Les Certificats électroniques

Les Certificats électroniques

TETE K.Senam:
Ingénieur en système et objets connectés

Certificat électronique

- C'est un document électronique qui fait correspondre une clé avec une entité (personne, entreprise, ordinateur…). Cette correspondance est validée par une autorité de certification (Certificate Authority : CA).
- Ces certificats sont utilisés pour identifier une entité et sont normalisés (norme X.509v3).

Certificat électronique

- Concrètement, les données utilisateur (identité du propriétaire de la clé, la clé publique et l'usage de la clé) sont elles-mêmes signées par l'autorité de certification, en y incluant certaines données propres (période de validité du certificat, l'algorithme de cryptage utilisé, numéro de série, etc...).

Certificat électronique

- Un certificat électronique, c'est donc une assurance de sécurité sur l'identité électronique d'un individu ou d'un système.

- Les infrastructures de Gestion de Clés (IGC), en anglais PKI (Public Key Infrastructure) sont conçues pour mettre en œuvre l'architecture correspondante.

Infrastructures de Gestion de Clés

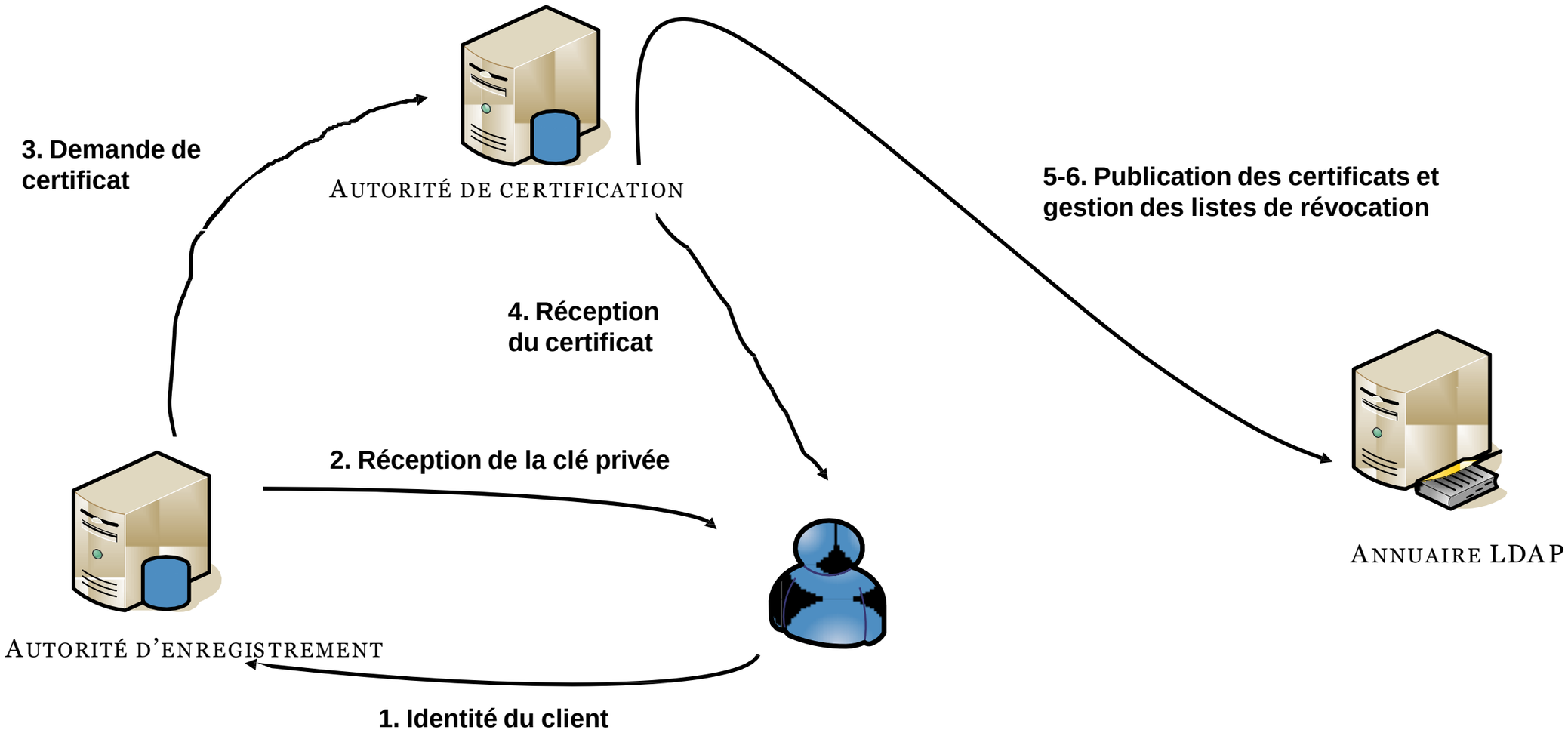
- Une IGC est une infrastructure composée d'un ensemble de systèmes, de procédures et de politiques, dont les fonctions sont les suivantes:
  - Enregistrer les entités désirant obtenir des certificats électroniques;
  - Fabriquer des biclés, c'est-à-dire des paires de clés privée et publique;

