

Les Infrastructures à Clés Publiques (PKI)

Module RSX112 - Sécurité des Réseaux

CNAM - Licence Système et Cybersécurité

 par Stéphane LARCHER



Introduction et Enjeux

Le Problème Fondamental

Comment établir la confiance dans le monde numérique ?
Alice veut envoyer un document confidentiel à Bob via Internet, mais :

- Comment Alice peut-elle être sûre qu'elle communique vraiment avec Bob ?
- Comment Bob peut-il vérifier que le message vient vraiment d'Alice ?
- Comment garantir que personne n'a modifié le message en transit ?
- Comment prouver légalement qui a envoyé quoi et quand ?

Définition d'une PKI

PKI (Public Key Infrastructure) : Ensemble de rôles, de politiques, de matériel, de logiciels et de procédures nécessaires pour créer, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques et gérer la cryptographie à clé publique.

En termes simples : Une PKI est le système qui permet d'établir la confiance dans le monde numérique.

Composants essentiels d'une PKI



Autorités de certification (CA)

Entités de confiance qui émettent les certificats numériques et garantissent l'authenticité des identités.



Certificats numériques

Documents électroniques prouvant l'identité d'une entité et liant cette identité à une clé publique.



Clés cryptographiques

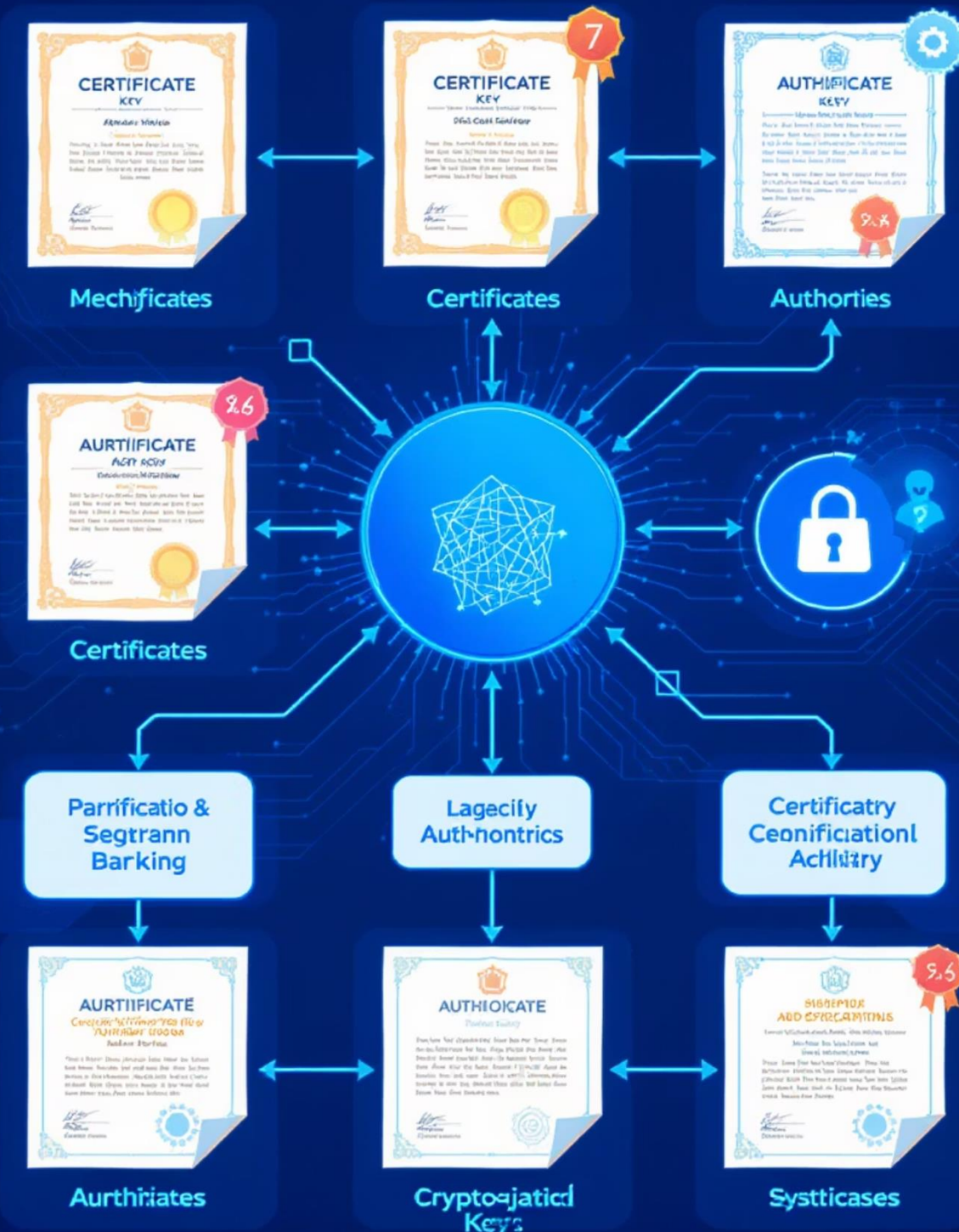
Paires de clés publiques et privées utilisées pour sécuriser les échanges et authentifier les parties.



Politiques et procédures

Règles régissant l'utilisation, l'émission et la gestion des certificats dans l'infrastructure.

