Le chiffrement pour ceux qui n’y connaissent rien

1er juillet 2020 @ PRISM

DEVOPS

TAHITI

PRISM

- https://prism.pf
- Incubateur de la CCISM
- 29 startups incubés dont 22 toujours vivants
- 69 candidatures sur l’appel à projets 2020

Clusir-PF

https://www.clusir-tahiti.org/

Tahiti DevOps

- https://devops.pf ou https://tahiti.dev
- DevOps = Dev + Ops
- une présentation chaque 1er mercredi du mois
- partager la connaissance
- faire des rencontres

DEVOPS

TAHITI

PRISM
INCUBATEUR DE PROJETS POLYNÉSIENS

DEVOPS
TAHITI

Informations pratiques

- slides disponibles sur https://devops.pf/chiffrement.pdf
- vous pouvez prendre des photos, mais pas du public
- vous pouvez posez des questions à n'importe quel moment
- il n'y a pas de questions idiotes

Moment wikipédia

- Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un **document** impossible à toute personne qui n'a pas la **clé** de (dé)chiffrement.

- https://fr.wikipedia.org/wiki/Chiffrement

Pourquoi chiffrer ?

- stocker ou envoyer une information en minimisant le risque qu'il soit lu ou modifié par un tiers
- vérifier qu'un document vient bien de l'expéditeur, et qu'il n'a pas été modifié
- exemple : envoyer un email, payer sur internet, consulter un site web, installer une application sur un smartphone

Pourquoi comprendre le chiffrement ?

- Est-ce que vous seriez d'accord pour que «les autorités» aient une copie de toutes vos clefs (voiture, maison, cadenas de vélo etc...) ?
- Pourquoi comprendre comment fonctionne le moteur de la voiture ?
- Le chiffrement est un enjeu pour la vie privée des jeunes dans l'avenir du futur de demain
- Mais en fait, c'est déjà un problème aujourd'hui

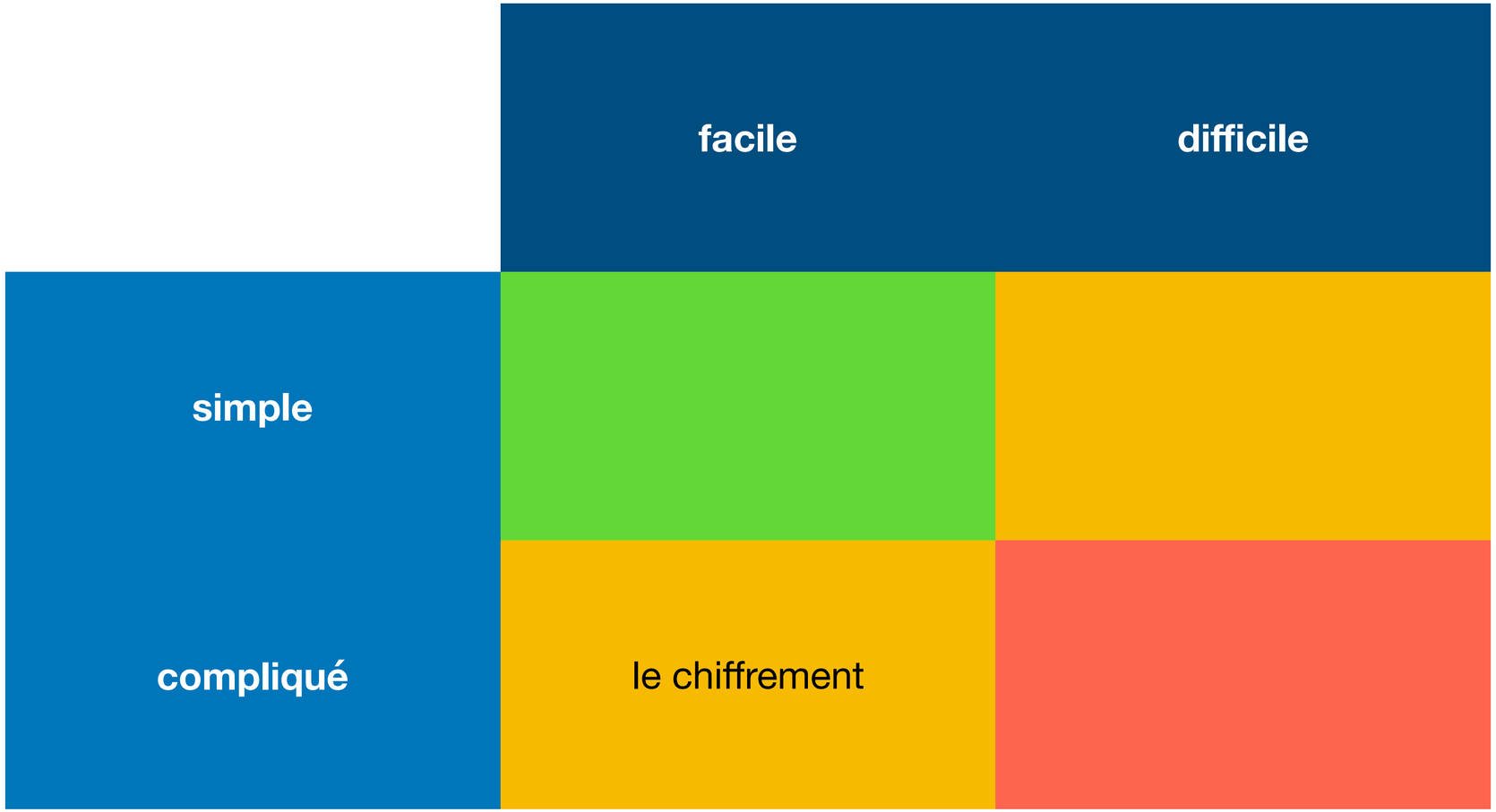
PRISM
INCUBATEUR DE PROJETS POLYNÉSIENS

DEVOPS
TAHITI

c’est pas difficile

	facile	difficile
simple	cligner des yeux	soulever une pierre de 100 kgs
compliqué	résoudre un puzzle de 1000 pièces	jongler avec des boules de bowling

