§§ 5.3.1. Certificats.

Le pb avec l'attaque MIM est que les clefs publiques ne sont pas authentiques. En pratique la clé publique est de la forme

$$k_A = (k_{pubA}, ID_A).$$ où ID_A : mail, nom, ...

que l'Oscar transforme en :

$$k_A = (k_{pubO}, ID_A)$$

D'où le titre le principe :

> Même si les protocoles à clé publique ne demande pas un canal sécurisé, ils exigent un canal d'authentification pour la distribution de clé

D'où en utilisant une signature

$$Cert_A = \left[(k_{pubA}, ID_A), sig_{k_{pr}}(k_{pubA}, ID_A)\right].$$

et le destinataire a un algorithme de vérification de la signature, qui est publique. La signature est faite par une 3ème partie appelé CA (Certification Authority).
CA génère et distribue des certificats à tous les utilisateurs du système, par deux façons :