PKI

Sommaire

- Introduction à la PKI : rôle et enjeux
- Fonctionnement : cryptographie symétrique & asymétrique
- Utilisation actuelle : combinaison des deux + limites
- Certificats numériques & Autorités de Certification (AC)
- Processus de création de certificats
- Hiérarchies d'AC et certificats racine
- Gestion de la révocation (CRL)
- Durée de vie et renouvellement des certificats

Qu'est-ce que PKI?

Comment sécuriser les échanges numériques ?

- **Clés de chiffrement** :
  - Clé publique → pour chiffrer
  - Clé privée (secrète) → pour déchiffrer
  - Utilisées par personnes, appareils et applications
- **Rôle de la PKI** :
  - Gérer et distribuer les clés
  - Émettre et contrôler les **certificats numériques**
  - Garantir l'**authenticité** et la **confiance** (comme un passeport numérique)
- **Exemples** :
  - Certificats **SSL/TLS** (sécurisation des sites web)
  - Signatures numériques
  - Authentification des utilisateurs, machines et objets connectés

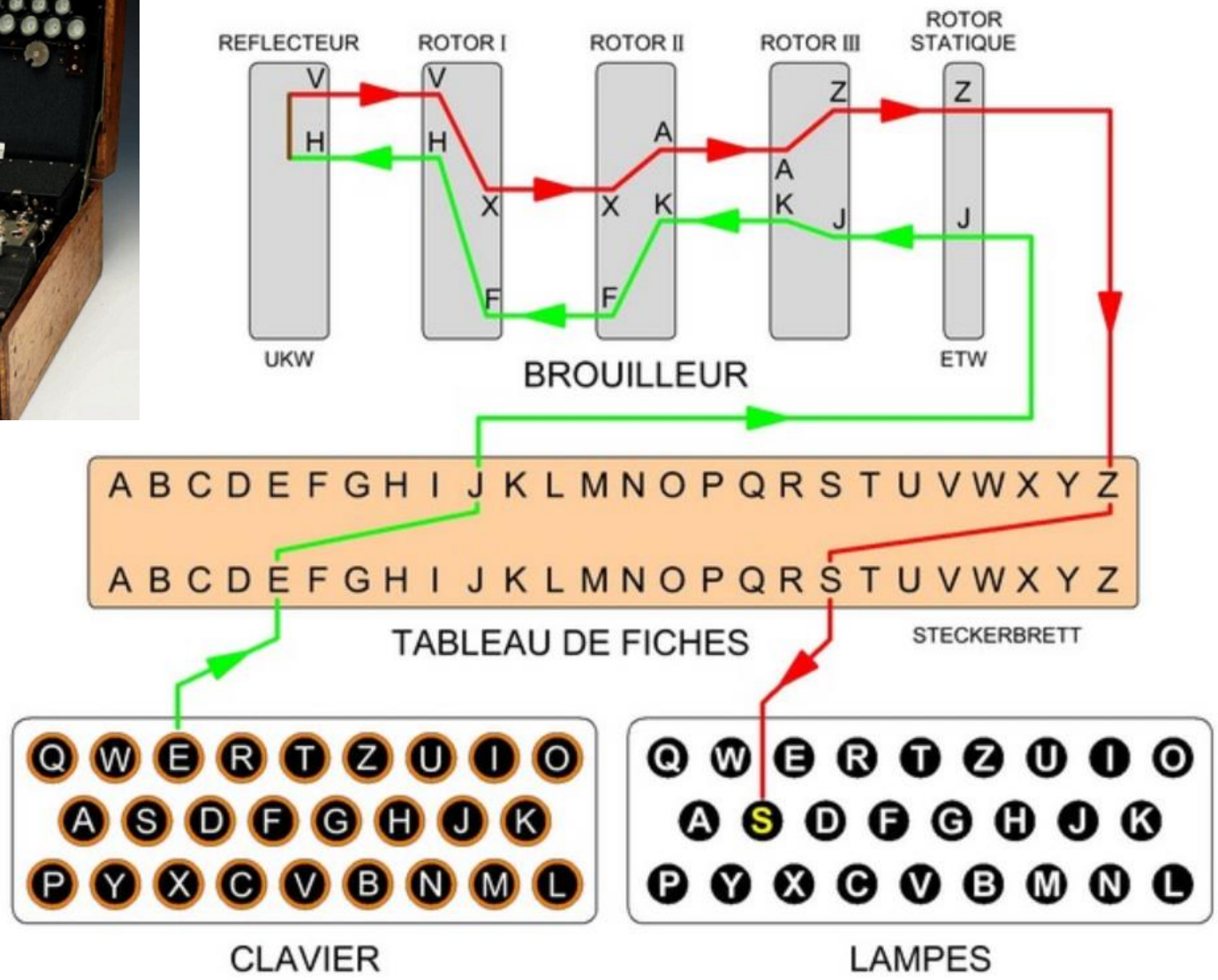
Comment fonctionne PKI ?