c’est juste compliqué



de quoi on va parler

- métadonnées
- hachage
- chiffrement (#CaptainObvious)
- signatures électroniques
- certificats

de quoi on ne va pas parler

- certificats de révocation
- collision d’algorithme de hachage
- courbes elliptiques
- PKI
- etc ...

Embêter les drosophiles

- en informatique, la précision est vitale, l'imprécision est fatale
- en français, le digital, c'est tout ce qui a rapport aux doigts («empreintes digitales»)
- en anglais, le «digital», c'est tout ce qui a rapport au «digit», i.e. les nombres
- donc le «digital» en anglais, c'est le «numérique» en français

Embêter les drosophiles

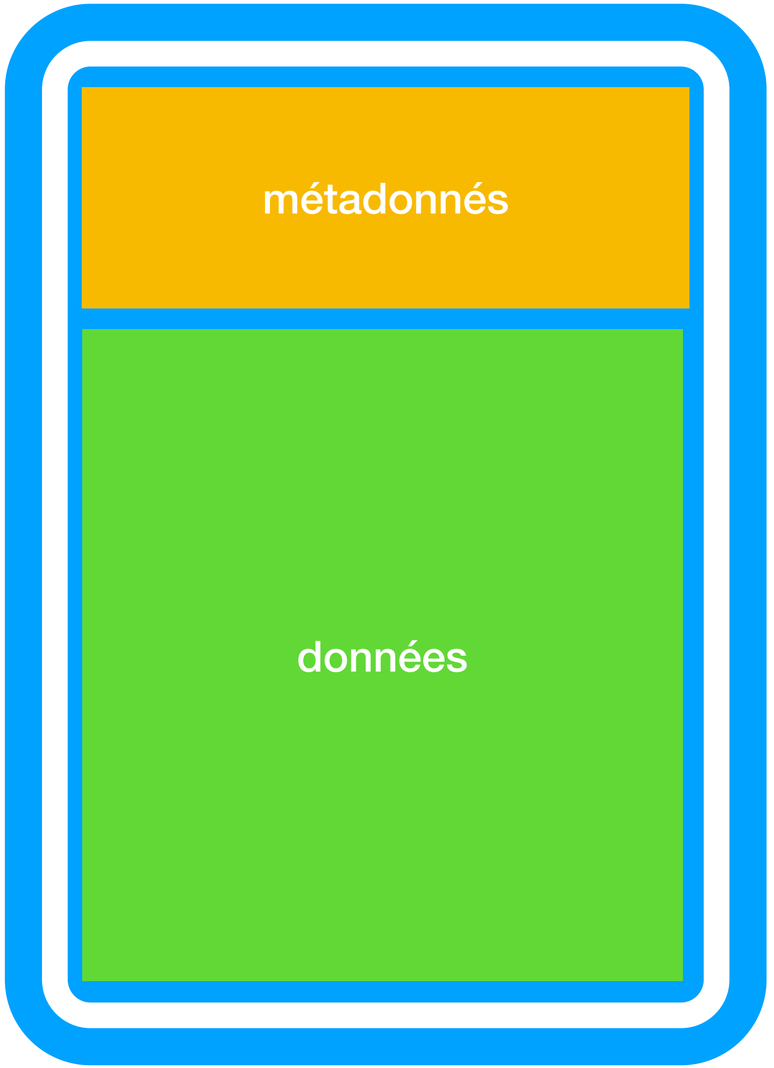
- «chiffrer» : numéroter, évaluer par des calculs, transformer un message par un procédé de chiffrement.
- «chiffrage» : faire un devis pour savoir combien va coûter la piscine
- «chiffrement» : transformer un message
- «cryptage» : ¯_(ツ)_/¯

de quoi on va parler

- **métadonnées**
- hachage
- chiffrement
- signatures électroniques
- certificats

métadonnées

- une partie du fichier distincte des donnés
- tags MP3
- données EXIF d’une photo



de quoi on va parler

- métadonnées
- **hachage**
- chiffrement
- signatures électroniques
- certificats

fonction de hachage

fonction de hachage

- si deux documents diffèrent d'un iota, le condensat (le *hash*) doit être différent
- il ne doit pas être possible de créer deux documents avec le même hash

