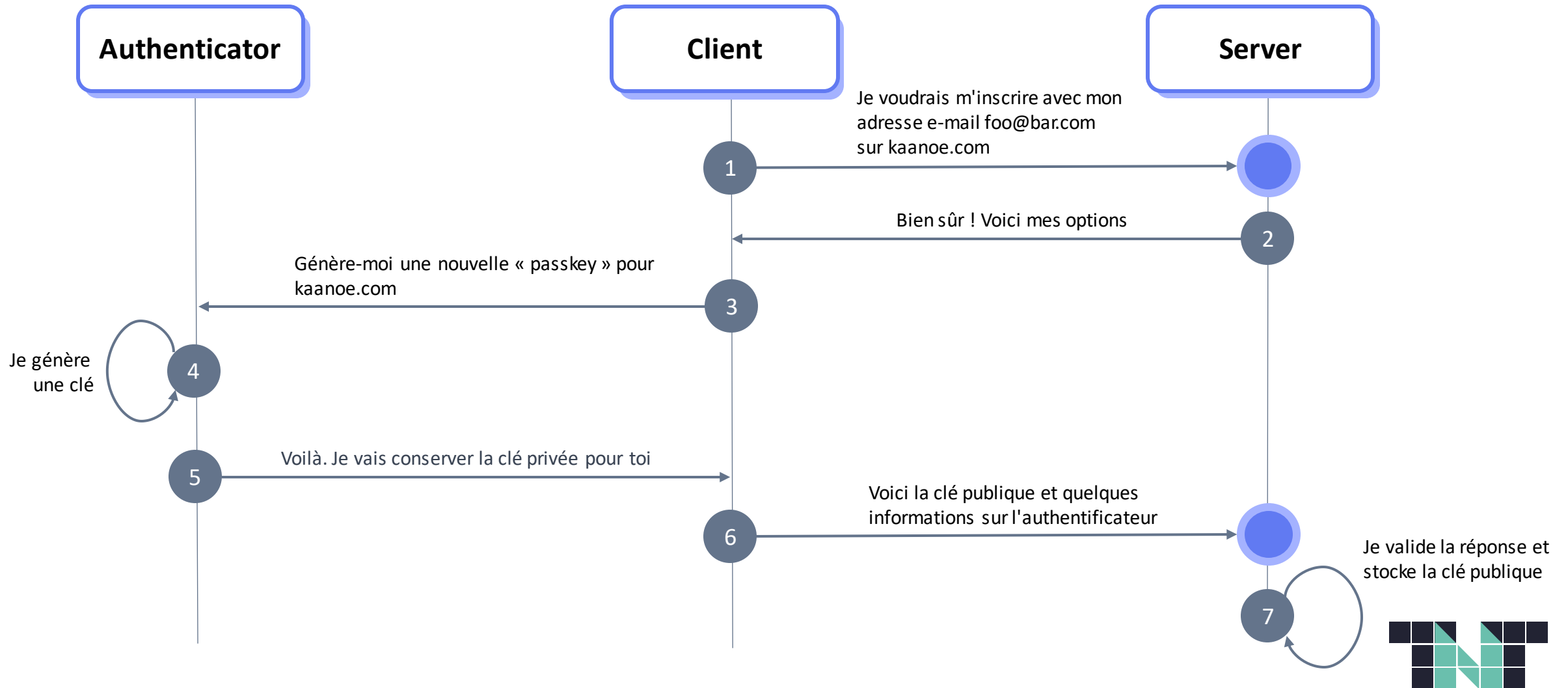


WebAuthn ceremonies

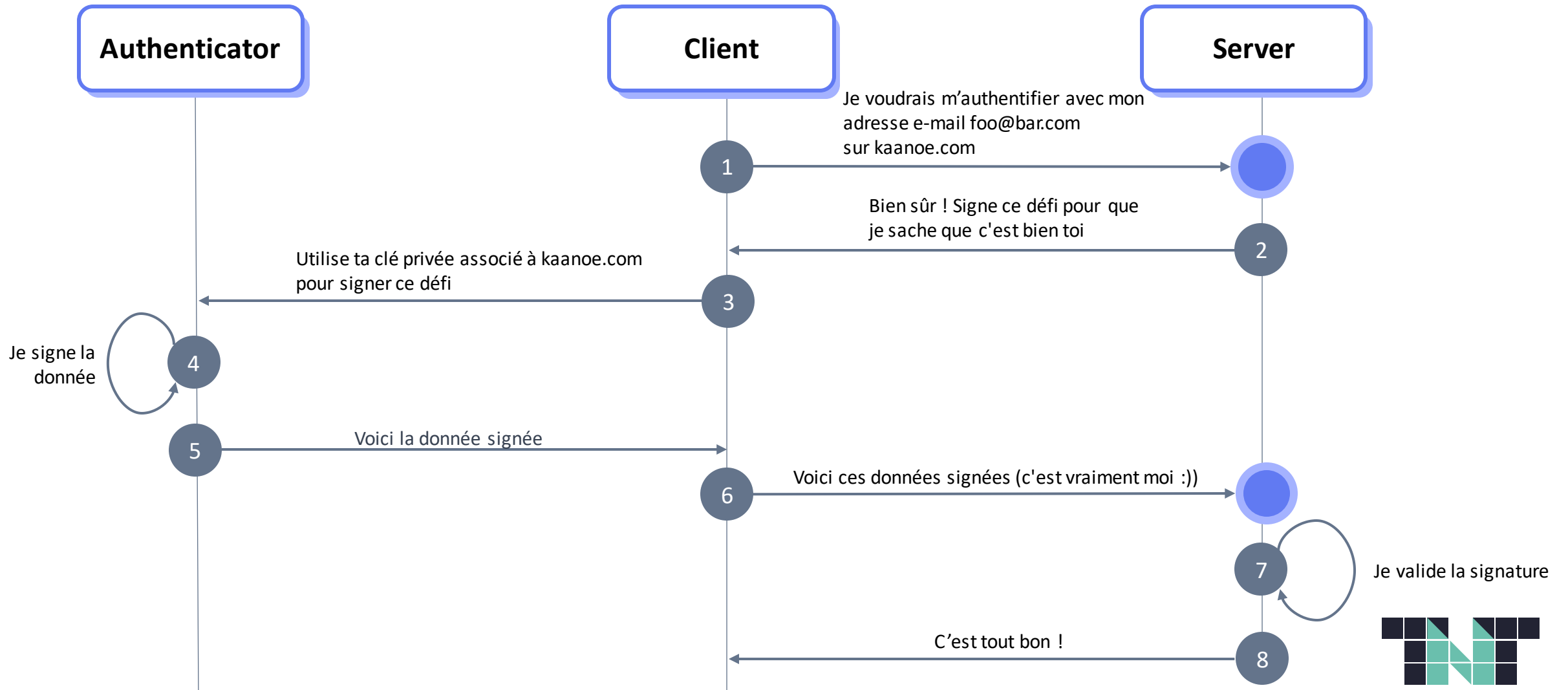
Ensemble des moyens (logiciel et humain) mis en œuvre dans le cadre de la génération et la conservation d'une clé privée



WebAuthn ceremonies / Registration



WebAuthn ceremonies / Authentication



