Sécurité des systèmes d'information

Extrait

“So cyberspace is real. And so are the risks that come with it.”

La cybermenace est l'un des plus sérieux défis auxquels nous soyons confrontés en tant que nation

Mai 2009.

Barack Obama

Président des Etats-Unis

Introduction

- Puisque le SI devient vital pour les entreprises, tout ce qui le menace est potentiellement mortel.
- Ces **menaces** peuvent être très diverses : atteinte à la disponibilité des systèmes et des données, destruction, corruption ou falsification de données, espionnage, vol ou usage illicite de ressources, usage d'un système compromis pour attaquer d'autres sources.
- Les menaces exploitent les **vulnérabilités** et engendrent des **risques** qui eux-mêmes peuvent être générateurs de coûts humains et financiers : perte de confidentialité de donnés sensibles, indisponibilité des infrastructures, paralysie des processus, etc.

Introduction

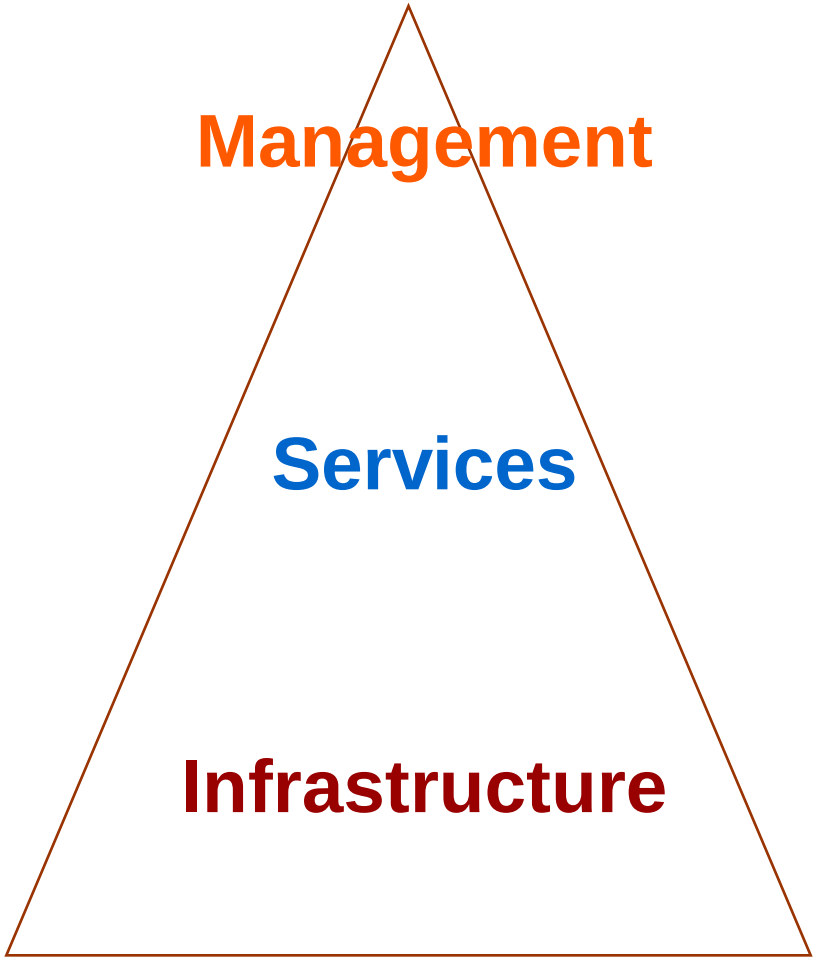
- L'activité industrielle et commerciale est par nature risquée. Certains risques, endogènes, sont dans la nature même du business : développer un nouveau produit, choisir une stratégie de prix, s'engager avec un partenaire.
- D'autres sont exogènes et ne sont que facteurs de perturbation pour le bon déroulement des affaires : panne d'un équipement, mauvaises conditions météo, incendie, inondation, acte terroriste, ..
- L'effet de tels évènements est accentué par les nouvelles pratiques de gestion qui privilégient l'interdépendance et la minimisation des sécurités spatiales (stocks) et temporelles (délais) : production « just-in-time », supply chain aux flux tendus, ...

Introduction

- Ces réductions ont été rendues possibles par la capacité à disposer d'information accessibles en permanence et actualisées en temps réel.
- La fiabilité du Système d'Information est donc devenue un élément clef.
- Ce système est composé d'éléments physiques matériels et humains ainsi que d'éléments logiques, donc de composants vulnérables aux dangers que nous évoquions plus haut.