md5 **sha-1** **sha-2** **sha-plin**

démo : *hash*-er un fichier

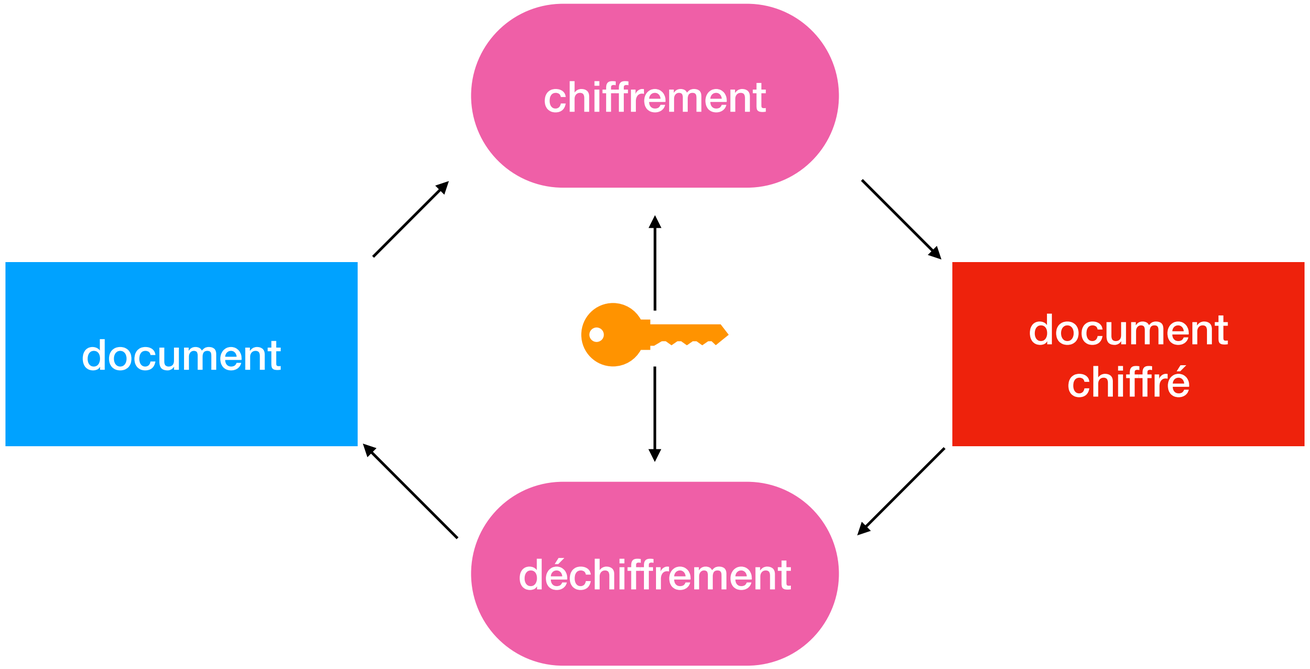
de quoi on va parler

- métadonnées
- hachage
- **chiffrement**
- signatures électroniques
- certificats