PKI COMPONENTS



Enjeux Actuels des PKI

Enjeux Économiques

- E-commerce : 4 000 milliards € de transactions en ligne en 2023
- Coût d'une violation : 4,45 millions \$ en moyenne (IBM Security Report 2023)
- Conformité réglementaire : RGPD, PCI-DSS, eIDAS



Enjeux Techniques

- Scalabilité : Des millions de certificats à gérer
- Performance : Validation en temps réel
- Interopérabilité : Standards internationaux

Enjeux Sociétaux

- Identité numérique : Passeports, cartes d'identité électroniques
- Vote électronique : Garantir l'intégrité démocratique
- Santé : Protection des données médicales
- Pass sanitaires : Usage massif récent (COVID-19)

Statistiques clés 2024 et Histoire

95%

Trafic web chiffré

La quasi-totalité du trafic web utilise désormais le chiffrement HTTPS

200M+

Certificats actifs

Let's Encrypt a révolutionné l'accès aux certificats TLS

60

Jours

Renouvellement moyen des certificats, tendance à la baisse

| Année | Événement | Impact |
|-------|------------------------|--------------------------------------|
| 1976 | Diffie-Hellman | Concept de cryptographie asymétrique |
| 1977 | RSA | Première implémentation pratique |
| 1988 | X.509 v1 | Premier standard de certificats |
| 1995 | SSL 1.0 (Netscape) | Sécurisation du web |
| 2016 | Let's Encrypt | Démocratisation HTTPS |
| 2024 | Post-quantum readiness | Préparation future |

Cryptographie Symétrique vs Asymétrique

Cryptographie Symétrique





Définition : Système de chiffrement utilisant une même clé K pour chiffrer ET déchiffrer.

Principe :

Alice → Chiffre(Message, K) → Message chiffré → Bob

Bob → Déchiffre(Message chiffré, K) → Message original

Caractéristiques :

-  Rapide et efficace
-  Adapté aux gros volumes de données
-  Distribution de clé problématique
-  Pas de non-répudiation

Algorithmes courants : AES, ChaCha20

Cryptographie Asymétrique

Définition : Système utilisant deux clés mathématiquement liées : une publique (pour chiffrer) et une privée (pour déchiffrer).





Principe :

Bob génère : Clé Publique (PubB) + Clé Privée (PrivB)

Alice → Chiffre(Message, PubB) → Message chiffré → Bob

Bob → Déchiffre(Message chiffré, PrivB) → Message original

Caractéristiques :

-  Pas de partage de secret nécessaire
-  Permet les signatures numériques
-  Plus lent (×1000 que symétrique)
-  Clés plus grandes

Algorithmes courants : RSA, ECC, DSA

RSA : Principe Mathématique

RSA (Rivest-Shamir-Adleman) : Algorithme de chiffrement asymétrique basé sur la difficulté de factoriser le produit de deux grands nombres premiers.

Génération des clés RSA

1. Choisir deux grands nombres premiers : p et q
2. Calculer $n = p \times q$ (module public)
3. Calculer $\varphi(n) = (p-1) \times (q-1)$ (indicateur d'Euler)
4. Choisir e (exposant public, généralement 65537)
5. Calculer d tel que $e \times d \equiv 1 \pmod{\varphi(n)}$ (exposant privé)

Résultat : Clé publique : (n, e) et Clé privée : (n, d)

Utilisation

Chiffrement : $C = M^e \pmod{n}$

Déchiffrement : $M = C^d \pmod{n}$

Sécurité

La sécurité repose sur le fait que factoriser n en p et q est computationnellement difficile pour de grands nombres (2048 bits ou plus).

RSA : $AIE_x = 1$

altortini() $1 \times 1a = 1$

$a = \binom{2}{0,7}, -c^2 = \frac{x}{8f}^{bv}$

$AA = \binom{2}{altotim} = 2 = c$

$A = \binom{2}{(2^2 + 10)}, -1 \times 5^2; = 60$

Courbes Elliptiques (ECC)

ECC (Elliptic Curve Cryptography) : Cryptographie basée sur les propriétés algébriques des courbes elliptiques sur des corps finis.

Équation générale

$$y^2 = x^3 + ax + b$$

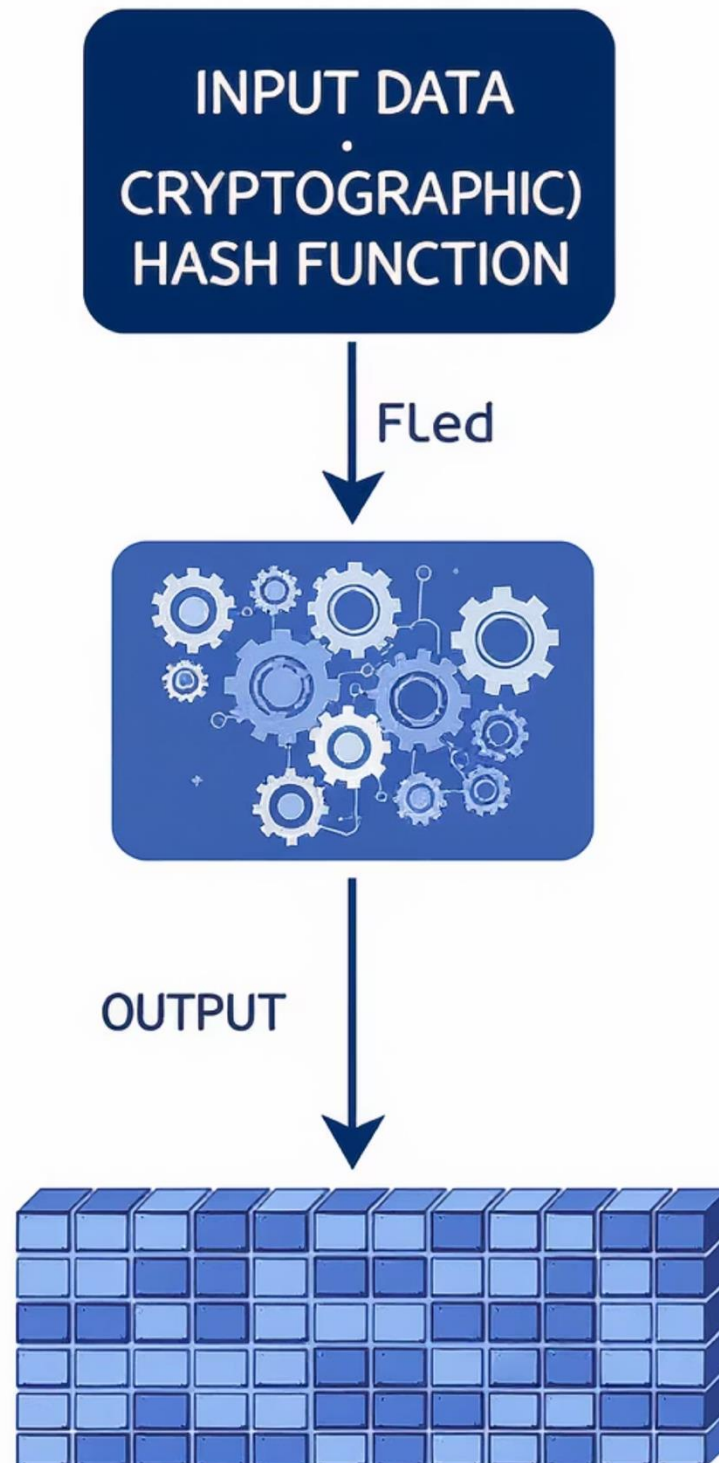
Les courbes elliptiques offrent une sécurité équivalente à RSA avec des clés beaucoup plus courtes, ce qui les rend particulièrement adaptées pour les environnements contraints en ressources.

