ECOLE MAROCAINE DES SCIENCES DE L'INGENIEUR
Membre de HONORIS UNITED UNIVERSITIES

Classe : 5IIR

Sécurité des Systèmes d'Information

Abdellah OUAGUID - Maître de conférence et Chercheur
Laboratoire : Informatique Intelligence Artificielle et Cyber Sécurité (2IACS)

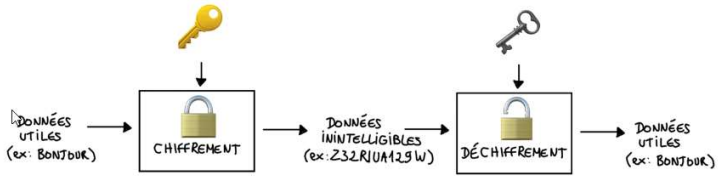
Sécurité des systèmes d'information

-3-
Mécanismes de sécurité (suite)

Rappel

CRYPTOGRAPHIE ASYMETRIQUE

- Le principe du chiffrement asymétrique repose sur **l'utilisation d'une paire de clés**, composée d'une **clé privée** et d'une **clé publique**.
- Lorsqu'un utilisateur **chiffre avec la clé publique**, il peut **déchiffrer** uniquement avec la clé privée correspondante
- **Inversement, dans le cadre d'une signature numérique**, un utilisateur **chiffre avec sa clé privée** et toute personne possédant la **clé publique** peut vérifier l'authenticité du message.
- Ces deux clés sont **mathématiquement liées**, généralement via des algorithmes comme **RSA, ECC** ou **ElGamal**.



À l'heure où les échanges se dématérialisent (contrats, factures, démarches administratives), la question de la **fiabilité** et de la **sécurité** des documents électroniques devient **essentielle**.

- Comment être certain qu'un document électronique **n'a pas été falsifié** et que le signataire est bien **celui qu'il prétend être** ?
- Comment être sûr qu'un document signé en ligne **n'a pas été modifié** et que le signataire est bien **authentique** ?
- Comment la **signature numérique** permet-elle d'assurer **l'authenticité**, **l'intégrité** et la **non-répudiation** des documents électroniques ?

Signature Numérique

Signature numérique : être sûr de l'expéditeur

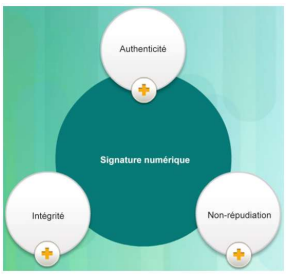
La signature numérique peut être utile pour **s'assurer** de l'**identité** de l'émetteur d'un contenu.

La signature numérique ou **signature électronique avancée** selon les termes de la législation européenne est une **technique mathématique** utilisée pour assurer **l'authenticité**, **l'intégrité** et la **non-répudiation** sous la forme de certificats numériques et de signature de code.

Signature numérique : être sûr de l'expéditeur

Les propriétés des signatures numériques :

- **Authenticité** : La signature n'est pas falsifiable et prouve que le signataire a signé le document (et personne d'autre).
- **Inaltérable** : Une fois signé, un document ne peut pas être modifié.
- **Non réutilisable** : La signature du document ne peut pas être transférée vers un autre document.
- **Non-répudiation** : Le document signé est considéré comme le même qu'un document physique. La signature est la preuve que le document a été signé par la personne réelle.



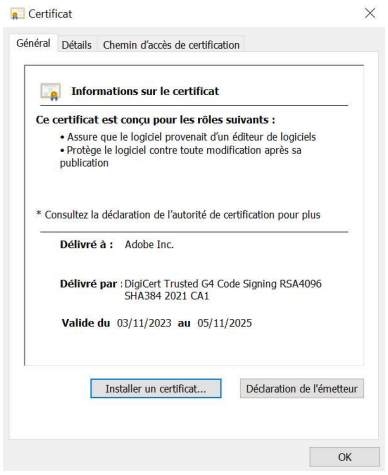
Signature numérique : être sûr de l'expéditeur

- Les signatures numériques sont couramment utilisées dans les deux situations suivantes :
  - **Signature de code** : permet de vérifier l'intégrité des fichiers exécutables téléchargés à partir du site web d'un fournisseur.
  - **Certificats numériques** : utilisés pour authentifier l'identité d'un système et échanger des informations confidentielles

