Chapitre III
Gestion des Clés Publiques : Cas de PKI

Liaison d'une clé publique à une entité

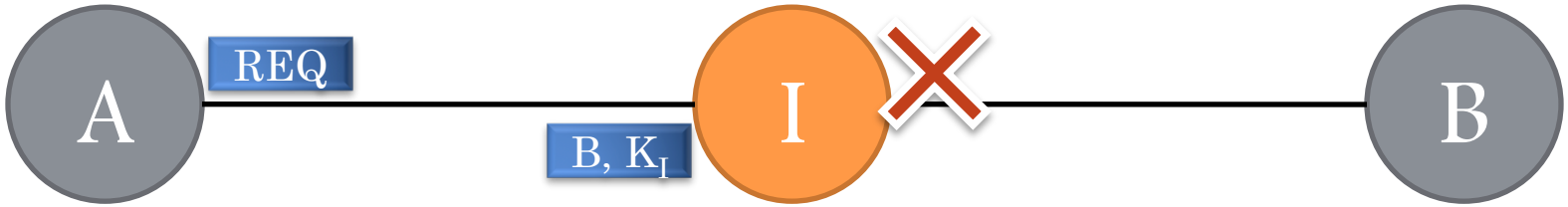
Modèles de certification

Révocation & annuaires des certificats

Exemples d'application

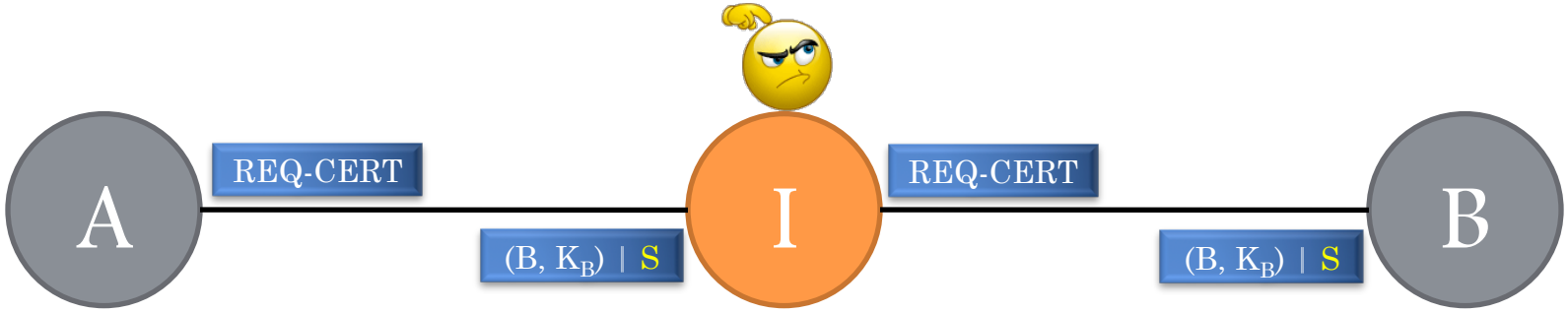
Partage du pouvoir de certification

Liaison d'une entité à sa clé publique



- « A » envoie à « B » une requête pour avoir sa clé publique
- « I » interrompt la requête
- « I » répond à « A » avec (B, K_I) en se faisant passer pour « B »
- Comment « A » peut vérifier la validité de cette liaison ?
- Certificat est un document électronique signé par une autorité permettant de lier une entité à sa clé publique

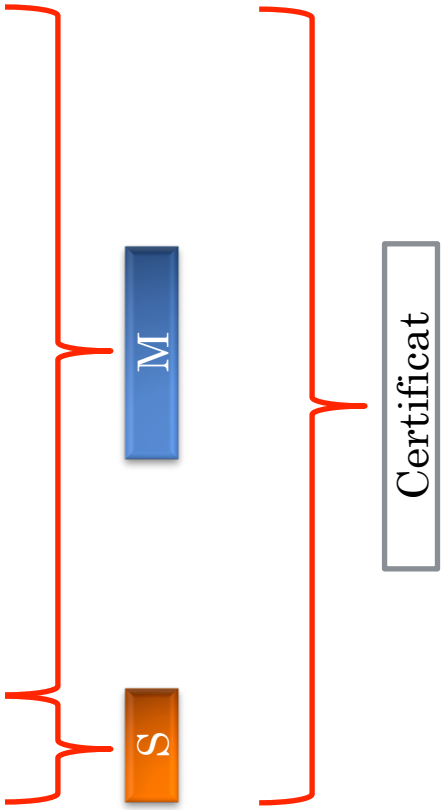
Liaison d'une entité à sa clé publique



- « A » envoie à « B » une requête pour avoir son certificat
- « I » interrompt la requête ?
- « B » répond à « A » avec (B, K_B) signé par une autorité
- « I » peut-il tricher sur cette liaison ?
- « A » vérifie la signature numérique
  ⇒ A peut faire confiance à cette liaison