Fondements cryptographiques

- Chiffrement **symétrique** : une clé unique (ex. Enigma, 2nde GM).
  → Problème : distribution et sécurité de la clé.

- Chiffrement **asymétrique** : une paire de clés (publique / privée).
  → Confidentialité, authenticité, intégrité.

Principe de ENIGMA



Principe clé publique / clé privée

- Clé publique : peut être partagée.
- Clé privée : reste secrète.
- Exemple : Alice chiffre avec la clé publique de Bob → seul Bob peut lire avec sa clé privée.

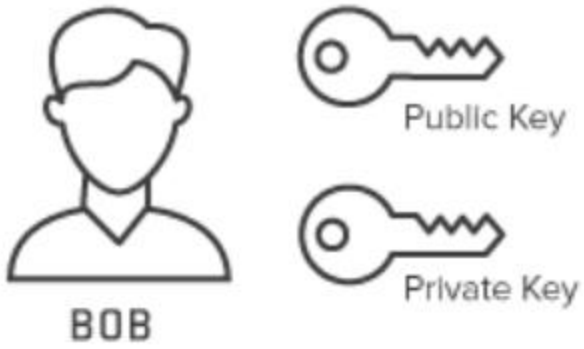
Signatures numériques

- Garantissent l'identité de l'expéditeur.
- Assurent que le message ou document n'a pas été modifié.

Algorithmes utilisés

- RSA (facteurisation de grands nombres premiers).
- ECC (courbes elliptiques).
- Diffie-Hellman (échange de clés).

