Sécuriser sa messagerie avec PGP et S/MIME

Travaux pratiques

Patrick Maigron - Télécom SudParis
patrick.maigron@telecom-sudparis.eu

Septembre 2024

Plan du TP

- Introduction

- Créer des clés PGP
- Envoyer des mails sécurisés par PGP
- Utiliser un serveur de clés PGP
- Déterminer la confiance dans les clés
- Certifier des clés PGP
- Révoquer des clés PGP

- Créer des certificats S/MIME
- Envoyer des mails sécurisés par S/MIME

Introduction

- **PGP et S/MIME sont deux techniques permettant de sécuriser les échanges de mail de bout en bout**
  - **Signature**
  - **Chiffrement**

- **Ce sont des standards IETF (RFC)**
  - **OpenPGP : Open Pretty Good Privacy**
  - **S/MIME : Secure/Multipurpose Internet Mail Extensions**

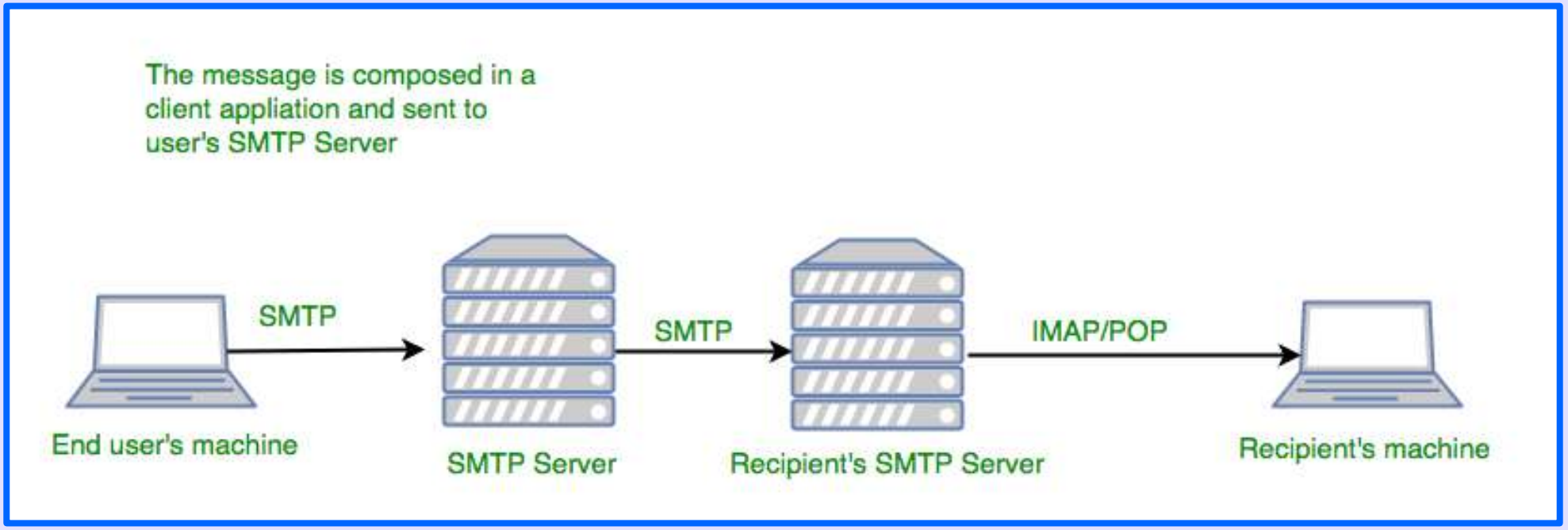
Pourquoi utiliser PGP et S/MIME ?

- **Problèmes de sécurité liés à la messagerie électronique**
  - Écoutes : sniffers
  - Usurpation d'identité : « telnet 25 »
  - Litiges : répudiation par l'émetteur ou le destinataire
  - Modification des mails en transit : attaques de type « Man in the Middle »
- **Services de sécurité offerts par PGP et S/MIME**
  - Confidentialité par chiffrement
  - Authentification par signature électronique
  - Non-répudiation de l'émetteur par signature électronique
  - Intégrité par signature électronique

Mécanismes de PGP et S/MIME

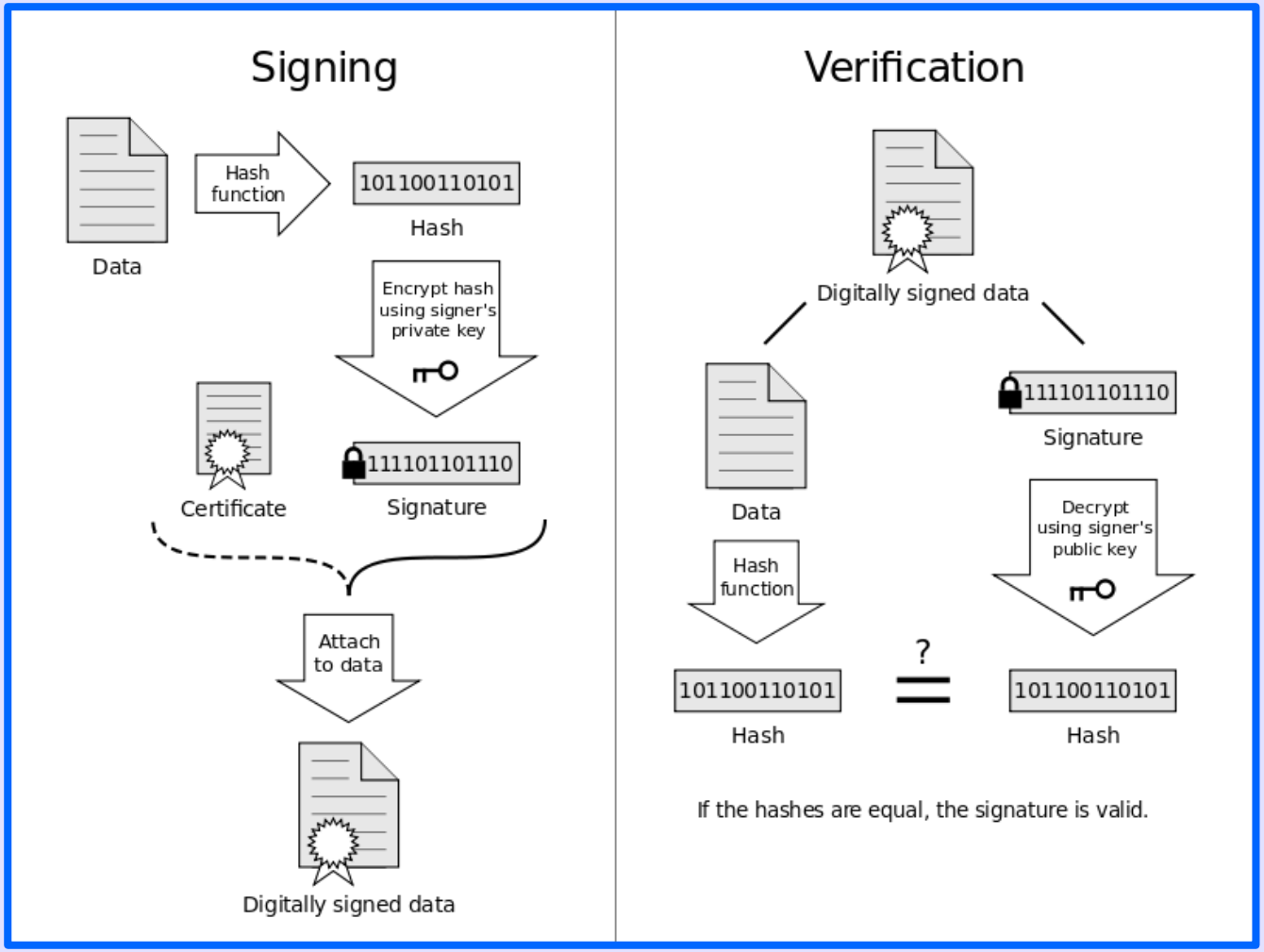
- **Les architectures de messagerie utilisent différents mécanismes de sécurité**
  - **Les échanges entre agents de messagerie et serveurs de mail, ainsi que les échanges entre serveurs de mail, doivent être protégés au moyen des protocoles TLS/SSL**
  - **PGP et S/MIME offrent en complément un service de sécurité de niveau applicatif entre les individus (de bout en bout)**
- **PGP et S/MIME utilisent plusieurs techniques**
  - **Cryptographie asymétrique**
  - **Cryptographie symétrique**
  - **Fonctions de hachage**
  - **Certification des clés publiques**

