cethun

in innovation we trust

PKI implémentation

Public Key Infrastructure

Votre instructeur

Thierry DECKER
mail@thierry-decker.com

PKI Implémentation Sommaire

- Autorités de certifications publiques de confiance
- Autorités de certification (CA)
- Travailler avec les autorités d'enregistrement (RA)
- Gestion des clés
- Gestion des certificats
- Modèles de confiance
  - Hiérarchique
  - Par pont
  - Par maillage
  - Hybride

PKI Implémentation CA Publiques

- Un tiers de confiance (Trusted Third Party) publie et signe vos certificats numériques
- Les navigateurs font déjà confiance à ces tiers (TTP)
- Exemples de tiers de confiance :
  - VeriSign, GoDaddy, DigiCert, etc.
- Bonne pratique pour un serveur Web public
  - Un certificat auto-signé provoquera des avertissements
- Pour :
  - Confiance implicite des navigateurs
  - Peu de gestion des certificats (Révocation gérée par le navigateur)
- Contre :
  - Coûts

PKI Implémentation CA internes

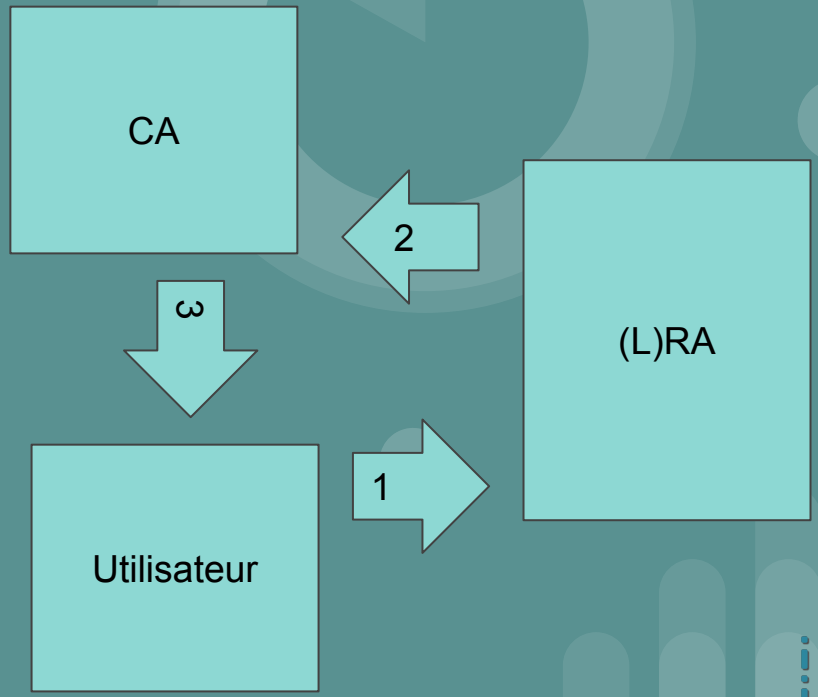
- Utilisées pour les intranets et autres usages internes
  - Chiffrement de disques
  - Documents signés électroniquement
  - Emails
- Pour :
  - Coût moins élevé
  - Plus de contrôle
- Contre :
  - Surplus de gestion
    - Configuration, support des protocoles, systèmes et des applications
    - Quel modèle de confiance et sa mise à l'échelle ?
    - Interopérabilité avec les tiers (extranet)

PKI Implémentation CA internes

- Certain systèmes d'exploitation peuvent être configurés pour fournir les services de PKI
- Microsoft Stand-alone CA vs Enterprise CA
  - Stand-alone CA ne nécessitent pas de service AD
- Enterprise CA s'appuie sur AD pour son service de répertoire
  - Templates de création
  - Certificats liés aux utilisateurs
  - CRL diffusées

PKI Implémentation Travailler avec les RA

- Parfaites pour vérifier les informations d'identification des utilisateurs en personne
- Autorités d'enregistrement locales (LRA) lorsque l'organisation possède de multiples sites



cethun
in innovation we trust

PKI Implémentation Gestion des clés

- Génération des clés et signature
  - Centralisée
    - Créées et stockées par la CA
  - Décentralisée
    - Créées par l'utilisateur et soumise à la CA pour la signature (via la RA)
    - La CA ne garde pas de copie des clés
- Répertoire des clés
  - Les clés publiques peuvent être stockées en un point central