CERTIFICAT D'IDENTITÉ X.509

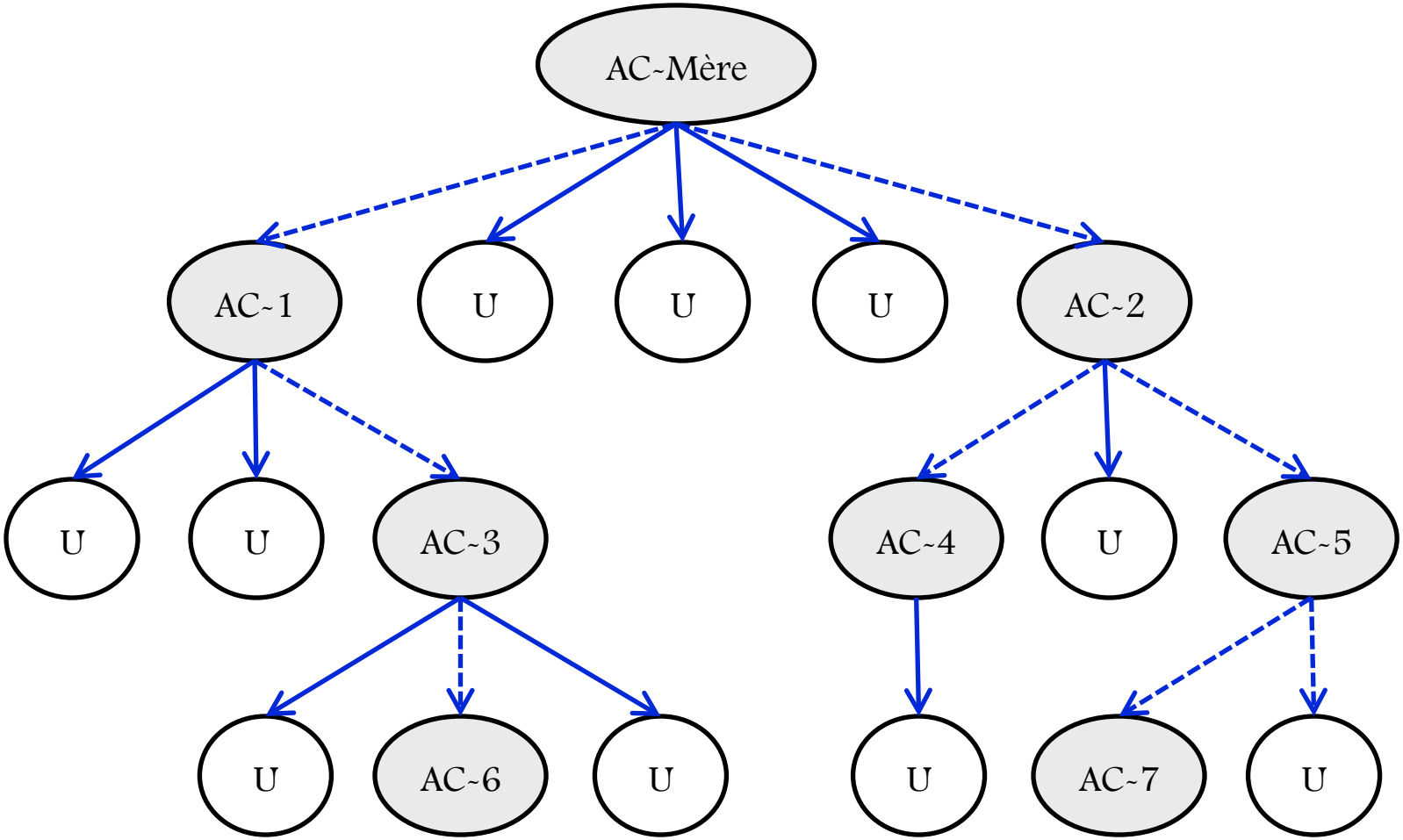
- Version du standard
- Numéro de série du certificat
- Fonction de hachage utilisée
- Algorithme de signature utilisé
- L'identité du signataire
- Période de validité du certificat
- L'identité de l'utilisateur
- La clé publique de l'utilisateur
- Signature de l'autorité de confiance



