

Journée d’Actualité

Identité Numérique et Certificats

18 novembre 2025

Sommaire

1 **Contexte & Présentation**

2 **Certificats numériques**

3 **Identité numérique**

4 **Questions / Réponses**

1 Contexte et Présentation



L’importance de + en + forte de l’identité en ligne

Post-Covid : Le basculement vers une vie numérique

- Explosion des usages en ligne : réunions, jeux, apprentissage, télétravail
- Services publics de plus en plus dématérialisés
- Le “numérique” devient le point d’accès principal à de nombreuses activités

La fin progressive du pseudo Anonymat

- Avant un simple mail suffisait, maintenant : vérifications, numéros de téléphone obligatoires
- Mails jetables interdits sur la plupart des plateformes
- Débat politique sur la fin du pseudonymat

Une identité numérique plus précise

- Données personnelles demandées : téléphone, adresse, date de naissance
- Objectif : un utilisateur = un seul profil fiable
- Plus de profils multiples pour un même individu

La bataille des géants de l’identité

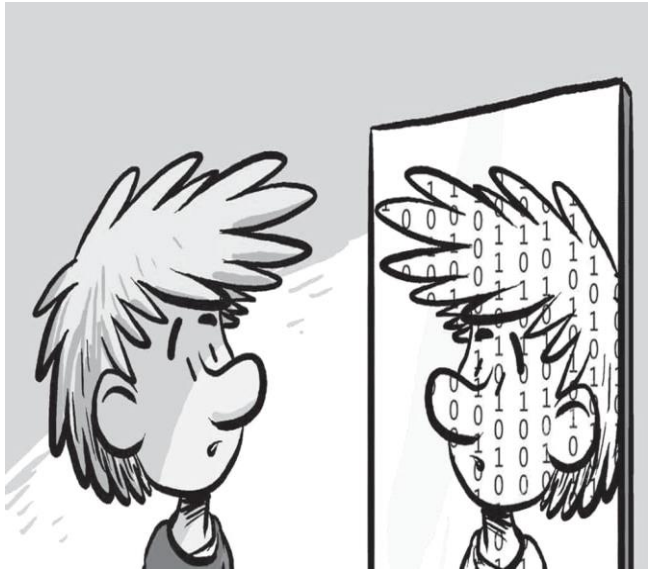
- Systèmes d’authentification : Google, Facebook, Apple, Microsoft…
- Celui qui contrôle l’identité contrôle l’accès aux services et aux données
- Enjeu stratégique et économique

Maîtriser les interactions et des données

- Savoir "qui fait quoi" en ligne et comprendre quels services interagissent entre eux
- Maîtriser quelles données sont échangées
- Importance croissante pour la cybersécurité et la confiance numérique

L’identité numérique

- L’identité numérique est devenue incontournable
- Elle conditionne l’accès, la sécurité et la confiance dans les services
- Les collectivités doivent anticiper et accompagner ces évolutions



2 Certificats numériques

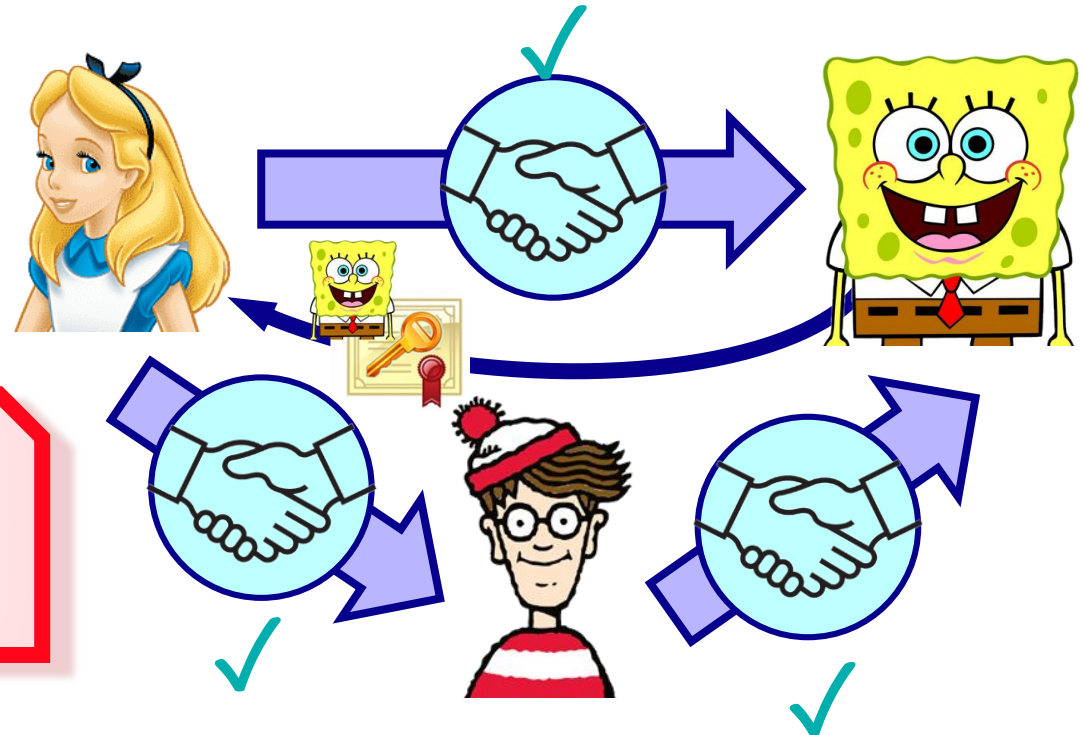


Certificats numériques

Introduction

- Démocratisation des certificats numériques
  - Besoin de confiance au début de l'interconnexion de réseaux hétéroclites (Internet) et dans les services qui y sont proposés (web)
  - Faire le lien entre une personne ou organisation et sa « représentation numérique »