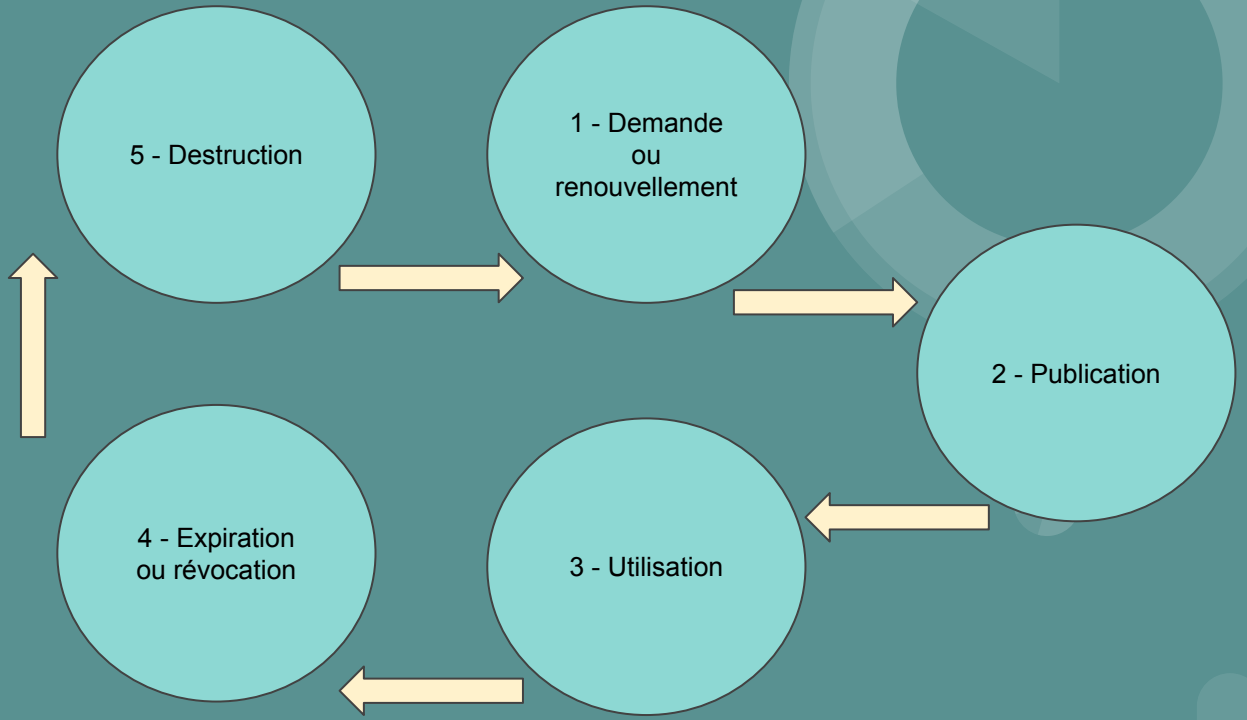
PKI Implémentation Gestion des clés

- Récupération des clés
  - Archivage des clés
    - Configurer des outils pour faire cet archivage automatiquement
  - Désigner des utilisateurs (agents de récupération) comme agents de récupération
  - Contrôle M de N
    - M : Nombre d'employés
    - N : Nombre d'agents de récupération
    - Définir le nombre d'agent nécessaire pour récupérer une clé

PKI Implémentation Gestion des certificats

- Règles de gestion et procédure de gestion
- Les certificats doivent être gérés en accord avec les règles de sécurité de l'organisation
- Définition des règles d'utilisation des certificats
- La DSI définie et documente ces règles et en informe la RH
- Politique de gestion des certificats :
  - Publication, utilisation, renouvellement et archivage
  - Que doit faire l'utilisateur en cas de perte ou de compromission des clés
- Certificate Practice Statement (CPS)
  - Procédures que la CA doit suivre et qu'elle s'attend à être suivies par les utilisateurs

PKI Implémentation Gestion des certificats



cethun
in innovation we trust

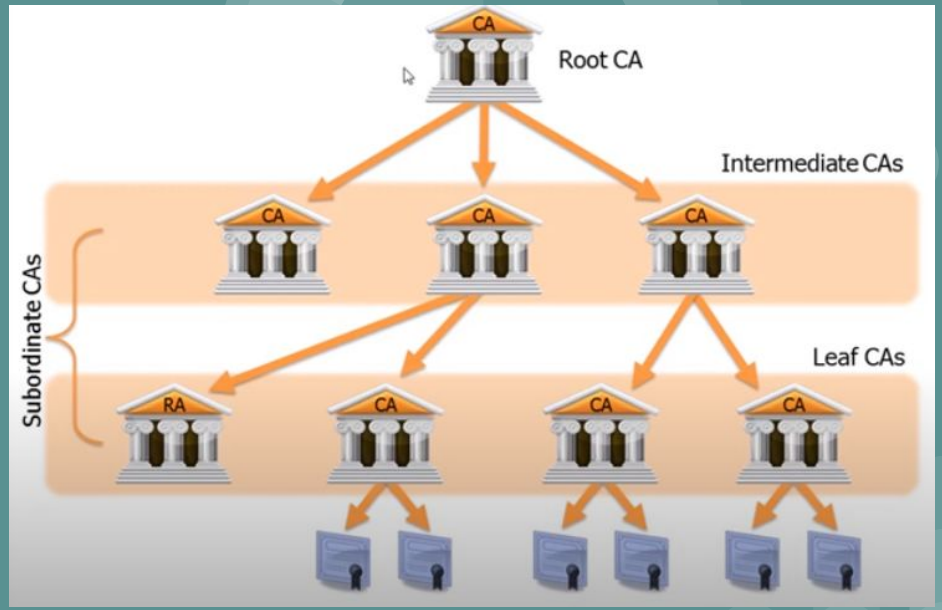
PKI Implémentation Modèles de confiance

- Concept de confiance en une autorité de certification
- Si un certificat est signé par un tier de confiance alors on a confiance dans le certificat