- Trois algorithmes DSS (Digital Signature Standard) sont utilisés pour **générer et vérifier les signatures numériques** :
  - Algorithme DSA (Digital Signature Algorithm)
  - Algorithme RSA (Rivest-Shamir Adelman Algorithm)
  - Algorithme ECDSA (Elliptic Curve Digital Signature Algorithm)

Signatures numériques de signature de code

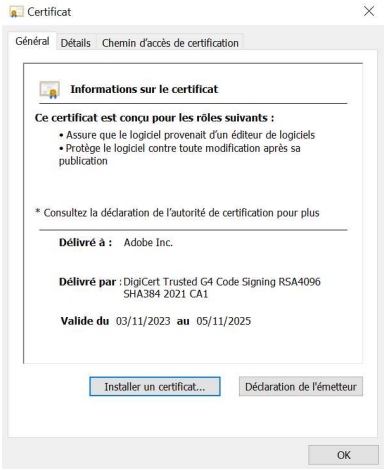
- Les signatures numériques sont couramment utilisées pour **garantir** **l'authenticité** et **l'intégrité** du code logiciel.
- Les fichiers exécutables sont encapsulés dans une enveloppe **signée** numériquement, ce qui permet à l'utilisateur final de **vérifier** la signature avant d'installer le logiciel.
- La signature numérique du code offre plusieurs garanties sur le code :
  - Le code est **authentique** et provient de l'éditeur.
  - Le code **n'a pas été modifié** depuis qu'il a quitté l'éditeur de logiciels.
  - C'est indéniablement l'éditeur qui a publié le code. Cela assure la **non-répudiation** de l'acte de publication.



Signatures numériques de signature de code

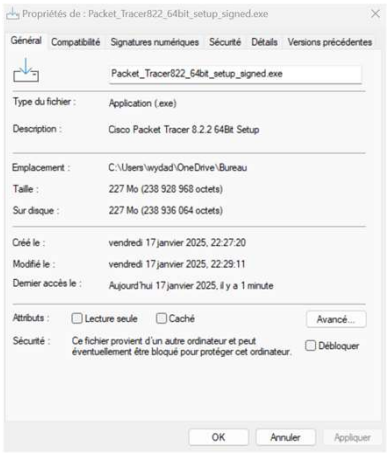
La publication FIPS (Federal Information Processing Standard) 140-3 du gouvernement des États-Unis précise que les logiciels disponibles pour téléchargement sur Internet **doivent être signés numériquement et vérifiés**.

- ➔ La signature numérique des logiciels vise à assurer que ceux-ci n'ont pas **été falsifiés** et qu'ils proviennent bien de la source de **confiance indiquée**.
- ➔ Les signatures numériques servent à vérifier que le code n'a pas été altéré par des acteurs de la menace et que le code malveillant n'a pas été inséré dans le fichier par un tiers.



Signatures numériques de signature de code

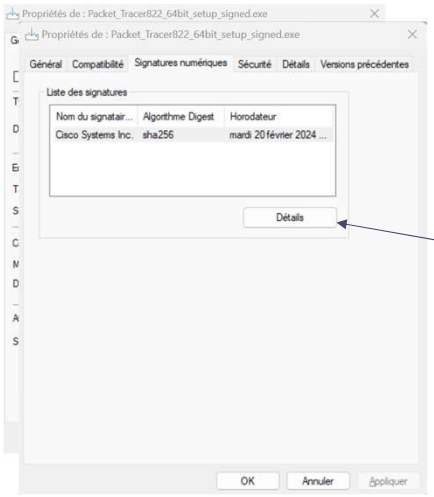
Exemple d'un fichier doté d'un certificat signé numériquement



Propriétés du fichier :
Ce fichier exécutable a été téléchargé sur Internet. Il s'agit de **Cisco Packet Tracer**, un outil innovant de simulation de configuration réseau.

Signatures numériques de signature de code

Exemple d'un fichier doté d'un certificat signé numériquement

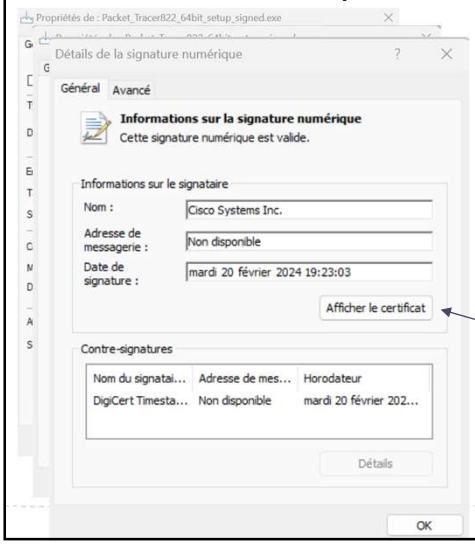


Signatures numériques :
En cliquant sur l'onglet ***Signatures numériques*** vous découvrez que le fichier provient d'une entreprise de confiance, **Cisco Systems Inc**. Le résumé du fichier a été créé avec l'algorithme sha256. La date à laquelle le dossier a été signé est également fournie.