Principe clé publique / clé privée



Decrypt: $D(K_{priv}, C) = M$

Sign: $S = E(K_{priv}, M)$

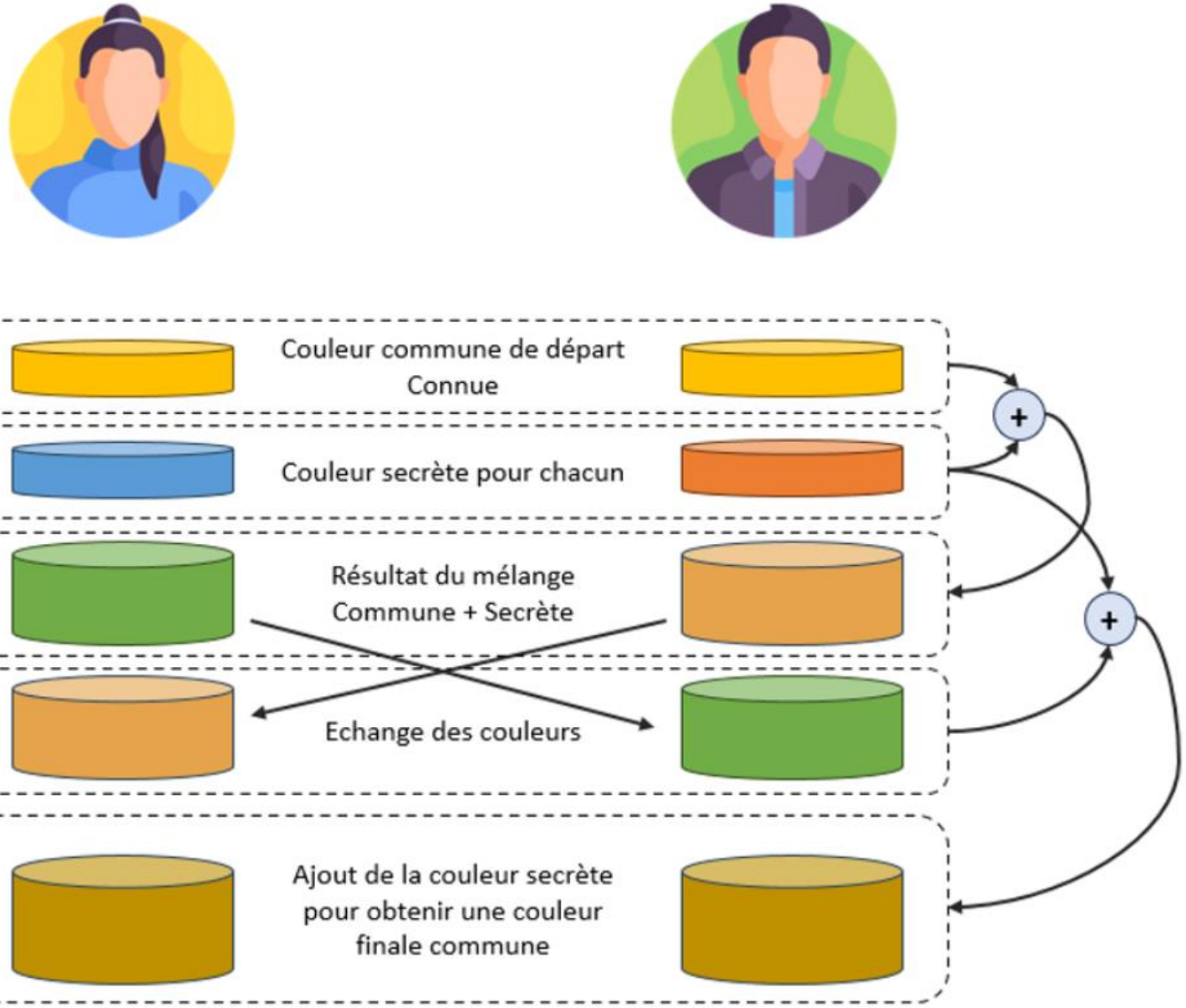
Encrypt: $C = E(K_{pub}, M)$

Verify: $D(K_{pub}, S) = M$

RSA, Diffie-Hellman, ECC

- SSH
- SSL / TLS
- S/MIME encrypted email
- Code Signing
- Bitcoin / Blockchain
- Signal Private Messenger
- Public Key Infrastructure

DEFFIE HELLMAN



Comment le chiffrement symétrique et asymétrique est-il utilisé aujourd'hui ?