chiffrement symétrique

- une clé **unique** pour chiffrer et déchiffrer

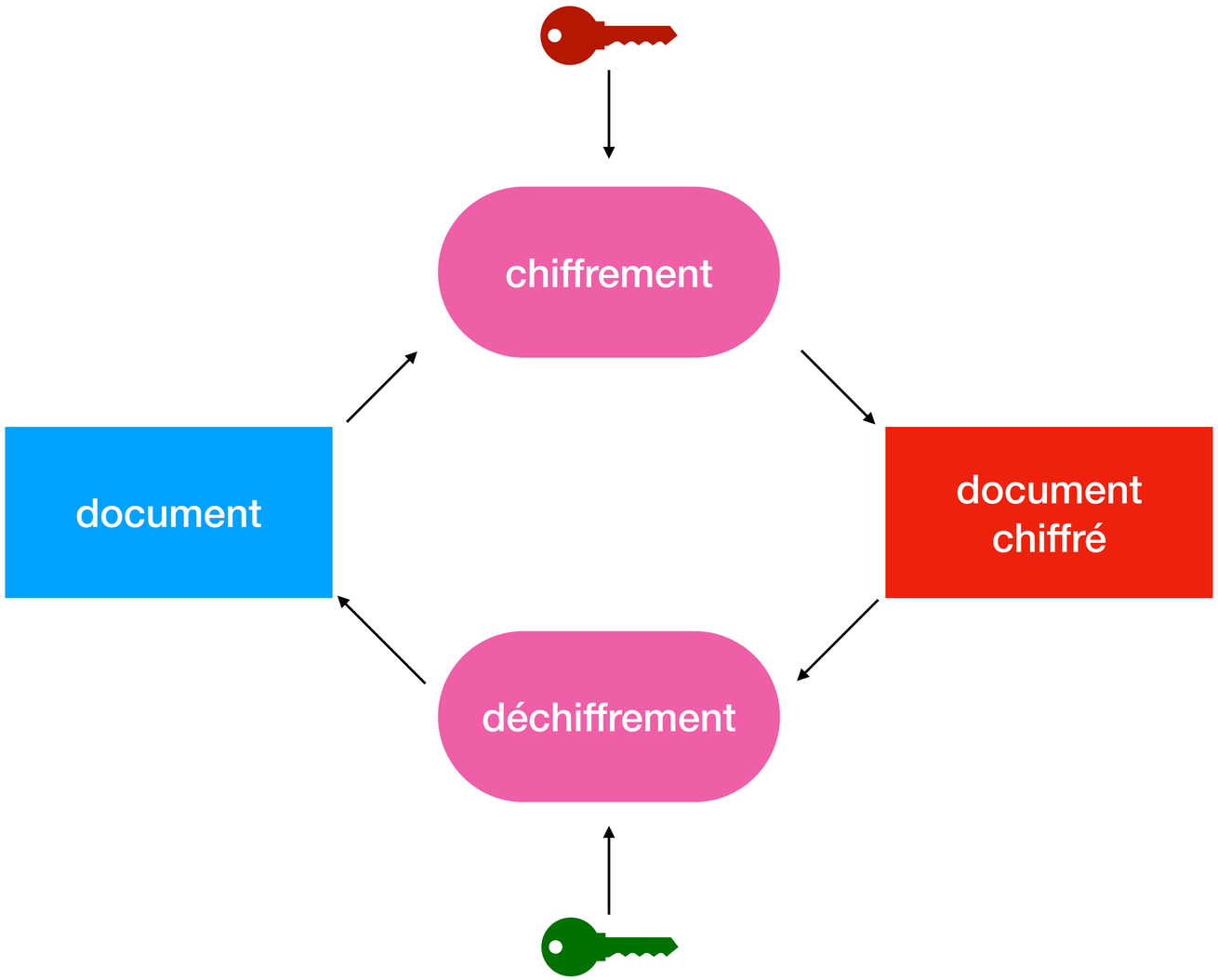
Chiffrement symétrique



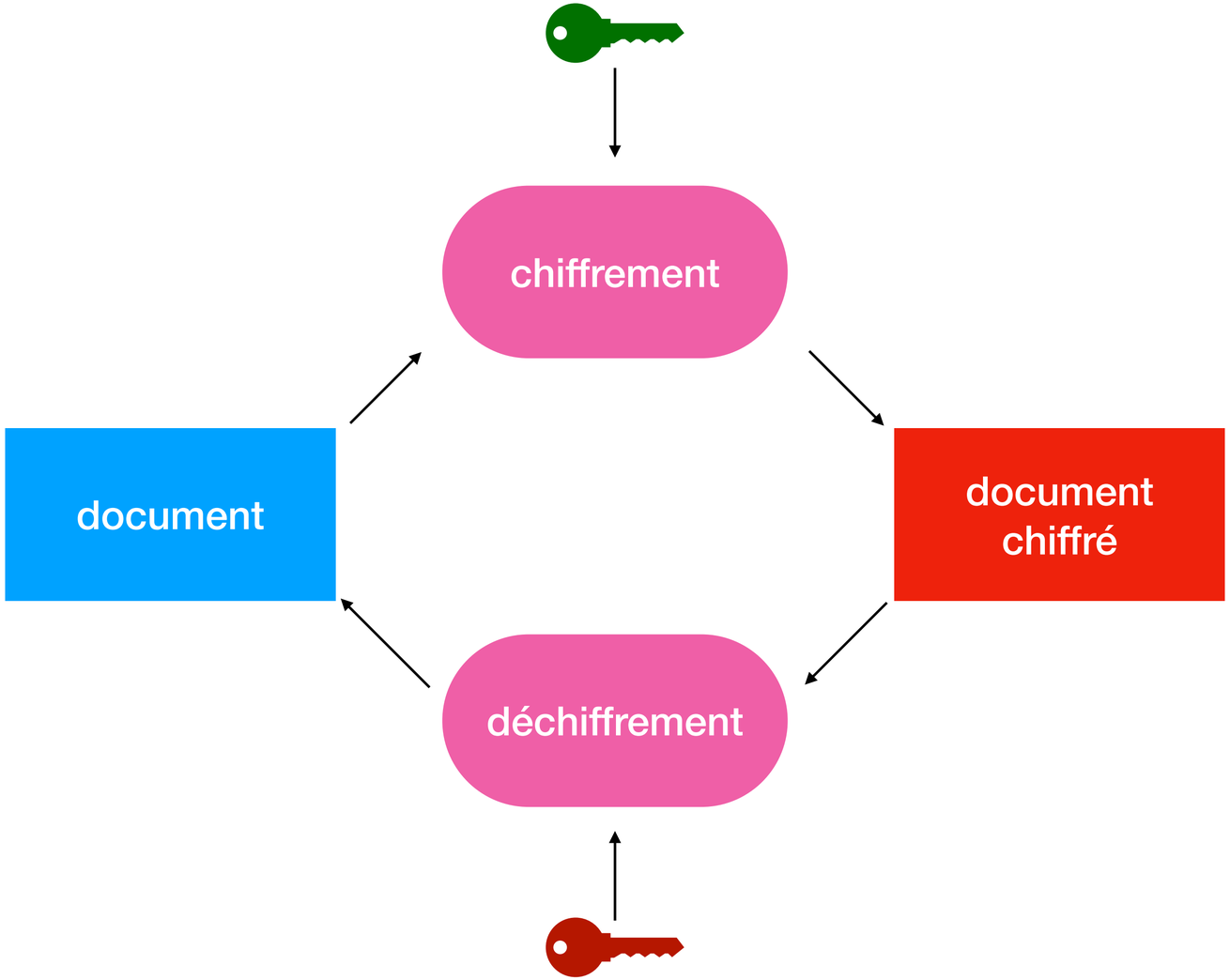
Chiffrement asymétrique

- paire de clés: une clé **privée** et une clé **publique**
- si je chiffre avec la clé **privée**, je déchiffre avec la clé **publique**
- si je chiffre avec la clé **publique**, je déchiffre avec la clé **privée**
- le plus connu : RSA