- Principe du tiers de confiance



Le certificat numérique est la preuve de cette confiance

2.2

Les fondations

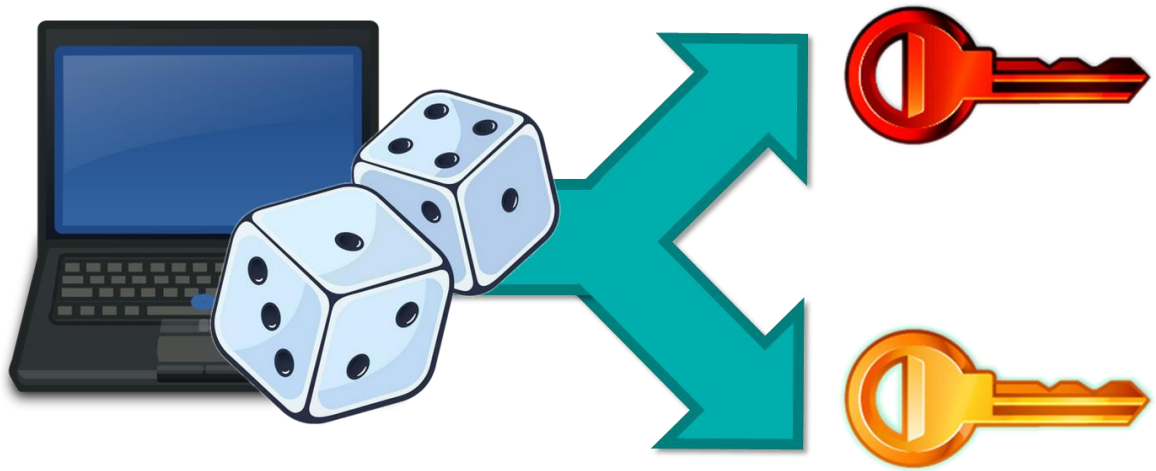
Certificats numériques



Certificats numériques

Les fondations

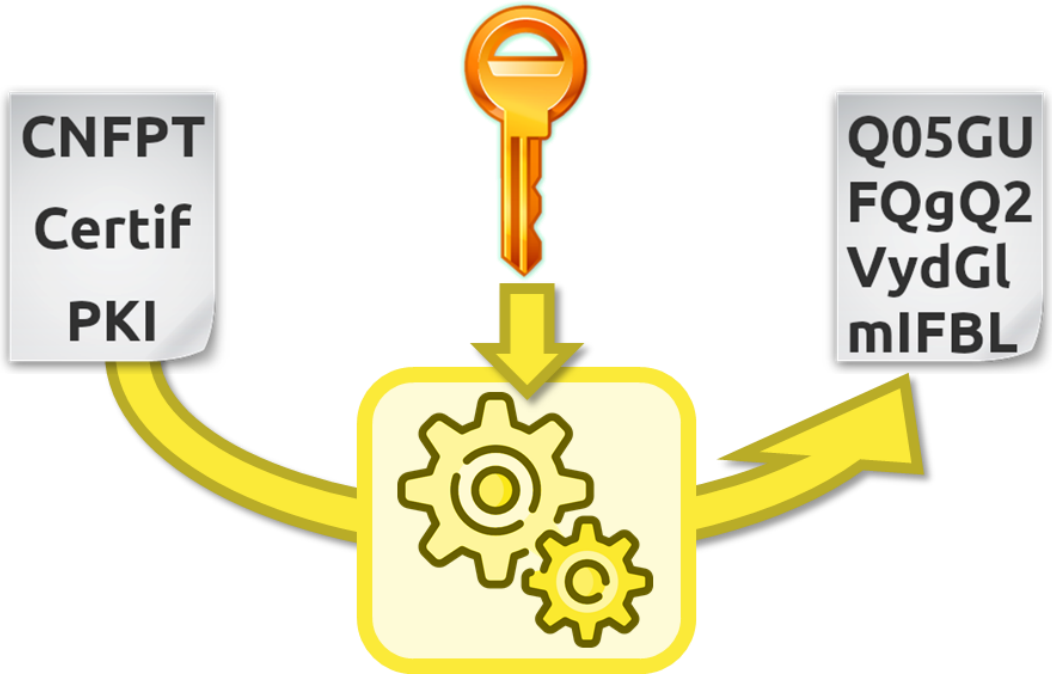
- Cryptographie symétrique
  - 1 clef unique
- Cryptographie asymétrique
  - 2 clefs différentes mais associées
  - Impossible de calculer une clef à partir de l'autre

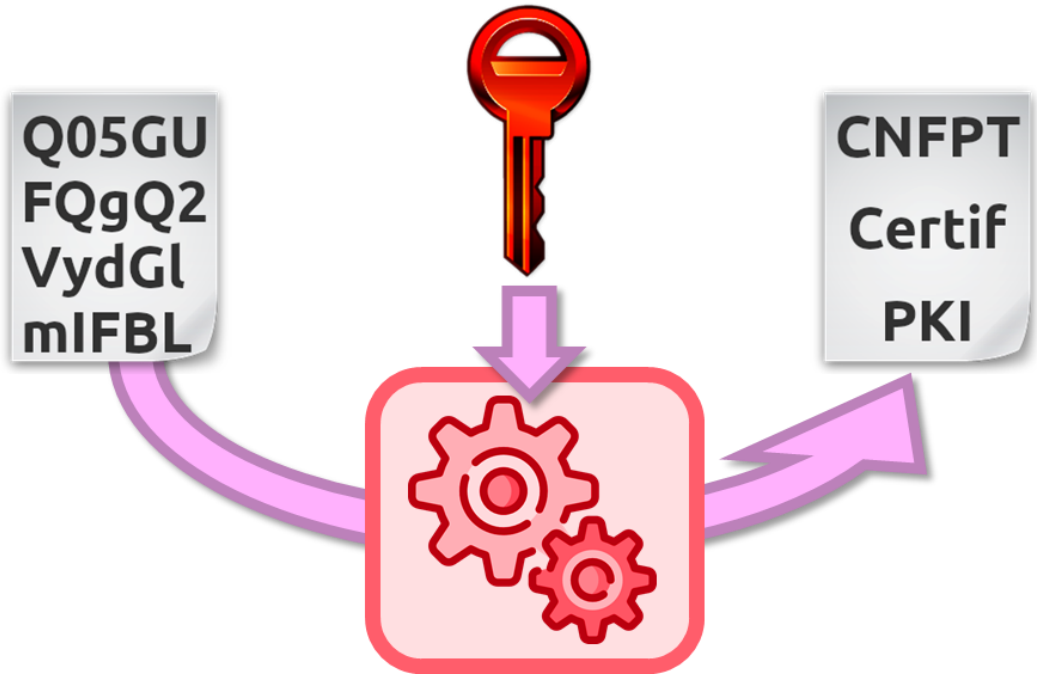


Certificats numériques

Les fondations

- Cryptographie asymétrique
  - Chiffrer par une clef ⟷ Déchiffrer par l'autre (vice versa suivant les usages)
    - Basé sur des problèmes mathématiques complexes et trop long à résoudre
  - Par convention : une clef est publique et l'autre clef est privée