- Cliquez sur **Détails** pour ouvrir la fenêtre « Détail de la signature numérique »

Signatures numériques de signature de code

Exemple d'un fichier doté d'un certificat signé numériquement

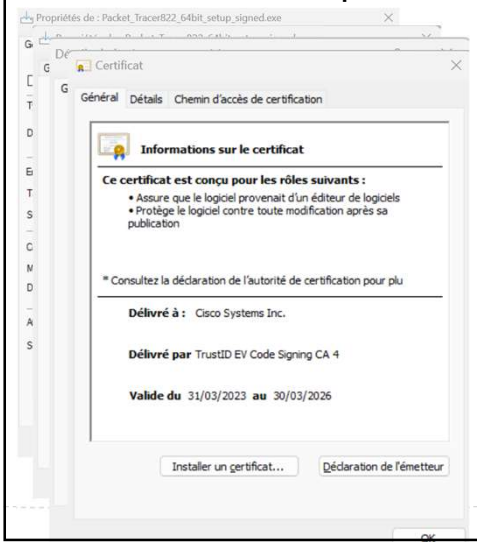


Détails de la signature numérique :
La fenêtre *Détails* de la signature numérique révèle que le fichier a été signé par **Cisco Systems, Inc** en Février 2024. Cette vérification a été faite par contresignature fournie par l'autorité **DigiCert TimeStamp 2023** le jour même où elle a été signée par Cisco.

- Cliquez sur *Afficher le certificat* pour afficher les détails du certificat lui-même.

Signatures numériques de signature de code

Exemple d'un fichier doté d'un certificat signé numériquement



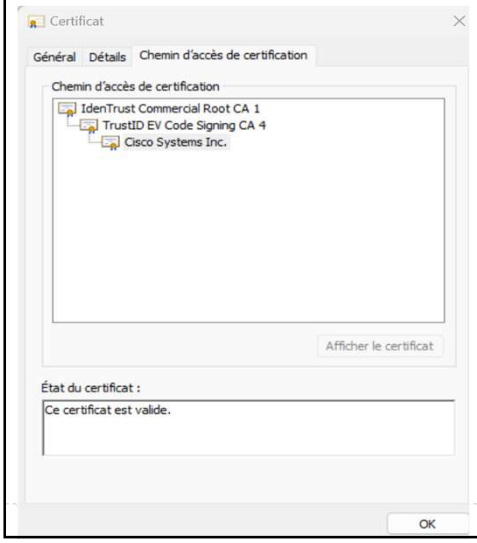
Informations sur le certificat :

L'onglet **Général** indique les objectifs du certificat, à qui le certificat a été délivré et par qui. Il affiche également la période pour laquelle le certificat est valide.
Des certificats non valides peuvent empêcher l'exécution du fichier.

15

Signatures numériques de signature de code

Exemple d'un fichier doté d'un certificat signé numériquement

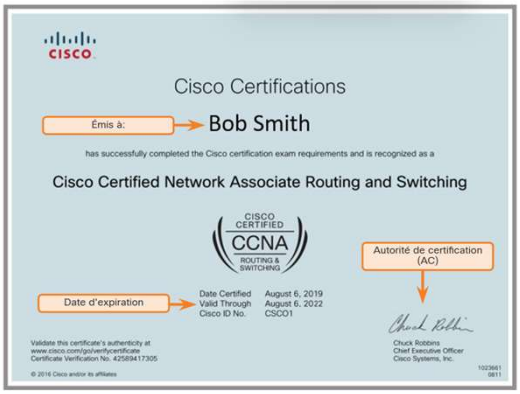


Parcours du certificat :
Cliquez sur l'onglet **Chemin d'accès de certification** pour voir que le fichier a été signé par *Cisco Systems Inc*, tel que vérifié par IdenTrust . Dans certains cas, une entité supplémentaire peut vérifier indépendamment le certificat.