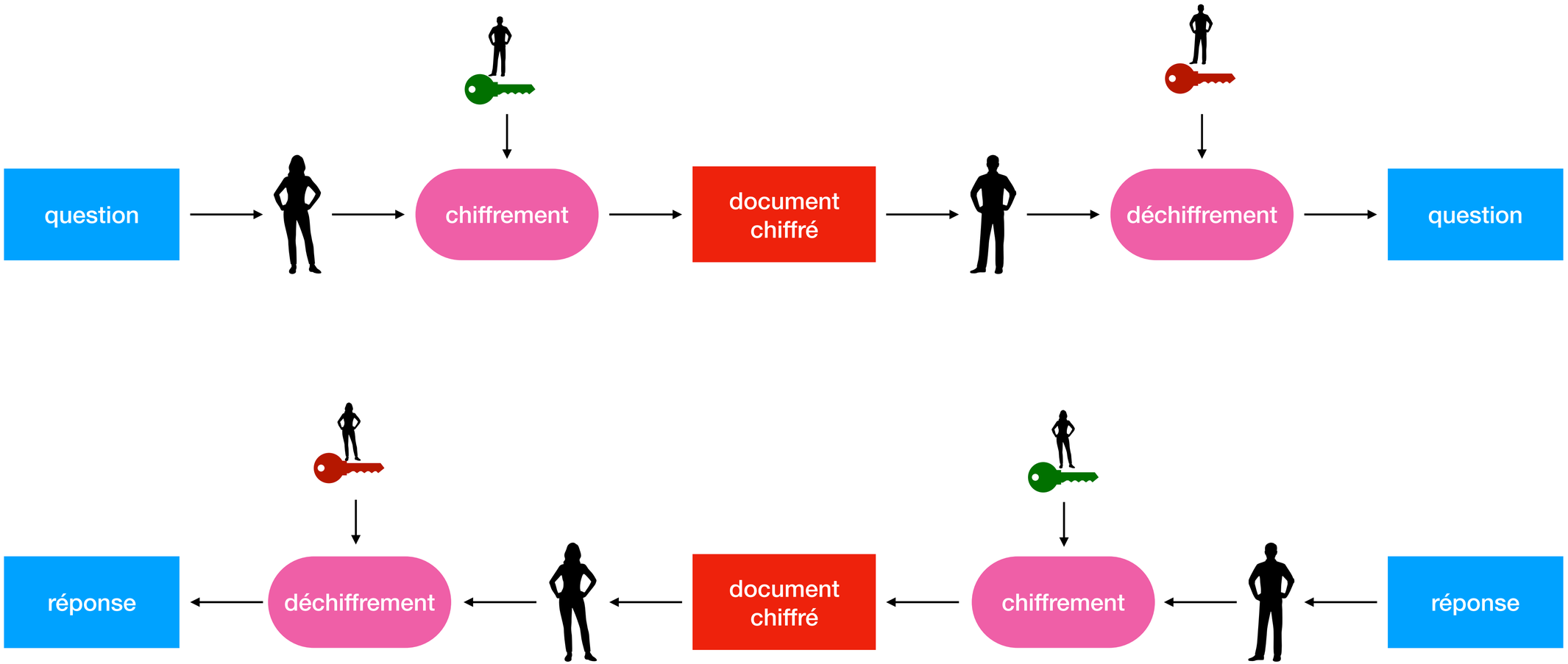
Chiffrement asymétrique



Chiffrement asymétrique



Communication chiffrée

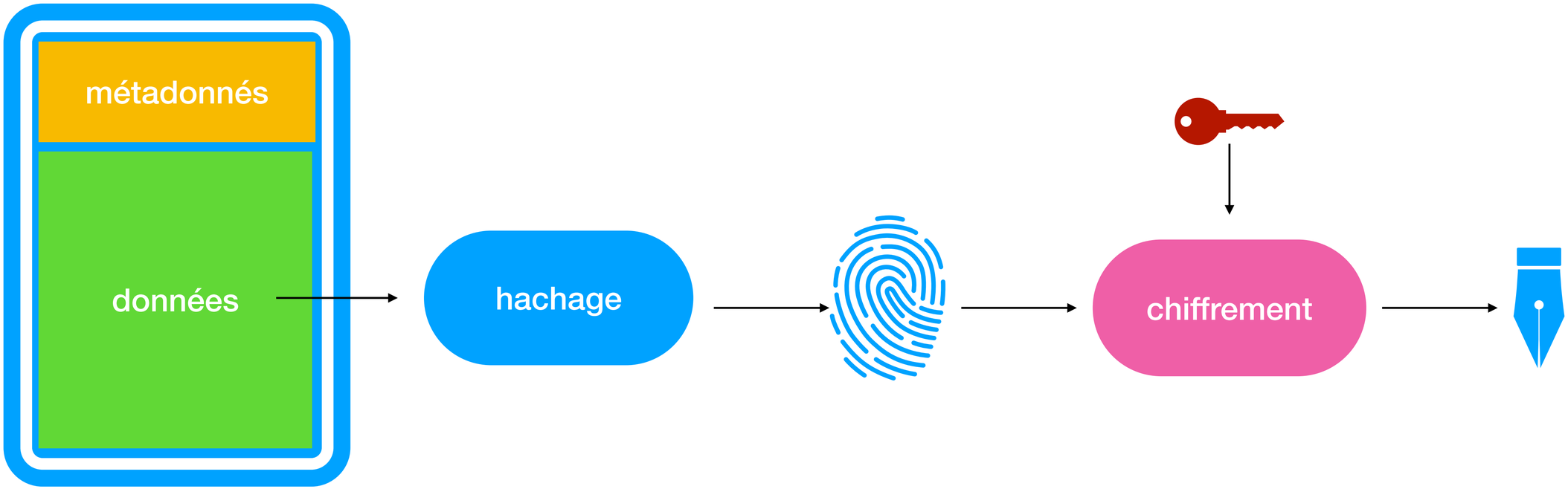