Utilisation combinée

- Asymétrique = lent
- Symétrique = rapide

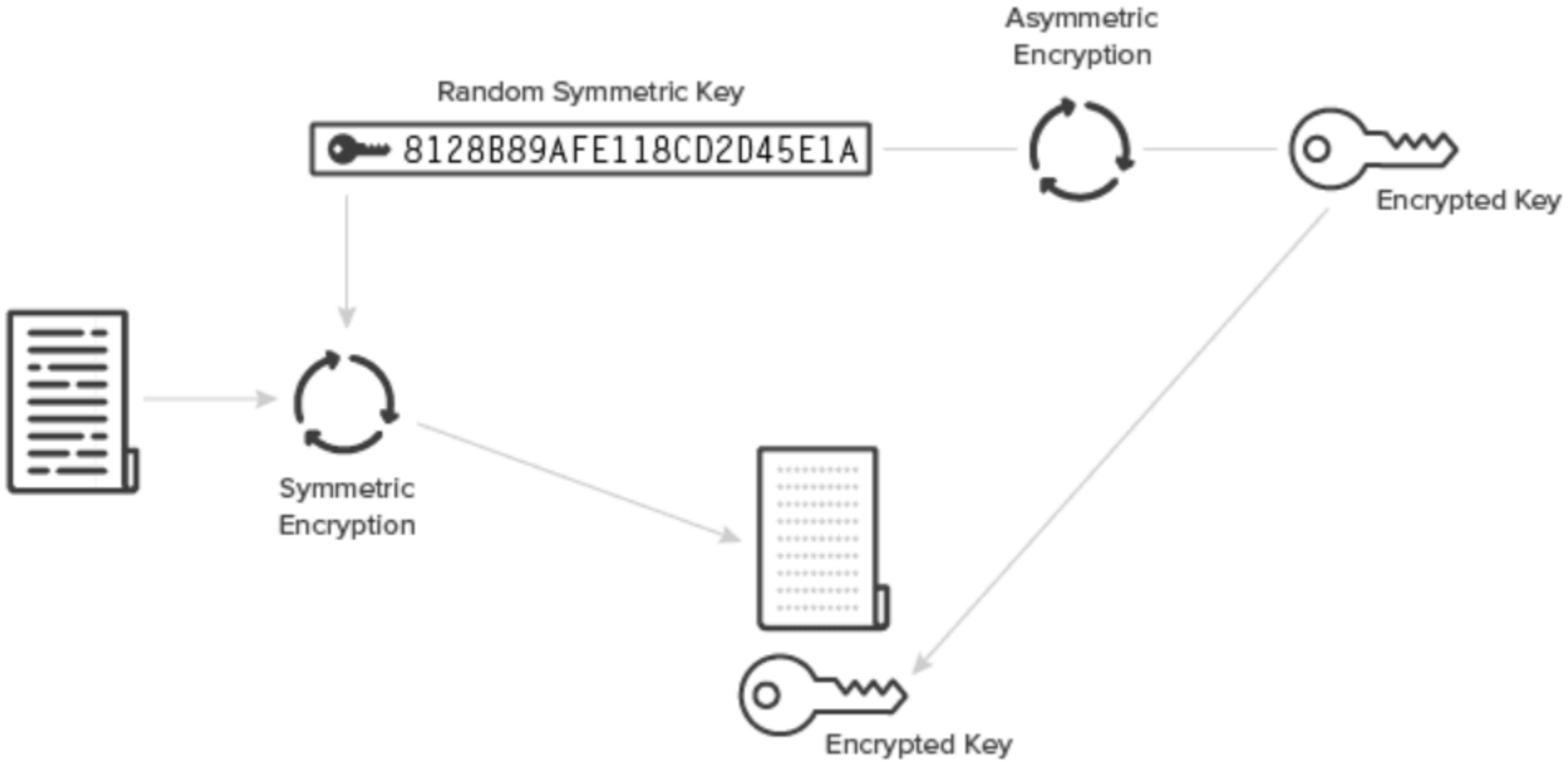
  On chiffre le message avec **symétrique**

  On chiffre la clé symétrique avec asymétrique (TLS/SSL)

Exemples d'usage

- SSH
- SSL/TLS
- Email sécurisé (S/MIME)
- Signature de code
- Blockchain / Bitcoin
- Messageries chiffrées (Signal, WhatsApp)
- Signatures numériques

Principe chiffrement
symetrique+ asymetrique



Le rôle des certificats numériques dans la PKI

Certificat numérique (X.509) = Passeport numérique

- Identité électronique (personne, organisation, machine)
- Délivré par un **tiers de confiance** (AC)
- Caractéristiques :
  - Authentique et difficile à falsifier
  - Traçable jusqu'à l'émetteur
  - Expiration prévue
  - Présenté pour validation (ex. HTTPS)

Autorités de Certification (AC)

- Vérifient l'identité des demandeurs
- Délivrent différents types de certificats (SSL, signature code, etc.)
- Définissent les politiques et procédures
- Documentent officiellement leurs pratiques
- Inspirent la confiance des utilisateurs/navigateurs