16

Signatures numériques pour les certificats numériques

- Un certificat numérique est l'équivalent **d'un passeport électronique**. Il permet aux utilisateurs, hôtes et entreprises **d'échanger** des informations sur Internet de manière **sécurisée**.
- Un certificat numérique permet **d'authentifier** et de vérifier que l'expéditeur d'un message est bien celui qu'il prétend être.



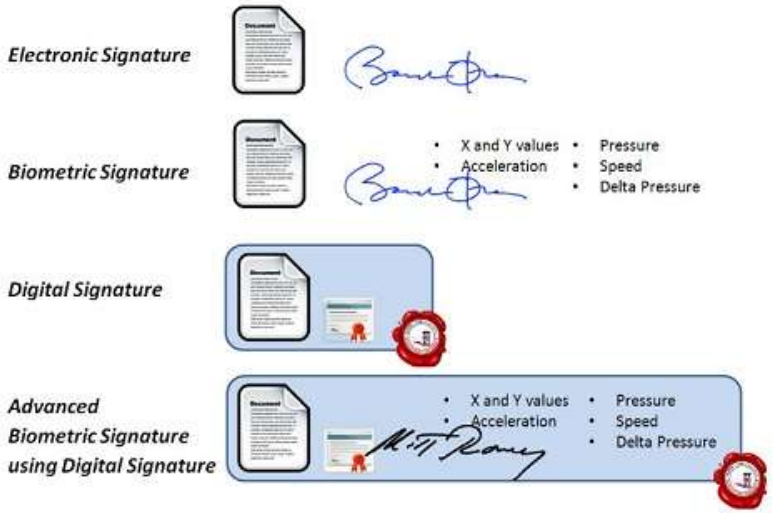
Signature numérique Vs Signature électronique

- Une **signature électronique** est, comme son équivalent papier, un **concept juridique**. Selon la loi américaine intitulée *U.S Electronic Signatures in Global and National Commerce Act,*

> Une signature **électronique** est un «symbole ou processus électroniques liés à un contrat ou un autre document et adoptés par une personne qui a l'intention de signer ce document. »

- **La signature numérique** est une technologie cryptographique utilisée pour vérifier l'authenticité et l'intégrité d'un document. Elle **ne prouve pas**, en soi, l'intention d'une personne de **signer le document ou d'être juridiquement liée par un contrat**.

Signature numérique Vs Signature électronique



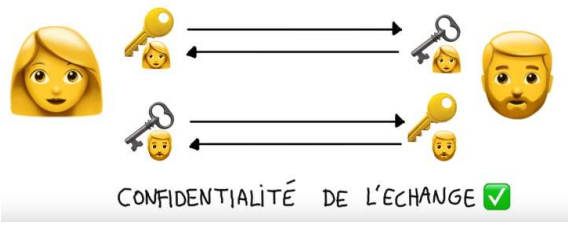
La cryptographie à **clé publique** permet de s'affranchir du problème de **l'échange** de la clé, facilitant le travail de l'expéditeur.

- Mais comment s'assurer de **l'authenticité** de l'envoi?
- Comment être sûr **que personne n'usurpe l'identité** de l'émetteur pour vous envoyer un message?
- Comment être sûr que l'émetteur ne va pas **nier** vous avoir envoyé ce message?

Problématique

CRYPTOGRAPHIE ASYMETRIQUE

- Il existe cependant un problème, **au niveau de la transmission de la clé publique**. Une personne malveillante peut se positionner entre Alice et Bob et se faire passer pour l'un d'eux. ➔ Elle pourra ensuite transmettre sa clé publique à la place. ➔ Cette attaque est appelée **Man In The Middle.**
- Cette personne tierce va **diffuser sa clé publique** à Bob en **se faisant passer** pour Alice. Bob croit alors que c'est la clé publique d'Alice et inversement.
- Alice et Bob ont tous les deux la clé publique du MITM **en pensant avoir celles de leurs interlocuteurs**. MITM a donc intercepté et modifié les échanges des clés entre Alice et Bob.