WebAuthn conditional UI



```
<input type="text" id="username" autoComplete="username webauthn" />
```

Sign in

Email



john.doe@mail.com



Passkey created on Feb 12, 2022



Pour conclure

Privacy By Design

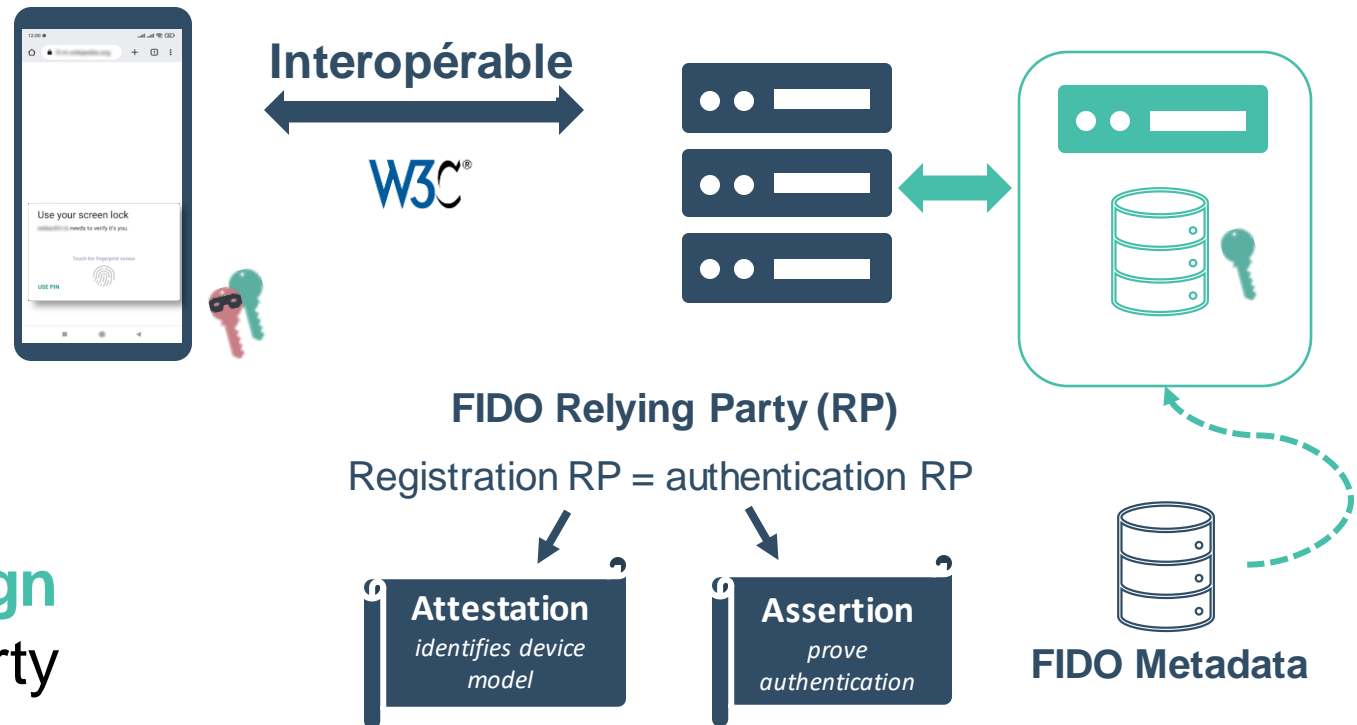
Stockage local et
décentralisé des données
biométriques

