Authenticité des certificats

Les autorités de certification signent les certificats émis. Cela permet de valider l'intégrité ainsi que l'authenticité des certificats utilisés.

Cette fonction est essentielle car elle vous permet, après vérification de la signature, de faire confiance.

1. Processus de signature d'un certificat

À l'installation d'une autorité de certification racine, l'autorité installée dispose d'un certificat autosigné. Ce certificat est associé à une paire de clés publique/privée.

L'autorité de certification utilise sa clé privée afin de signer le certificat délivré.

Une signature doit être unique. L'autorité utilise donc un élément qu'elle est la seule à détenir, sa clé privée, pour signer le certificat.

2. Processus de validation de la signature d'un certificat

Le client vérifie la signature du certificat en utilisant la clé publique de l'autorité de certification.

Les clés sont utilisées ici à l'inverse de leur utilisation lors d'un processus de chiffrement, la clé privée de l'autorité de certification est utilisée pour signer et la clé publique correspondante est utilisée pour vérifier la signature.

Si la signature peut être vérifiée, c'est qu'elle a bien été signée avec la clé privée correspondante, détenue uniquement par l'autorité de certification. Le certificat a donc bien été signé par l'autorité de certification, il est validé et peut être utilisé.

Si la signature ne peut pas être vérifiée, le certificat n'a pas été signé par l'autorité de certification. Il n'est pas digne de confiance et ne doit pas être utilisé.

3. Validation de l'intégrité d'un certificat

Vérifier la signature ne suffit pas. Un certificat signé par une autorité de certification peut être intercepté et modifié dans un but malveillant. La propriété **Nom du sujet** du certificat peut être par exemple modifiée afin d'usurper l'identité d'un autre utilisateur ou d'un autre ordinateur.

Afin d'empêcher toute modification d'un certificat, un processus de vérification de l'intégrité doit être appliqué.

a. Calcul de Hash

Certains algorithmes mathématiques, appliqués à un ensemble de données binaires (ici un certificat) permettent le calcul d'une valeur unique (de 128 ou 256 bits). Cette valeur est appelée valeur de Hash.

La particularité d'une valeur de Hash, par rapport, par exemple, au simple calcul d'une somme de contrôle, et qu'en cas de modification minime des données binaires, le nouveau calcul prendra une valeur totalement différente.

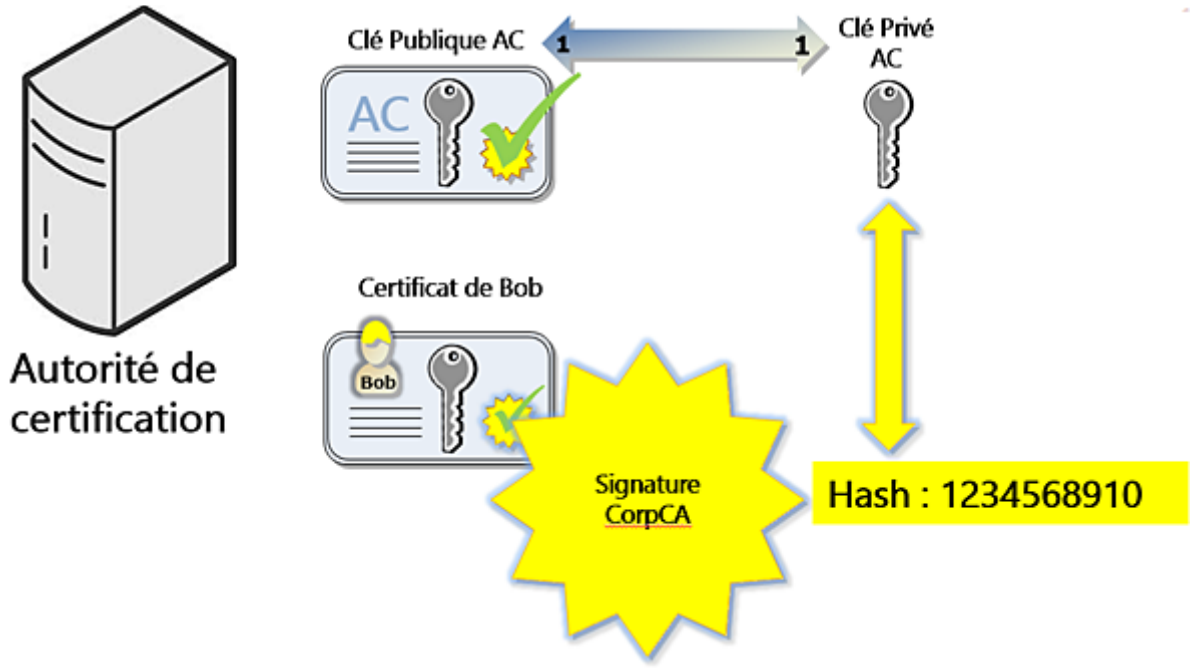
Si l'on calcule, par exemple, une valeur de Hash sur un fichier texte, que l'on modifie très légèrement le fichier texte (ajout ou suppression d'un seul caractère), que l'on recalcule la valeur de Hash, le résultat obtenu est totalement différent ! (voir l'atelier Algorithmes de hachage plus loin dans ce chapitre).