Problématique

CRYPTOGRAPHIE ASYMETRIQUE

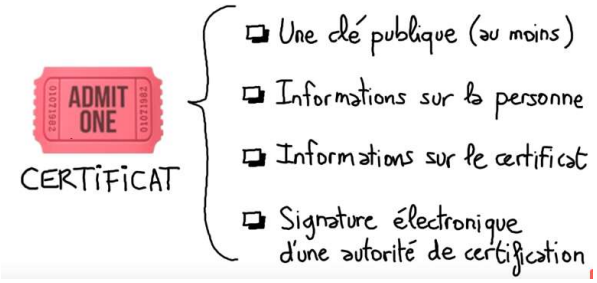
Pour éviter le problème du ***Man In The Midle,*** il faudrait pouvoir **certifier l'identité du porteur de cette clé** et ça c'est le rôle du **certificat numérique**

-7-
Certificats numériques

Certificat numérique

CRYPTOGRAPHIE ASYMETRIQUE

Certificat numérique : c'est un **fichier** contenant un ensemble de données, comprenant au minimum une **clé publique**, des informations permettant **d'identifier la personne**, telles que son nom, son email, sa localisation, ainsi que des informations liées aux certificats, notamment sa date de validité et une **signature numérique** d'une autorité de certification.

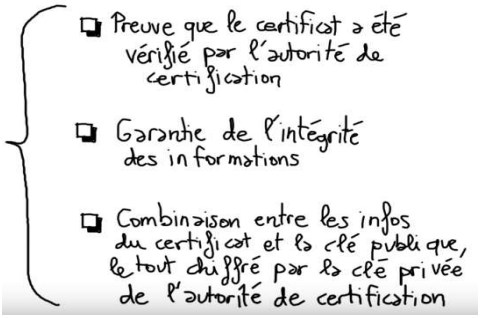


Signature numérique

CRYPTOGRAPHIE ASYMETRIQUE

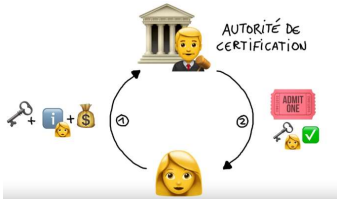
La **signature numérique** est la preuve que le certificat **a bien été vérifié par l'autorité de certification** puisqu'il y a sa signature.
Elle est donc garante de son intégrité ➔ la preuve que le document n'a pas subi d'altération entre l'instant où il a été signée par son auteur et celui où il a été consulté.

La signature numérique du certificat est la combinaison entre les informations sur la personne et celle de sa clé publique, le tout **chiffré par la clé privée de l'autorité**

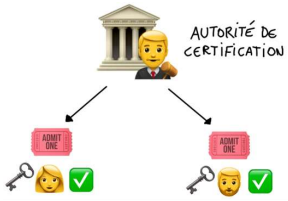


Autorité de certification

- **Une autorité de certification** est **l'institution** responsable d'émettre ces certificats, son rôle est de **garantir** que les informations contenues dans les certificats sont correctes.
- Dans notre cas, si Alice veut créer sont certificat, il faut qu'elles fournissent à l'autorité de certification sa clé publique et des information sur elle, ensuite l'autorité de **certification va créer un certificat** pour Alice sur lequel il y aura la **signature numérique de l'autorité de certification.**



- Le certificat **atteste donc que la clé publique contenue** dans le certificat appartient bien à la personne désignée dans le certificat.



Autorité de certificats numériques

Définition

- **Autorité de certificats numérique : Organisme** garantissant **l'authenticité** et la **validité** des clés publiques dans les échanges sécurisés de données (ex. TLS).
  - Responsable de la **délivrance et gestion** des certificats numériques.
  - Essentielles pour la **sécurité et la confiance numérique** dans les échanges d'informations.
  - Jouent un rôle central dans **l'authentification** et la protection des données.

- **Fonctions Clés des Certificats Numériques :**
  - **Authentification** des parties en communication.
  - **Sécurisation** des échanges de données via chiffrement asymétrique
- **Éléments Importants d'un Certificat** : Rôles du certificat, numéro de série, algorithme de signature, Dates de validité, émetteur, objet, clé publique du titulaire, usage de la clé.

Autorité de certificats numériques

ANSSI | Agence nationale de la sécurité des systèmes d'information

- En France : **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)**
  - Elle assure la mission **d'autorité** en matière de sécurité des systèmes d'information
  - Elle assure un service de **veille**, de **détection**, **d'alerte** et de réaction aux attaques informatiques
  - Elle est chargée d'organiser la délivrance des **labels de sécurité** à des produits et à des prestataires de services de confiance
  - Plus de 20 autorités de certification présentes.