Security By Design

One keypair per relying party
Keys stay on authenticator
Protocol protects against attacks

On device biometrics

Offre une expérience conviviale et
un processus de connexion simplifié



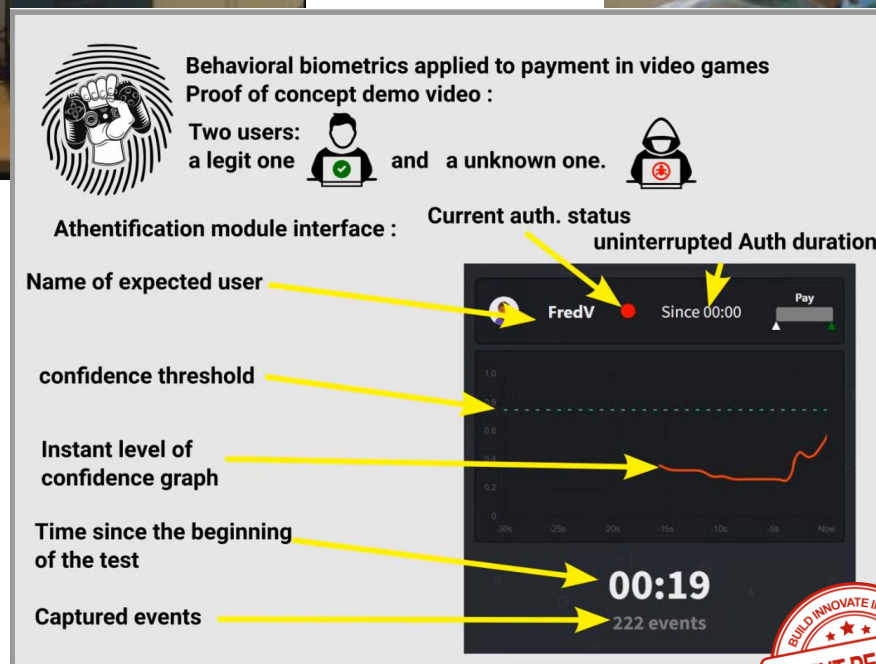
Exploration



First results: measuring efficiency KPI → Is it good enough for payment?



Payment score is continuously processed



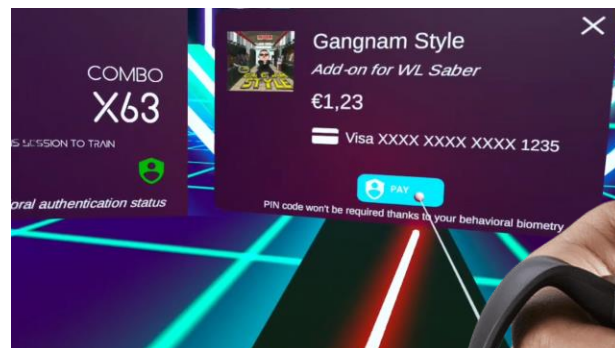
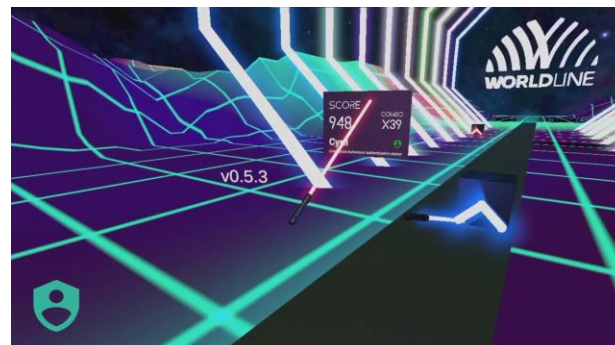
In case of an usurper
the score decreases
drastically
Tunning threshold
integrating time factor : 30s



Immersive Payment in VR-Gaming



Looking forward to innovative uses cases



Virtual Reality

Exploration of Virtual worlds and their impacts on new customer journey

Immersive and instant payment in VR-gaming



Démo sur le stand Worldline



Behavioral biometrics for gaming



Merci pour votre feedback