Les algorithmes mathématiques les plus connus et les plus utilisés pour ce type de calcul sont MD5 et SHA. MD5 est plus rapide mais donné comme moins fiable et inversement SHA est plus lent mais plus fiable.

b. Intégrité du certificat

Le processus de vérification de l'intégrité d'un certificat est le suivant :

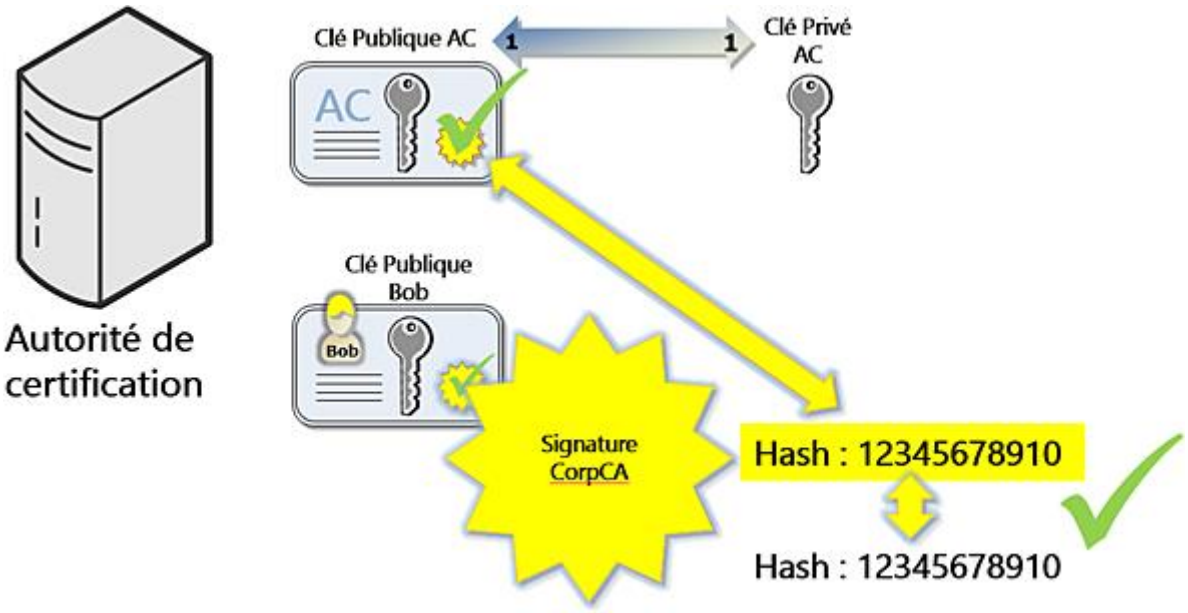
- L'autorité de certification calcule la valeur de Hash du certificat



Calcul et signature de la valeur du Hash initial du certificat et signature de cette valeur avec la clé privée de l'autorité de certification.

- Avant utilisation du certificat, la valeur de Hash du certificat est recalculée et comparée à la valeur initiale. Si les deux valeurs sont les mêmes, le certificat n'a pas été modifié, il est intègre et peut être utilisé. Si les deux valeurs sont différentes, le certificat a été modifié, il n'est pas intègre et ne peut être utilisé.

La valeur de Hash calculée par l'autorité de certification est également signée par elle-même afin d'empêcher toute modification de cette valeur de Hash initiale. Si un utilisateur mal intentionné modifie cette valeur de Hash, il ne pourra pas la signer avec la clé privée de l'autorité de certification.



Validation de la signature de la valeur du Hash, recalcul et comparaison avec la valeur du Hash initial avant utilisation du certificat.

Types d'autorités de certification

Deux types d'autorité peuvent être sélectionnés lors de la configuration de l'autorité de certification.