démo : (dé)chiffrer un fichier

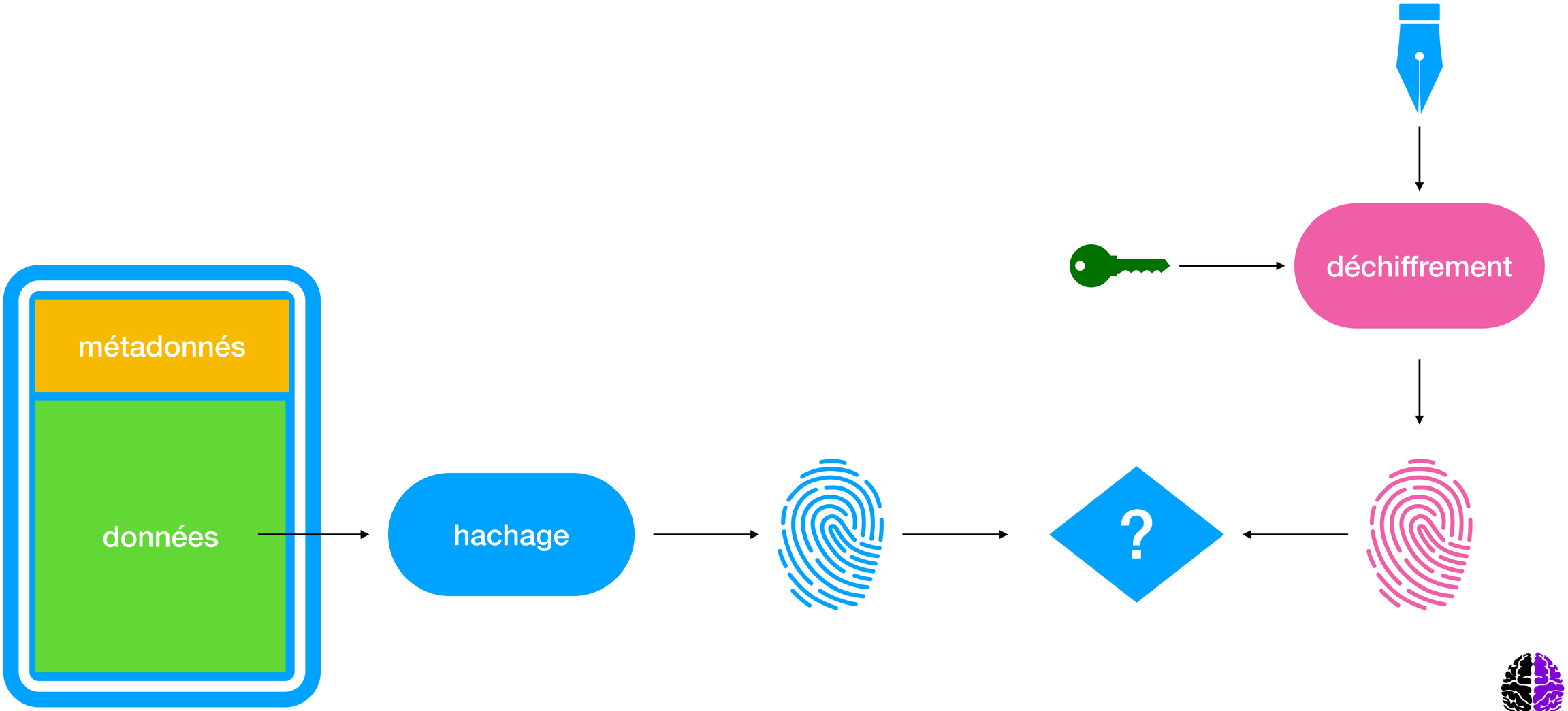
de quoi on va parler

- métadonnées
- hachage
- chiffrement
- **signatures électroniques**
- certificats