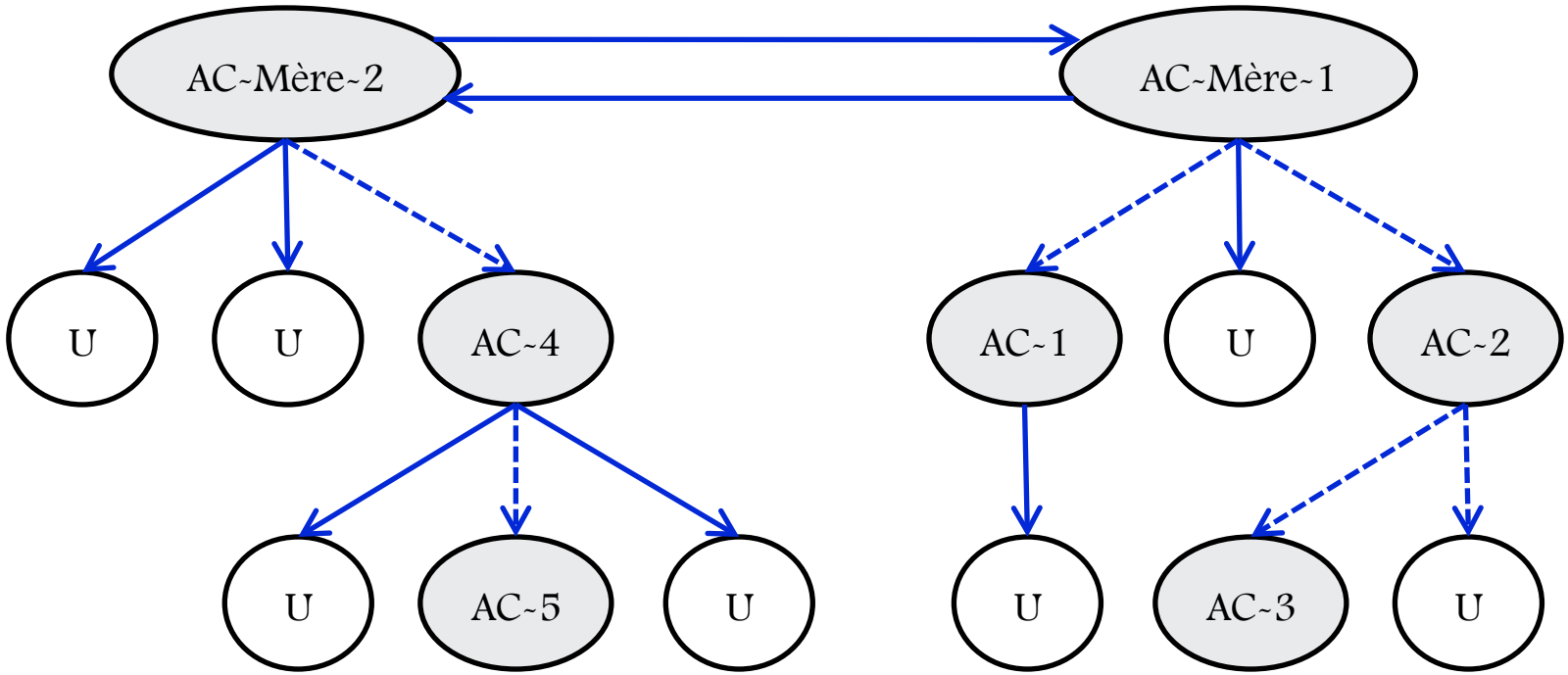
Modèles de certification

- PKI : *Public Key Infrastructure*
- Autorité de certification
- Délégation du pouvoir de certification ⇒ Certificat d'attribut
- Modèle de certification hiérarchique
- Modèle de certification croisé
- Modèle de certification en graphe
- Modèle de certification complètement distribué

