La gestion des clés

La gestion des clés

La gestion des clés est constituée de quatre domaines :

- La génération des clés : il faut prendre garde aux caractères choisis, aux clés faibles, ... et veiller à utiliser des générateurs fiables.
- Le transfert de la clé : l'idéal est de se rencontrer, ou d'utiliser un canal de transmission protégé (cela est souvent impossible). Aussi, si A et B ont des communications sûres avec un tiers C (intermédiaire de confiance), ce dernier peut relayer la clé entre A et B.
- La vérification des clés : par hachage, ou utilisation de certificats.
- Le stockage des clés : que ce soit dans des fichiers, sur supports extérieurs, …

Cas 1: Distribution des Clés symétriques.

Dans le cas de chiffrement symétrique, il est nécessaire pour les deux usagers de partager une clé secrète commune

Comment distribuer sûrement cette clé ?

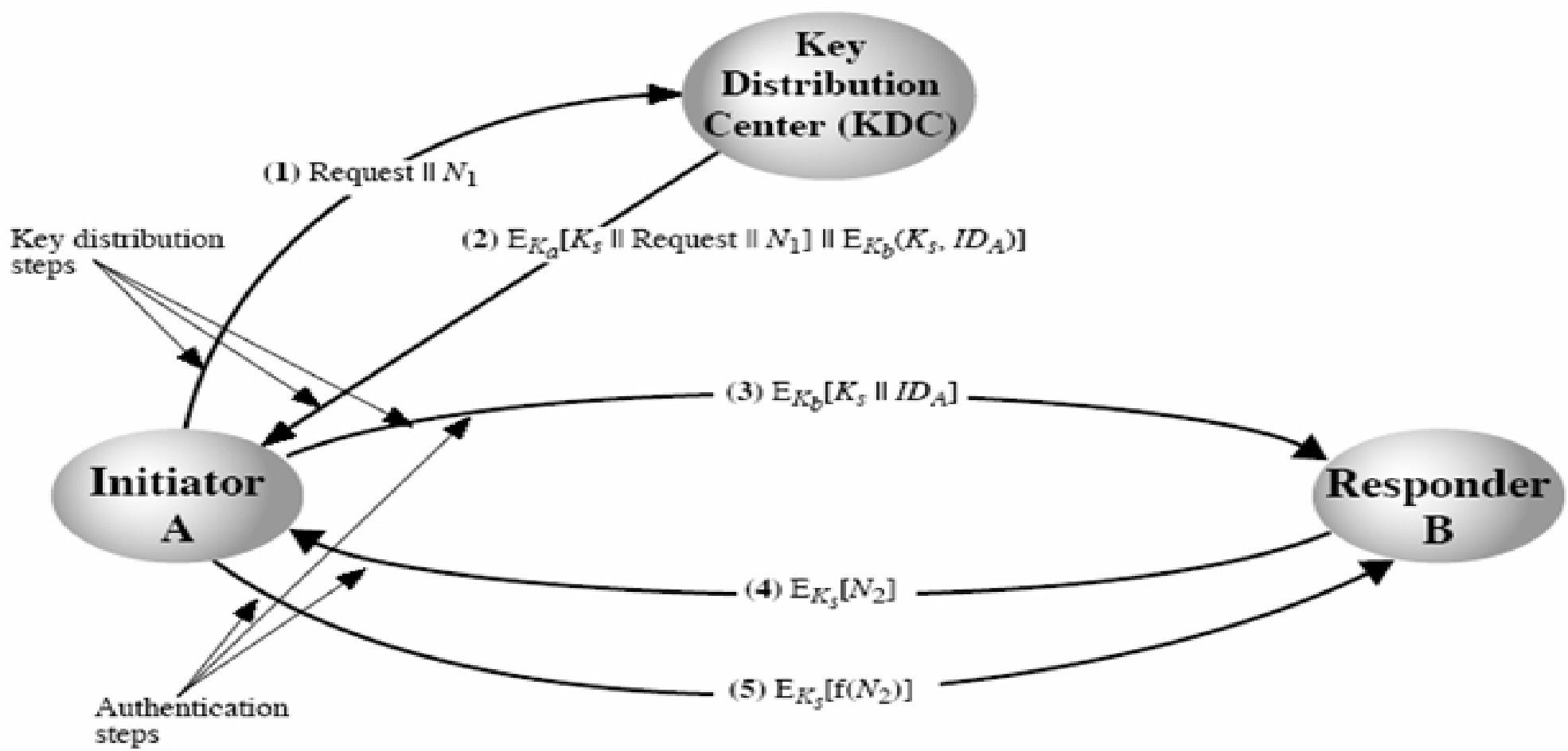
– Physiquement : par une rencontre, un canal de transmission protégé, ...