Avantages par rapport à RSA

| Sécurité équivalente | RSA | ECC | Ratio |
|----------------------|------------|----------|-------|
| 80 bits | 1024 bits | 160 bits | 6:1 |
| 128 bits | 3072 bits | 256 bits | 12:1 |
| 256 bits | 15360 bits | 512 bits | 30:1 |

Applications

- Particulièrement adapté pour l'IoT et les environnements contraints en ressources
- Utilisé dans Bitcoin et autres cryptomonnaies
- Standard dans les protocoles modernes (TLS 1.3)



Fonctions de Hachage Cryptographiques

Fonction de hachage : Fonction qui transforme une donnée de taille arbitraire en une empreinte de taille fixe.

Propriétés essentielles

1. **Déterministe** : $H(x)$ donne toujours le même résultat
2. **Rapide** : Calcul efficace
3. **Unidirectionnelle** : Impossible de retrouver x depuis $H(x)$
4. **Résistance aux collisions** : Difficile de trouver $x \neq y$ tel que $H(x) = H(y)$
5. **Effet avalanche** : Petit changement dans l'entrée \rightarrow grande différence dans le hash

Algorithmes courants

| Algorithme | Taille | Statut | Usage |
|------------|----------|------------|---------------------|
| MD5 | 128 bits | ✗ Obsolète | Legacy uniquement |
| SHA-1 | 160 bits | ⚠ Déprécié | Migration urgente |
| SHA-256 | 256 bits | ✓ Sûr | Standard actuel |
| SHA-3 | Variable | ✓ Sûr | Alternative moderne |
| BLAKE3 | 256 bits | ✓ Sûr | Haute performance |

Signatures Numériques

Signature numérique : Mécanisme cryptographique permettant de garantir l'authenticité, l'intégrité et la non-répudiation d'un document.



SIGNATURE

1. $\text{Hash} = H(\text{Document})$
2. $\text{Signature} = \text{Chiffrer}(\text{Hash}, \text{CléPrivée_Alice})$
3. Envoyer : Document + Signature



VÉRIFICATION

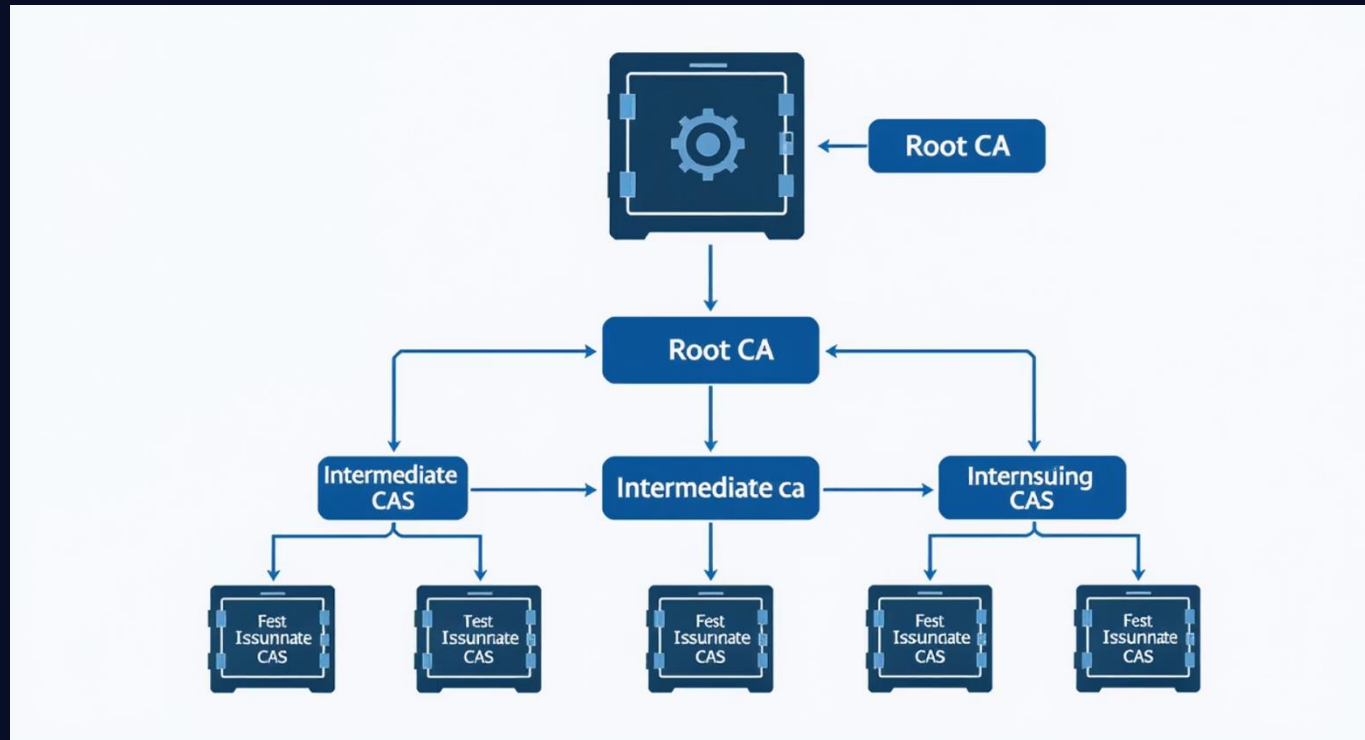
1. $\text{Hash1} = H(\text{Document_reçu})$
2. $\text{Hash2} = \text{Déchiffrer}(\text{Signature}, \text{CléPublique_Alice})$
3. Si $\text{Hash1} == \text{Hash2} \rightarrow \text{Signature Valide } \checkmark$