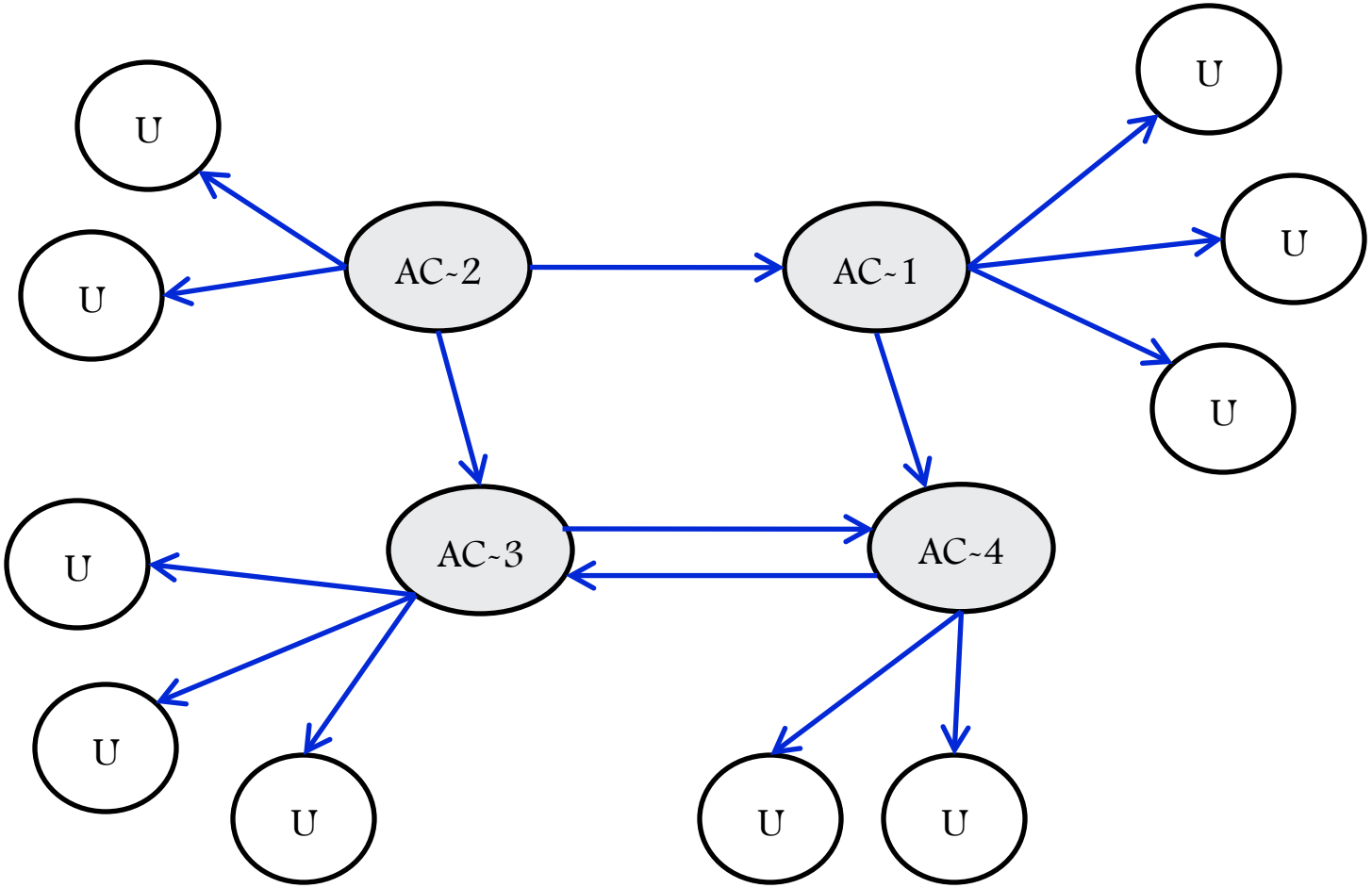
Modèle de certification hiérarchique



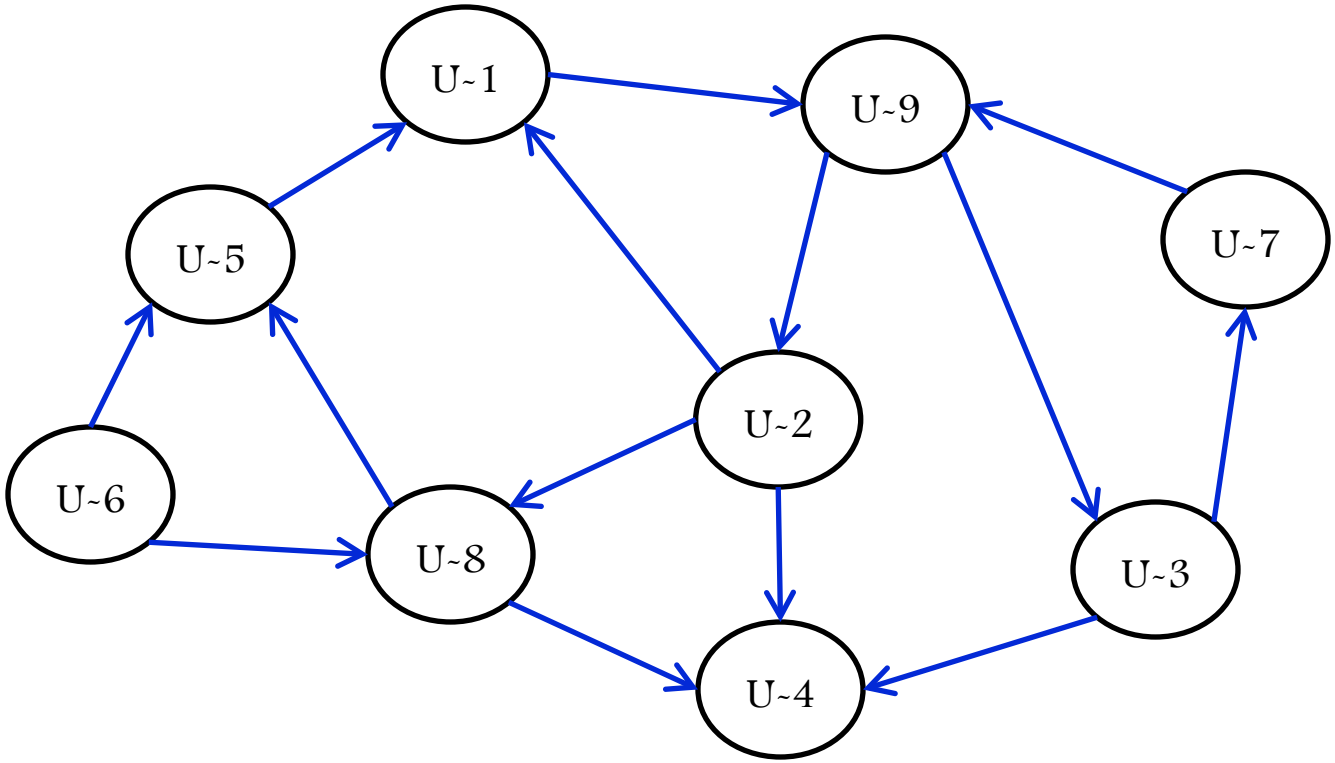
Modèle de certification croisé



Modèle de certification en graphe

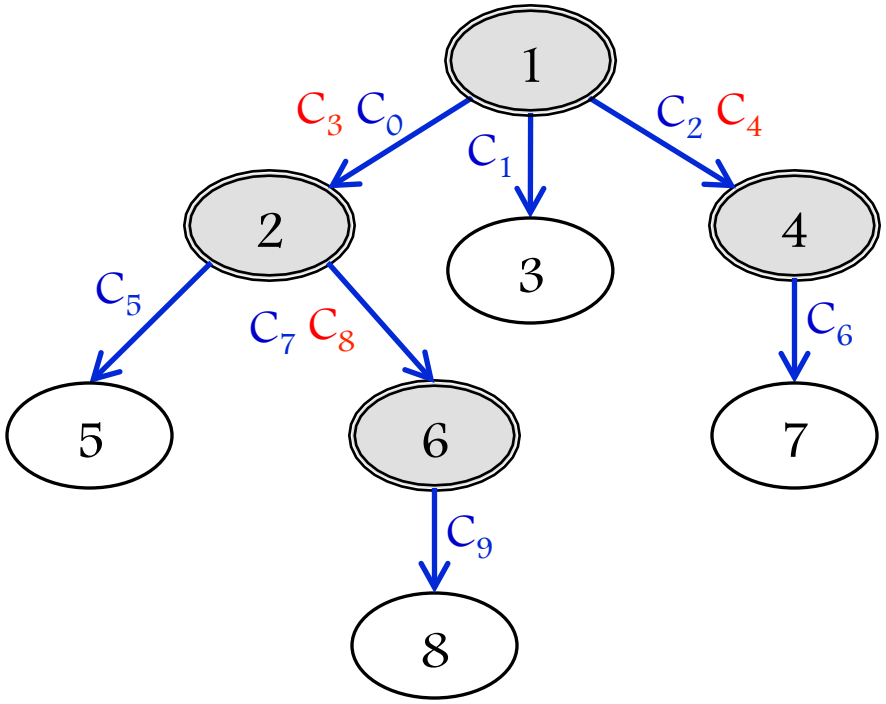


Modèle complètement distribué



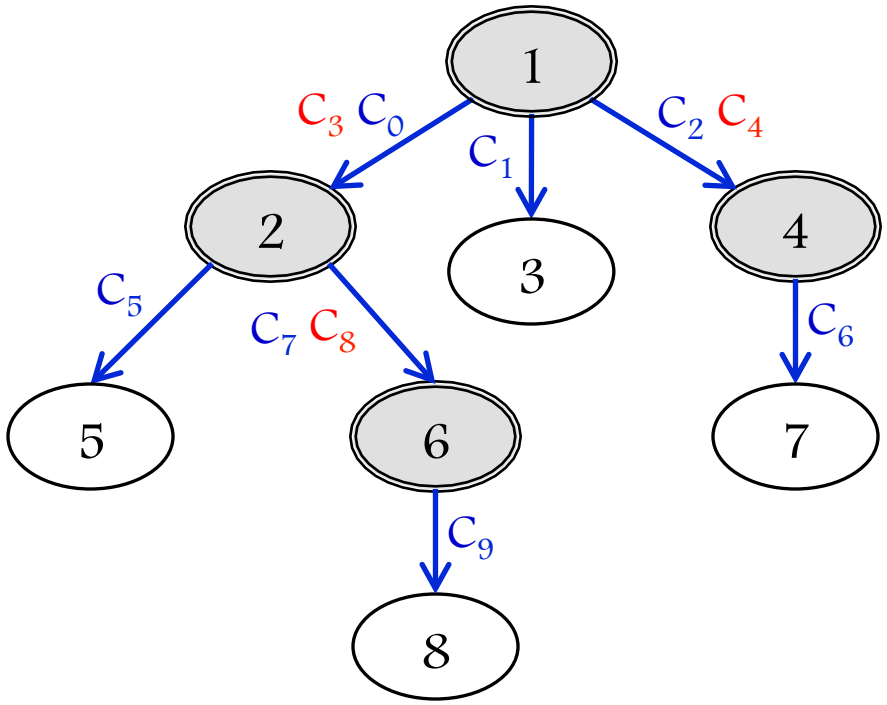
EXEMPLE 1 (MODÈLE HIÉRARCHIQUE)

- Format du certificat ⇒ [ID_{AC}, ID_U, CLE_U, Signature]
- L'autorité de certification mère porte l'identité « 1 »
- Les certificats de délégation sont définis avec $CLE_U = -1$
- L'annuaire du système de certification :
  - C_0=[1, 2, 13, 217]
  - C_1=[1, 3, 51, 171]
  - C_2=[1, 4, 17, 107]
  - C_3=[1, 2, –1, 553]
  - C_4=[1, 4, –1, 881]
  - C_5=[2, 5, 18, 409]
  - C_6=[4, 7, 41, 167]
  - C_7=[2, 6, 19, 284]
  - C_8=[2, 6, –1, 335]
  - C_9=[6, 8, 47, 591]