Mécanismes de PGP et S/MIME



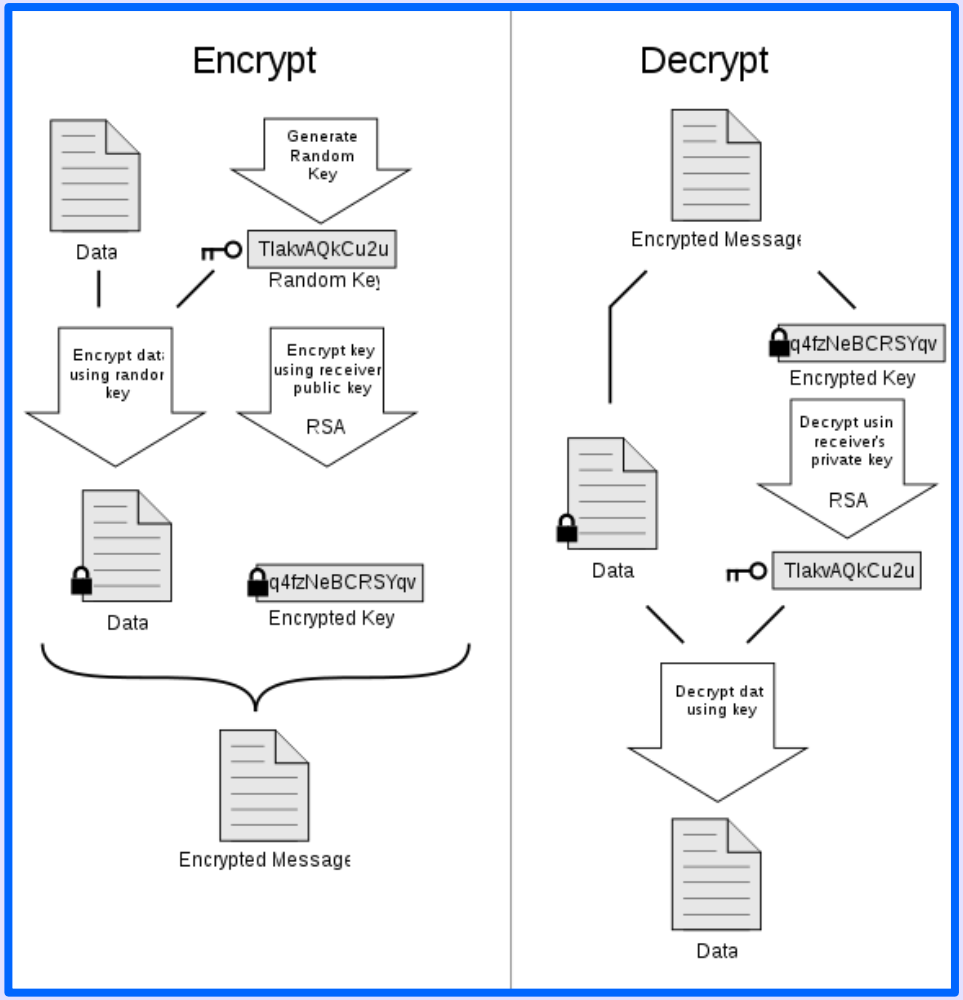
Source : GeeksforGeeks

Mécanismes de PGP et S/MIME



Source : Wikipédia

Mécanismes de PGP et S/MIME



Source : Wikipédia

Logiciels PGP et S/MIME

- **Logiciels PGP**
  - **Logiciel libre : GnuPG (GNU Privacy Guard)**
  - **Logiciel commercial : PGP (Symantec / Broadcom)**

- **Ces logiciels s'intègrent dans les agents de messagerie au moyen d'extensions (plugins)**
  - **Thunderbird : intégré en natif depuis 2020 (pas besoin de plugin)**
  - **Outlook, Outlook Express : GpgOL (inclus dans Gpg4win)**
  - **Zimbra : zimlet OpenPGP (à installer sur le serveur)**
  - **Webmails : plugins dans les navigateurs web (FlowCrypt, Mailvelope…)**

Logiciels PGP et S/MIME

- **Logiciels S/MIME**
  - **S/MIME est implémenté nativement dans la plupart des agents de messagerie modernes : Outlook/Outlook on the web, Thunderbird**
  - **En entreprise, les certificats S/MIME générés par une autorité de certification peuvent être enregistrés dans le serveur de domaine Active Directory et distribués automatiquement vers les postes clients**

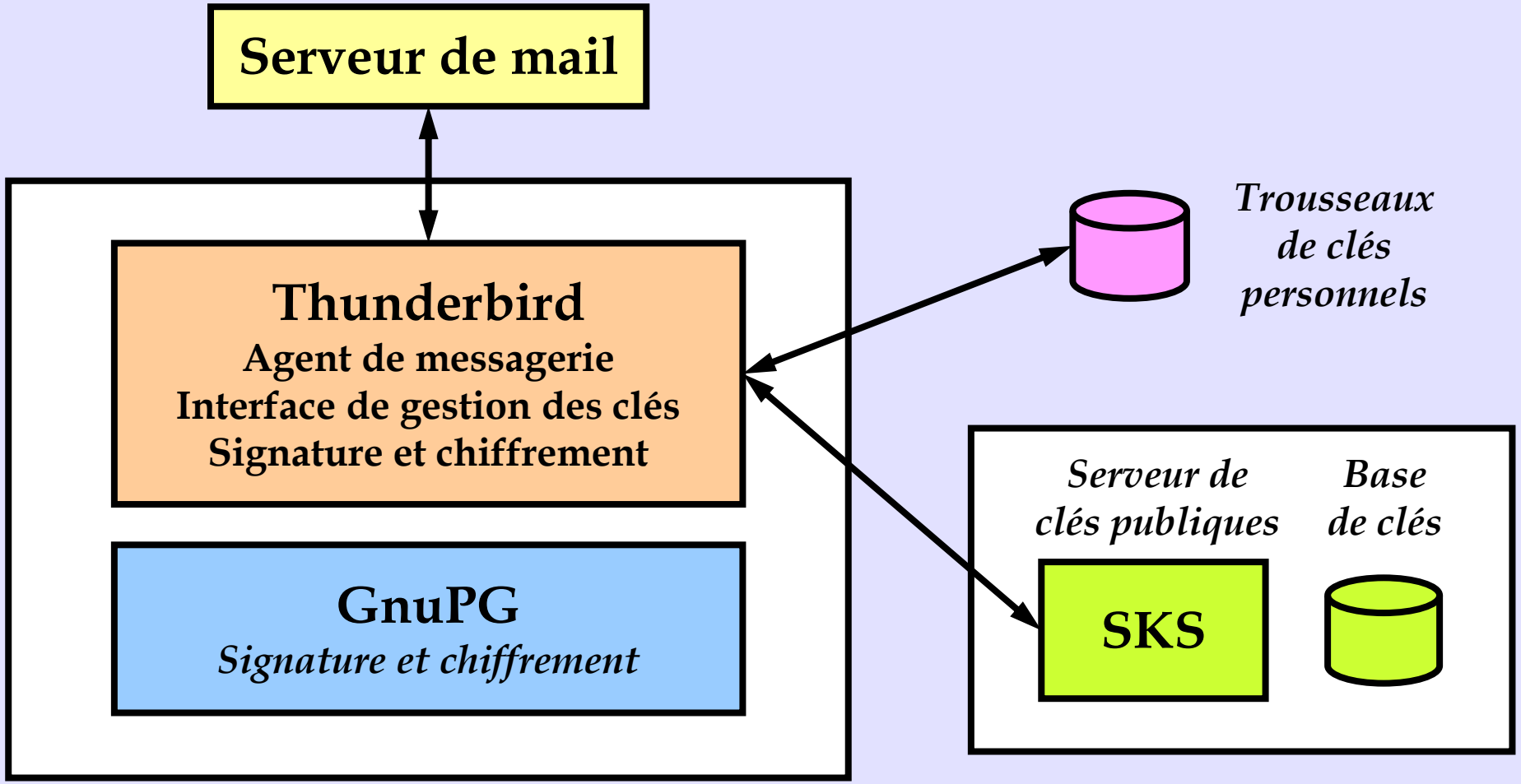
Logiciels PGP et S/MIME

- **Microsoft 365 / Outlook**
  - **« Microsoft Purview Message Encryption » permet d'envoyer des mails chiffrés vers des adresses Microsoft ou non Microsoft (Gmail, Yahoo…)**
  - **Les clés de chiffrement sont gérées par Microsoft**
  - **Les utilisateurs non Microsoft sont redirigés vers un portail permettant leur authentification**
- **Google Workspace / Gmail (pour certains abonnements)**
  - **Utilisation de S/MIME avec chiffrement par Google : les clés S/MIME sont uploadées vers Google (S/MIME hébergé)**
  - **Utilisation de S/MIME avec chiffrement côté client (Gmail CSE) : les clés S/MIME sont fournies par un fournisseur externe et non accessibles par Google (depuis 2022)**

Logiciels PGP et S/MIME

- **Utilisations de PGP et S/MIME autres que le mail**
  - **Les packages des distributions Linux sont signées par GnuPG avec les clés privées des distributions (par exemple SecureApt)**
  - **Le logiciel de transfert de fichiers « Axway Transfer CFT » permet de signer et chiffrer les fichiers envoyés avec PGP ou S-MIME (une paire de clés par partenaire)**

Logiciels PGP utilisés dans le TP



Visualiser les algorithmes supportés

Terminal

- Ouvrez un terminal
- Visualisez les algorithmes disponibles dans votre version du logiciel GnuPG :
  `gpg --version`
- Identifiez les algorithmes de cryptographie asymétrique, symétrique, de hachage et de compression

Visualiser les algorithmes supportés


```
$ gpg --version
gpg (GnuPG) 2.2.27
libgcrypt 1.9.4
Copyright (C) 2021 Free Software Foundation, Inc.
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/patrick/.gnupg
Algorithmes pris en charge :
Clef publique : RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Chiffrement : IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256,
              TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256
Hachage : SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression : Non compressé, ZIP, ZLIB, BZIP2
```

Configurer Thunderbird

Thunderbird

- Lancez Thunderbird
- Fermez la fenêtre demandant un mot de passe en cliquant sur « Annuler »
- Édition / Paramètres des comptes
- Mettez à jour les informations suivantes :
  - Nom : *Prénom Nom (Formation/Année)*
  - Adresse e-mail : *prenom.nom@telecom-sudparis.eu*
- Cette adresse sera utilisée dans le champ « From: » des mails envoyés
- Copiez l'adresse mail

Configurer Thunderbird

Thunderbird

- Cliquez sur l'onglet « Paramètres serveur » à gauche
  - Nom d'utilisateur : collez votre adresse mail ***prenom.nom@telecom-sudparis.eu***
- Cette adresse sera utilisée pour vous authentifier auprès du serveur de courrier entrant (serveur IMAP sur TLS)
- Validez la saisie avec la touche Entrée ou en cliquant n'importe où dans l'interface
- Redémarrez Thunderbird lorsqu'une fenêtre le propose

Configurer Thunderbird

Thunderbird

- **Entrez le mot de passe pour le serveur entrant et sélectionnez l'option « Utiliser le gestionnaire de mots de passe pour se souvenir de ce mot de passe »**