Autorité de certificats numériques

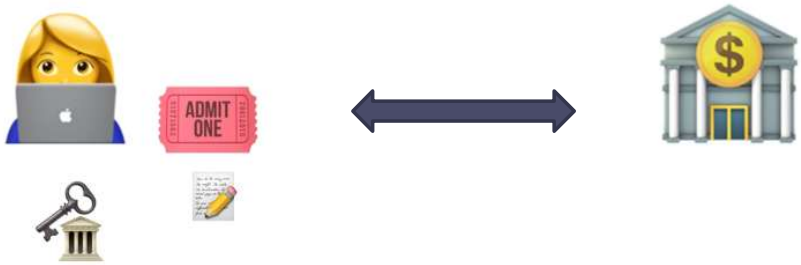
- Au Maroc : **Barid eSign**
  - conformément à la loi n°53-05, l'Agence Nationale de Règlementation des Télécommunications (ANRT) a choisi **Barid eSign** comme plateforme nationale de production de certificats numériques.
  - L'ANRT a délivré de même un **certificat de conformité** à Gemalto Classic TPC IM CC pour la carte à puce TPC, qui est une carte à puce destinée aux applications basées sur la cryptographie à clé publique.
  - **Maroc Numeric 2013** a créé le label **e-thiq@** qui vise à **instaurer** la confiance dans l'achat en ligne, pour **promouvoir** le commerce électronique et encourager la confiance numérique au Maroc.

Barid eSign

Exemple d'application : CHIFFREMENT SSL/TLS

Vous voulez vous connecter à votre banque:

- vous tapez l'adresse en **https** et vous lui envoyez une **demande de connexion sécurisée.**
- Votre banque va alors vous **envoyer son certificat avec sa clé publique,**
- votre navigateur va alors **vérifier** la signature du certificat et sa **validité** (à savoir que le navigateur a déjà un certain nombre de clés publiques d'autorité de certification dans sa base de données).



Exemple d'application : CHIFFREMENT SSL/TLS

- Le navigateur va chercher dans sa base de données la clé publique de **l'autorité de certification** qui a certifié le certificat de la banque,

  ➔ il va alors essayer de **déchiffrer la signature du certificat.**

  ➔ S'il y arrive, cela veut dire que le **certificat est de confiance** car seule l'autorité de certification possède la clé privée associée pour chiffrer le certificat.

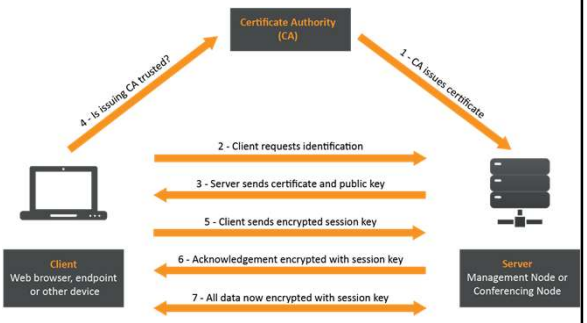
Exemple d'application : CHIFFREMENT SSL/TLS

- Si tout est ok le client et le serveur **négocient ensemble** pour se mettre d'accord sur une **clé secrète** commune qu'ils vont utiliser pour cette session d'échanges comme dans la **cryptographie symétrique,**
- et c'est avec cette **clé** que vous allez chiffrer et déchiffrer vos échanges avec votre banque et donc communiquer de façon sécurisée.

Autorité de certificats numériques

Le Rôle Clé de l'Autorité de Certification dans TLS

- Dans le cadre du protocole TLS (Transport Layer Security), qui vise à **sécuriser** les communications sur Internet, l'autorité de certification joue un rôle crucial en authentifiant les parties impliquées dans l'échange.
- Ce processus d'authentification est complété par la **garantie de la confidentialité**, assurée par des **algorithmes de chiffrement**, et de **l'intégrité**, vérifiée grâce à des **signatures numériques**.
- Reposant sur la **cryptographie hybride**, TLS facilite ainsi l'établissement d'une connexion sécurisée entre un client et un serveur, grâce à l'intervention essentielle de **l'autorité de certification** pour valider les identités.