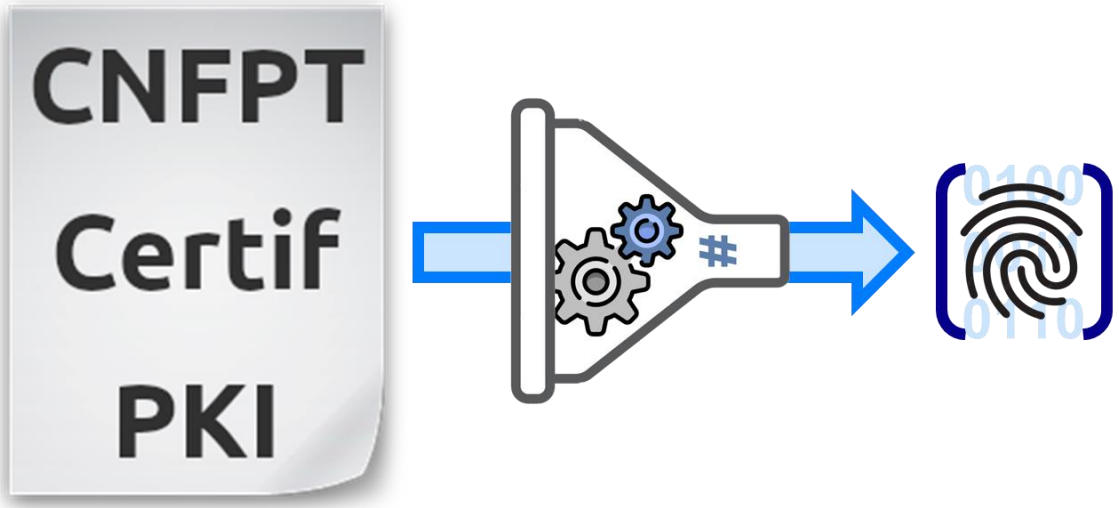


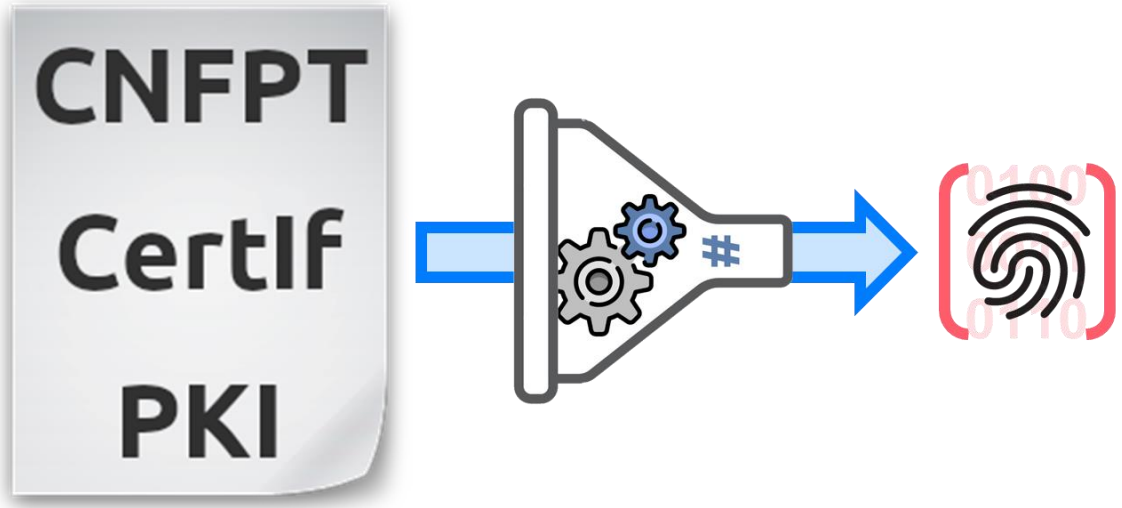
Certificats numériques

Les fondations

Également utilisé pour stocker les mots de passe !

- Fonction de hachage
  - Concept de l'empreinte digitale
    - Petit condensat numérique identifiant une plus grande quantité de données
  - Fonction mathématique à sens unique
    - Impossible de remonter à l'information initiale à partir du condensat
  - **Léger changement dans les données ➔ grand changement dans le condensat**

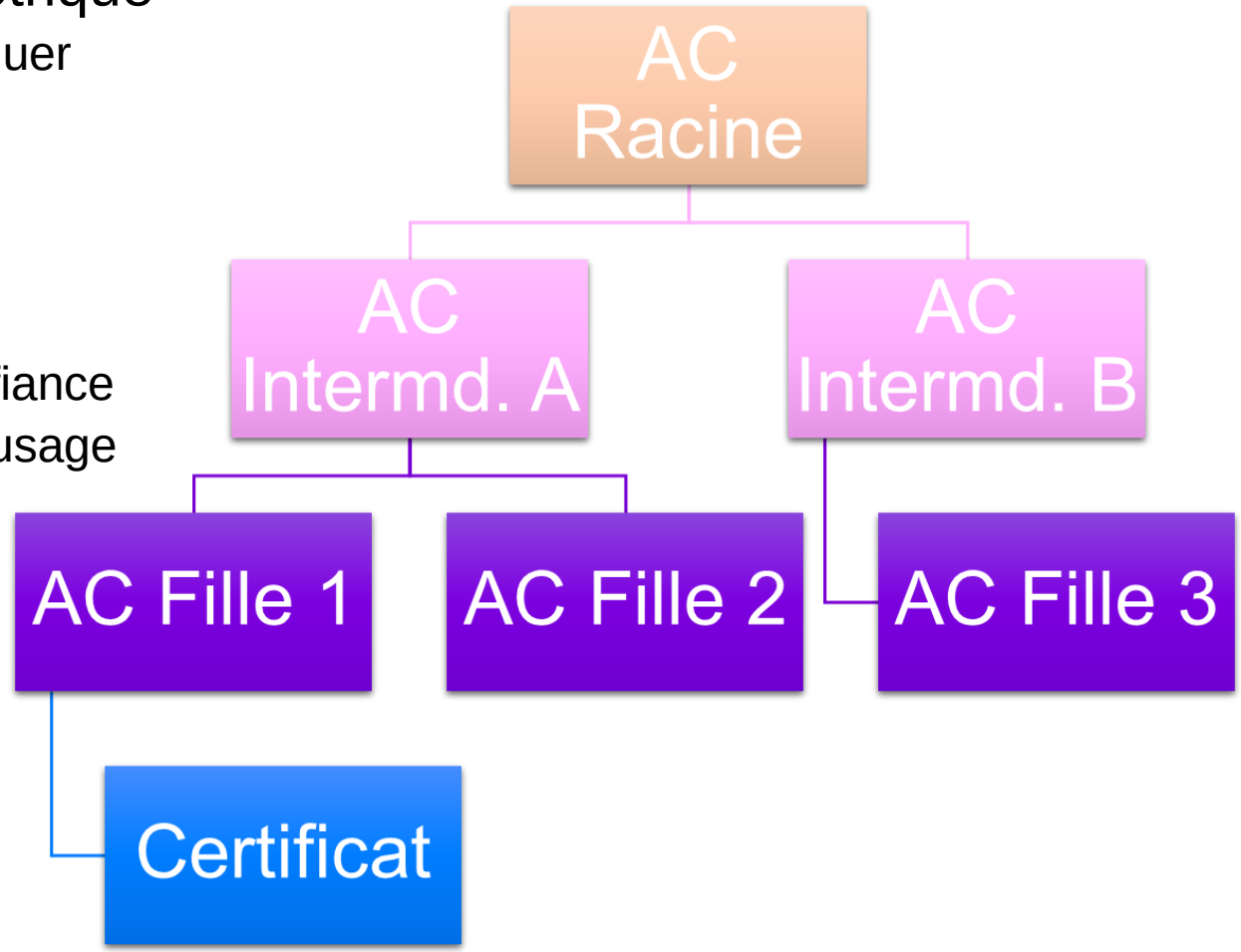




Certificats numériques

Infrastructure de Gestion de Clefs (IGC / PKI)

- Infrastructure de confiance bâtie autour des mécanismes de la cryptographie asymétrique
  - Beaucoup de normes et procédures à appliquer
- **Autorité de Certification**
  - Tiers de confiance
  - Délivre les certificats (et les révoque)
- Structure d'arbre pyramidale
  - Facilite la gestion et la distribution de la confiance
  - Contraintes sécurité différentes par niveau, usage ou norme
  - Plus résilient aux changements
- D'autres services associés
  - Gestion des CRL / OCSP
  - Horodatage



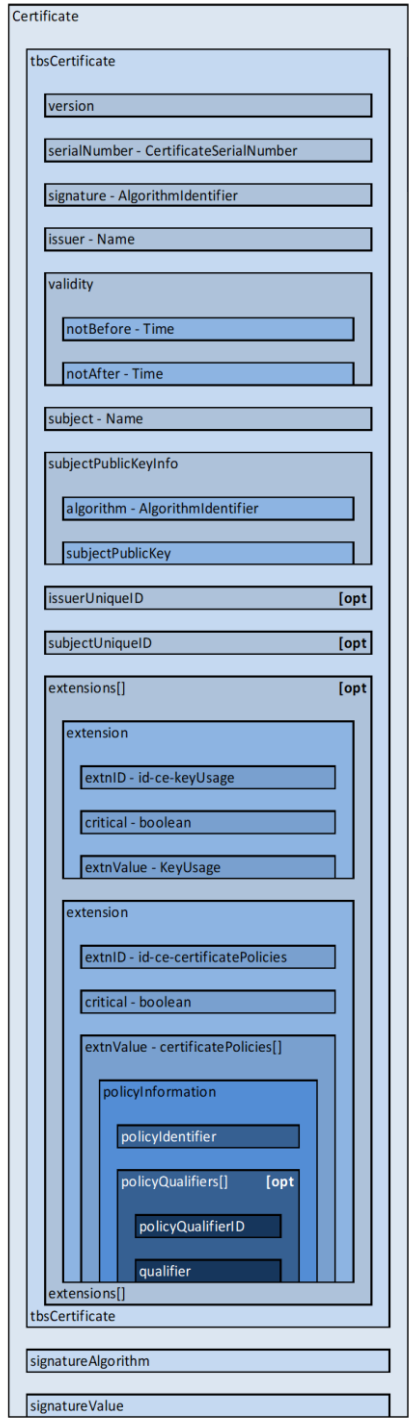
Certificats numériques

Composition

- **Identité du porteur** ou du service
  - Celui qui possède et utilise le certificat
- **Identité du tiers de confiance**
  - C'est l'Autorité de Certification
  - Garantie l'identité du porteur
- **Dates de validités** de cette confiance
- **Clef publique du porteur**
- Quelques méta-données