Configurer Thunderbird

Thunderbird

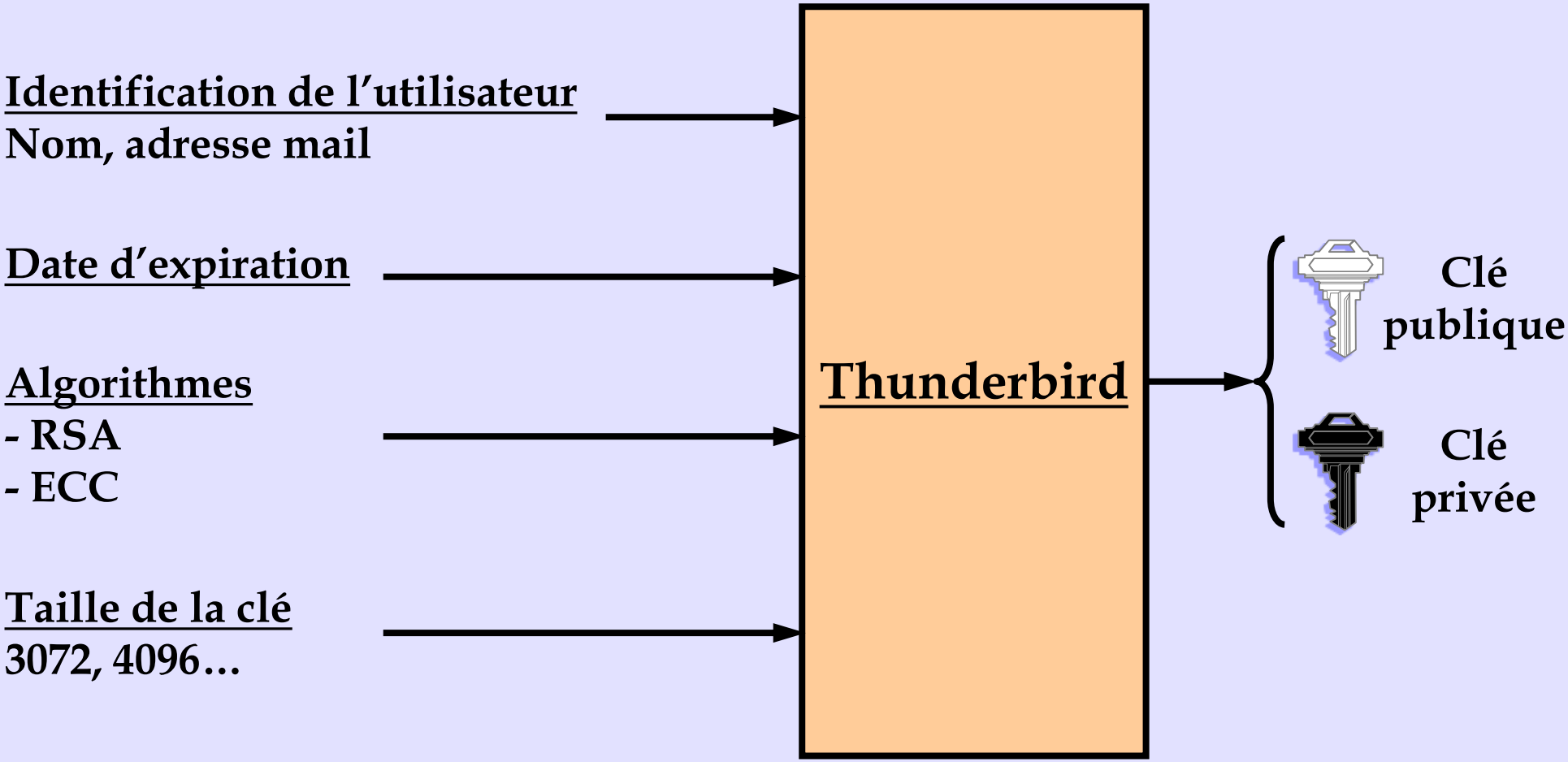
- Cliquez sur l'onglet « Serveur sortant (SMTP) » à gauche en bas du menu
- Sélectionnez le serveur « Zimbra IMT »
- Cliquez sur « Modifier… » à droite
  - Nom d'utilisateur : collez votre adresse mail ***prenom.nom@telecom-sudparis.eu***
- Cette adresse sera utilisée pour vous authentifier auprès du serveur de courrier sortant (serveur SMTP sur TLS)
- Validez puis fermez l'onglet « Paramètres des comptes »

Configurer Thunderbird

Thunderbird

- Cliquez sur « Courrier entrant » à gauche
- Vérifiez que le contenu de votre boîte aux lettres s'affiche correctement
- Testez l'envoi de mail en vous envoyant un mail à votre adresse
- Entrez le mot de passe pour le serveur sortant et sélectionnez l'option de mémorisation du mot de passe

Créer sa paire de clés PGP



Créer sa paire de clés PGP

- **Stockage des clés**
  - **Les clés publiques et privées sont stockées dans des fichiers « pubring.gpg » et « secring.gpg »**
  - **Le fichier de clés privées ne doit être accessible qu'à l'utilisateur : droits d'accès du système d'exploitation, utilisation d'une clé USB externe ou d'une smartcard…**
  - **Ce fichier peut également être chiffré avec un mot de passe (mot de passe principal de Thunderbird)**
  - **Le logiciel GnuPG utilise un mot de passe spécifique pour chiffrer le fichier de clés privées**

Créer sa paire de clés PGP

Thunderbird

- **Ouvrez l'outil de gestion des clés de Thunderbird :**
  - **Outils / Gestionnaire de clés OpenPGP**
- **Cet outil permet de gérer son trousseau de clés : créer des paires de clés, afficher les informations sur des clés, importer et exporter des clés, supprimer des clés…**

Créer sa paire de clés PGP

Gestionnaire de clés OpenPGP

- **Vérifiez la date et l'heure du PC et mettez à jour si nécessaire (car Thunderbird refuse une clé créée dans le futur)**
- **Créez votre paire de clés PGP :**
  - **Génération / Nouvelle paire de clés**
- **Entrez les informations suivantes :**
  - **Expiration de la clé**
  - **Type de clé**
  - **Taille de la clé**
- **Bouton « Générer la clé »**

Créer sa paire de clés PGP

Gestionnaire de clés OpenPGP

- **Validez la génération de la clé**
- **Votre paire de clés apparaît en gras**
- **La génération des clés utilise un générateur de nombres pseudo-aléatoires intégré dans le système d'exploitation**
- **Le générateur de Linux collecte des éléments de différentes sources matérielles de manière à créer de l'entropie et à produire des nombres pseudo-aléatoires cryptographiquement sûrs (utilisation des disques, du processeur…)**

Visualiser les informations sur sa clé PGP

Gestionnaire de clés OpenPGP

- **Effectuez un double-clic sur votre clé**
- **Vérifiez les informations générales sur votre clé : propriétaire, date de création et d'expiration**
- **Cliquez sur l'onglet « Structure »**
- **Observez la structure de votre clé, qui se compose d'une clé principale de signature et d'une sous-clé de chiffrement**

Analyser le contenu de sa clé PGP

- **Enregistrez votre clé publique dans un fichier**

Gestionnaire de clés OpenPGP

- **Effectuez un clic droit sur votre clé**
- **Exporter une ou des clés publiques vers un fichier**
- **Enregistrez votre clé dans un fichier « ma-clé.asc »**

Analyser le contenu de sa clé PGP

- **Analysez le contenu de votre clé publique**

Terminal

– **Affichez la structure de votre clé publique avec GnuPG :**

```
gpg --list-packets --verbose ma-clé.asc
```

Analyser le contenu de sa clé PGP


```
$ gpg --list-packets --verbose ma-clé.asc
# off=0 ctb=c6 tag=6 hlen=3 plen=397 new-ctb
:public key packet:
        version 4, algo 1, created 1689766764, expires 0
        pkey[0]: D4738C49D2A899229C7855A7E01D9FB97E4D3F0FBF1417A4E98306C6B [...]
        pkey[1]: 010001
        keyid: 7C20C92E6AAF37A7
# off=400 ctb=cd tag=13 hlen=2 plen=65 new-ctb
:user ID packet: "Patrick Maigron (TEST/2024) <patrick.maigron@telecom-sudparis.eu>"
# off=467 ctb=c2 tag=2 hlen=3 plen=461 new-ctb
:signature packet: algo 1, keyid 7C20C92E6AAF37A7 [...]
# off=931 ctb=ce tag=14 hlen=3 plen=397 new-ctb
:public sub key packet:
        version 4, algo 1, created 1689766764, expires 0
        pkey[0]: D6387EA5D8F95892F0E11F5BB16CEC31649249C2B74724F826F5C456D [...]
        pkey[1]: 010001
        keyid: 288038943B783CC5
# off=1331 ctb=c2 tag=2 hlen=3 plen=444 new-ctb
:signature packet: algo 1, keyid 7C20C92E6AAF37A7 [...]
```

Analyser le contenu de sa clé PGP

- **Le bloc « public key packet » correspond à la partie publique de la clé principale de signature**
  - **Identifiez l'algorithme utilisé (« algo » : 1 pour RSA, 22 pour EdDSA) et l'identifiant de la clé (« keyid »)**
  - **Les paramètres de la clé publique sont notés pkey[0], pkey[1]…**
  - **Avec RSA, pkey[0] est le module (produit de deux grands nombres premiers) et pkey[1] l'exposant public**
- **Le bloc « user ID packet » correspond à l'identité du propriétaire de la clé (nom et adresse mail)**
- **Le bloc « signature packet » correspond à une auto-signature de la clé publique principale par la clé privée**

Analyser le contenu de sa clé PGP

- **Le bloc « public sub key packet » correspond à la partie publique de la sous-clé de chiffrement**
  - **Identifiez l'algorithme utilisé (« algo » : 1 pour RSA, 18 pour ECDH), l'identifiant de la clé et les paramètres constituant la clé publique**

- **Le bloc « signature packet » correspond à une auto-signature de la sous-clé publique par la clé privée**