Fonctionnement du processus de création de certificats

- **1 Géneration de certificats:**

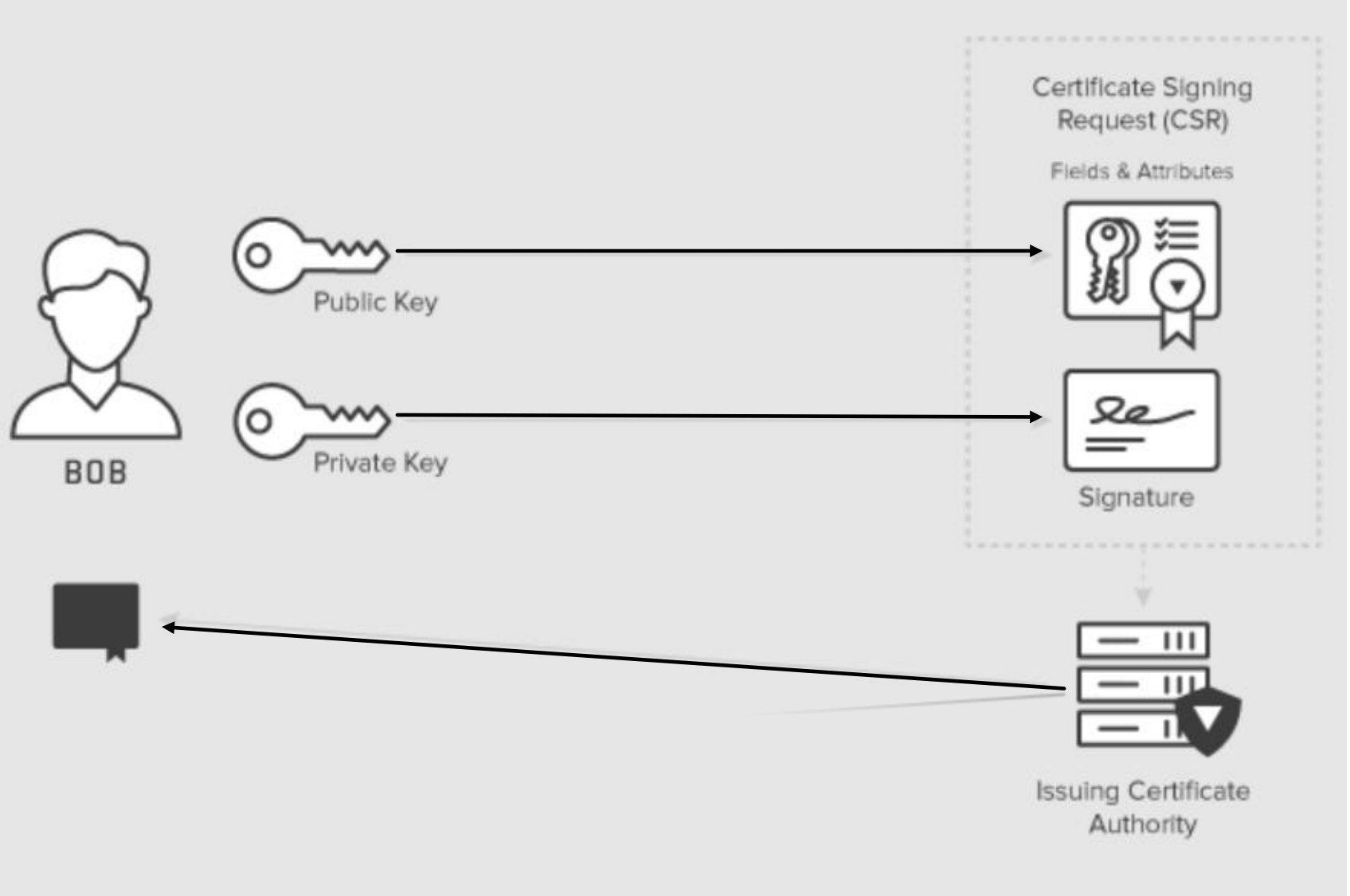
- Génération d'une **paire de clés** : clé privée + clé publique
- Collecte et vérification des **informations d'identification** par l'AC
- Création d'une **CSR** (Certificate Signing Request) : clé publique + attributs d'identification
- Signature de la CSR par le propriétaire (preuve de possession de la clé privée)
- Validation de la demande par l'AC

Fonctionnement du processus de création de certificats

- **2 Émission du certificat** : signé par la clé privée de l'AC

- **3 Vérification** :
- La clé publique du certificat permet de confirmer :
  - qu'il a bien été émis par l'AC,
  - que les données chiffrées ou signées par la clé privée du détenteur sont authentiques.