Infrastructures de Gestion de Clés

- Certifier des clés publiques afin de créer des certificats et de publier ces dernierssur des annuaires publics, généralement des serveurs LDAP;
- Révocation de certificats et gestion de listes de révocation.

Procédures d'obtention d'un certificat

L'obtention d'un certificat numérique doit suivre des procédures et politiques très strictes:



Un certificat électronique

- Un certificat électronique, ou passeport électronique, contient toutes les informations relatives à l'identité d'une personne, ainsi que d'autres champs non détaillés ci-dessous:
  - Numéro de version associé au certificat, par exemple X.509 v3;
  - Numéro de série fourni par l'autorité de certification ayant délivré le certificat;

Un certificat électronique

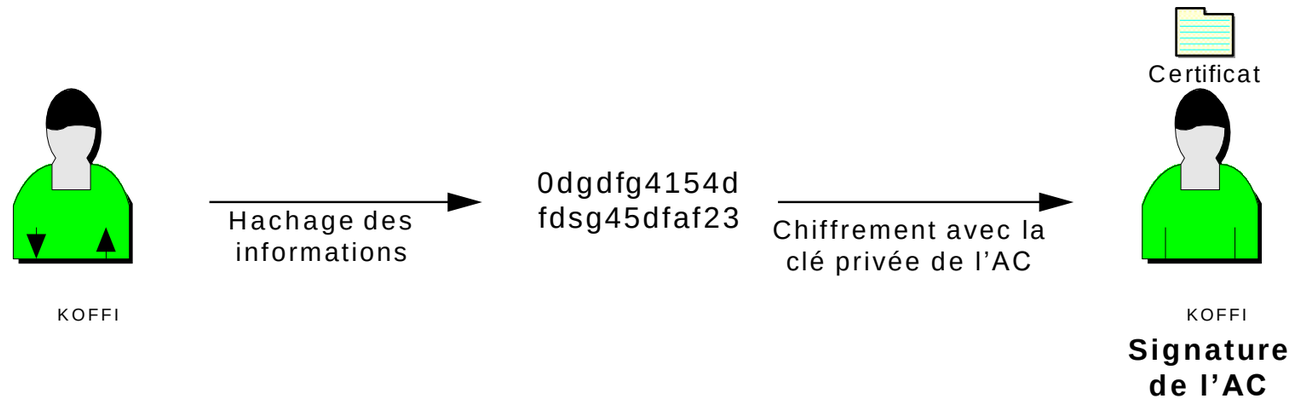
- Algorithme utilisé pour la signature du certificat;
- Nom de l'autorité ayant délivré le certificat;
- Date de validité du certificat (dates de création et d'expiration);
- Nom de la personne de destination du certificat;
- Clé publique de la personne certifiée, etc.