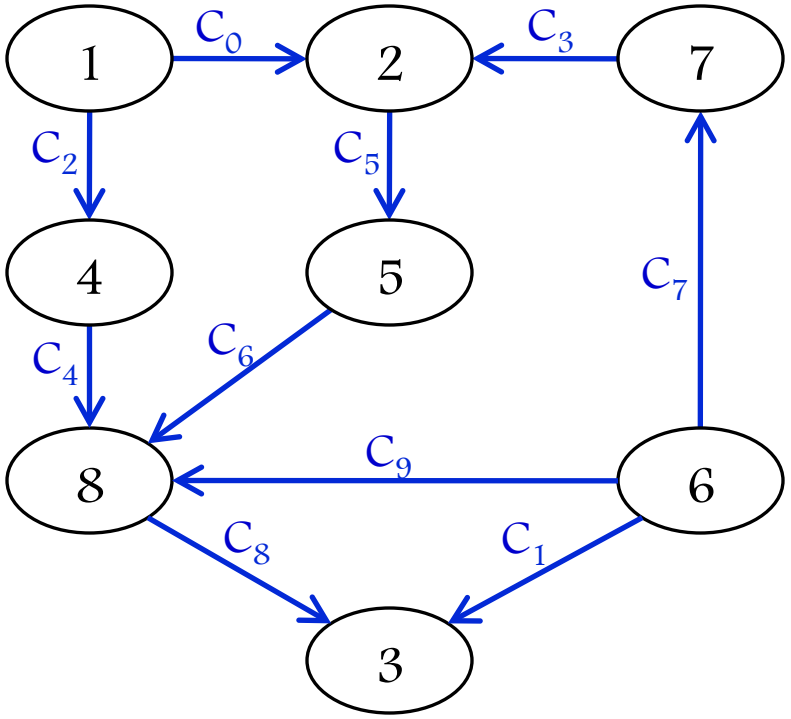
EXEMPLE 1 (MODÈLE HIÉRARCHIQUE)

- Quels sont les certificats nécessaires à vérifier pour que l'utilisateur X puisse vérifier la clé publique de Y ?
  - X=4 & Y=3
  - { C_1}
  - X=3 & Y=5
  - {C_0, C_3, C_5}
  - X=5 & Y=3
  - {C_1}
  - X=7 & Y=8
  - {C_0, C_3, C_7, C_8, C_9}
  - X=8 & Y=4
  - {C_2}



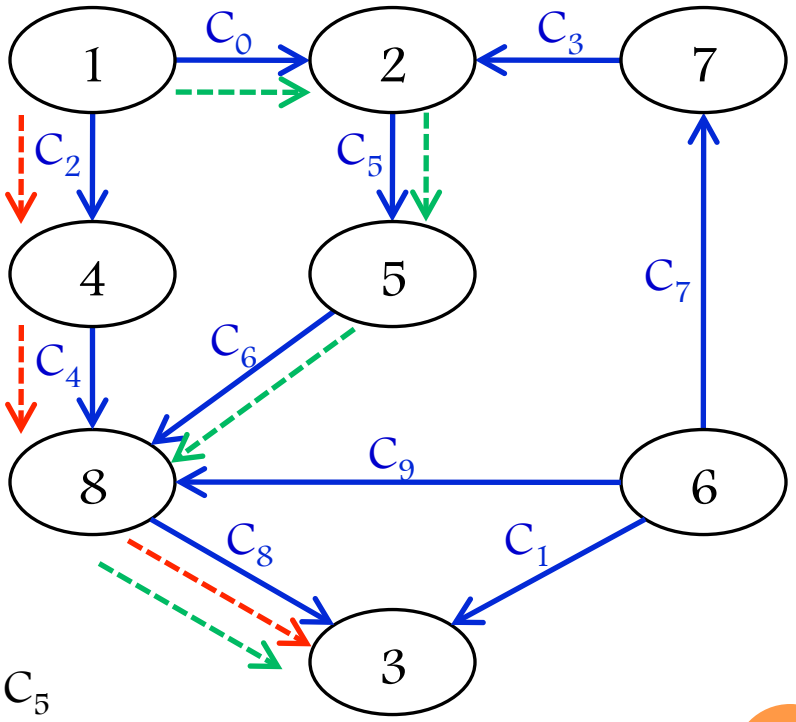
EXEMPLE 2 (MODÈLE COMPLÈTEMENT DISTRIBUÉS)

- Format du certificat ⇒ [ID_{U1}, ID_{U2}, CLE_{U2}, Signature]
- L'annuaire du système de certification :
  - C_0=[1, 2, 13, 217]
  - C_1=[6, 3, 51, 171]
  - C_2=[1, 4, 17, 107]
  - C_3=[7, 2, 13, 553]
  - C_4=[4, 8, 47, 881]
  - C_5=[2, 5, 18, 409]
  - C_6=[5, 8, 47, 167]
  - C_7=[6, 7, 19, 284]
  - C_8=[8, 3, 51, 335]
  - C_9=[6, 8, 47, 591]