Principe clé publique / clé privée

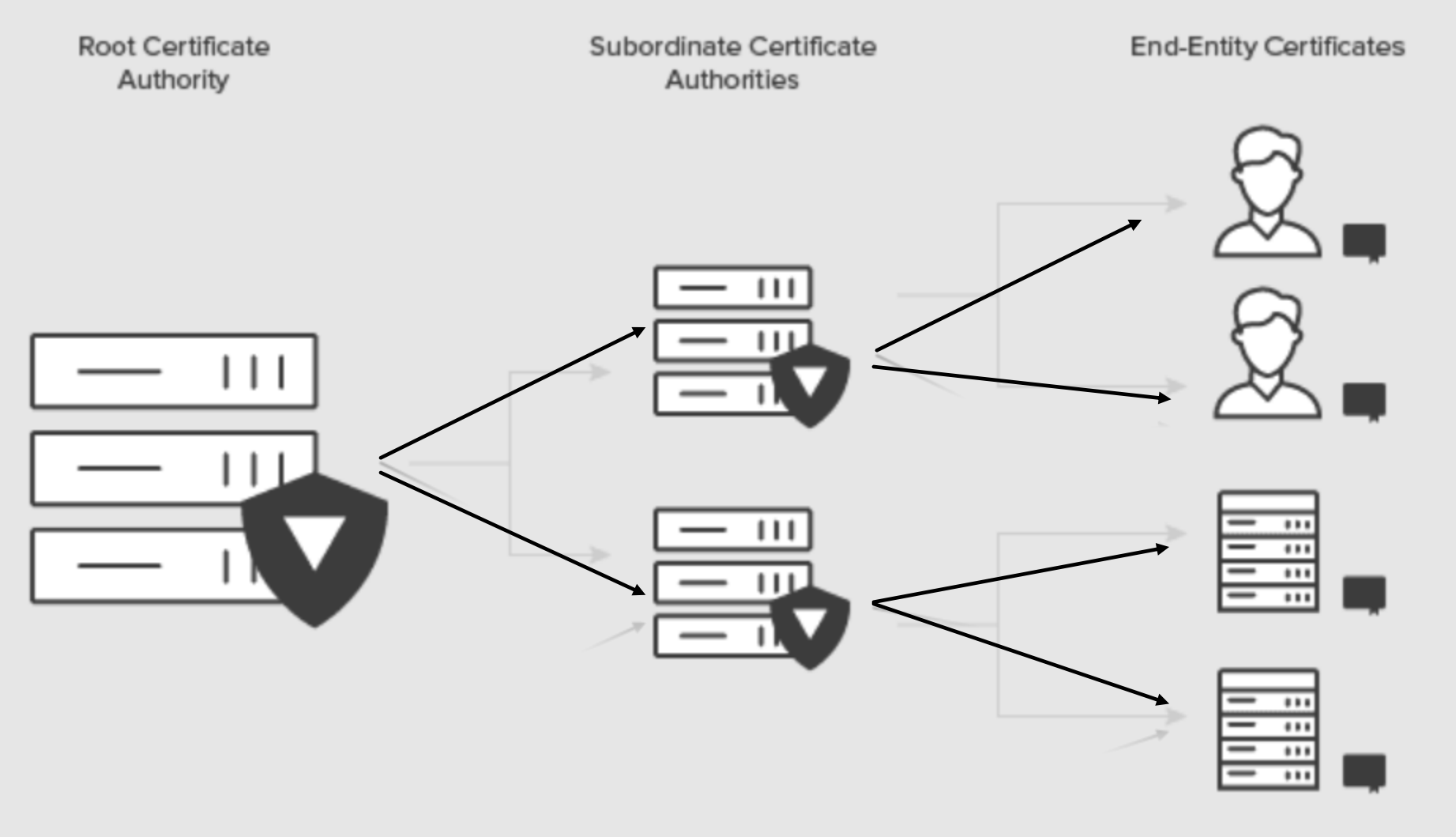


Comment les hiérarchies d'AC et les AC racine créent des couches de confiance

Chaque AC possède son propre certificat → création de **couches de confiance**

- Les certificats racine sont **auto-signés** → la confiance repose directement sur l'AC racine
- Importance cruciale de la **sécurité de la clé privée** d'une AC, surtout pour la racine
- Si une AC racine est compromise → impossible de révoquer → catastrophe de sécurité