Propriétés garanties

- **Authenticité** : Vient bien d'Alice (seule à avoir la clé privée)
- **Intégrité** : Document non modifié (hash différent sinon)
- **Non-répudiation** : Alice ne peut nier avoir signé

Modèles de Confiance

Modèle Hiérarchique (X.509)



Caractéristiques :

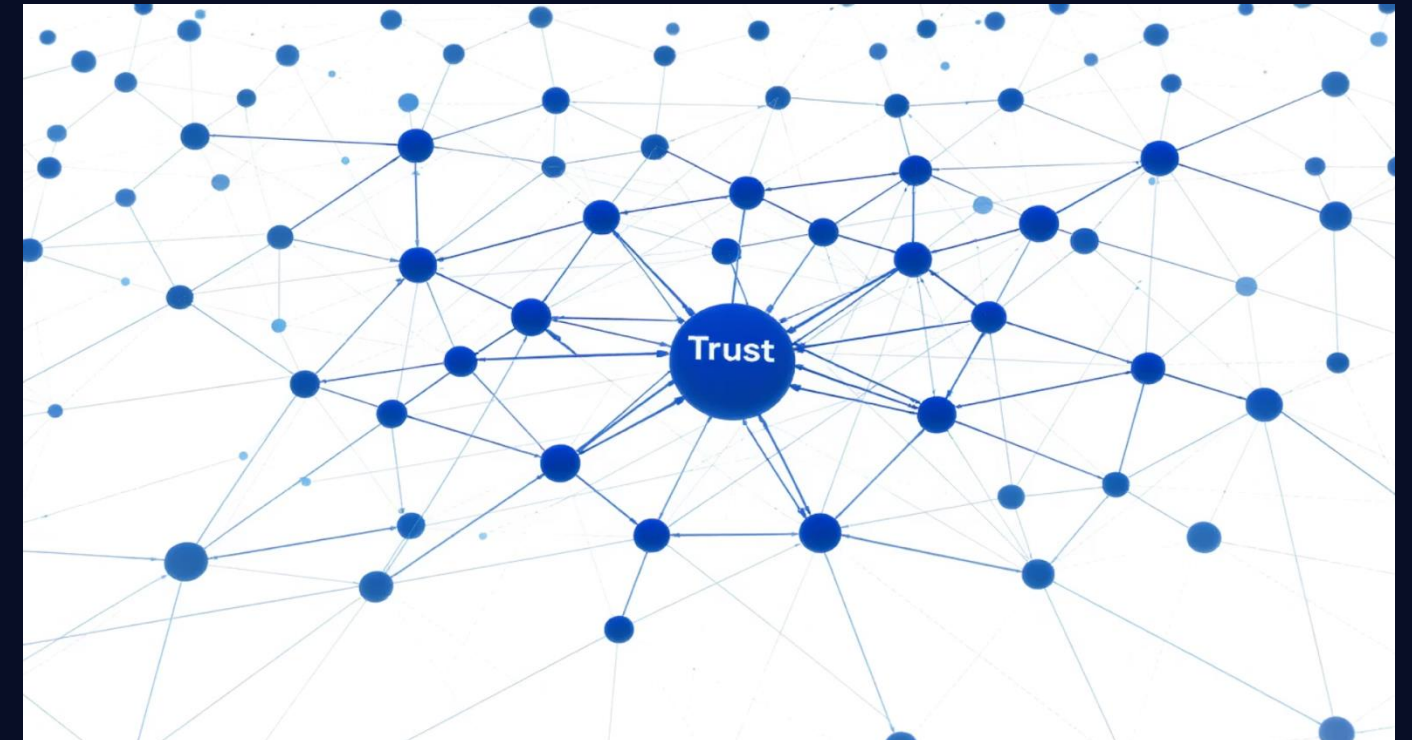
- ☒ Confiance descendante claire
- ☒ Révocation centralisée
- ☒ Scalable
- ☒ Point unique de défaillance

Usage : Navigateurs web, entreprises

Modèle Hybride (DANE)

Combine PKI + DNS + Blockchain pour une confiance distribuée

Modèle Web of Trust (PGP)