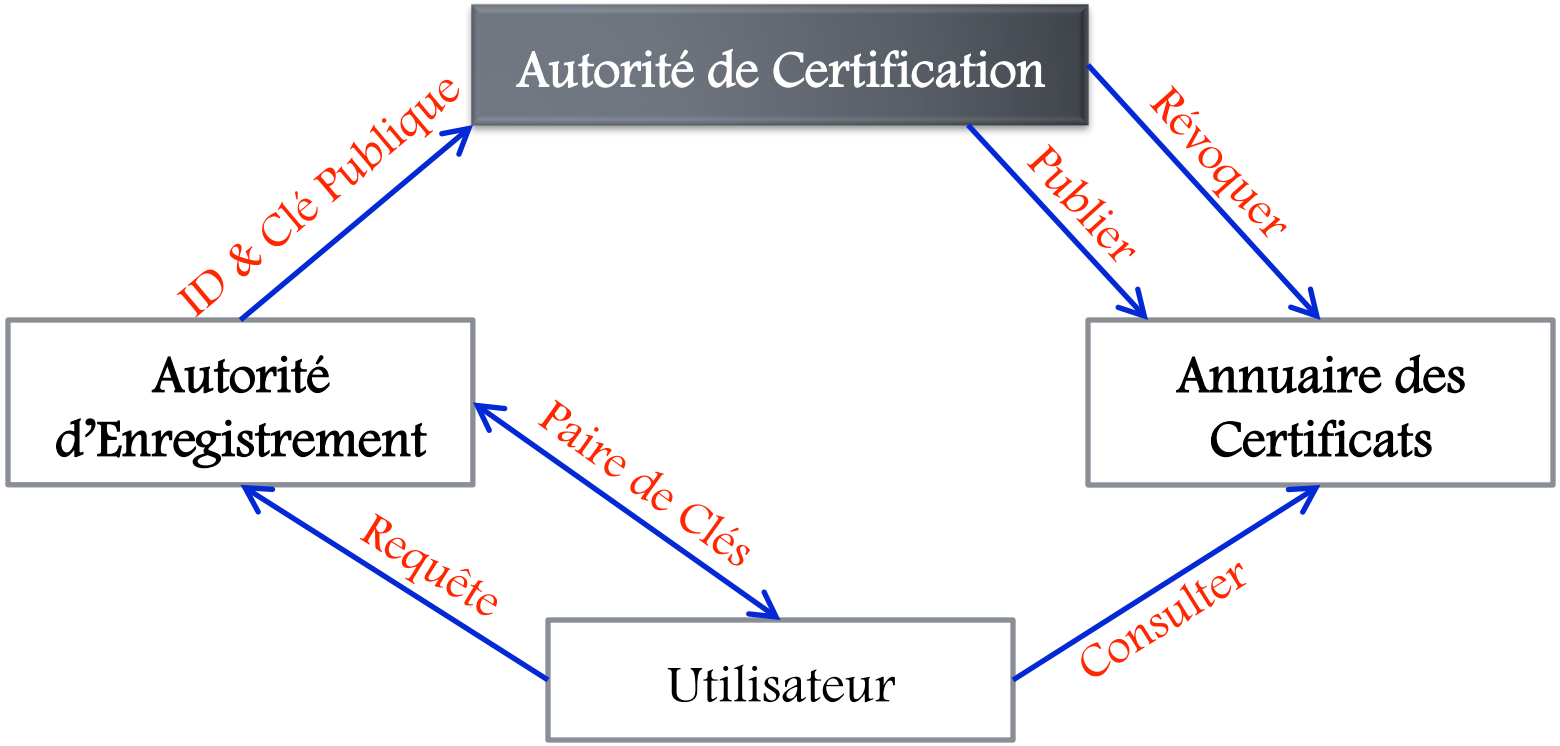


EXEMPLE 2 (MODÈLE COMPLÈTEMENT DISTRIBUÉS)

- Quels sont les certificats nécessaires à vérifier pour que l'utilisateur 1 puisse vérifier la clé publique de 3 ?
  - Chaine 1 ⇒ $\{C_2, C_4, C_8\}$
  - Chaine 2 ⇒ $\{C_0, C_5, C_6, C_8\}$
- Vérification de « Chaine 2 »
  - C_8 contient la clé publique de 3
  - Vérifier C_8 ⇒ Clé publique de 8 ?!
  - C_6 contient la clé publique de 8
  - Vérifier C_6 ⇒ Clé publique de 5 ?!
  - C_5 contient la clé publique de 5
  - Vérifier C_5 ⇒ Clé publique de 2 ?!
  - C_0 contient la clé publique de 2
  - Vérifier C_0 ⇒ Clé publique de 1
  - Avec sa clé publique ⇒ 1 vérifie C_0
  - Avec la clé publique de 2 ⇒ 1 vérifie C_5
  - Avec la clé publique de 5 ⇒ 1 vérifie C_6
  - Avec la clé publique de 8 ⇒ 1 vérifie C_8



La certification dans une PKI



Les annuaires de certificats

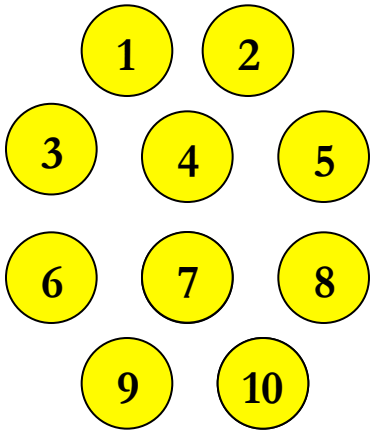
- Les certificats émis par les autorités de certification doivent être rendus accessibles
- Les certificats sont publiés sur un annuaire à accès libre
  - Mode de lecture
  - Mode d'ajout
  - Mode de suppression ⇒ révocation des certificats
- Il contient aussi une liste de révocation ⇒ datés et signés par les autorités de certification