Principe clé publique / clé privée

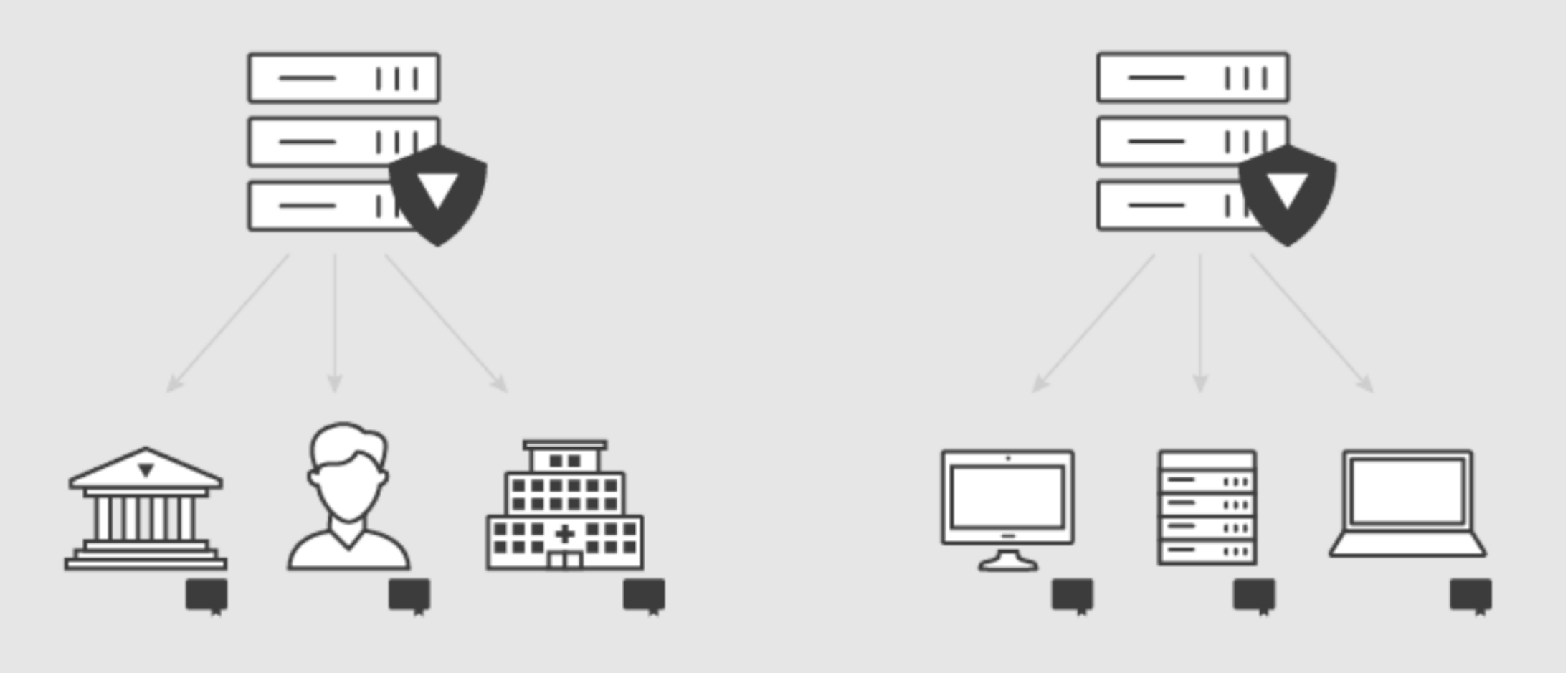


- Les AC racine doivent être **hors ligne 99,9 % du temps**
- Clés stockées dans des coffres-forts hautement sécurisés
- Accès limité, surveillance 24/7, meilleures pratiques de sécurité
- Mise en ligne uniquement pour :
- création/renouvellement de clés,
- émission de nouveaux certificats,
- vérification d'intégrité (environ 2 à 4 fois/an)

Durée de vie d'un certificat racine : 15–20 ans (vs ~7 ans pour les AC subordonnées)

- Hiérarchie minimale : 2 niveaux
- AC racine (hors ligne) → AC subordonnées (en ligne, émettent les certificats finaux)
- Plus il y a de niveaux → plus de complexité (politiques, procédures, évolutivité)

Principe clé publique / clé privée



Gestion de la révocation au moyen de listes de révocation de certificats

- Une AC peut révoquer un certificat (compromission, erreur, abus, etc.)
- Elle publie alors une **CRL** (Certificate Revocation List) contenant tous les certificats invalides
- Les consommateurs de certificats peuvent vérifier la CRL pour valider un certificat
- Vérification = plus sécurisé mais ralentit l'authentification
- Les navigateurs et services vérifient de plus en plus systématiquement les CRL
- Les CRL ont une **date d'expiration** → doivent être mises à jour régulièrement
- Si une CRL expire, tous les certificats de l'AC deviennent invalides
- Les CRL sont essentielles pour maintenir la **confiance et la sécurité** dans la PKI