- La **signature** de toutes ces informations par le tiers de confiance
  - Confirmation que seule l'Autorité de Certification ait pu délivrer le certificat
  - La moindre modification d'une donnée, même minime, sera très visible

Certificat numérique = clef publique + attestation de validité



Certificats numériques

Idées reçues

- Un Infrastructure de Gestion de Clef (PKI) ce n'est pas :
  - Que de l'informatique
  - Juste les certificats numériques
  - Une technologie particulière
    - Algorithme RSA prépondérant mais d'autres existent et sont standardisés : DSA, Courbes elliptiques, GOST (Russie)
  - L'unique usage de la cryptographie asymétrique (SSH, Blockchain)
- **Un certificat seul ne sert à rien**
  - Il faut une infrastructure de confiance
  - Et l'autre partie de la paire de clef
- Le coût le plus important est le coût organisationnel et humain

Une PKI est **facile** à déployer **techniquement**
Mais **très compliqué** à mettre en œuvre **organisationnellement**



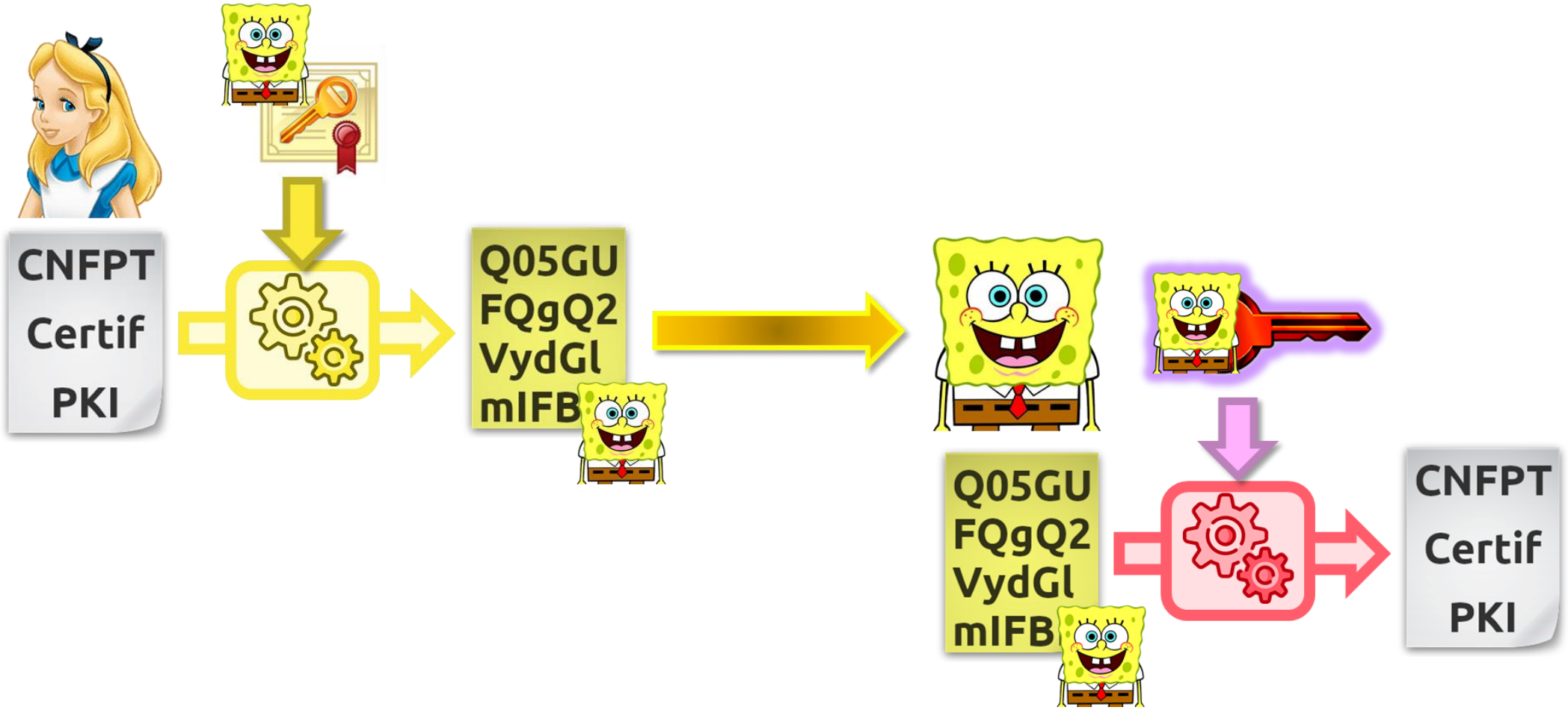
2.3 Fonctionnement

Certificats numériques

Certificats numériques

Fonctionnement – Chiffrer des données

- Alice souhaite envoyer des données confidentielles à Bob



Certificats numériques

Fonctionnement – Signature numérique

- Alice souhaite signer un document pour l'envoyer à Bob



L'insertion d'un **scan d'une image de signature** manuscrite dans un PDF **n'a pas de valeur légale** !

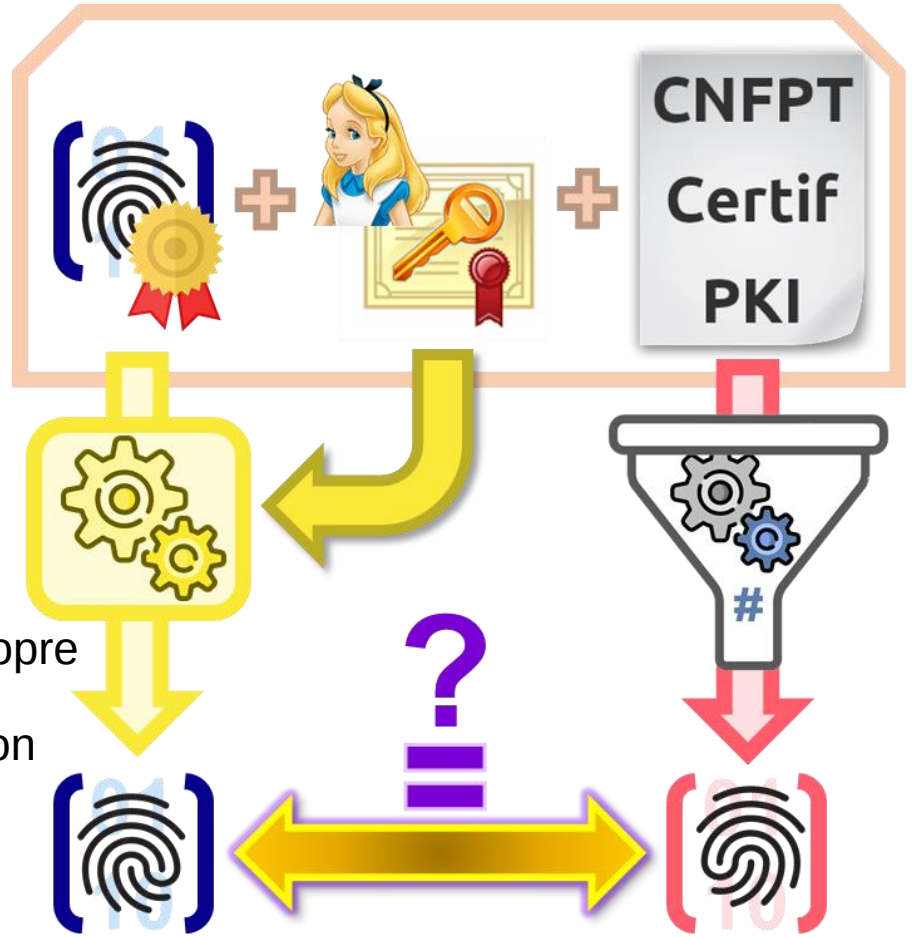
On **ne *signe* pas un PDF avec son certificat** mais avec la **clef privé** associée à ce certificat.