– Utiliser un tiers de confiance: Celui-ci choisit et fournit la clé.

– Utiliser une ancienne clé pour chiffrer une nouvelle clé (ce qui suppose cependant un échange préalable de cette ancienne clé).

– Distribution automatique de clés à la demande des utilisateurs: Cette solution nécessite une totale confiance au système de chiffrement utilisé.

Cas 1: Distribution des Clés symétriques.



Cas 2: Distribution des Clés Asymétriques.

Le chiffrement par clé publique permet de résoudre les problèmes de distribution de clés secrètes.

Il existe quatre solutions permettant un transfert des clés dans le cas asymétrique :

a – Annonce publique

b – Répertoire publiquement disponible

c – Autorité de clés publique

d – Certificats de clé publique

Cas 2: Distribution des Clés Asymétriques.

A- Annonce Publique

La distribution des clés publiques se fait directement aux destinataires ou par broadcast à la communauté. Il est par exemple possible d'envoyer la clé publique par emails ou les poster dans des newsgroups ou mailing-lists.

Il s'agit d'une diffusion de la clé publique

Problème: Mais le risque majeur avec cette méthode est la contrefaçon : n'importe qui peut créer une clef en prétendant être quelqu'un d'autre et la publier (A se prend pour B).

Cas 2: Distribution des Clés Asymétriques.

b – Répertoire publiquement disponible (Solution pour a)

On enregistre ici des clés dans un répertoire public, ce qui implique de faire confiance à ce répertoire.

Ce dernier doit avoir plusieurs propriétés :

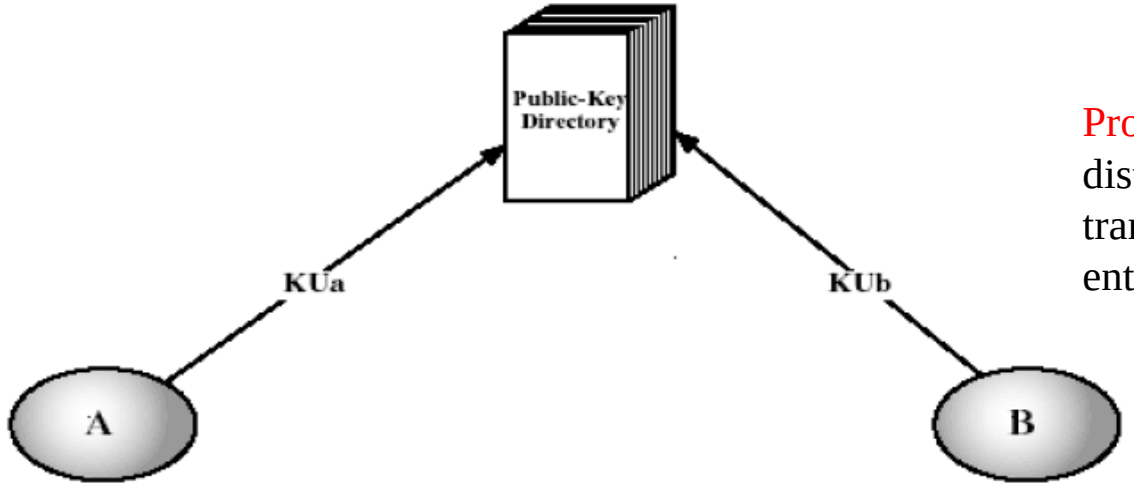
– Il doit contenir les entrées {nom, clef publique}.