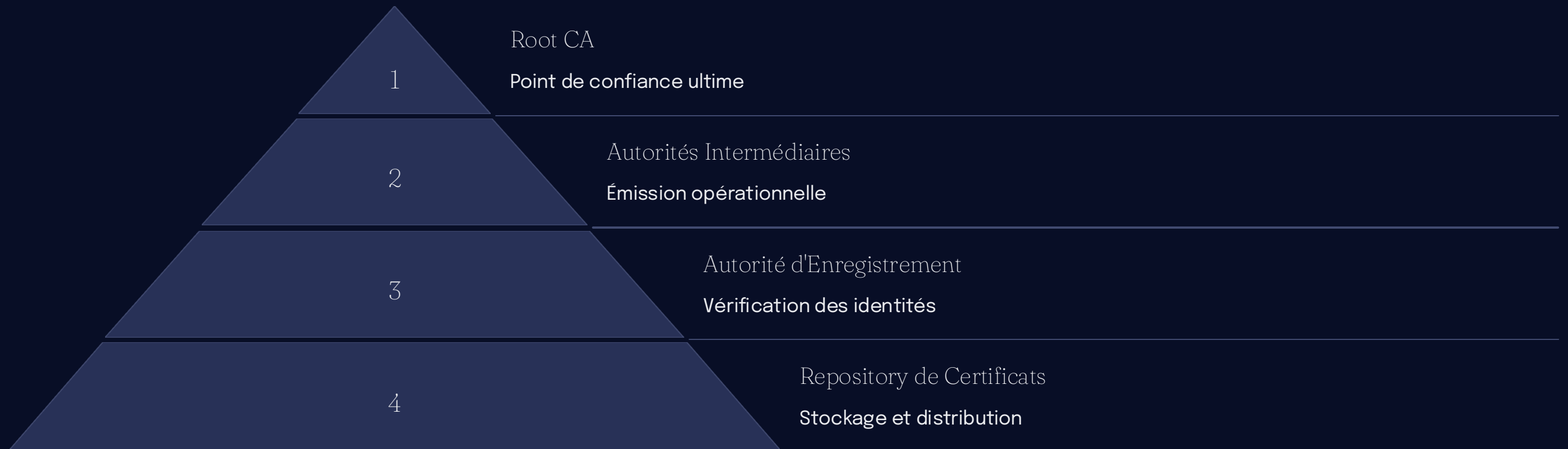


Caractéristiques :

- ☒ Pas d'autorité centrale
- ☒ Confiance peer-to-peer
- ☒ Résilient
- ☒ Difficile à gérer à grande échelle

Usage : Communautés open source

Composants d'une PKI Hiérarchique



Autorité de Certification Racine (Root CA)

Point de confiance ultime avec certificat auto-signé, généralement maintenu hors ligne (air gap).

- Durée de vie : 15-25 ans
- Stockage : Coffre-fort, HSM dédié
- Usage : Signer les CA intermédiaires uniquement
- Sécurité : Cérémonie de clés, accès ultra-restreint

Autorités Intermédiaires (Subordinate CA)

Émission opérationnelle des certificats avec spécialisation possible (SSL, Email, Code Signing).

Avantages :

- Révocation granulaire possible
- Limite l'impact d'une compromission
- Permet la délégation

Cycle de Vie d'un Certificat

GÉNÉRATION

- Création paire de clés
- Création CSR (Certificate Signing Request)

RÉVOCATION/EXPIRATION

- Ajout à la CRL/OCSP
- Archivage pour audit

MAINTENANCE

- Renouvellement avant expiration
- Re-key si nécessaire



VALIDATION

- Vérification identité
- Validation domaine/organisation

ÉMISSION

- Signature par CA
- Publication dans le repository

UTILISATION

- TLS/SSL
- Signature email
- Authentification

Format X.509 v3

X.509 : Standard ITU-T définissant le format des certificats de clé publique.

Structure d'un certificat

```
Certificate: Version: 3 (0x2) Serial Number:
04:00:00:00:00:01:15:4b:5a:c3:94 Signature Algorithm:
sha256WithRSAEncryption Issuer: C=FR, O=Example CA, CN=Example
Root CA Validity: Not Before: Jan 1 00:00:00 2024 GMT Not
After : Dec 31 23:59:59 2024 GMT Subject: C=FR, O=Company,
CN=www.example.com Subject Public Key Info: Public Key
Algorithm: rsaEncryption RSA Public-Key: (2048 bit) X509v3
extensions: X509v3 Subject Alternative Name:
DNS:www.example.com, DNS:example.com X509v3 Key Usage: critical
Digital Signature, Key Encipherment
```

Extensions importantes

- **Basic Constraints** : CA:TRUE/FALSE, pathlen
- **Key Usage** : digitalSignature, keyEncipherment, keyCertSign
- **Extended Key Usage** : serverAuth, clientAuth, codeSigning, emailProtection
- **Subject Alternative Name (SAN)** : Domaines multiples, IPs, wildcards



Types de Validation de Certificats

DV (Domain Validation)

Vérifications : Contrôle du domaine uniquement

- DNS TXT
- HTTP
- Email

Délai : Minutes

Coût : Gratuit - €

Usage : Sites personnels, blogs

OV (Organization Validation)

Vérifications : Existence légale

- Kbis
- Factures
- Appel téléphonique

Délai : 1-3 jours

Coût : €€

Usage : Sites d'entreprise

EV (Extended Validation)

Vérifications : Vérification approfondie

- Audit physique
- Vérifications multiples
- Procédures strictes






Délai : 1-2 semaines

Coût : €€€

Usage : Banques, e-commerce critique

Note : La barre verte EV a été retirée des navigateurs modernes car les utilisateurs ne la comprenaient pas.

DIGITAL CERTIFICATE VALIDATION TYPES

| VALIDATION DV | CERTIFICATE OV | VALIDATION OV |
|--|---|---|
|  |  |  |
| DV (DOMAIN VALIDATION) | EXTENDED VALIDATION | EXTENDED VALIDATION |
| Organization Verifications | Extended Certifications | Stricter Certification |
| Security: Trust Indicators |  |  |

Certificate Signing Request (CSR)

CSR : Demande de signature de certificat contenant la clé publique et les informations d'identité du demandeur.