Configurer Thunderbird

Thunderbird

- **Configurez la clé PGP à utiliser :**
  Édition / Paramètres des comptes
  Onglet « Chiffrement de bout en bout »
  Paragraphe « OpenPGP »
- **Sélectionnez la clé PGP que vous avez créée précédemment**

S'envoyer un mail signé et/ou chiffré

Thunderbird

- **Envoyez à vous-même un mail signé et non chiffré en sélectionnant l'option correspondante dans le menu « OpenPGP »**
- **Lisez le mail signé reçu**
- **Cliquez sur le bouton « OpenPGP » en haut à droite pour afficher le résultat : « Signature numérique correcte » et identifiant de la clé du signataire**

S'envoyer un mail signé et/ou chiffré

Thunderbird

- Envoyez à vous-même un mail chiffré et non signé, en conservant l'option « Chiffrer le sujet » et en décochant « Signer numériquement »
- Le sujet du mail reçu n'est pas visible tant que le mail n'a pas été déchiffré, il est remplacé par le texte « ***UNCHECKED*** ... »
- Lisez le mail chiffré reçu
- Affichez le résultat : « Ce message est chiffré » et identifiant de la clé et de la sous-clé de déchiffrement

S'envoyer un mail signé et/ou chiffré

Thunderbird

- **Envoyez enfin à vous-même un mail à la fois signé et chiffré**
- **Le contenu du mail est d'abord signé avec votre clé privée, puis l'ensemble du contenu et de sa signature est chiffré avec votre clé publique**
- **Lisez le mail signé et chiffré reçu et affichez le résultat**

Analyser un mail signé

- **Enregistrez le mail signé reçu dans un fichier texte**

Thunderbird

- **Effectuez un clic droit sur le mail uniquement signé (non chiffré) que vous avez reçu**
- **Enregistrer sous…**
- **Enregistrez le mail signé dans le fichier « mail-signé.eml »**
- **Affichez le contenu du mail signé**

Analyser un mail signé


```
Content-Type: multipart/signed; micalg=pgp-sha256; protocol="application/pgp-signature"

This is an OpenPGP/MIME signed message (RFC 4880 and 3156)

Content-Type: multipart/mixed; protected-headers="v1"
From: "Patrick Maigron (TEST/2024)" <patrick.maigron@telecom-sudparis.eu>
To: patrick.maigron@telecom-sudparis.eu
Message-ID: <90b0dfc1-6851-4889-49b2-b4ccdd747717@telecom-sudparis.eu>
Subject: Mail signe

Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: base64

Texte du mail (codé en base64)

Content-Type: application/pgp-signature; name="OpenPGP_signature.asc"
Content-Description: OpenPGP digital signature
Content-Disposition: attachment; filename="OpenPGP_signature.asc"

-----BEGIN PGP SIGNATURE-----
iQIzBAEBCgAdFiEEiYBSzJfQRGUFLszu5FsgUBltNLYFAl7nbmYACgkQ5FsgUBlt [...]
=nNIh
-----END PGP SIGNATURE-----
```

Analyser un mail signé

- La ligne
  « `Content-Type: multipart/signed; protocol="application/pgp-signature";` »
  indique que le mail contient un bloc de texte et sa signature PGP
- La ligne
  « `Content-Type: multipart/mixed; protected-headers="v1"` »
  indique que certains champs d'en-tête sont signés (From, To, Message-ID, Subject)
- La signature figure en bas entre les lignes
  « `BEGIN PGP SIGNATURE` » et « `END PGP SIGNATURE` »
- La taille de la signature dépend de l'algorithme asymétrique utilisé et de la taille de la clé

Analyser un mail signé

Terminal

- **Affichez la structure du mail signé :**
  `gpg --list-packets --verbose mail-signé.eml`
- **Identifiez les informations contenues dans le fichier signé :**
  - **Algorithme asymétrique utilisé (« algo »)**
  - **Identifiant de la clé publique utilisée (« keyid »)**
  - **Algorithme de hachage utilisé (« digest algo 8 » pour SHA256)**
  - **Date de création et d'expiration de la signature**
  - **Contenu binaire de la signature (texte en clair haché, puis chiffré avec l'algorithme asymétrique)**

Analyser un mail signé


```
$ gpg --list-packets --verbose mail-signé.eml
# off=0 ctb=c2 tag=2 hlen=3 plen=441 new-ctb
:signature packet: algo 1, keyid 7C20C92E6AAF37A7
        version 4, created 1689771966, md5len 0, sigclass 0x00
        digest algo 8, begin of digest c8 fe
        hashed subpkt 33 len 21 (issuer fpr v4 FCC257F8CAF045109FD4E52F7C20C92E...)
        hashed subpkt 2 len 4 (sig created 2024-08-23)
        hashed subpkt 3 len 4 (sig does not expire)
        subpkt 16 len 8 (issuer key ID 7C20C92E6AAF37A7)
        data: A9FB7BA14CE7F2E4F082F401AEA930323858451683A5A6B54986BD0E33 [...]
```

Analyser un mail chiffré

- **Enregistrez le mail chiffré reçu dans un fichier texte**

Thunderbird

- **Effectuez un clic droit sur le mail uniquement chiffré (non signé) que vous avez reçu**
- **Enregistrer sous…**
- **Enregistrez le mail chiffré dans le fichier « mail-chiffré.eml »**
- **Affichez le contenu du mail chiffré**

Analyser un mail chiffré


```
Date: Fri, 23 Aug 2024 17:45:34 +0200
To: patrick.maigron@telecom-sudparis.eu
From: "Patrick Maigron (TEST/2024)" <patrick.maigron@telecom-sudparis.eu>
Subject: ***UNCHECKED*** ...
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted"

This is an OpenPGP/MIME encrypted message (RFC 4880 and 3156)

Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----
hQIMAwYY3tKiBPJoAQ/+MLMuejDDlyVXN6K+nuRJmZvLdiqmuw95YEZkqZRg+zTL [...]
=xzmQ
-----END PGP MESSAGE-----
```

Analyser un mail chiffré

- La ligne « `Subject:` » montre que l'objet du mail est chiffré
- La ligne « `Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";` » indique que le mail contient un bloc de texte chiffré par PGP
- Le bloc chiffré figure en bas entre les lignes « `BEGIN PGP MESSAGE` » et « `END PGP MESSAGE` »

Analyser un mail chiffré

Terminal

- **Affichez la structure du mail chiffré :**
  `gpg --list-packets --verbose mail-chiffré.eml`

Analyser un mail chiffré


```
$ gpg --list-packets --verbose mail-chiffré.eml
gpg: la clef publique est 288038943B783CC5
gpg: la clef publique est 288038943B783CC5
gpg: chiffré avec une clef RSA, identifiant 288038943B783CC5
gpg: chiffré avec une clef RSA, identifiant 288038943B783CC5
gpg: échec du déchiffrement : Pas de clef secrète
# off=0 ctb=c1 tag=1 hlen=3 plen=396 new-ctb
:pubkey enc packet: version 3, algo 1, keyid 288038943B783CC5
        data: D1EECEDEE0924F8A6FB31D4A3EADDBCE48CA4928DA2769EF7BEEE599 [...]
# off=399 ctb=c1 tag=1 hlen=3 plen=396 new-ctb
:pubkey enc packet: version 3, algo 1, keyid 288038943B783CC5
        data: 8880118747E5F67B31B127035B00DAD139489217C4E632FB26034C54 [...]
# off=798 ctb=d2 tag=18 hlen=3 plen=546 new-ctb
:encrypted data packet:
        length: 546
        mdc_method: 2
```

Analyser un mail chiffré

- **Les deux blocs « pubkey enc packet » correspondent à la clé de session symétrique chiffrée avec l'algorithme asymétrique**
  - **Il y a un bloc de ce type pour l'émetteur et un pour chaque destinataire du mail**
  - **Identifiez l'algorithme asymétrique utilisé (« algo »), l'identifiant de la clé publique (« keyid ») et le contenu binaire de la clé de session chiffrée**

- **Le bloc « encrypted data packet » correspond au contenu du mail chiffré avec la clé de session symétrique**

Envoyer un mail signé

Thunderbird

- **Envoyez à votre interlocuteur un mail signé**
- **Lisez le mail signé reçu de votre interlocuteur**
- **La vérification de la signature n'est pas possible car vous ne disposez pas actuellement de la clé publique de votre interlocuteur (icône avec un point d'interrogation bleu)**
- **Le bouton « Rechercher… » permet de rechercher une clé manquante depuis un serveur public de clés**
- **Dans un premier temps, vous allez échanger votre clé publique avec votre interlocuteur par mail**

Échanger sa clé publique PGP par mail

Thunderbird

- **Composez un nouveau mail à votre interlocuteur**
- **Cliquez sur « Joindre / Ma clé publique OpenPGP » à droite puis envoyez le mail**
- **Lisez le nouveau mail reçu de votre interlocuteur**
- **Il contient sa clé publique dans une pièce jointe de nom « OpenPGP_*KeyID*.asc »**

Échanger sa clé publique PGP par mail

Thunderbird

- **Effectuez un clic droit sur la pièce jointe**
- **Importer une clé OpenPGP**
- **Sélectionnez l'option « Acceptée (non vérifiée) » et validez**
- **Accepter une clé indique que vous utiliserez cette clé pour envoyer des messages chiffrés à ce correspondant**
- **Alternativement on peut aussi cliquer sur le bouton « OpenPGP » à droite puis sur le bouton « Importer… »**

Échanger sa clé publique PGP par mail

Thunderbird

- Vérifiez dans le gestionnaire de clés OpenPGP que la clé publique de votre interlocuteur a été ajoutée
- Effectuez un double-clic sur la clé de votre interlocuteur
- L'onglet « Votre acceptation » indique que vous acceptez sa clé mais que vous n'avez pas encore vérifié que c'est effectivement la sienne
- On peut également rejeter une clé ou ne pas l'accepter