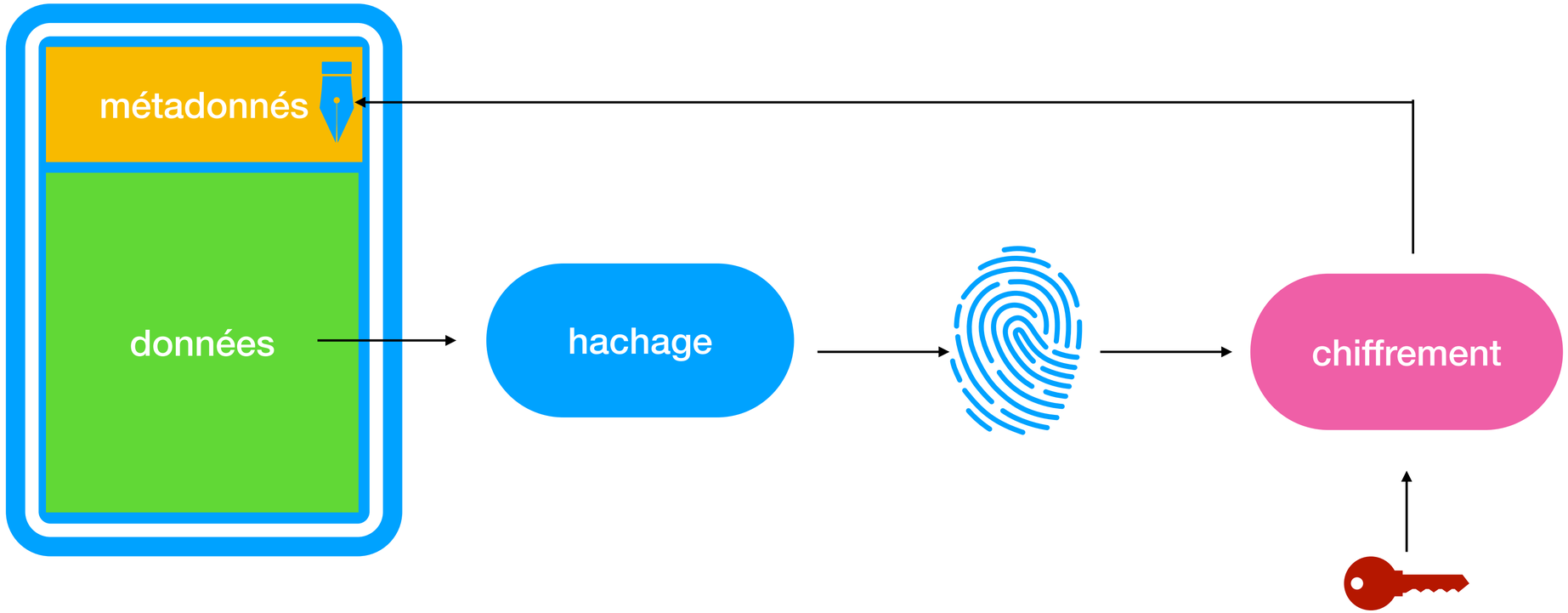
signature électronique



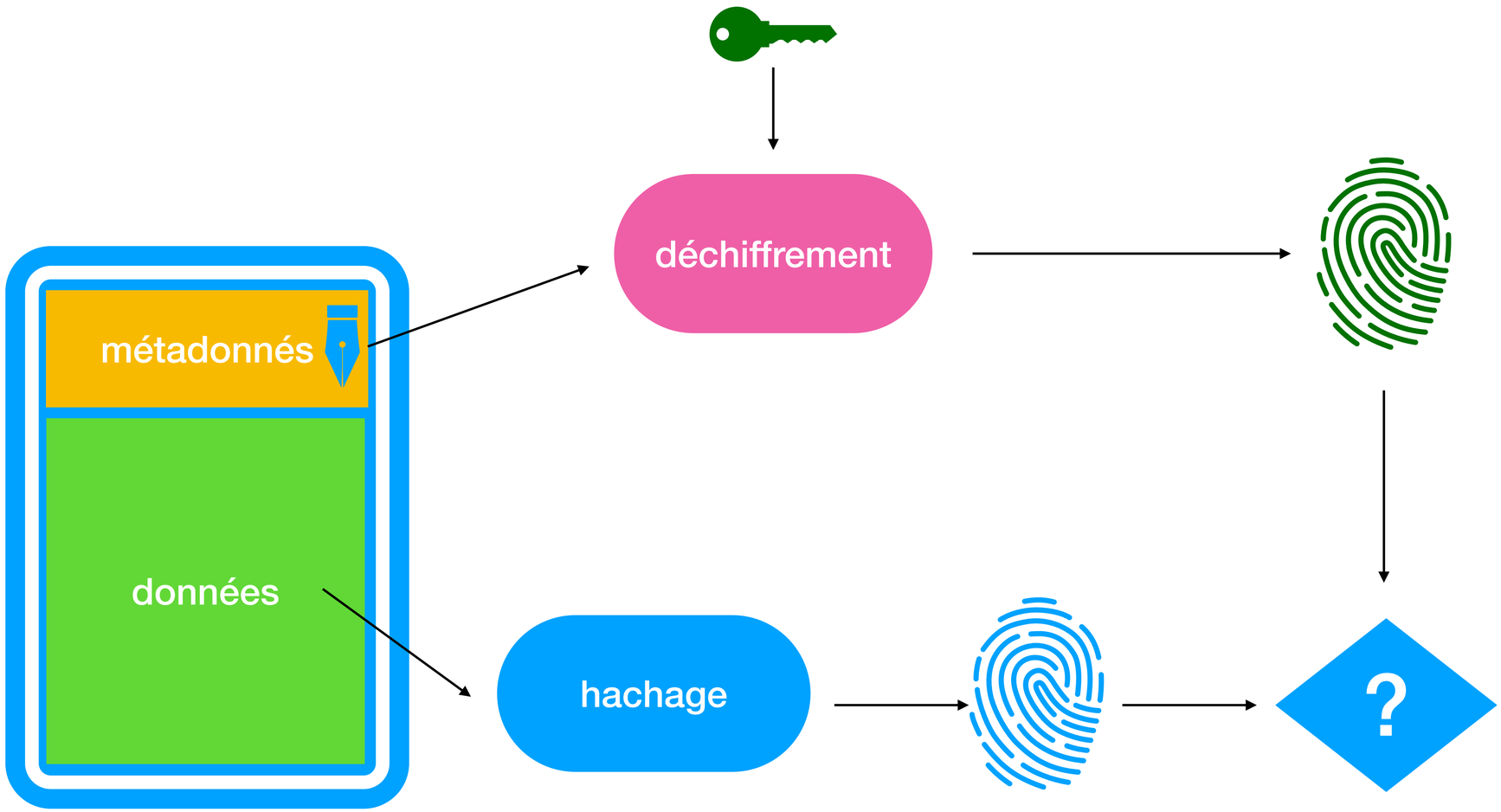
vérification



signature électronique 😎



vérification 😎



démo : créer une signature

de quoi on va parler

- métadonnées
- hachage
- chiffrement
- signatures électroniques
- **certificats**

qui est qui ?

- générer une paire de clés est une simple opération mathématique
- au moment de générer une paire de clé, on s’identifie
- comment s’authentifier ?