Génération d'un CSR

```
# Génération interactiveopenssl req -new -key  
private.key -out request.csr# Génération  
automatiséeopenssl req -new -key private.key -out  
request.csr \-subj  
"/C=FR/ST=IDF/L=Paris/O=Company/CN=www.example.com"
```

Contenu d'un CSR

Distinguished Name (DN) :

- **C** (Country) : Code pays ISO 3166
- **ST** (State) : Région/État
- **L** (Locality) : Ville
- **O** (Organization) : Nom de l'organisation
- **OU** (Organizational Unit) : Service/Département
- **CN** (Common Name) : FQDN ou nom
- **emailAddress** : Adresse email

Révocation de Certificats

Raisons de révocation



Compromission

Compromission de la clé privée nécessitant une révocation immédiate



Erreur

Erreur dans le certificat nécessitant une correction



Changement

Changement d'organisation ou de structure nécessitant une mise à jour





Cessation

Cessation d'activité rendant le certificat obsolète



CRL (Certificate Revocation List)

Définition : Liste signée des certificats révoqués, mise à jour périodiquement.

Avantages :

-  Simple à implémenter
-  Peut être mise en cache



Inconvénients :

-  Taille croissante
-  Délai de mise à jour



OCSP (Online Certificate Status Protocol)

Définition : Protocole temps réel pour vérifier le statut d'un certificat spécifique.

Avantages :

-  Réponse en temps réel
-  Réponse ciblée

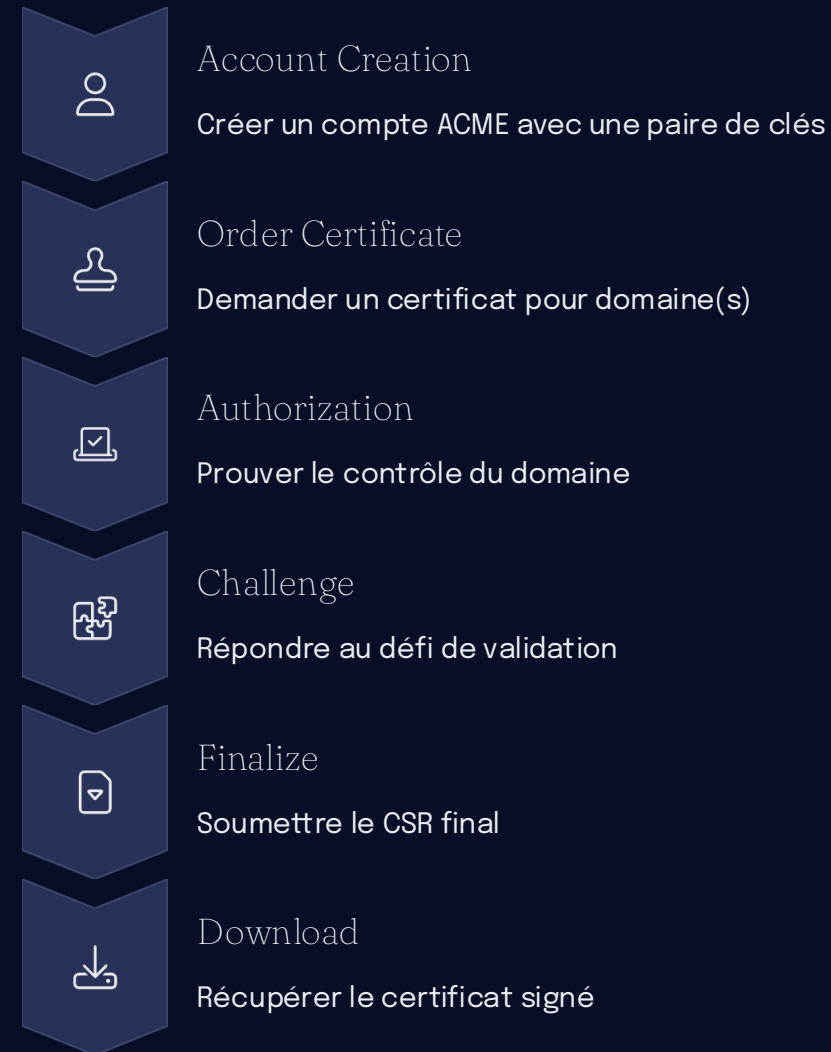
Inconvénients :

-  Charge serveur
-  Privacy (le CA sait ce que vous visitez)

OCSP Stapling : Le serveur inclut la réponse OCSP dans le handshake TLS, combinant le meilleur des deux approches.

Protocole ACME

ACME (Automatic Certificate Management Environment) : Protocole permettant l'automatisation complète du cycle de vie des certificats, popularisé par Let's Encrypt.




Types de challenges

- **HTTP-01** : Placer un fichier spécifique sur le serveur web
- **DNS-01** : Créer un enregistrement TXT DNS spécifique
- **TLS-ALPN-01** : Répondre avec un certificat auto-signé spécial


Hardware Security Modules (HSM)

HSM : Dispositif physique dédié à la protection et gestion des clés cryptographiques.