Échanger sa clé publique PGP par mail

Thunderbird

- **Lisez à nouveau le mail signé reçu précédemment de votre interlocuteur**
- **L'icône OpenPGP de signature contient cette fois-ci un panneau orange à la place du point d'interrogation bleu, car vous n'avez pas encore vérifié que la clé reçue est effectivement celle de votre interlocuteur**
- **Cliquez sur le bouton « OpenPGP » et vérifiez que la signature est correcte**

Envoyer un mail chiffré

Thunderbird

- **Envoyez à votre interlocuteur un mail chiffré**
- **Lisez le mail chiffré reçu de votre interlocuteur**
- **Envoyez enfin à votre interlocuteur un mail à la fois signé et chiffré**
- **Lisez le mail signé et chiffré reçu de votre interlocuteur**

Utiliser un serveur de clés PGP

Terminal

- Des serveurs de clés PGP permettent de déposer sa clé publique afin de la rendre accessible en ligne
- Dans ce TP, vous utiliserez un serveur de clés dédié et non pas un serveur public
- Notez l'adresse IP du serveur de clés qui vous est fournie : *aaa.bbb.ccc.ddd*
- Vérifiez que le serveur de clés est effectivement accessible :
  `ping aaa.bbb.ccc.ddd`

Interroger le serveur de clés PGP

Navigateur web

- Affichez dans un navigateur web la page d'accueil du serveur de clés en entrant l'url : `aaa.bbb.ccc.ddd`
- Entrez une chaîne de caractères dans le champ de recherche
- Validez pour visualiser les clés correspondantes
- Effectuez des recherches similaires en affichant les empreintes digitales (fingerprints), les sous-clés et les signatures (verbose index) et le contenu ASCII des clés (ascii-armored keys)

Exporter sa clé vers le serveur de clés

Gestionnaire de clés OpenPGP

- **Effectuez un clic droit sur votre clé**
- **Copier / Clé publique**
- **Votre clé publique est copiée dans le presse-papiers sous un format d'échange ASCII**

Exporter sa clé vers le serveur de clés

Navigateur web

- **Cliquez dans le champ de saisie rectangulaire sous le paragraphe « Submit a key » en bas de l'interface du serveur de clés**
- **Collez le presse-papiers et validez avec le bouton « Submit this key » (conservez les balises « BEGIN » et « END »)**
- **Vérifiez dans le navigateur web que votre clé publique apparaît effectivement sur le serveur de clés**

Importer des clés depuis le serveur de clés

Navigateur web

- Dans l'interface du serveur de clés, sélectionnez l'option « Retrieve ASCII-armored keys » et cherchez le texte suivant : ***Formation/Année***
- Le résultat correspond à l'ensemble des clés publiques du groupe sous un format d'échange ASCII
- Copiez le contenu de la page dans le presse-papiers en incluant les balises « BEGIN » et « END » mais SANS le titre « Public Key Server -- Get » (sélectionnez la première ligne, descendez en bas de la page puis faites « Majuscule Clic » à la fin de la dernière ligne)

Importer des clés depuis le serveur de clés

Gestionnaire de clés OpenPGP

- **Édition / Importer une ou des clés depuis le presse-papiers**
- **Sélectionnez l'option « Acceptée (non vérifiée) » et validez**
- **Vérifiez que les clés publiques du groupe ont effectivement été importées dans votre trousseau de clés publiques**

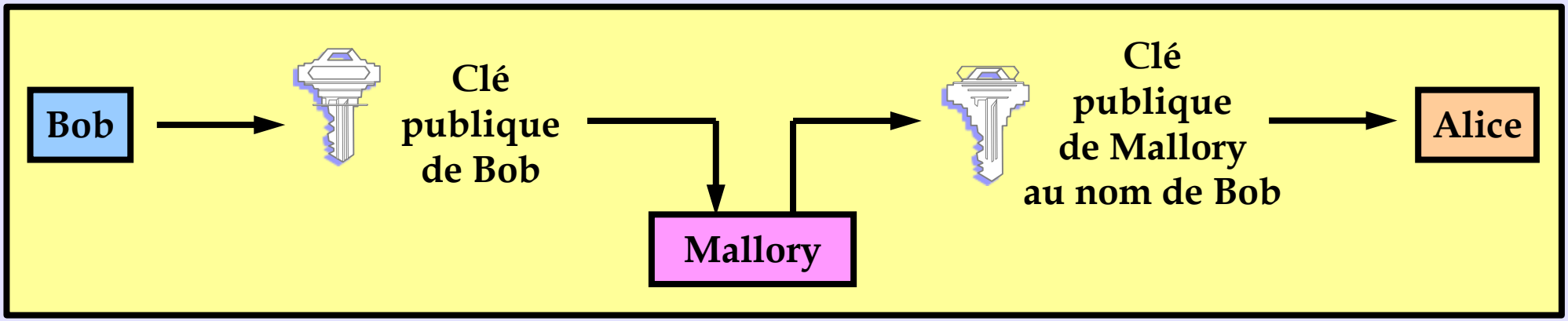
Risque de contrefaçon des clés

- **L'association entre une clé et une adresse mail n'est pas assurée**
  - **Lorsqu'une personne crée une paire de clés associée à une adresse mail, on ne vérifie pas que cette personne est effectivement propriétaire de l'adresse mail**
  - **Un attaquant peut donc créer une paire de clés en l'associant à l'adresse d'une autre personne (contrefaçon)**

- **Une clé contrefaite peut ensuite être diffusée sur des serveurs de clés**

Risque de contrefaçon des clés

- **L'attaquant peut aussi insérer une clé contrefaite dans le cas d'un échange de clé par mail (attaque de type MITM)**



- **Si l'attaquant réussit à diffuser une clé contrefaite :**
  - **Il pourra signer des mails au nom de la victime**
  - **Il pourra déchiffrer des mails chiffrés envoyés à la victime**

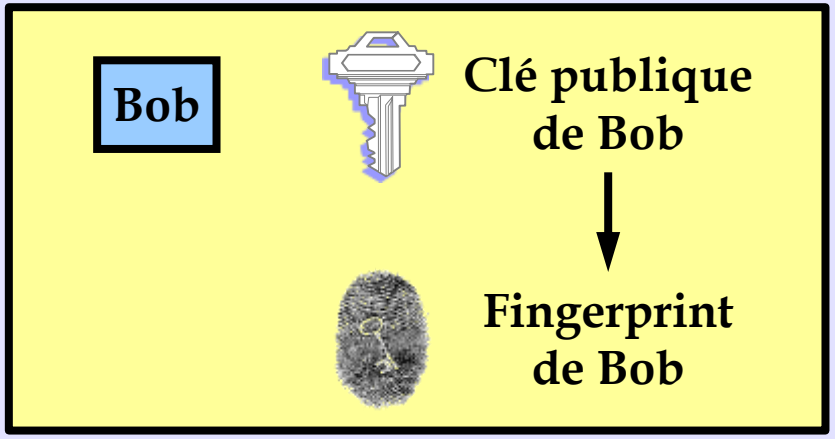
Certification des clés

Déterminer la confiance dans les clés

- **Les clés doivent donc être certifiées pour éviter les contrefaçons**
  - **La certification permet de prouver qu'une clé donnée appartient bien à la personne possédant l'adresse mail associée à la clé**
- **Différences entre PGP et S/MIME**
  - **Leur fonctionnement est identique en ce qui concerne les fonctions de signature et de chiffrement (cryptographie asymétrique)**
  - **Ils se distinguent par la manière de certifier les clés : elles sont certifiées par chaque utilisateur dans le cas de PGP et par une autorité de certification dans le cas de S/MIME**
  - **Du fait de ces modes de fonctionnement, PGP est plus adapté à un usage par des particuliers et S/MIME par des entreprises**

Certification des clés PGP

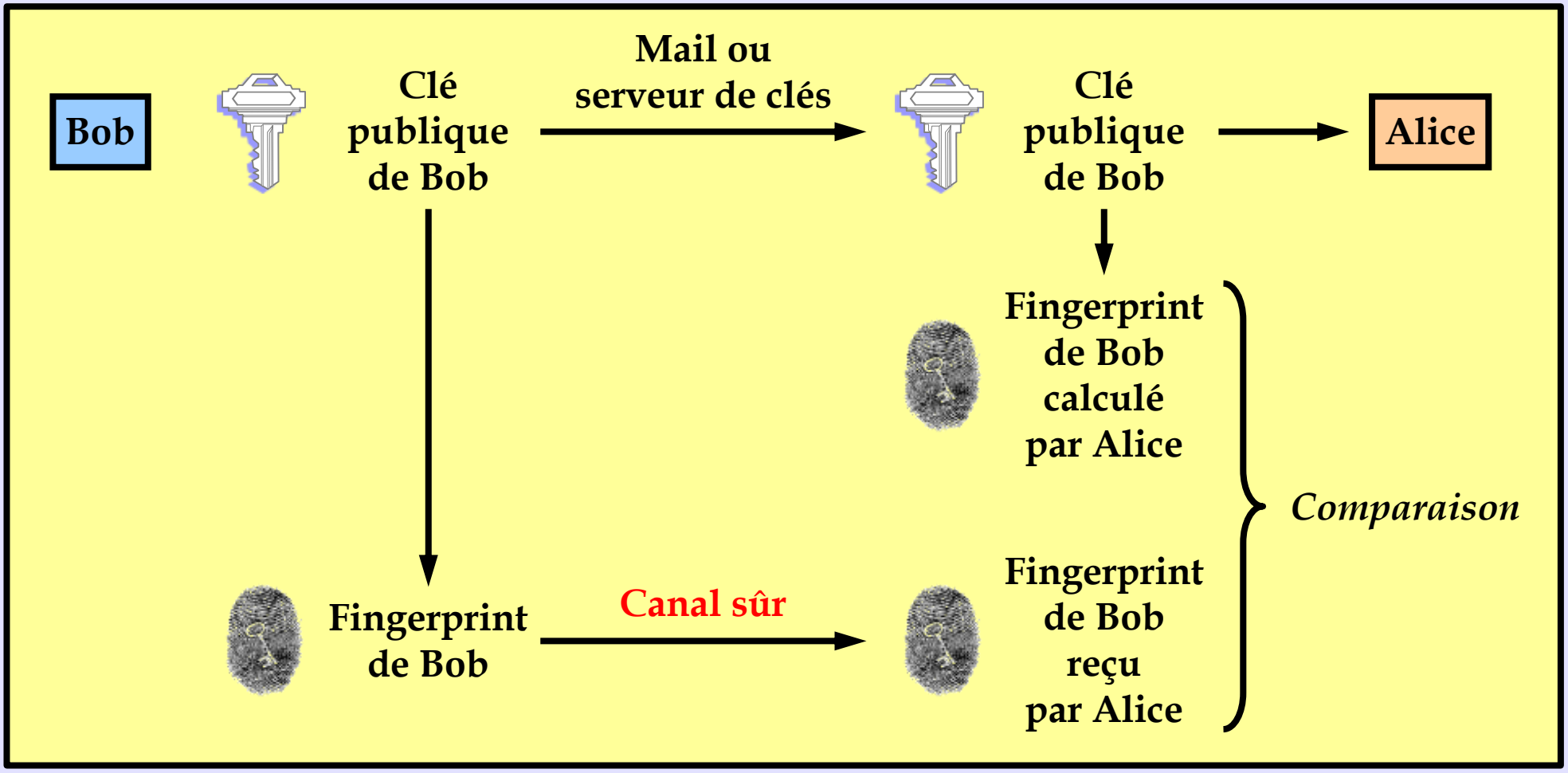
- **Chaque utilisateur vérifie la validité des clés publiques de ses interlocuteurs au moyen d'une empreinte digitale**
  - **Une empreinte digitale ou fingerprint est le résultat d'un calcul effectué sur une clé publique (fonction de hachage cryptographique)**
  - **L'empreinte digitale est plus petite que la clé publique**
  - **Si deux clés ont la même empreinte digitale, elles ont une très forte probabilité d'être identiques**