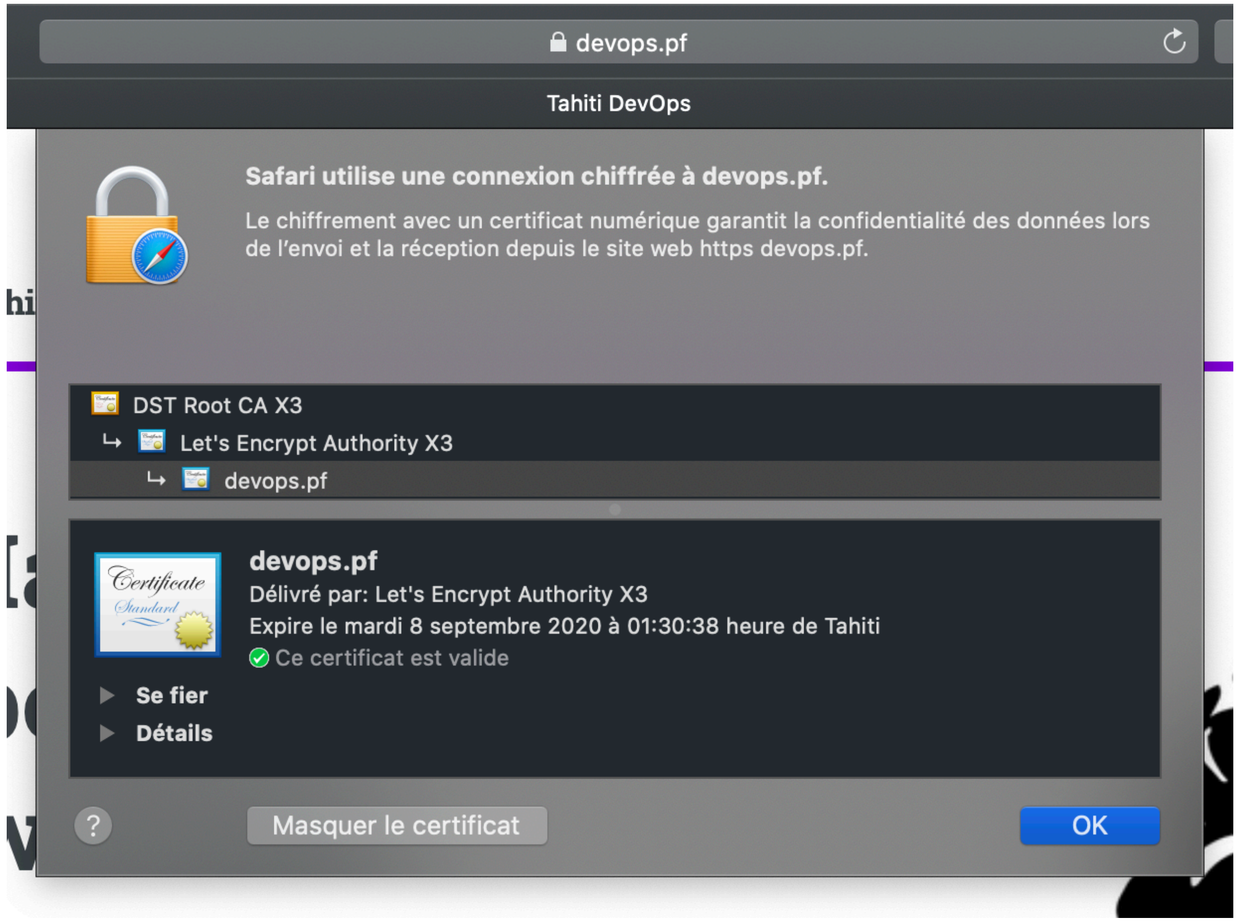
Le certificat

- un fichier qui associe une clé publique avec des informations «réelles»
- ce fichier est signé par une «Autorité de Certification»
- les certificats de ces AC sont inclus par défaut dans vos appareils

L’autorité de certification

- organisme qui s’assure que vous êtes bien qui vous prétendez être
- Certificat RGS 1* ou 2* ou 3*

vous utilisez déjà des certificats



Merci. Questions ?