Vraie entropie

Générateur hardware de nombres aléatoires pour une sécurité maximale




Clés non exportables

Les clés privées ne quittent jamais le HSM, limitant les risques




Performance

Accélération matérielle des opérations cryptographiques



Conformité

FIPS 140-2 Level 3/4, Common Criteria pour les exigences réglementaires



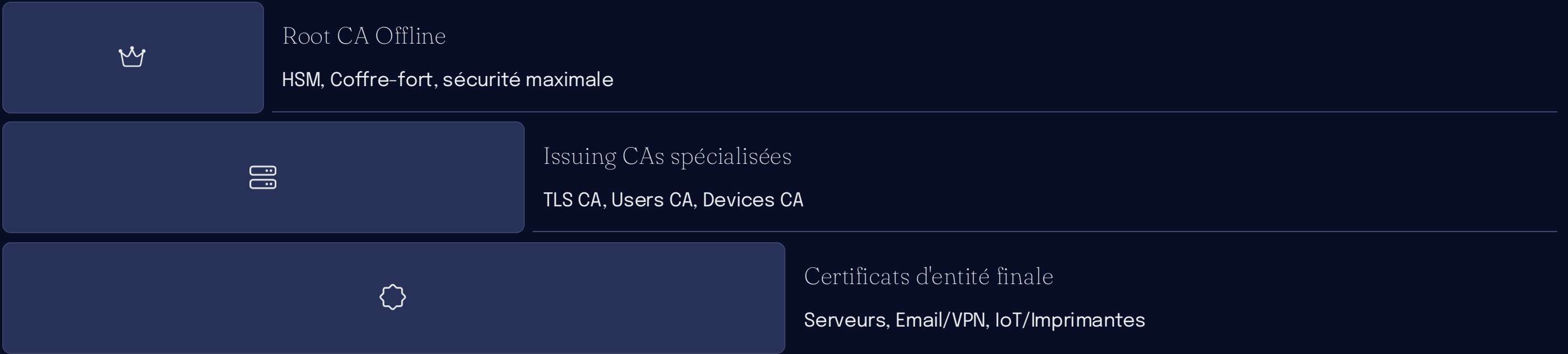
Tamper-proof

Autodestruction en cas d'intrusion physique pour protection maximale

| Type | Usage | Performance | Coût |
|-------------|---------------------|-------------|--------|
| Network HSM | Datacenter, partagé | Très haute | €€€€ |
| PCIe HSM | Serveur dédié | Haute | €€€ |
| USB Token | Dev, petite CA | Moyenne | €€ |
| Cloud HSM | Services cloud | Variable | €/mois |

Architecture PKI d'Entreprise

Architecture recommandée



Dimensionnement selon la taille

| Taille Entreprise | Employés | Certificats/an | Architecture |
|-------------------|----------|----------------|----------------------|
| PME | <100 | <500 | 1 Root + 1 Issuing |
| ETI | 100-5000 | 500-50k | 1 Root + 2-3 Issuing |
| Grande entreprise | >5000 | >50k | 2 Root + 5+ Issuing |

Règle d'or : La Root CA doit TOUJOURS être hors ligne (air gap) pour maximiser la sécurité.

Cérémonie de Clés

Key Ceremony : Processus formel et audité de génération des clés de la Root CA avec témoins et procédures strictes.



Sécurisation de l'Infrastructure PKI

Sécurité Physique

- Datacenter sécurisé Tier 3+
- Accès biométrique
- Surveillance 24/7
- Coffre-fort pour Root CA

Sécurité Système

- OS durci (CIS Benchmarks)
- Firewall restrictif
- Pas de services inutiles
- Audit logging complet

Sécurité Cryptographique

- HSM certifié FIPS 140-2
- Clés \geq 2048 bits (RSA)
- Rotation régulière
- Algorithmes approuvés

Sécurité Organisationnelle

- Séparation des tâches
- Principe du moindre privilège
- Formation du personnel
- Background checks

Procédures

- CP/CPS documentés
- Procédures d'urgence
- Plan de continuité
- Tests réguliers

Audit et Conformité

- Audit annuel WebTrust
- Conformité eIDAS
- Logs immutables
- Monitoring 24/7

Monitoring et KPIs

Métriques Clés (KPIs)

Opérationnelles :

- Certificats émis/jour
- Temps moyen d'émission
- Taux de renouvellement automatique
- Certificats proche expiration
- Taille de la CRL

Performance :

- Requêtes OCSP/seconde
- Temps de réponse OCSP
- Disponibilité services (SLA)
- Utilisation HSM
- Bande passante CRL

Alertes Critiques

- Certificat CA expire dans <90 jours
- HSM utilisation > 80%
- Échecs de validation répétés
- Tentatives d'accès non autorisées
- CRL non mise à jour depuis >24h

Outils de Monitoring

Open Source

EJBCA, Boulder, Prometheus
+ Grafana

Commercial

Microsoft ADCS, DigiCert
CertCentral, Venafi

Réponse aux Incidents PKI

Scénarios d'incidents critiques

Compromission Clé Privée

1. Révoquer immédiatement (raison: keyCompromise)
2. Générer nouvelle paire de clés
3. Émettre nouveau certificat
4. Mettre à jour CRL/OCSP
5. Notifier les parties affectées
6. Investigation forensique

Compromission CA

URGENCE MAXIMALE

1. Isoler la CA compromise
2. Révoquer TOUS les certificats émis
3. Notification d'urgence (CERT + clients)
4. Audit forensique complet
5. Reconstruction depuis backup
6. Possible migration vers nouvelle hiérarchie

Erreur d'Émission

1. Identifier l'étendue (nombre de certificats)
2. Révoquer les certificats erronés
3. Ré-émettre avec informations correctes
4. Post-mortem et amélioration process

Plan de communication crise

- Équipe de crise identifiée 24/7
- Templates de communication prêts
- Liste de contacts à jour
- Procédure d'escalade claire

Applications Actuelles de la PKI



🌐 TLS/SSL pour le Web

Statistiques 2024 :

- 95% du trafic web chiffré
- 200M+ certificats Let's Encrypt actifs
- Renouvellement moyen : 60-90 jours
- Migration vers certificats courte durée (7-14 jours)



✉️ Email Sécurisé (S/MIME)

Adoption :

- Entreprises : 60%
- Particuliers : <5%

Défis :

- Gestion des clés complexe
- Interopérabilité clients email
- Alternative : PGP/GPG



🔒 Authentification Forte

Applications :

- VPN d'entreprise
- WiFi 802.1X (EAP-TLS)
- Smart cards / Badges
- SSH certificates

Applications Sectorielles de la PKI

Santé

- Cartes professionnelles de santé (CPS)
- Prescriptions électroniques
- Dossiers médicaux partagés (DMP)
- Pass sanitaires COVID-19

IoT et Industrie 4.0

Défis spécifiques :

- Ressources limitées (CPU, RAM)
- Durée de vie longue (10+ ans)
- Mise à jour difficile

Solutions :

- ECC pour économie ressources
- Certificats longue durée
- Bootstrap sécurisé (EST-coaps)

Finance

- 3D Secure pour paiements en ligne
- Open Banking (PSD2)
- Blockchain/DLT



Blockchain et PKI

Convergence des technologies

PKI Traditionnelle

-  Standards matures
-  Performance élevée
-  Support universel
-  Centralisation
-  Point unique défaillance

Blockchain

-  Décentralisation
-  Immuabilité
-  Transparence
-  Performance limitée
-  Coûts élevés

Applications hybrides



Certificate Transparency Logs

Blockchain pour l'audit des certificats, permettant une vérification publique et immuable de tous les certificats émis.