Infrastructure de clé publique (ou PKI)

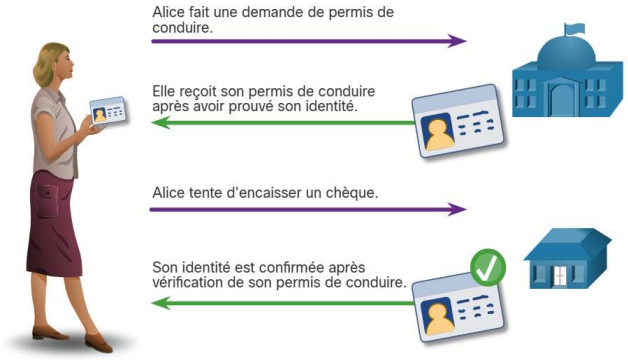
Infrastructure de clé publique (ou PKI)

Public Key Infrastructure

- Le trafic Internet correspond au trafic entre les **deux parties**. Lorsqu'ils établissent une **connexion** asymétrique entre deux hôtes, les hôtes échangent leurs informations **de clé publique**.

➔ Nécessité d'une entité qui permet de soutenir une **distribution** de grande envergure et l'identification des **clés de chiffrement publiques**, **garantir l'identité** des correspondants afin de favoriser une **relation de confiance** hautement évolutive

➔ Ces tiers de confiance fournissent des **services semblables** à ceux des bureaux de délivrance de licences publiques (carte d'identité national, permis de conduire, passeport, …)

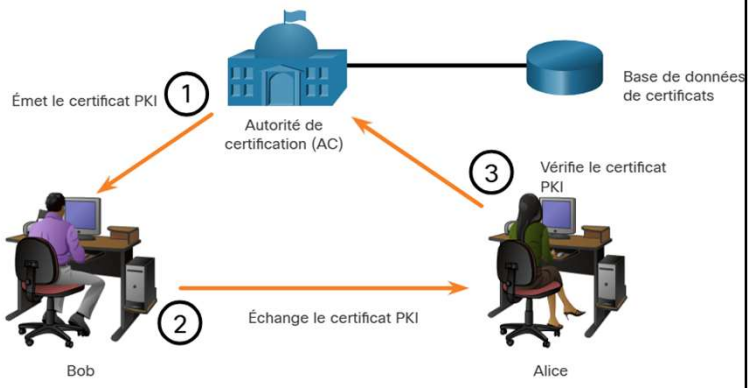


Infrastructure de clé publique (PKI)

Public Key Infrastructure

Exemple :

1. Bob a reçu son **certificat numérique** de **l'autorité de certification**. Ce certificat est utilisé chaque fois que Bob communique avec d'autres parties.
2. Bob communique avec Alice.
3. Lorsqu'Alice reçoit le certificat numérique de Bob, elle **communique** avec l'autorité de certification pour **valider l'identité** de Bob.



Infrastructure de clé publique (PKI)

Public Key Infrastructure

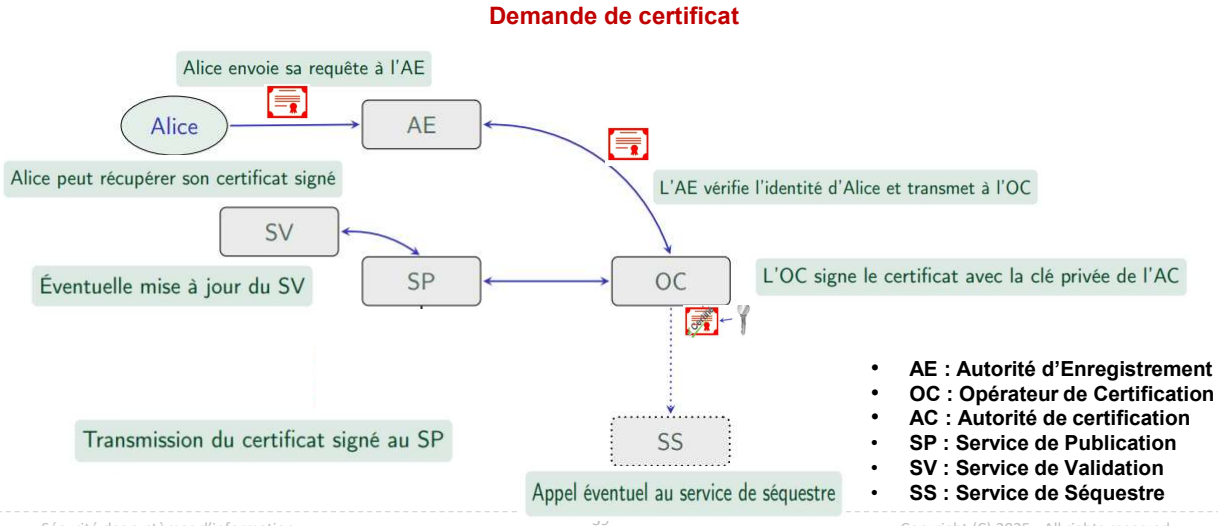
- PKI (Public Key Infrastructure) est un **ensemble de personnes, matériels et logiciels**, régis par des règles, politiques et des procédures et permettant de **créer, gérer stocker, distribuer et révoquer des certificats numériques.**