- Autorité de certification autonome

Ce type d'autorité de certification ne requiert pas une infrastructure Active Directory. Le serveur d'autorité de certification est en mode Groupe de travail (Workgroup).

Les demandes de certificats sont effectuées exclusivement par navigateur Internet. Les utilisateurs doivent fournir des informations d'identification précises (cartes d'identité, preuve d'appartenance à une entreprise…) et les demandes restent en attente jusqu'à l'approbation manuelle d'un administrateur de l'autorité (après vérification de l'identité du demandeur).

Les modèles de certificat délivrés ne sont pas personnalisables.

Ce type d'autorité n'est pas adapté à l'entreprise et n'est utilisé que dans des architectures sécurisées (voir chapitre Architectures PKI sécurisées).

- Autorité de certification d'entreprise

Ce type d'autorité de certification requiert une infrastructure Active Directory. Le serveur d'autorité de certification doit être membre du domaine ainsi que les utilisateurs et ordinateurs clients.

Les requêtes de certificats sont automatiquement approuvées sans que les utilisateurs aient à fournir des informations d'identifications.

> Les clients, utilisateurs et ordinateurs, étant membres du domaine, ont déjà été authentifiés lors de l'ouverture de session par le protocole Kerberos ! Le processus manuel d'authentification par validation des informations fournies par l'utilisateur (carte d'identité, attestations de son entreprise...) n'est plus nécessaire ici.

Les demandes de certificats peuvent s'effectuer par navigateur web mais également par les composants enfichables certificats utilisateur (certmgr.msc) ou ordinateur (certlm.msc).

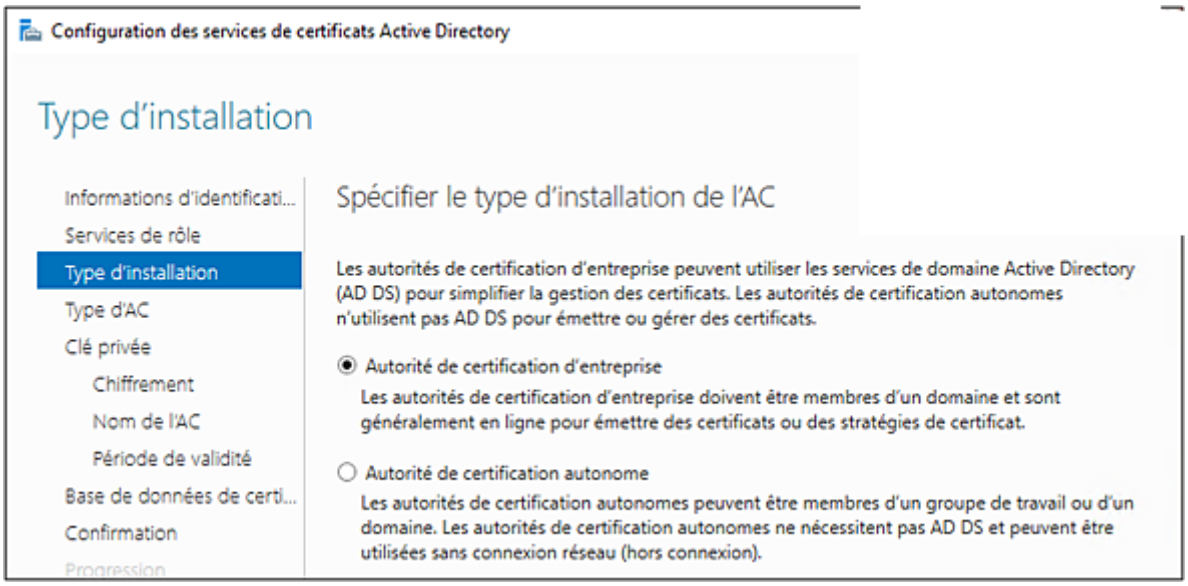
Les certificats pourront aussi être déployés automatiquement par stratégies de groupe (voir chapitre Gestion automatisée de certificats).

Un agent d'inscription peut être utilisé pour inscrire des certificats pour le compte d'un autre utilisateur ou d'un autre ordinateur (voir chapitre Utilisation de cartes à puce).

Les modèles de certificats sont personnalisables de façon à les adapter aux besoins de l'entreprise (modification de la durée de vie d'un certificat par exemple…).

Les certificats émis peuvent être automatiquement archivés si nécessaire.

Ce type d'autorité n'est totalement adapté à l'entreprise et à un usage interne automatisé et sécurisé.



Choix du type d'autorité lors de la configuration de l'autorité de certification.