Smart Contracts PKI

Automatisation de l'émission/révocation des certificats via des contrats intelligents sur blockchain.



Identité souveraine (SSI)

L'utilisateur contrôle ses credentials, avec une approche décentralisée de la gestion d'identité.



Blockcerts

Système de diplômes universitaires sur blockchain avec vérification PKI, garantissant l'authenticité des diplômes.

Cryptographie Post-Quantique

 La menace quantique

Algorithme de Shor : Permet de factoriser de grands nombres et résoudre le logarithme discret en temps polynomial sur un ordinateur quantique.



RSA-2048

✗ Vulnérable - Migration urgente requise



ECC-256

✗ Vulnérable - Migration urgente requise



AES-128

⚠ Affaibli - Passer à AES-256



SHA-256

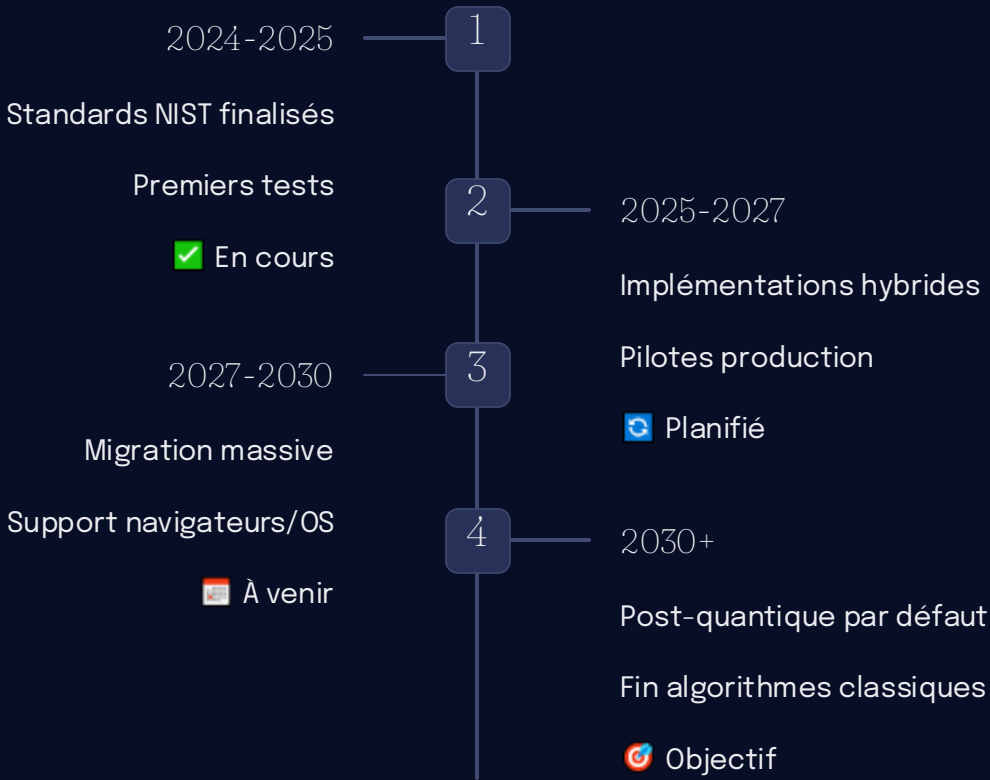
✓ Résistant - Surveillance recommandée

Solutions post-quantiques (NIST)

- **CRYSTALS-Kyber** : Chiffrement basé sur les réseaux
- **CRYSTALS-Dilithium** : Signatures basées sur les réseaux
- **FALCON** : Signatures compactes
- **SPHINCS+** : Signatures basées sur hash (conservateur)

Timeline de Migration Post-Quantique et Innovations Futures

Timeline de Migration



Innovations Futures



Zero-Knowledge Proofs

Prouver la possession d'un certificat sans le révéler, pour l'authentification anonyme et la vérification d'âge préservant la vie privée.



Certificats Éphémères

Durée de vie en minutes/heures, génération à la demande, pas de révocation nécessaire pour une sécurité maximale.



PKI Décentralisée

Pas de CA centrale, consensus blockchain, identité auto-souveraine pour une résilience maximale.



Intelligence Artificielle

Détection d'anomalies, prédiction de compromissions, automatisation de la réponse aux incidents.







Synthèse et Conclusion

Les 10 Commandements de la PKI

1. Tu **protégeras ta clé privée** comme le plus précieux des trésors
2. Tu **ne réutiliseras jamais** une clé compromise
3. Tu **vérifieras toujours** la chaîne de certification
4. Tu **révoqueras rapidement** les certificats compromis
5. Tu **automatiseras** le renouvellement des certificats
1. Tu **auditeras régulièrement** ton infrastructure
2. Tu **documenteras** toutes les procédures
3. Tu **formeras** tes utilisateurs continuellement
4. Tu **planifieras** la migration post-quantique
5. Tu **maintiendras** une veille technologique active

La PKI est le fondement invisible mais essentiel de la confiance numérique moderne. Sans elle, le commerce électronique, les communications sécurisées et l'identité numérique seraient impossibles.

Compétences Clés à Retenir

-  Comprendre la cryptographie asymétrique et son rôle
-  Concevoir une architecture PKI adaptée
-  Implémenter les protocoles standards (X.509, ACME)
-  Gérer le cycle de vie complet des certificats
-  Répondre efficacement aux incidents de sécurité
-  Anticiper les évolutions futures (post-quantique)

Document rédigé pour le module RSX112 - Sécurité des Réseaux