Certificats numériques

Fonctionnement – Vérification de signature numérique

- Bob souhaite vérifier le document signé par Alice

Vérification au préalable **des infos du certificat d'Alice** et de la **validité de sa signature** par l'Autorité de Cert.





- Vérification de la signature du certificat d'Alice
  - Via la clef publique contenue dans le certificat de l'Autorité de Certification qui a délivrée le certificat d'Alice ;
  - Puis vérification du certificat de cette AC par sa propre Autorité de Certification parente
  - Et ainsi de suite en suivant le chemin de certification jusqu'à une Autorité de Certification de confiance (déjà pré-configurée)



2.4

Cas d’usage

Certificats numériques

Certificats numériques

2.4

Rôle des certificats numériques

Les certificats numériques assurent la confidentialité, l'intégrité et l'authenticité des données dans les échanges numériques

- **Certificats SSL/TLS**

Les certificats TLS sécurisent les communications applicatives pour protéger les échanges en ligne

Le RGS est obligatoire uniquement lorsqu'un service en ligne correspond à un **téléservice administratif** ou produit un effet juridique pour l'usager (ex. dépôt de dossier, paiement d'une redevance, signature électronique ...)

- **Certificats RGS***

Le certificat RGS* est le niveau d'entrée du RGS. Il permet d'authentifier l'identité d'une personne ou d'une organisation pour des signatures électroniques courantes et des accès sécurisés

- **Certificats RGS**** – token physique

Ces certificats offrent des niveaux renforcés pour les signatures électroniques et l'accès aux systèmes critiques

Certificats numériques

2.4

HTTPS - SSL/TLS : sécurisation des sites web

Fonctionnement de TLS

TLS établit une connexion sécurisée entre client et serveur via des certificats SSL/TLS

Confidentialité et intégrité

Les certificats garantissent la confidentialité, l'intégrité des données et « l'authenticité » du site visité

Importance réglementaire

HTTPS est requis pour la conformité réglementaire et améliore le référencement des sites web

La présence d'un certificat SSL/TLS et du cadenas dans la barre d'adresse garantit la confidentialité des échanges, ***mais ne prouve en aucun cas que le site est légitime*** *: par exemple un site de phishing peut aussi afficher un cadenas*

Certificats numériques

2.4

Dématérialisation : contrôle de légalité

Objectif : Garantir la légalité des actes administratifs (arrêtés, délibérations)

Utilisation : Certificat RGS** via token pour signature électronique

Exemple : parapheur électronique**,** marchés publics, tiers de télétransmission

Certificats numériques RGS**

Les certificats RGS** garantissent la signature électronique sécurisée des documents officiels

Signature électronique officielle

La signature électronique assure l'intégrité et l'authenticité des actes officiels signés numériquement

Automatisation et conformité

Les plateformes comme Chorus automatisent la validation tout en garantissant la conformité aux obligations légales

Certificats numériques

Autre cas d'usage

Chiffrement des emails (S/MIME)

Objectif : Protéger la confidentialité des échanges par email

Utilisation : Certificat S/MIME pour chiffrer et signer les messages

Exemple : Communication interne/externe sécurisée

Accès VPN

Objectif : Authentifier les utilisateurs et sécuriser les connexions distantes

Utilisation : Certificat client pour établir la connexion VPN

Exemple : Télétravail sécurisé

Certificats numériques

2.4

Autre cas d’usage

Double authentification M365

Objectif : Renforcer la sécurité des accès aux services cloud

Utilisation : Certificat utilisateur pour le second facteur

Utilisé à la Métropole Européenne de Lille

Réduction des risques et conformité

Cette approche empêche les accès non autorisés en limitant la connexion aux seules machines de la MEL, tout en évitant de contraindre les utilisateurs à utiliser leur smartphone personnel

Certificats numériques

2.4

Nouvelle réglementation sur la durée des certificats

Réduction progressive de la durée

La durée des certificats SSL/TLS publics sera réduite de 200 jours en 2026 à 47 jours en 2029, renforçant la sécurité

Objectif de sécurité renforcée

Ces mesures visent à limiter les risques liés aux certificats compromis ou mal configurés par un renouvellement plus fréquent

Défis pour les administrateurs

Les administrateurs doivent gérer un volume accru de renouvellements, nécessitant une automatisation pour éviter les interruptions

Importance de l’automatisation

L’automatisation est essentielle pour prévenir les expirations non détectées et garantir la continuité et la sécurité des services.

Certificats numériques

2.4

Répondre aux contraintes avec l'automatisation

ACME : Automatisation de la demande, du renouvellement et du déploiement des certificats SSL/TLS

Réduction des risques : Renouvellement automatique → moins d'expiration et d'interruptions

Attention cependant a bien sécurisé ACME : anssi-fondamentaux-securisation-acme-v1-1.pdf

Conformité et sécurité : Respect des exigences SSL/TLS

Cas particulier RGS/eIDAS : Obligations réglementaires → vérification administrative annuelle

CLM (Certificate Lifecycle Management) : Gestion globale (SSL/TLS + RGS/eIDAS), visibilité, alertes ...



2.5 Pour suite

Certificats numériques

Certificats numériques

2.5

Cadre légal : de nombreux acteurs

- État français : **ANSSI**
  - Cadre légal et technique pour les services de confiance et les certificats dans les administrations publiques : RGS
  - Ensemble de recommandations et guides de bonnes pratiques
- Union Européenne : **eIDAS, ETSI**
  - eIDAS : Règlement entre états membres
  - ETSI : Défini les standard techniques européen
- États-Unis : **NIST**
  - Définis les standards au niveau de l'état fédéral américain : FIPS et SP
- Consortium entreprises privée : **CA Browser Forum**
  - Autorités de certification et acteurs du web
  - Défini la réglementation sur l'utilisation des certificats sur le web
- Communauté internationale de standardisation : **IETF**
  - Défini des standards purement techniques pour le web : RFC

Certificats numériques

Quid du quantique ?