Révocation des certificats

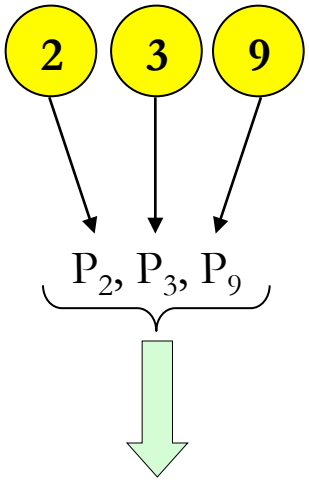
- L'expiration de la période de validité
  - Révocation automatique
- La divulgation de la clé privée de l'utilisateur
  - Sur demande
  - Mise à jour de la paire de clés
- L'utilisateur n'est plus considéré digne de confiance
  - Par rapport à son comportement

La cryptographie à seuil

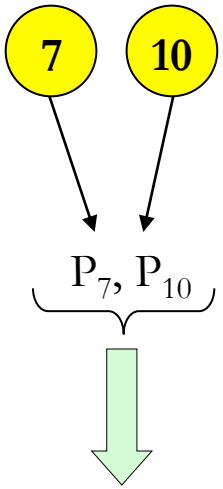
- Adi Shamir en 1979
- Un schéma de (k, n) permet à n entités de partager un secret S pour avoir l'habilité d'effectuer une opération cryptographique
- Au moins k entités peuvent coopérer



k = 3

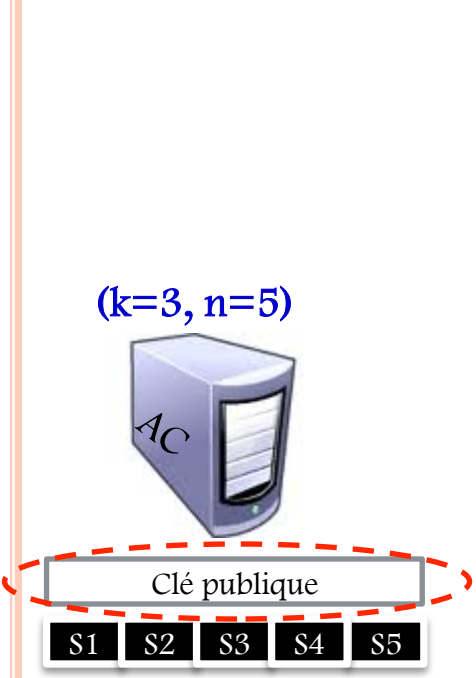


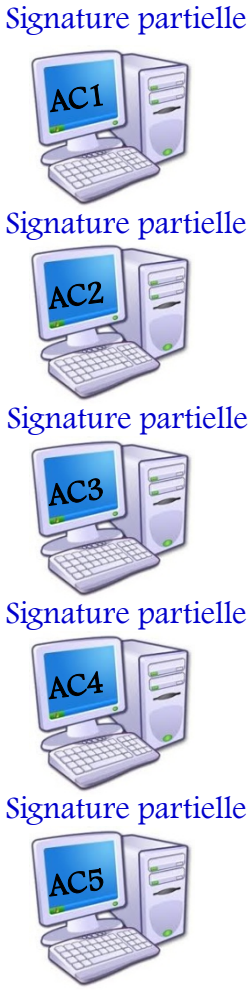
S



?

PARTAGE DE POUVOIR DE CERTIFICATION





IMPLÉMENTATION AVEC RSA

- Générer les paramètres de RSA : (n, φ(n), e, d)
  - La clé publique (e, n) ⇒ à envoyer aux utilisateurs
  - La clé privée (d, n) ⇒ à partager entre les serveurs
- Créer un polynôme $F(x) = d + a_1x^1 + \ldots + a_{k-1}x^{k-1}$
- Calculer pour chaque serveur s_i sa part privée :
  - $S_i = F(i) \bmod \varphi(n)$
- Chaque serveur s_i génère une signature partielle :
  - $SP_i = C^{Si} \bmod n$
- Calculer L_i : $\mathcal{L}_i = \prod_{j=1, j\neq i}^{j=k} \frac{j}{j-i} \bmod \phi(n)$
- Calculer la signature complète : $\mathcal{SC} = \prod_{i=1}^{i=k} \mathcal{SP}_i^{\mathcal{L}_i} \bmod n$
- $C = SC^e \bmod n$?

EXEMPLE

- $n=527, e=11, d=131, \varphi(n)=480, C=6, F(x)=131+x+x^2$

- $S_1=F(1) \bmod 480=133$
- $S_2=F(2) \bmod 480=137$
- $S_3=F(3) \bmod 480=143$
- $SP_1=6^{133} \bmod 527=347$
- $SP_2=6^{137} \bmod 527=181$
- $SP_3=6^{143} \bmod 527=88$
- $L_1=3, L_2=477, L_3=1$
- $SC=347^3 \times 181^{477} \times 88^1 \bmod 527=522$
- $522^{11} \bmod 527=6$