Vérification des clés publiques PGP

- **Vérification de l'empreinte digitale lors de la réception d'une clé**
  - **Bob envoie sa clé publique à Alice**
  - **Pour éviter une contrefaçon de la clé de Bob lors de son envoi, Alice doit vérifier que la clé reçue est effectivement la clé envoyée par Bob**
  - **Alice calcule l'empreinte digitale de la clé reçue de Bob**
  - **Bob transmet à Alice l'empreinte digitale de sa clé par un canal sûr, par exemple un appel téléphonique**
  - **Alice compare l'empreinte digitale calculée à partir de la clé reçue de Bob avec l'empreinte digitale de la clé de Bob transmise par ce canal sûr**
  - **Une fois qu'Alice a vérifié l'empreinte digitale de la clé reçue de Bob, elle certifie cette clé**

Vérification des clés publiques PGP



Vérification des clés publiques PGP

- **Comment communiquer l'empreinte digitale de sa clé PGP par un canal sûr**
  - **Lors d'une rencontre en face à face si on connaît la personne**
  - **Par un appel téléphonique en reconnaissant la voix de la personne**
  - **Par des messageries instantanées type Signal ou WhatsApp**
  - **En affichant son empreinte digitale PGP sur différents supports : réseaux sociaux, site web personnel, dans la signature de ses mails…**
  - **Exemple : Edward Snowden et la journaliste Laura Poitras communiquent en 2013 au moyen de comptes mail anonymes en utilisant PGP, Snowden vérifie l'empreinte digitale de Poitras en demandant qu'on l'affiche dans un compte Twitter**

Certifier une clé publique PGP

Gestionnaire de clés OpenPGP

- **Effectuez un double-clic sur la clé publique de votre interlocuteur**
- **Visualisez l'empreinte digitale de sa clé publique**
- **On suppose que vous avez vérifié l'empreinte digitale avec votre interlocuteur en utilisant un canal sûr**
- **Sélectionnez l'option « J'ai vérifié en personne que l'empreinte est correcte » et validez avec le bouton « OK »**

Certifier une clé publique PGP

Thunderbird

- **Lisez le mail signé reçu précédemment de votre interlocuteur**
- **Vérifiez que l'icône OpenPGP de signature contient une coche verte à la place du panneau orange (signature valide d'une clé vérifiée)**

Révoquer sa clé publique PGP

- **La révocation des clés publiques**
  - **Il est parfois nécessaire de révoquer sa clé publique (pourquoi ?)**
  - **Pour cela, un certificat de révocation a été créé en même temps que la paire de clés au début du TP (pourquoi le créer à ce moment là ?)**
  - **Le certificat de révocation est signé avec la clé privée correspondante (pour prouver qu'on est bien le titulaire de la clé)**
  - **Le certificat de révocation est sauvegardé dans un fichier texte qui doit être gardé confidentiel (pourquoi ?)**
  - **S'il devient nécessaire de révoquer sa clé publique, on utilise ce certificat de révocation**
  - **Il faut ensuite envoyer sa clé révoquée à ses interlocuteurs et/ou aux serveurs de clés afin de les informer de la révocation de sa clé**

Révoquer sa clé publique PGP

- **Révoquer sa clé publique dans son trousseau de clés**

Gestionnaire de clés OpenPGP

- **Effectuez un clic droit sur votre clé**
- **Révoquer la clé**
- **Vérifiez que la clé apparaît comme révoquée dans votre trousseau de clés (elle est écrite en caractères italiques)**

Révoquer sa clé publique PGP

- **Exporter sa clé révoquée vers le serveur de clés**

Gestionnaire de clés OpenPGP

- **Copiez votre clé publique dans le presse-papiers**

Navigateur web

- **Collez le presse-papiers dans l'interface du serveur de clés pour envoyer la clé révoquée sur le serveur**
- **Vérifiez que votre clé publique est effectivement signalée comme révoquée sur le serveur**

Prendre en compte la révocation des clés PGP

- **Mettre à jour les clés révoquées depuis le serveur de clés**

Navigateur web

- **Récupérez sur le serveur le bloc de clés correspondant au texte `Formation/Année` et copiez-le dans le presse-papiers**

Gestionnaire de clés OpenPGP

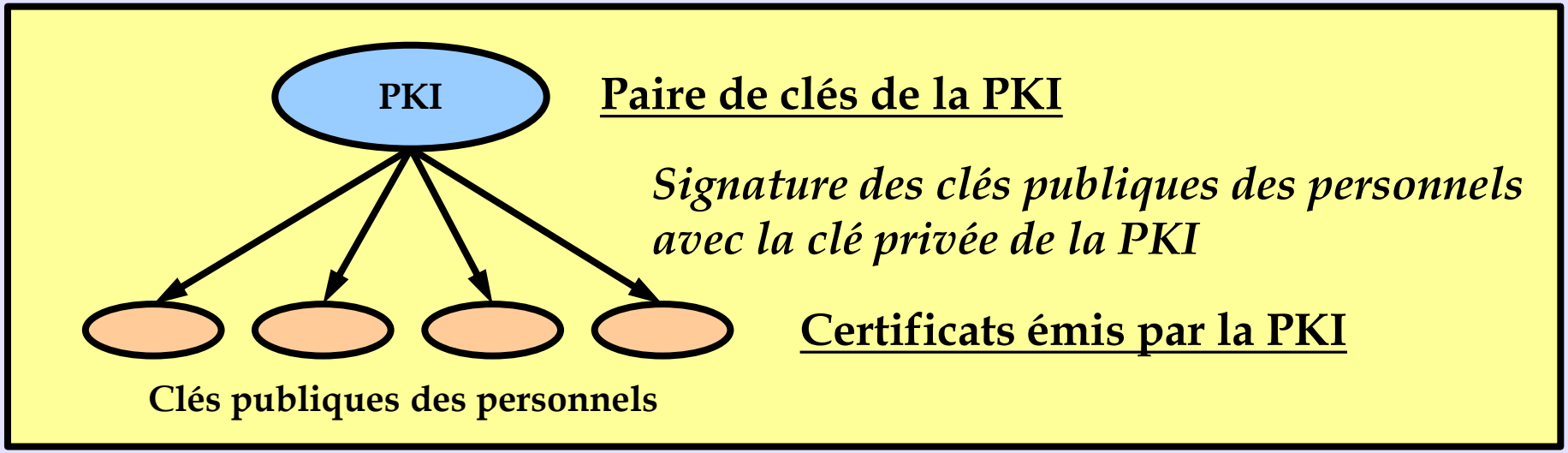
- **Importez les clés depuis le presse-papiers dans votre trousseau de clés avec l'option « Acceptée (non vérifiée) »**
- **Vérifiez que toutes les clés apparaissent comme révoquées dans votre trousseau de clés**

Certification des clés S/MIME

- **La certification des clés S/MIME**
  - **Les certificats S/MIME sont fournis par une autorité de certification (AC), ils peuvent être payants ou gratuits (pour une durée limitée)**
  - **Le format des certificats utilisés est X.509 (comme les certificats SSL/TLS pour HTTPS)**
  - **Il existe plusieurs classes de certificats S/MIME selon le niveau de vérification effectué par l'AC**
    - **Classe 1 : simple vérification de l'adresse mail**
    - **Classe 2 : adresse mail et identité du titulaire**
    - **Classe 3 : adresse mail, identité et entreprise du titulaire**
  - **En entreprise, on peut aussi utiliser une PKI (infrastructure à clés publiques) interne qui jouera le rôle d'une AC locale**