- La cryptographie asymétrique actuelle repose sur des problèmes mathématiques très looooong à calculer
  - Factorisation de grand nombre entier, calculer un logarithme discret...
- Le système de qubits et de superposition quantique permet de tester énormément de combinatoire instantanément.
- **Sur le principe l'ordinateur quantique cassera ce type de cryptographie**
- **MAIS**
  - Dernières avancées quantique en mai 2024 sur la factorisation de grands nombres par l'université de Shanghai : factorisation de nombres entier jusqu'à 50 bits (versus 2048 bits minimum pour les certificats)
    - Il y a plus de 30 ans avec l'informatique classique : factorisation de nombre entiers jusqu'à 330 bits
    - Février 2020 avec l'informatique classique : factorisation de nombre entiers jusqu'à 829 bits
  - Les algorithmes résistants sont déjà disponibles même si peu implémenté
    - FIPS 203 ML-KEM en février 2025 (échange de clef)
    - FIPS 204 ML-DSA en janvier 2025 et FIPS 205 SLH-DSA en aout 2024 (signature numérique)

Certificats numériques

2.5

Pour suite

- La réduction de la durée de validité pour les certificats TLS
  - Systématisation de ACME
  - Utilisation de logiciel de gestion de certification et d'orchestration de l'automatisation

- ACME et les certificats pour services publics
  - Dérogation pour les certificats Internet (CA/B Forum)
  - Respecter les recommandations ANSSI sur ACME et participer à l'évolution du guide
  - N'utiliser que des certificats « qualifiés » au titre du règlement eIDAS

Date d'émission	Durée max de validité
Avant 15 mars 2026	398 jours
A partir du 15 mars 2026	200 jours
A partir du 15 mars 2027	100 jours
A partir du 15 mars 2029	47 jours



3 L’identité numérique

Comprendre, sécuriser et anticiper les nouvelles méthodes d’authentification

L’identité numérique

2.0

Plan

1. Introduction : qu’est-ce qu’une identité numérique ?
2. Les méthodes d’authentification (simple => multi-facteur MFA => passkey)
3. La fédération et la délégation d’identité
4. Protéger son identité numérique
5. Les évolutions et le futur de l’authentification
6. Conclusion et bonnes pratiques



Qu’est-ce qu’une identité numérique ?

L’identité numérique

Qu’est-ce qu’une identité numérique ?

2.1

- Définition : l’ensemble des données permettant d’identifier une personne sur les services numériques (nom, mail, identifiants, traces en ligne).
- Distinction entre :
  - Identité numérique (qui je suis en ligne)
  - Authentification (comment je prouve que c’est bien moi)
- Cycle de vie d’une identité : création → usage → modification → suppression





Les méthodes d’authentification

L’identité numériques

Les méthodes d’authentification

1. **Authentification simple**
    - Un facteur = un mot de passe.
    - Avantages : simple, rapide.
    - Inconvénients : vulnérable (phishing, réutilisation, fuite de données).
2. **Authentification multi-facteurs (MFA)**
    - Combiner plusieurs facteurs :
    - Ce que je sais → mot de passe
    - Ce que je possède → smartphone, clé USB (YubiKey), certificat, clé OTP
    - Ce que je suis → empreinte, visage
    - Exemples : code SMS, application d’authentification, clé FIDO.





La fédération et la délégation d’identité

L’identité numérique

La fédération et la délégation d’identité

1. Fédération d’identité

- Un fournisseur d’identité (IdP) authentifie l’utilisateur pour plusieurs services.
- Exemple : FranceConnect, qui relie les comptes Impôts, Ameli, La Poste…
- Standards : SAML, OAuth 2.0, OpenID Connect.

2. Délégation de l’authentification

- Un site délègue la gestion du login à un service externe.
- Exemple : “Se connecter avec Google / Facebook / Microsoft”.
- Avantage : simplifie l’accès, évite de créer un nouveau compte.
- Risques : dépendance à un tiers, traçage potentiel.





Protéger son identité numérique

L’identité numérique

Protéger son identité numérique

2.4

1. Sécurité des mots de passe

- Règles : longueur ≥ 12 caractères, unique par site, pas de mot commun, rotation régulière.
- Utiliser un gestionnaire de mots de passe (Bitwarden, KeePass…).
- Chiffrement et hachage côté serveur.

2. Risques fréquents

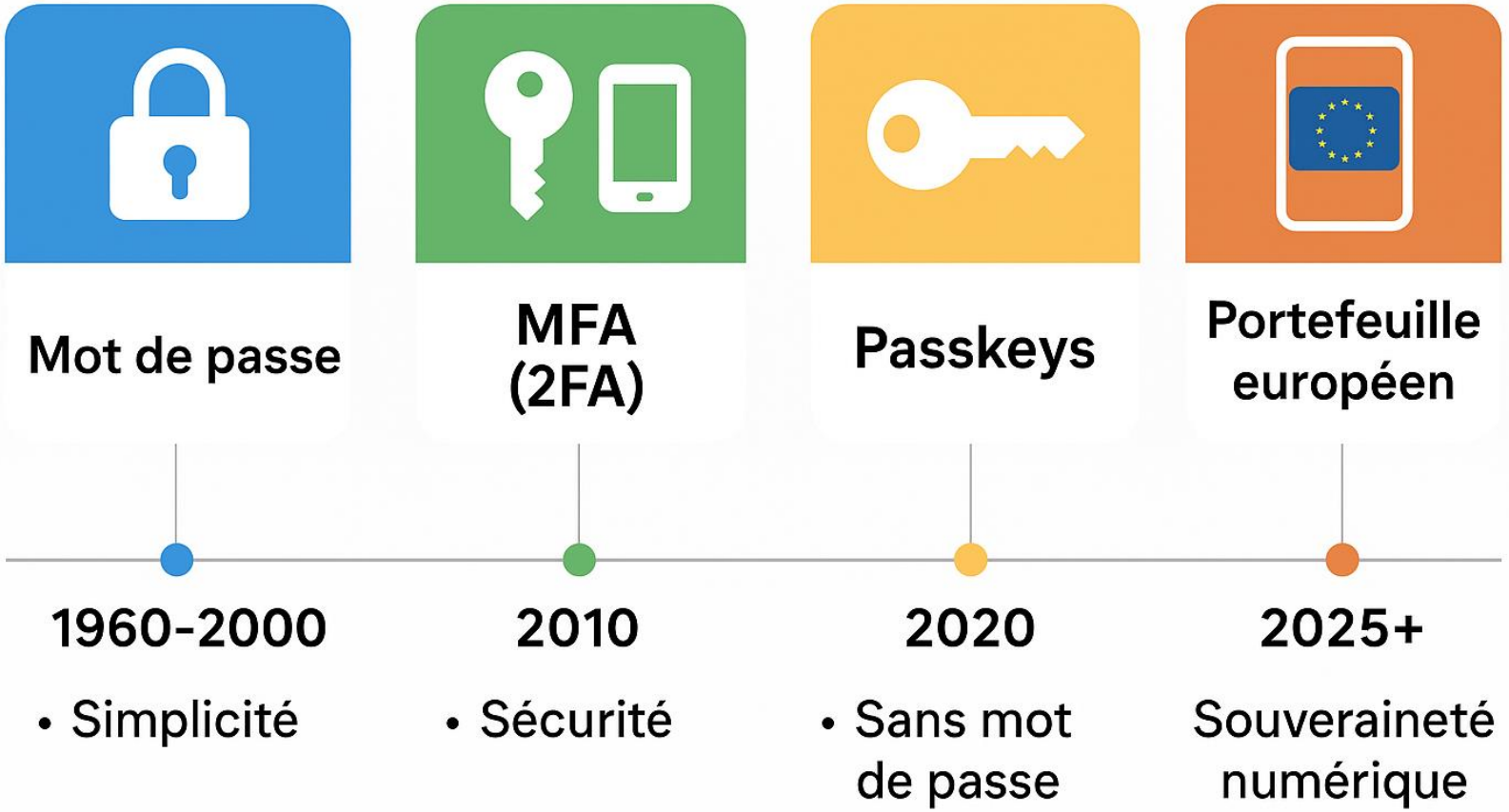
- Phishing, vol de base de données, fuite de tokens, ingénierie sociale.
- Importance des sauvegardes et de la vérification des connexions.
- Enregistrement des mots de passe dans un lieu non sécurisé (navigateur, fichier texte ...)
- Vol de données de données d'authentification (très recherché)
  - Surveillance sur TOR
  - HaveIveBeenPwned



Les évolution et le futur de l’authentification

L’identité numérique

Les évolutions et le futur de l'authentification



Les évolutions et le futur de l’authentification

2.5

1. Années 1960–2000 : l’ère du mot de passe

Le mot de passe apparaît dès les débuts de l’informatique (MIT, années 60).