– Il doit être possible de s'inscrire de manière sécurisée dans le répertoire.

– On doit pouvoir remplacer la clef à tout moment (tout participant peut remplacer sa clé publique).

– Le répertoire doit être publié périodiquement (la mise a jour).

– Il devrait également permettre la consultation électronique.



Problème: un individu pourrait détourner le répertoire et distribué des clefs publiques contrefaites, c.-à-d. ne pas transmettre les clés correspondant aux demandes des entités communicantes.

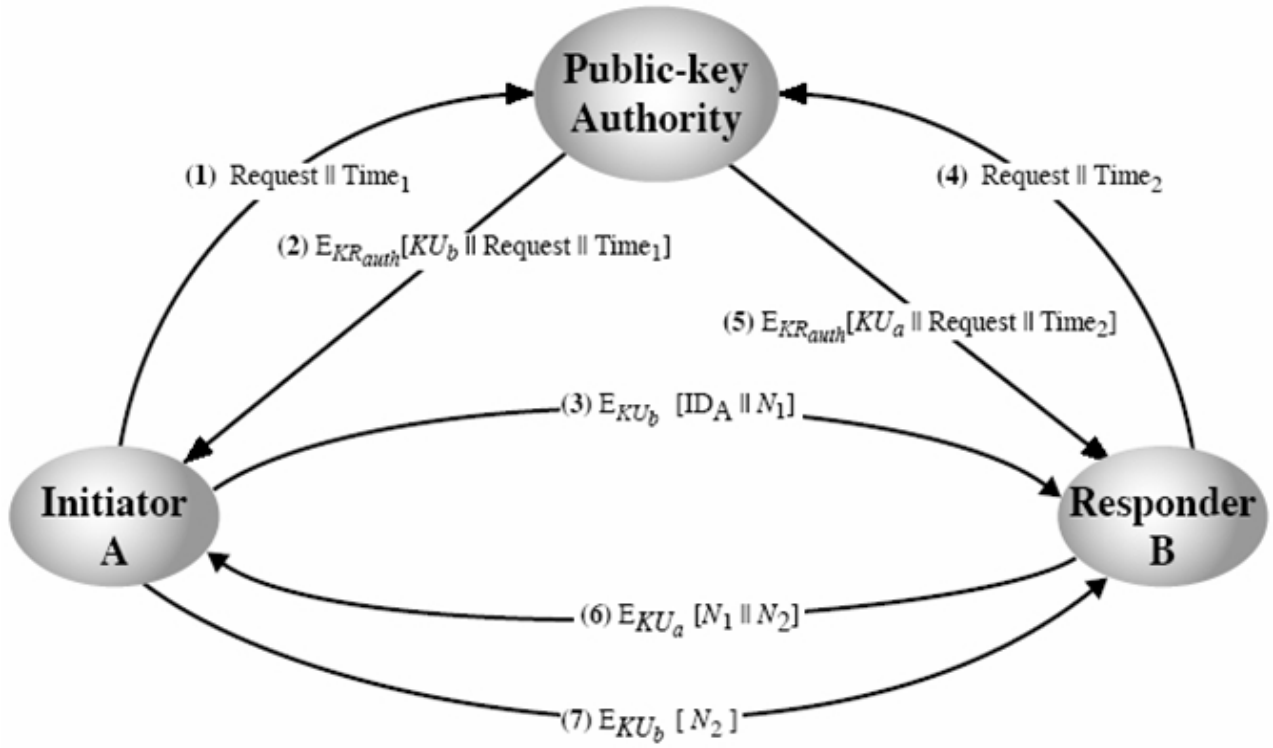
Cas 2: Distribution des Clés Asymétriques.

c- Autorité de clés publique

- Il s'agit de renforcer la sécurité de la distribution des clefs à partir d'un répertoire (solution pour b).
- Chaque participant dispose de la clé publique de l'autorité (KU auth). Ainsi, lorsqu'un participant désirera obtenir la clé publique d'un correspondant, il enverra une requête daté à l'autorité par l'utilisation d'un marqueur temporel (timestamp).
- En retour, l'autorité renverra la clé demandée, le timestamp pour prouver le non-rejeu d'un ancien message, le tout chiffré avec sa clé privée (KR auth).
- De cette manière, l'entité A, possédant la clé publique de l'autorité, pourra vérifier la bonne provenance de la clé publique de B.
- L'entité B pourra pratiquer de la même manière.

