

Ajout aux diapos du cours DRT-3808 (cryptographie)

**CERTIFICAT
(SUPPLÉMENT)**

Préparation d'un certificat – 1

- Celui qui cherche une certification fournit les informations requises par le prestataire de certificats (art. 48) et notamment, dans le cas d'un certificat préparé avec les techniques de la cryptographie asymétrique, sa clé publique
- Le prestataire prépare un résumé au moyen d'une fonction de hachage des informations à certifier et de la clé publique fourni par l'individu cherchant une certification

Preparation d'un certificat – 2

- Le prestataire signe le résumé de hachage obtenu et prépare le certificat qui sera formé notamment
 - Du nom (ou de l'identifiant de la ressource)
 - De sa clé publique (en clair)
 - De l'identité du prestataire de certificat et de sa signature du certificat
- Le certificat sera généralement stocké dans un répertoire, là où il peut être consulté par des programmes informatiques

Vérification d'un certificat – 1

- Un programme trouve le certificat d'une personne (ou d'un site web) dans un répertoire
- Vérification
 - Il identifie le prestataire de certification qui a signé le certificat
 - Il accède à un répertoire où se trouve le certificat du prestataire de certificats, il prend la clé publique du prestataire
 - Avec la clé publique du prestataire, il déchiffre la signature du certificat à vérifier

Vérification d'un certificat – 2

- Vérification (suite)
 - Il compare le résumé de hachage trouvé suite au déchiffrement de la signature avec le résumé de hachage qu'il produit à partir des informations du certificat et de la clé publique
 - Si les résumés de hachage sont identiques, c'est que le certificat qu'il a vérifié a été signé tel quel par le prestataire du service de certification