Il devient la norme pour accéder aux systèmes informatiques, puis aux comptes en ligne (emails, réseaux sociaux…).

- Forces : simple, universel.
- Faiblesses : facile à oublier, à deviner ou à voler (phishing, fuites de données).

Les évolutions et le futur de l'authentification

2. Années 2010 : l'authentification multi-facteurs (MFA)

Face aux piratages massifs et aux vols de mots de passe, les entreprises ajoutent un second facteur.

Popularisation des codes SMS, applications (Google Authenticator, Authy), et clés physiques (YubiKey).

- Forces : renforce fortement la sécurité.
- Faiblesses : peut être contraignant pour l'utilisateur, charges organisationnelle et financière
- Exemple : connexion à un compte bancaire avec application mobile

Les évolutions et le futur de l'authentification

3. Années 2020 : les Passkeys et la fin du mot de passe

Face à la vulnérabilité des mots de passe, introduction des passkeys (clés d'accès) basées sur le standard FIDO2 / WebAuthn.

Utilisent la cryptographie asymétrique : une clé privée sur l'appareil, une clé publique côté serveur.

Gérés par Apple, Google, Microsoft, etc.

- Forces : très forte sécurité, résistante au phishing, transparente pour l'utilisateur (empreinte, reconnaissance faciale)
- Faiblesses : dépendance à l'écosystème du fournisseur (Apple, Google), complexe avec plusieurs appareils

NB : Certains services en ligne envoient un mail avec un code dans la boite mail de l'utilisateur

Les évolutions et le futur de l’authentification

2.5

4. Années 2025 et après : portefeuille d’identité numérique européen

Mise en œuvre du règlement eIDAS 2.0.

Création d’un **portefeuille européen d’identité numérique** : une application officielle permettant à chaque citoyen d’accéder à ses services publics et privés de manière sécurisée et interopérable.

- Objectif :

Offrir un moyen d’authentification unique et souverain à l’échelle de l’UE.

Gérer ses justificatifs (diplômes, permis, documents d’identité…) de manière numérique et contrôlée.



Conclusion et bonnes pratiques

L’identité numériques

Conclusion et bonnes pratiques

2.6

- L’identité numérique, c’est notre “moi” en ligne : il faut la protéger.
- Le mot de passe seul est dépassé : privilégier MFA ou passkeys.
- Attention à la réutilisation et au partage de ses identifiants.
- La sécurité doit toujours s’équilibrer avec la simplicité d’usage.

4 Questions / Réponses







Diapos Bonus !

Certificats numériques

Mécanismes d'ACME

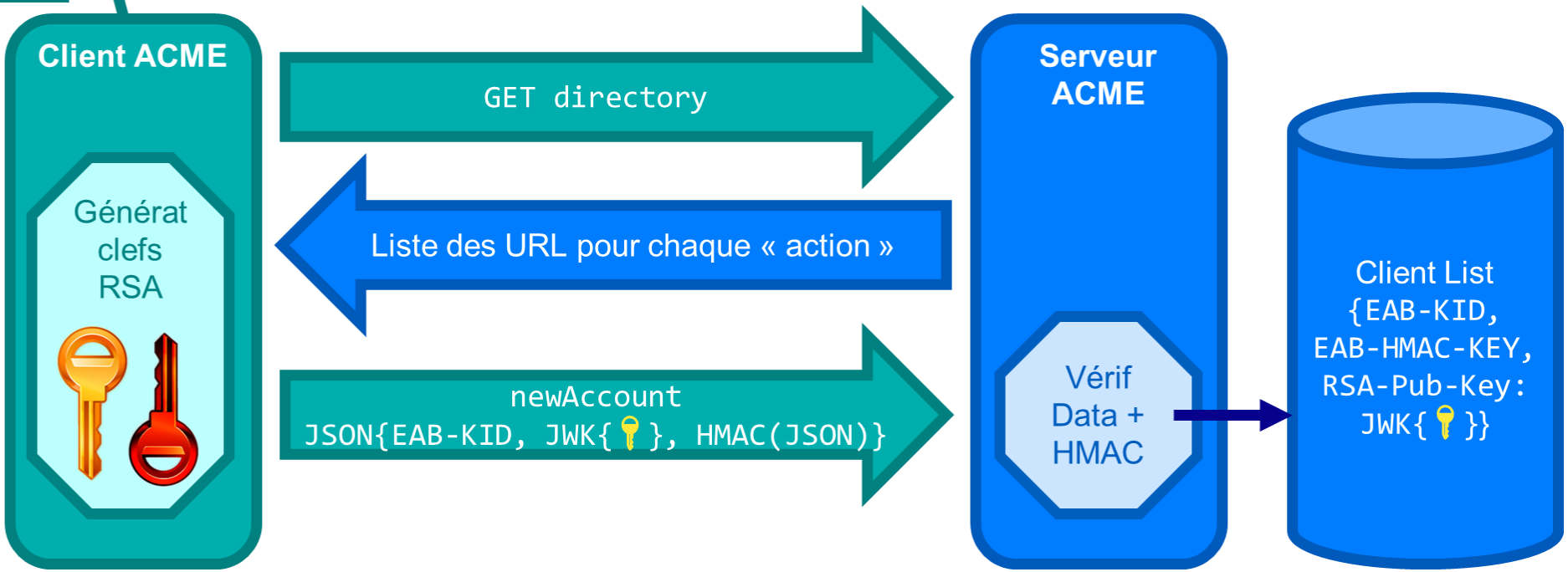
- ACME : Automated Certificate Management Environment
  - Standardisé par IETF (RFC 8555)
  - Pas le seul protocole : EST, SCEP, Windows AD
  - Fonctionne avec un agent client (serveur web) et un agent serveur (IGC)
    - ~ 10 aine de clients pour chaque partie
  - ACME v2 (2018) permet de gérer les certificats wildcard
- Actions possibles via ACME (généralement via des URL différentes)
  - Création/Initialisation d'un client ACME (newAccount)
  - Demander un certificat (newOrder)
  - Émission du certificat
  - Déploiement en local du certificat et sa clef privée associée
  - Révocation et renouvellement automatique du certificat
- Repose sur l'envoi de fichier JSON signé (JWS)
- Utilisation de « nonce » (nombre aléatoire) pour éviter les rejeux
- Vérifier que le représentant est bien légitime = il contrôle bien le domaine