Cas 2: Distribution des Clés Asymétriques.

c- Autorité de clés publique

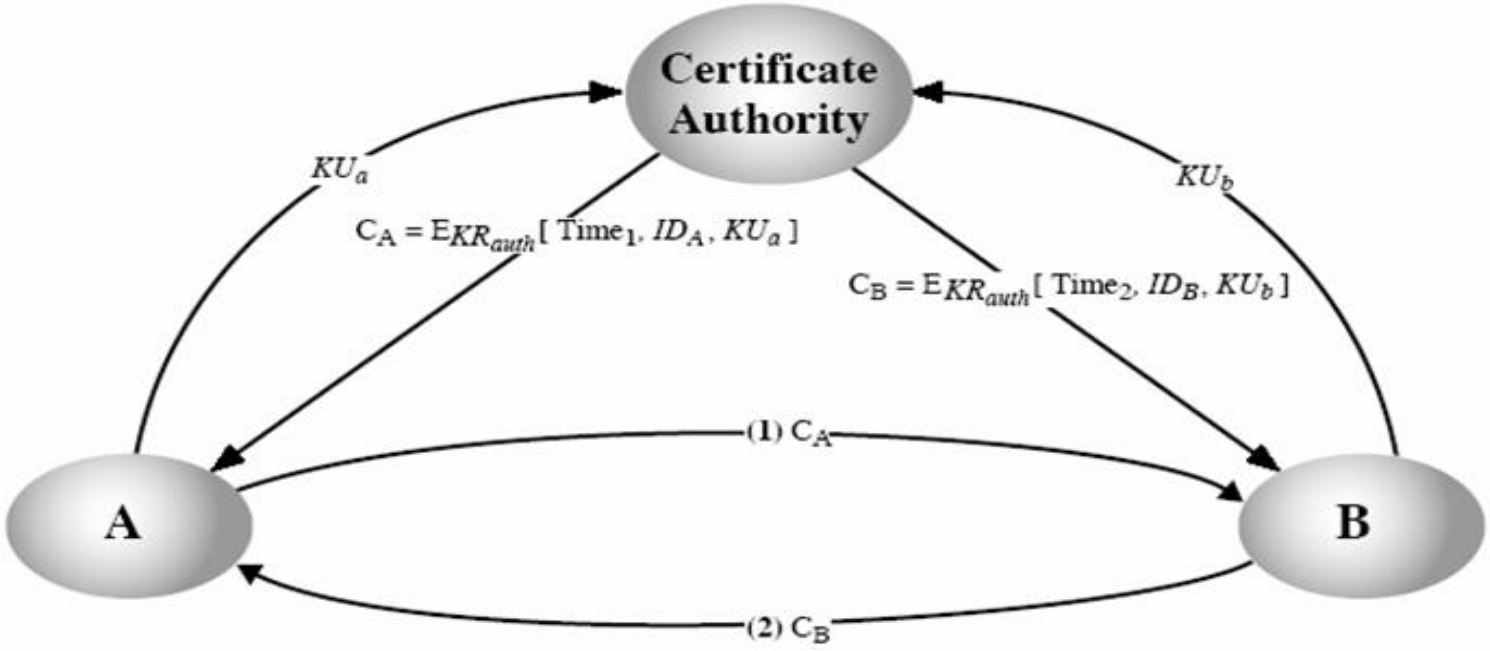


Problème: centralisation + 7 messages

Cas 2: Distribution des Clés Asymétriques.

d- Certificats de clés publiques

- Échange de clés sans passé par l'autorité de clé publique.
- Un certificat de clé publique = clé publique certifiée par personne de confiance.
- C'est une façon de contrecarrer le remplacemen de clé par un autre usager.
- Certificat = clé publique + informations {nom, adresse, ...} signé par qlq'un de confiance → autorité de certification:
  1- Chaque participant peut lire le certificat (nom et clé publique)
  2- Chaque participant peut vérifier la provenance
  3- Seule l'autorité de ceritification peut créer et mettre à jour les certificats



Cas 3: Distribution des Clés Asymétriques pour l'échange d'une clé de session.