  ➔ C'est donc à la fois une entité **administrative** et une entité **technique** qui aura en charge l'ensemble des procédures concernant les certificats dont elle a la responsabilité.

- L'infrastructure PKI est **nécessaire** pour soutenir une **distribution** de grande envergure et l'identification des clés de chiffrement publiques.
- Les certificats PKI ne sont pas tous directement générés par l'autorité de certification. Ils peuvent être émis par une autorité **CA subordonnée** (ou **CA intermédiaire**) **sous l'autorité** d'une **CA racine**
- La vérification des identités des demandeurs de certificats peut être assuré par une entité distinct appelé **Autorité d'enregistrement** (AE) ➔ cette entité **n'émet pas directement de certificats** mais joue un rôle clé dans le **processus d'approbation.**

Infrastructure de clé publique (PKI)

Public Key Infrastructure



Infrastructure de clé publique (PKI)

Public Key Infrastructure

Donc, PKI assure les missions suivantes :

- **création et révocation** des certificats X.509,
- **diffusion et publication** des certificats X.509 (via un annuaire LDAP par exemple),
- un service de listes de **révocations** (CRL) pour indiquer les certificats qui **ne sont plus valides** : Certificat remplacé par un autre, Certificat déclaré volé, CA compromis,…
- plus rarement, un service de séquestre et de recouvrement des clés privées. Ce service est bien sûr très utile en **cas de perte de la clé privée** de votre certificat. Le problème est que votre clé privée **perd toute légitimité** car vous la partagez avec un tiers !!!!!!!

Infrastructure de clé publique (PKI)

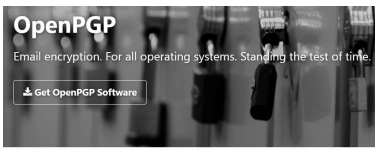
Public Key Infrastructure

Interopérabilité des différents fournisseurs d'infrastructure PKI

- L'interopérabilité entre une infrastructure PKI et ses services d'assistance revêt une **importance** particulière, car de nombreux fournisseurs CA ont préféré proposer et implémenter des solutions **propriétaires** plutôt que **d'attendre la publication de normes**
- Pour résoudre ce problème d'interopérabilité, **l'IETF (Internet Engineering Task Force)** a publié une politique sur les certificats des infrastructures à clé publique Internet X.509 et instauré un cadre sur **les** pratiques de certification (RFC 2527).
- Le **standard X.509 version 3** (X.509v3) définit le format d'un certificat numérique.

OpenPGP

X.509 est le **plus répandu** (grâce à HTTPS) mais il existe aussi le format **OpenPGP** :



- Utilise les mêmes principes (chiffrement asymétrique + symétrique)
- Peut contenir plusieurs identités
- Chaque identité peut avoir plusieurs signatures

➔ Et cela permet de créer une « toile de confiance » : un modèle de confiance décentralisé

Obtenir un certificat

- ✓ Via un enregistreur de noms de domaines
- ✓ Via une institution (DigiCert, Entrust, Verisign…)
- ✓ Via Let's Encrypt (gratuit)
- ✓ Être son propre **Certificate Authority** (CA) : Il faut créer une demande de signature de certificat CSR, puis qu'elle soit signée par un CA (le plus commun pour les CSR est la spécification PKCS#10)

A retenir

- Un certificat numérique est une **carte d'identité** numérique dont l'objet est **d'identifier** une entité physique ou non-physique.
- Le certificat numérique **est un lien** entre l'entité physique et l'entité numérique (Virtuel).
- **L'autorité de certification** fait foi de tiers de confiance et atteste du lien entre l'identité physique et l'entité numérique.
- Le standard le plus utilisé pour la création des certificats numériques est le **X.509**.

TP 3 :
Atelier– Chiffrement et déchiffrement de données à l'aide d'un outil pirate

TP 4 :
Atelier : Générer et utiliser une signature numérique