Certificats numériques

newAccount : Initialisation du client

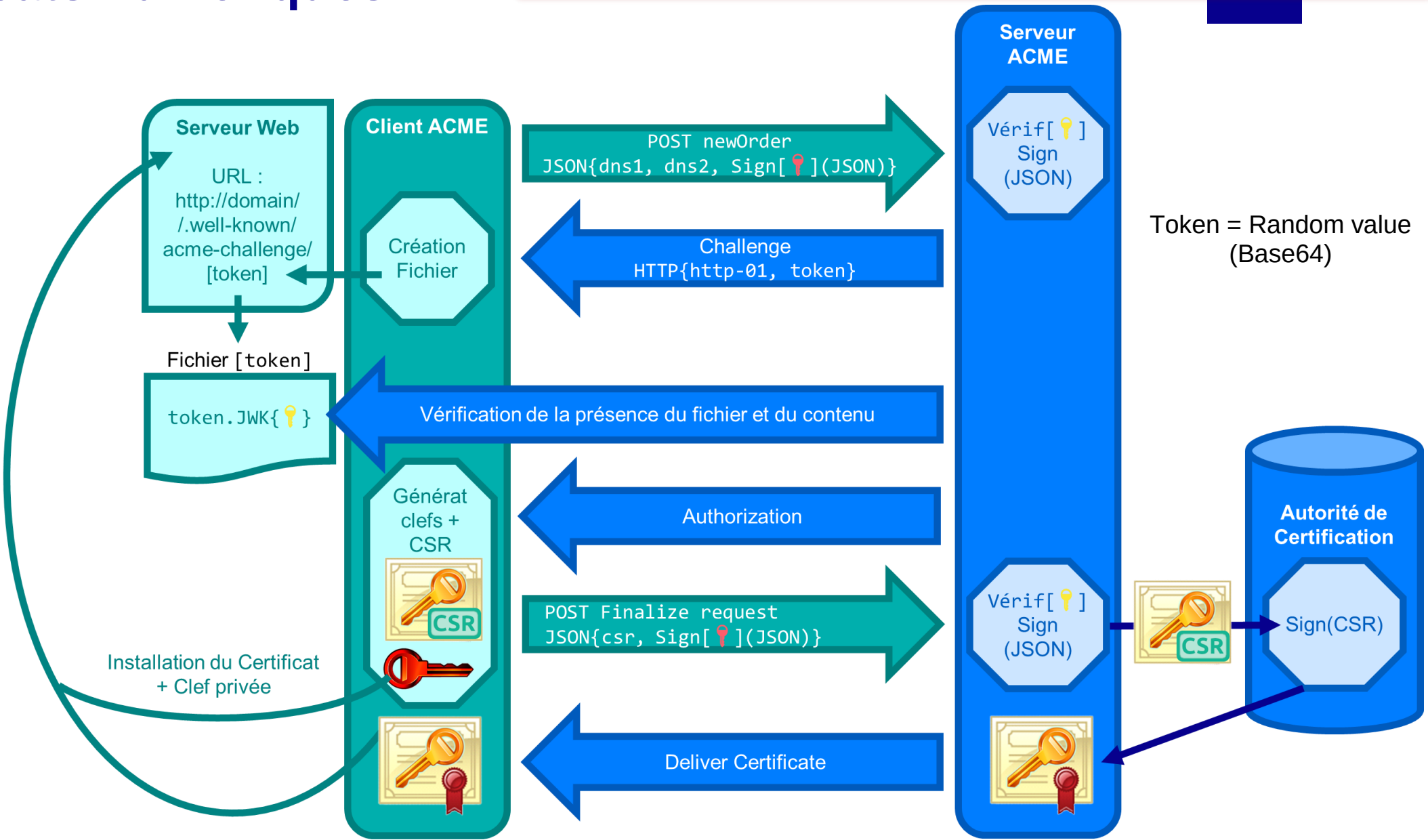
HMAC : Fonction de **hachage avec clef symétrique** pour authentifier des messages

Config initiale :
- Domaines Clients
- EAB-KID
- EAB-HMAC-KEY
- Serv. ACME Directory URL



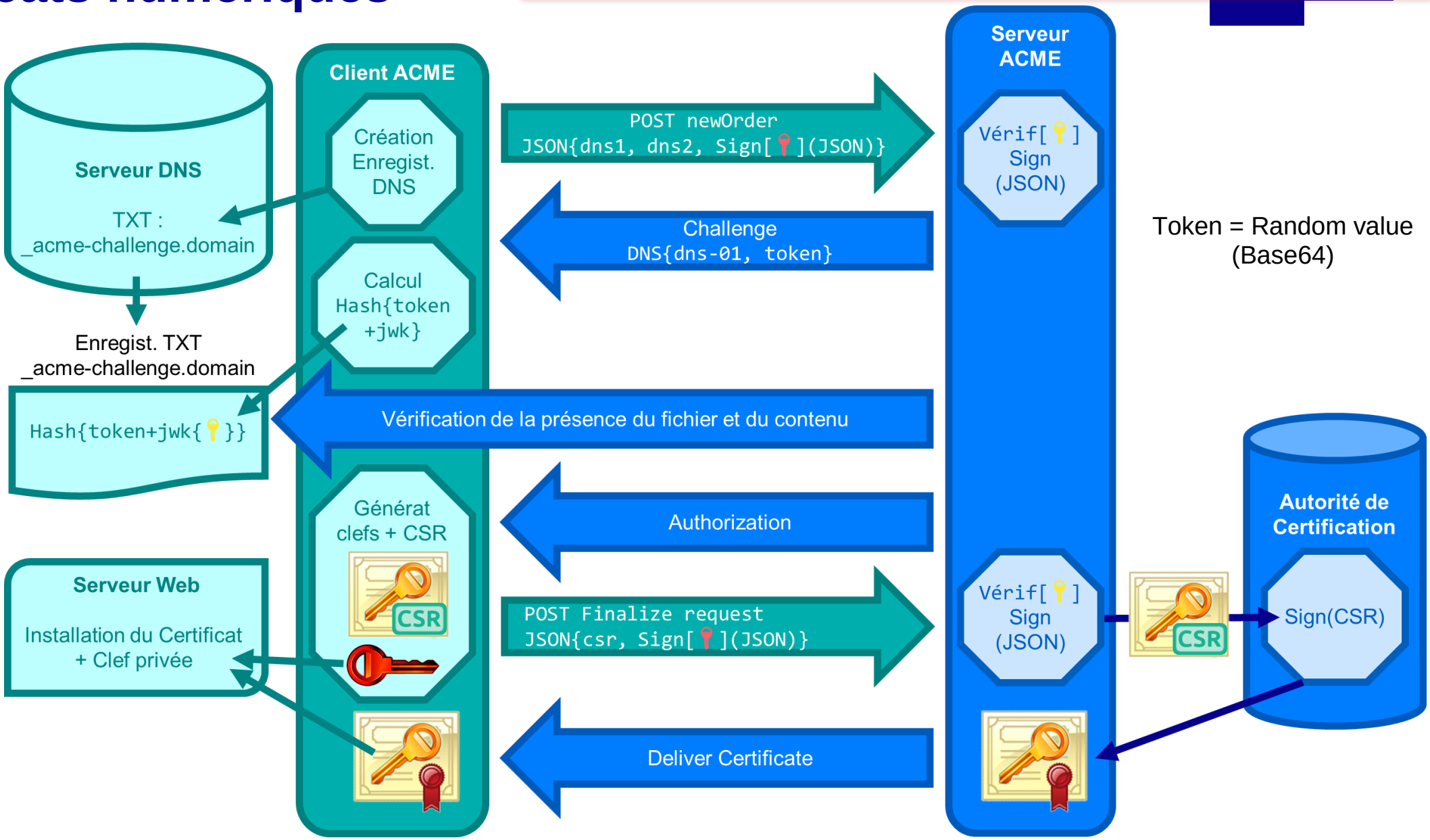
Certificats numériques

Demande de Certificat – Challenge HTTP



Certificats numériques

Demande de Certificat – Challenge DNS



Certificats numériques

Synthèse ACME

- Simple, sécurisé et pratique

- MAIS
  - HTTP Challenge : besoin d'ouvrir le port 80 au moins la 1ère fois
  - DNS Challenge : donner les accès pour mettre à jour les enregistrements DSN
  - Nécessite que l'équipement soit connecté à Internet
  - Coût financier élevé (sauf si non RGS avec Let's Encrypt)
  - Les anciens challenges basés sur TLS ne sont pas assez sécurisés (depuis 2019)
    - TLS-SNI-01 & TLS-SNI-02 : TLS Server-Name-Indication

- D'autres challenges en cours de standardisation (IETF/RFC)
  - TLS-ALPN-01 : TLS Application-Layer Protocol Negotiation