L'objectif de la cryptographie est de protéger le contenu d'un message, soit par l'utilisation des clés symétrique ou des clés asymétrique.

La distribution de clés publiques (Asymétrique) est simple et permettant la confidentialité et l'authentification, mais elle est lente.

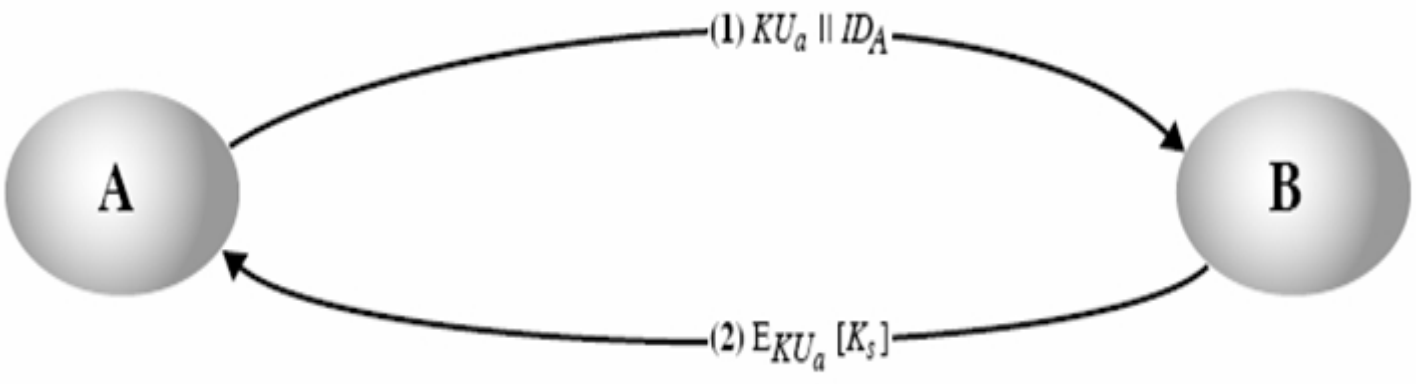
→ Une solution plus rapide est d'utiliser un système hybride permettant l'échange final d'une clé de session.

- Distribution simple de clé secrète.
- Distribution d'une clé secrète avec confidentialité et authentification

Cas 3: Distribution des Clés Asymétriques pour l'échange d'une clé de session.

Distribution simple de clé secrète.

1. A produit une nouvelle paire de clés publique/privée
2. A envoie à B sa clé publique et son identité
3. B produit une clé Ks de session et l'envoie à A (Ks est chiffrée par clé publique fournie par A)
4. A déchiffre la clé de session (Ks) et tous les deux l'emploient



Cas 3: Distribution des Clés Asymétriques pour l'échange d'une clé de session.

- Distribution d'une clé secrète avec confidentialité et authentification

1. A utilise la clé publique de B pour chiffrer un message contenant l'identité de A (IDA) et un nonce (N1), qui est employé pour indiquer la fraicheur du message.

2. B envoie un message à A chiffré avec KUa contenant le nonce de A (N1) ainsi qu'un nouveau nonce produit par B (N2). Puisque seul B pourrait avoir déchiffré le message (1).

3. la présence de N1 dans le message (2) assure A que le correspondant est B, a ce moment A retourne N2, chiffrés en utilisant la clé publique de B.

4. A choisit une clé de session Ks secrète et envoie M = EKUb [EKRa [Ks]] à B. Le chiffrement de cette clé avec la clef privée de A assure que seul A peut l'avoir envoyée.

5. B calcule DKUa [DKRb [M]] pour récupérer la clef secrète.

Cas 3: Distribution des Clés Asymétriques pour l'échange d'une clé de session.

- Distribution d'une clé secrète avec confidentialité et authentification