- Une CA unique
  - Petite PKI avec un seul certificat racine (Root Certificate)
- Hiérarchique
  - Structure de confiance “Top Down”
  - La CA la plus haute signe les certificats de ses subordonnés

PKI Implémentation Modèles de confiance

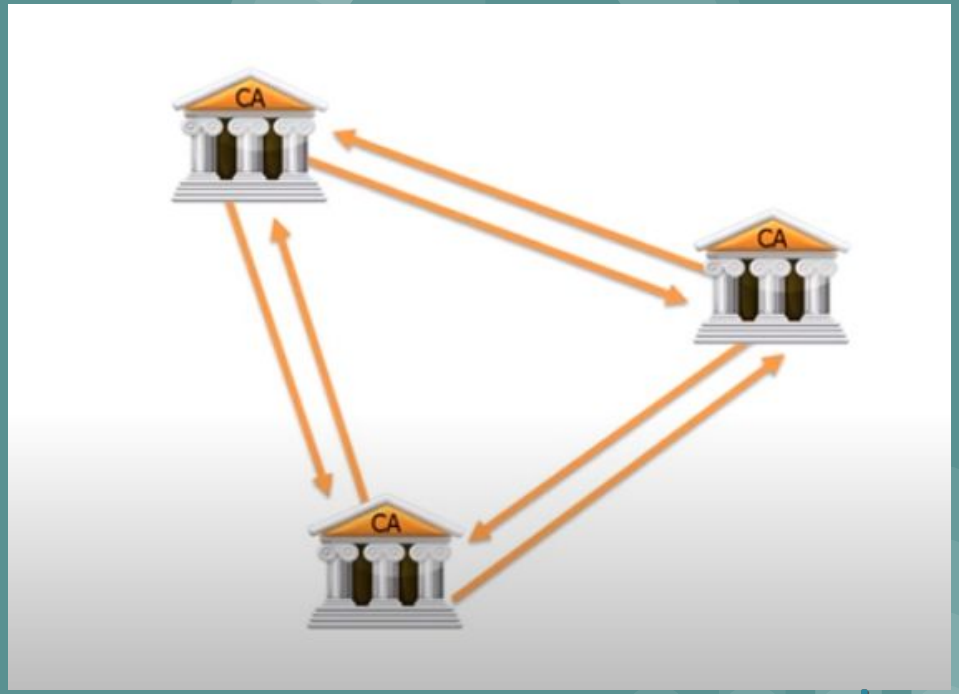
- Hiérarchique
  - Structure de confiance “Top Down”
  - La CA la plus haute signe les certificats de ses subordonnés



cethun
in innovation we trust

PKI Implémentation Modèles de confiance

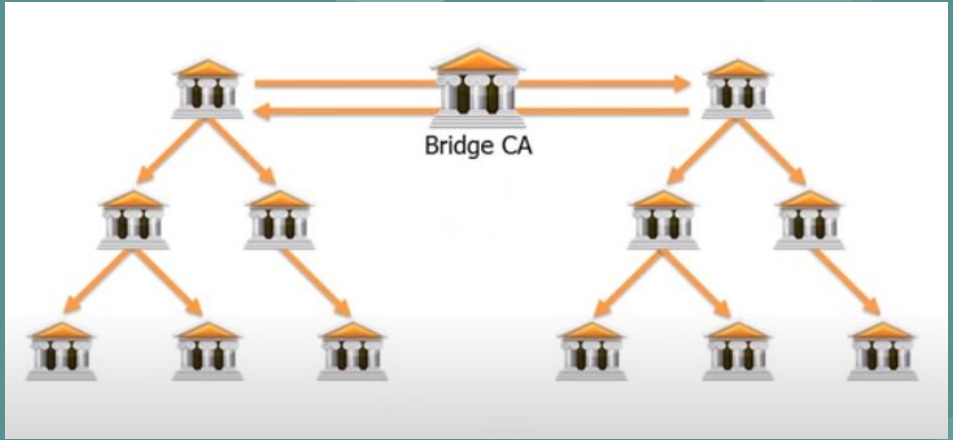
- Mesh
  - Toutes les CA se certifient entre elles
  - La confiance est acquise auprès d'un des CA seulement



cethun
in innovation we trust

PKI Implémentation Modèles de confiance

- Bridge



cethun
in innovation we trust

cethun
in innovation we trust

PKI implémentation - Q&A

Merci de votre attention !