Un certificat électronique

- D'autres informations concernant des attributs spécifiques associés au certificat dépendent de la version du certificat, etc.
- A partir de ces informations, dont l'autorité de certification vérifie préalablement la validité, cette même AC génère une signature de certification en créant dans un premier temps une empreinte de ces informations grâce à un algorithme de hachage et en chiffrant cette empreinte par un algorithme de chiffrement asymétrique grâce à la clé privée de l'AC.

Un certificat électronique

Le processus de création d'un certificat électronique par le hachage des informations concernant Koffi puis par la création de la signature en chiffrant avec la clé privée de l'AC le résultat de la fonction de hachage est illustré a la figure suivante:

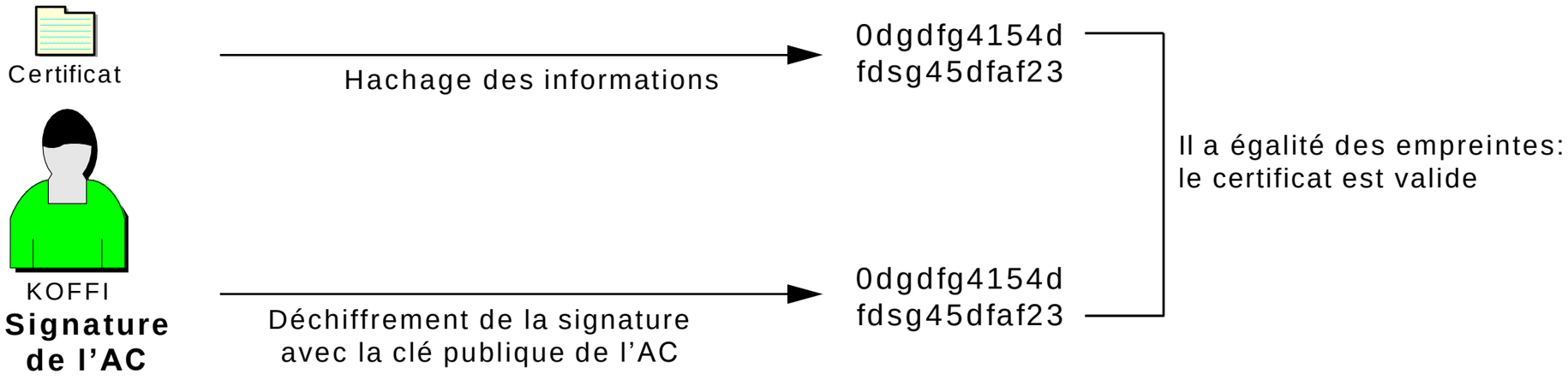


Un certificat électronique

- Pour vérifier une signature d'une AC, il suffit de prendre l'ensemble des informations du certificat, excepté la signature, afin de créer une empreinte puis de déchiffrer la signature de l'AC grâce à la clé publique de cette même autorité afin de retrouver l'empreinte initiale certifiée. La dernière étape consiste à comparer les deux empreintes. Si elles correspondent, le certificat est valide, sinon il ne peut être considéré comme de confiance.

Un certificat électronique

Le processus de vérification de la validité d'un certificat électronique en comparant les empreintes du certificat à celle signée par l'AC est illustré à la figure suivante:



Un certificat électronique

- Un certificat est disponible dans le domaine publique. En revanche, la clé privée associée au certificat est précieusement protégée sur un support physique sécurisé, tel qu'une carte à puce.
- L'accès à la carte à puce est protégé par un code PIN afin d'assurer une authentification forte de l'individu.

Un certificat électronique

- La publication des certificats des clés publiques utilise les structures d'annuaires de type LDAP (Lightweight Directory Access Protocol), définies dans la RFC 2251. les certificats révoqués sont regroupés dans des listes de révocation, ou CRL (Certificate Revocation List).

Un certificat électronique

- Les IGC offrent une assurance de sécurité pour un certificat électronique. Ce dernier peut être utilisé avec des applications telles que l'e-mail chiffré, le VPN fondé sur IPsec, le commerce électronique, etc.

?