Fonctions d'une PKI

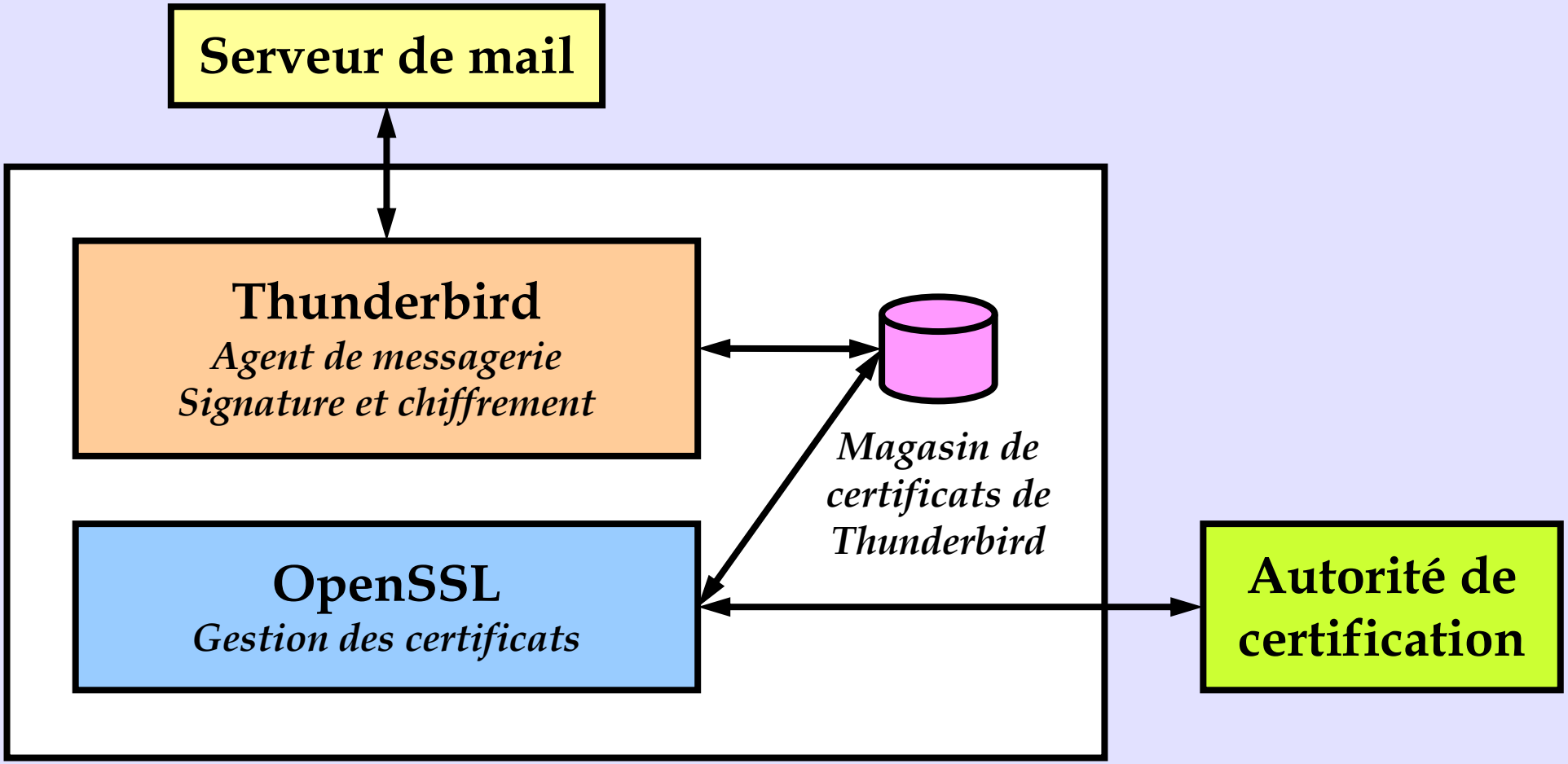
- **Générer les paires de clés des personnels de l'entreprise**
- **Certifier les clés publiques des personnels (fonction d'AC)**
  - **La PKI dispose de sa propre paire de clés**
  - **Les clés publiques des personnels sont signées avec la clé privée de la PKI**



Fonctions d'une PKI

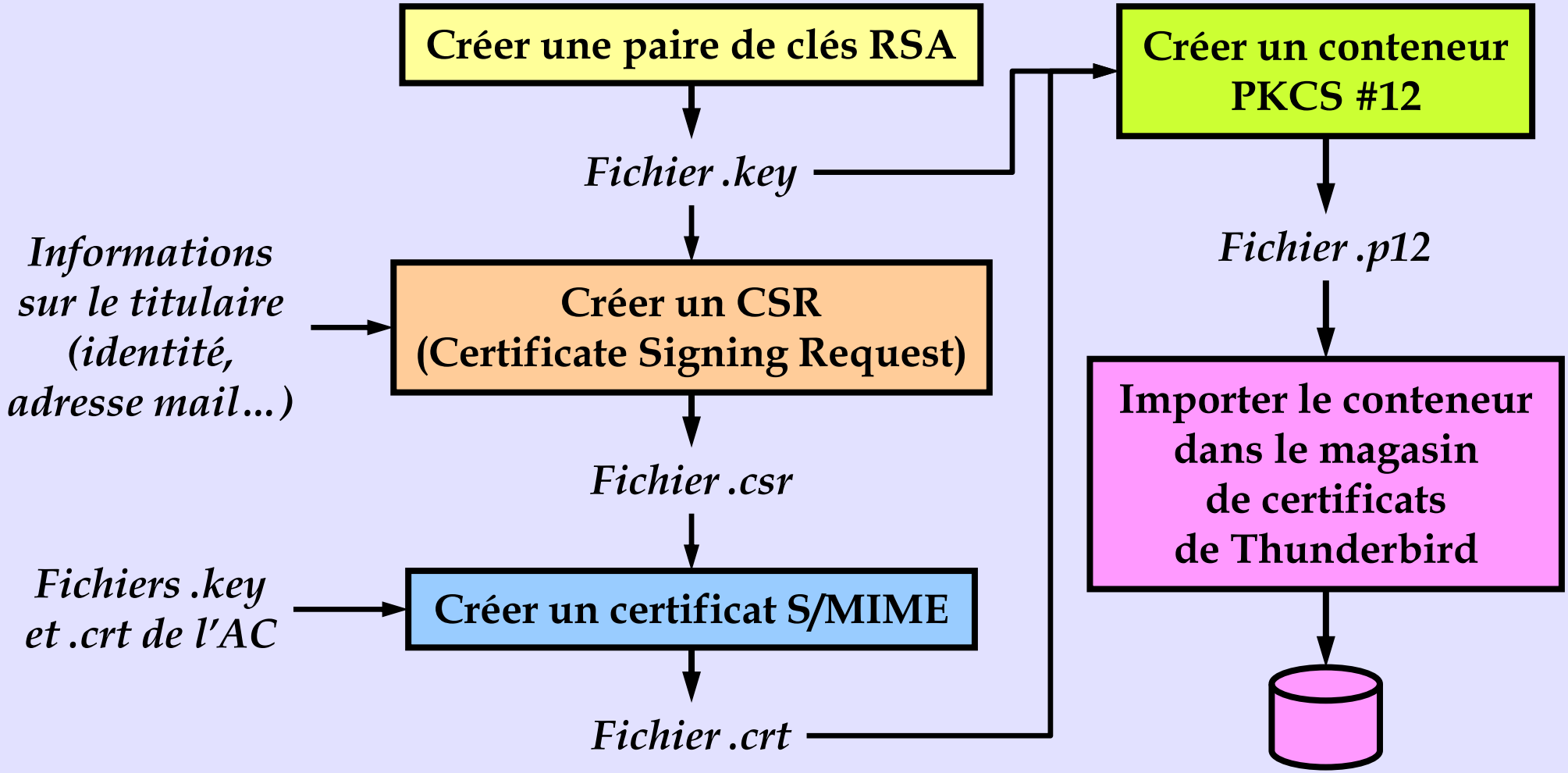
- **Stocker les paires de clés et les certificats émis (fonction de serveur de clés)**
  - **Les clés doivent être conservées même après leur expiration (pourquoi ?)**
- **Déployer les clés et les certificats vers les postes clients**
  - **Par exemple avec Active Directory**
- **Surveiller les dates d'expiration et régénérer les clés et les certificats au moment de leur expiration**

Logiciels S/MIME utilisés dans le TP



Mise en œuvre de S/MIME

Créer des certificats S/MIME



Mise en œuvre de S/MIME

Terminal

- Placez-vous dans le répertoire « `S-MIME` » :
  `cd S-MIME`
- Ce répertoire contient les fichiers de l'AC que vous utiliserez plus tard
- Il contient aussi un fichier « `Commandes-OpenSSL.txt` » avec la liste des commandes à utiliser dans la suite
- Ouvrez le fichier « `Commandes-OpenSSL.txt` » avec le gestionnaire de fichiers

Créer sa paire de clés S/MIME

Terminal

- Créez une clé privée RSA de 3072 bits pour votre certificat S/MIME :
  `openssl genrsa -aes256 -out smime.key 3072`
- Vous devrez entrer un mot de passe protégeant votre clé privée
- La clé privée RSA sera chiffrée avec AES256 en utilisant ce mot de passe
- Vérifiez qu'un fichier « `smime.key` » a été créé

Afficher les composants de sa clé privée

Terminal

- **Affichez les composants de votre clé privée RSA :**
  `openssl rsa -text -in smime.key -noout`
- **Vous devrez entrer votre mot de passe pour déverrouiller votre clé privée**

Afficher les composants de sa clé privée


```
$ openssl rsa -text -in smime.key -noout
Enter pass phrase for smime.key:
Private-Key: (3072 bit, 2 primes)
modulus:
    00:d8:85:5d:dc:05:e2:3f:ae:e8:27:a4:51:9a:17: [...]
publicExponent: 65537 (0x10001)
privateExponent:
    34:f0:a6:fa:5d:15:ec:ac:3f:67:31:ee:21:d7:0b: [...]
prime1:
    00:f7:6a:5f:20:33:9e:eb:b2:bf:1f:32:1d:53:d6: [...]
prime2:
    00:e0:08:94:45:b7:2f:e4:13:ca:9a:f2:e3:dc:52: [...]
exponent1:
    4a:eb:3d:f4:dd:4c:c1:28:76:31:37:16:a4:5d:88: [...]
exponent2:
    11:1f:76:bd:b1:57:9e:b6:08:89:39:41:43:28:a5: [...]
coefficient:
    00:a2:d0:3c:2a:63:5d:51:1a:45:f2:22:3b:db:17: [...]
```

Afficher les composants de sa clé privée

- **L'algorithme RSA utilise deux grands nombres premiers p et q : prime1 et prime2**
- **Le module est le produit des deux nombres premiers n=p·q : modulus**
- **L'exposant public est un nombre e premier avec (p-1)(q-1) : publicExponent**
- **L'exposant privé est l'inverse de e modulo (p-1)(q-1) : privateExponent**
- **Les paramètres exponent1, exponent2 et coefficient sont des valeurs intermédiaires qui interviennent dans les calculs**

Créer un CSR

Terminal

- **Pour obtenir un certificat S/MIME de la part de l'AC, il faut au préalable créer un CSR (Certificat Signing Request)**
- **Créez un CSR pour votre clé privée :**
  `openssl req -new -key smime.key -out smime.csr`
- **Vous devrez entrer votre mot de passe pour déverrouiller votre clé privée**

Créer un CSR

Terminal

- **Le certificat sera associé à un DN (Distinguished Name)**
- **Entrez les éléments suivants pour votre DN :**
  Country Name : `FR`
  Organization Name : `Societe.com`
  Common Name : *`Prénom Nom`*
  Email Address : *`prenom.nom@telecom-sudparis.eu`*
  Autres champs : entrez un caractère point « `.` » pour indiquer l'absence de valeur

Créer un CSR

Terminal

- **Vous pouvez utiliser d'autres valeurs pour ces champs, SAUF pour l'adresse mail qui doit être obligatoirement la vôtre, sinon Thunderbird ne pourra pas utiliser votre certificat S/MIME par la suite**
- **Vérifiez qu'un fichier « `smime.csr` » a été créé**

Créer un CSR


```
$ openssl req -new -key smime.key -out smime.csr
Enter pass phrase for smime.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Societe.com
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:Patrick Maigron
Email Address []:patrick.maigron@telecom-sudparis.eu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Afficher le CSR

Terminal

- **Affichez le CSR que vous venez de créer :**
  `openssl req -text -in smime.csr -noout`
- **Le CSR contient votre DN (Subject), les composants de votre clé publique RSA (Modulus et Exponent), ainsi qu'une signature de ces éléments avec votre clé privée RSA**

Afficher le CSR


```
$ openssl req -text -in smime.csr -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = FR, O = Societe.com, CN = Patrick Maigron,
          emailAddress = patrick.maigron@telecom-sudparis.eu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (3072 bit)
                Modulus:
                    00:d8:85:5d:dc:05:e2:3f:ae:e8:27:a4:51:9a:17: [...]
                Exponent: 65537 (0x10001)
        Attributes:
            (none)
            Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        9f:57:67:83:f8:a4:d0:df:29:aa:a5:5d:1c:14:52:ec:af:b1: [...]
```

Récupérer les fichiers de l'AC

Terminal

- La prochaine étape est de transmettre votre CSR à l'AC afin que celle-ci génère votre certificat
- Dans ce TP, vous allez générer vous-même votre certificat en jouant le rôle de l'AC
- Les fichiers nécessaires à la génération du certificat se trouvent dans le répertoire « `S-MIME` » :
  - `ca.key` : clé privée de l'AC
  - `ca.crt` : certificat de l'AC

Créer son certificat S/MIME

Terminal

- Créez votre certificat signé par l'AC à partir du CSR :
  `openssl x509 -req -days 365 -in smime.csr -CA ca.crt -CAkey ca.key -set_serial` ***numéro*** `-out smime.crt`
- Chaque étudiant doit utiliser un numéro de série différent
- Ce certificat sera valable pendant un an
- Vous devrez entrer le mot de passe de la CA qui vous sera communiqué pendant le TP
- Vérifiez qu'un fichier « `smime.crt` » a été créé

Afficher le certificat S/MIME

Terminal

- Affichez le certificat S/MIME que vous venez de créer :
  `openssl x509 -text -in smime.crt -noout`
- Le certificat contient le numéro de série, le DN de l'AC (Issuer), l'intervalle de validité, votre propre DN (Subject), les composants de votre clé publique RSA (Modulus et Exponent), ainsi qu'une signature de ces éléments avec la clé privée de l'AC

Afficher le certificat S/MIME


```
$ openssl x509 -text -in smime.crt -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = FR, O = Societe.com, CN = Societe.com Certificate Authority
        Validity
            Not Before: Aug 26 13:05:09 2024 GMT
            Not After : Aug 26 13:05:09 2025 GMT
        Subject: C = FR, O = Societe.com, CN = Patrick Maigron,
          emailAddress = patrick.maigron@telecom-sudparis.eu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (3072 bit)
                Modulus:
                    00:d8:85:5d:dc:05:e2:3f:ae:e8:27:a4:51:9a:17: [...]
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        d1:c1:23:ba:46:e4:0c:53:2a:df:f4:b8:7b:8d:ea:39:bf:94: [...]
```

Format PKCS #12

- **PKCS (Public-Key Cryptography Standards) est une famille de standards de la société RSA**
- **Le format PKCS #12 est un conteneur permettant de stocker plusieurs éléments cryptographiques**
- **Il est souvent utilisé pour stocker la clé privée et le certificat associé (ou une chaîne de certificats)**
- **Il peut être protégé par un mot de passe**
- **Il permet ensuite d'importer la clé privée et le certificat dans un navigateur web ou dans un agent de mail**

Exporter clé privée et certificat en PKCS #12

Terminal

- Exportez votre clé privée et votre certificat S/MIME au format PKCS #12 :
  ```
  openssl pkcs12 -export -in smime.crt
   -inkey smime.key -out smime.p12
  ```
- Vous devrez entrer votre mot de passe pour déverrouiller votre clé privée, puis un nouveau mot de passe qui servira à protéger le fichier PKCS #12 (deux fois)
- Vérifiez qu'un fichier « `smime.p12` » a été créé

Importer clés et certificats dans le magasin

Thunderbird

- **Importez votre clé privée et votre certificat S/MIME au format PKCS #12 dans le magasin de certificats de Thunderbird :**
  Édition / Paramètres
  Onglet « Vie privée et sécurité », paragraphe « Certificats » en bas, bouton « Gérer les certificats… »
  Onglet « Vos certificats », bouton « Importer… »
- **Sélectionnez le fichier PKCS #12 créé précédemment**
- **Vous devrez entrer le mot de passe du fichier PKCS #12**

Importer clés et certificats dans le magasin

Thunderbird

- **Effectuez un double-clic sur votre certificat S/MIME**
- **Observez les éléments contenus dans ce certificat : nom du sujet, nom de l'émetteur, dates de validité, informations sur la clé publique, numéro de série et empreintes numériques**
- **Votre certificat n'est pas utilisable pour le moment car le magasin de certificats ne contient pas le certificat de l'AC**

Importer clés et certificats dans le magasin

Thunderbird

- Importez le certificat de l'AC dans le magasin de certificats de Thunderbird :
  Onglet « Autorités », bouton « Importer… »
- Sélectionnez le fichier « `ca.crt` »
- Cochez l'option « Confirmer cette AC pour identifier les utilisateurs de courrier » et validez
- Fermez puis réouvrez le magasin de certificats
- Vérifiez que le certificat de l'AC apparaît dans le magasin de certificats et affichez son contenu (sous « Societe.com »)

Configurer Thunderbird

Thunderbird

- **Configurez les certificats S/MIME à utiliser :**
  Édition / Paramètres des comptes
  Onglet « Chiffrement de bout en bout »
  Paragraphe « S/MIME »
  Certificat personnel pour la signature numérique :
  bouton « Sélectionner un certificat… »
- **Sélectionnez votre certificat S/MIME**
- **Acceptez le même certificat S/MIME pour le chiffrement**

S'envoyer un mail signé et/ou chiffré

Thunderbird

- **Envoyez à vous-même un mail signé en choisissant la technologie de chiffrement S/MIME au lieu de OpenPGP**
- **Lisez le mail reçu et cliquez sur le bouton « S/MIME » à droite pour afficher les informations de sécurité**
- **Envoyez ensuite à vous-même un mail chiffré et affichez les informations de sécurité S/MIME**

Envoyer un mail signé et/ou chiffré

Thunderbird

- **Envoyez à votre interlocuteur un mail signé**
- **Lisez le mail signé reçu de votre interlocuteur**
- **Le certificat S/MIME de l'émetteur du mail est inclus automatiquement dans les mails signés**
- **Vérifiez que le certificat de votre interlocuteur apparaît dans votre magasin de certificats, dans l'onglet « Personnes » (sous « Societe.com »)**
- **Maintenant que vous possédez le certificat de votre interlocuteur, envoyez-lui un mail chiffré**

La révocation des certificats S/MIME

- **Il existe principalement deux manières de gérer la révocation des certificats**
  - **Les CRL (Certificate Revocation Lists) : l'AC gère une liste de certificats révoqués, le client mail interroge régulièrement l'AC afin d'obtenir la liste à jour des certificats révoqués et avant d'utiliser un certificat, il vérifie qu'il n'est pas dans cette liste**
  - **Les serveurs OCSP (Online Certificate Status Protocol) : avant d'utiliser un certificat, le client mail interroge le serveur OCSP de l'AC pour savoir si ce certificat a été révoqué**
  - **Les URL des CRL et des serveurs OCSP sont indiquées dans les certificats délivrés par l'AC**

Fermer la machine virtuelle

Machine hôte

- **Fermez la fenêtre de la machine virtuelle : Fichier / Fermer…**
- **Sélectionnez « Éteindre la machine » et « Restaurer l'instantané actuel Initial », puis validez**
- **En procédant de cette manière, la VM est restaurée dans son état d'origine et votre mot de passe de messagerie ne sera pas conservé**