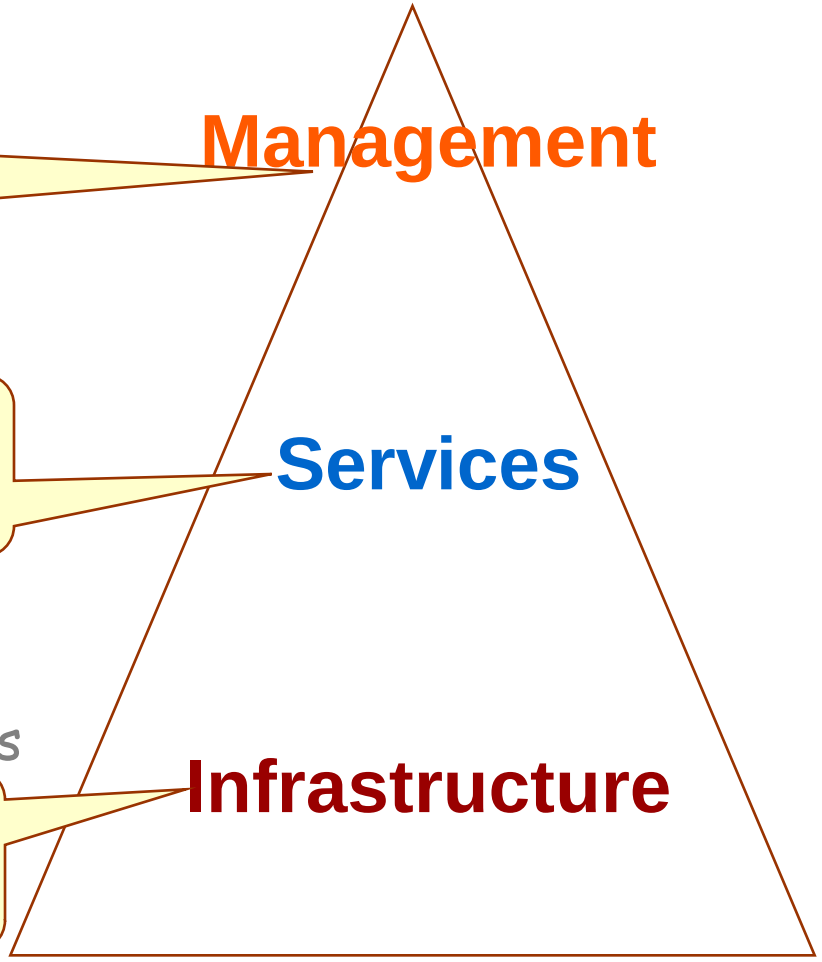
Un découpage en trois niveaux

- ✓ Piloter l'ensemble
- ✓ Organiser ces fonctions en un ensemble cohérent de services
- ✓ Mettre en place les moyens techniques nécessaires pour assurer les fonctions de collecte, stockage, traitement et communication des informations nécessaires à la bonne marche de l'organisation.



Situer le souci de sécurité

- ✓ ***Sensibiliser les individus à la sécurité***
- ✓ ***Sécurité logique des processus***
- ✓ Mettre en place les moyens techniques pour assurer les fonctions
  Sécurité physique des installations
  l'organisation.



Objectifs généraux

Ce module a pour objectif de sensibiliser les informaticiens et les utilisateurs à la problématique de la sécurité des systèmes d'information.

Objectifs pédagogiques

- A la fin de la formation, chaque participant devra :
  - avoir recensé les principaux risques pesant sur le bon fonctionnement d'un système d'information ;
  - avoir identifié les différents modes d'actions envisageables pour réduire les risques, atténuer leur impact et remédier à leurs conséquences.

Agenda

- A. Les principes et les enjeux
  - C01 Aspects et enjeux de la sécurité
  - C02 Enjeux économiques et modes d'action
  - C03 Plan de secours et plan de continuité des activités
  - C04 Sécurité et commerce électronique. Sécurité et banque
- B. Les méthodes et les outils
  - C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse.
  - C06 Architectures de sécurité
  - C07 Renforcer la sécurité des réseaux et des systèmes
  - C08 Renforcer la sécurité des accès et des contrôle d'identités
  - C09 Renforcer la sécurité des applications et des services
  - C10 Renforcer la sécurité des dispositifs mobiles
  - C11 Evaluer la sécurité
  - C12 Manager les risques dans les projets SI
- C. Bilan et perspectives

Agenda

- ***A. Les principes et les enjeux***
  - ***C01 Aspects et enjeux de la sécurité***
  - ***C02 Enjeux économiques et modes d'action***
  - ***C03 Plan de secours et plan de continuité des activités***
  - ***C04 Sécurité et commerce électronique. Sécurité et banque***
- ***B. Les méthodes et les outils***
  - ***C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse.***
  - ***C06 Architectures de sécurité***
  - ***C07 Renforcer la sécurité des réseaux et des systèmes***
  - ***C08 Renforcer la sécurité des accès et des contrôle d'identités***
  - ***C09 Renforcer la sécurité des applications et des services***
  - ***C10 Renforcer la sécurité des dispositifs mobiles***
  - ***C11 Evaluer la sécurité***
  - ***C12 Manager les risques dans les projets SI***
- ***C. Bilan et perspectives***

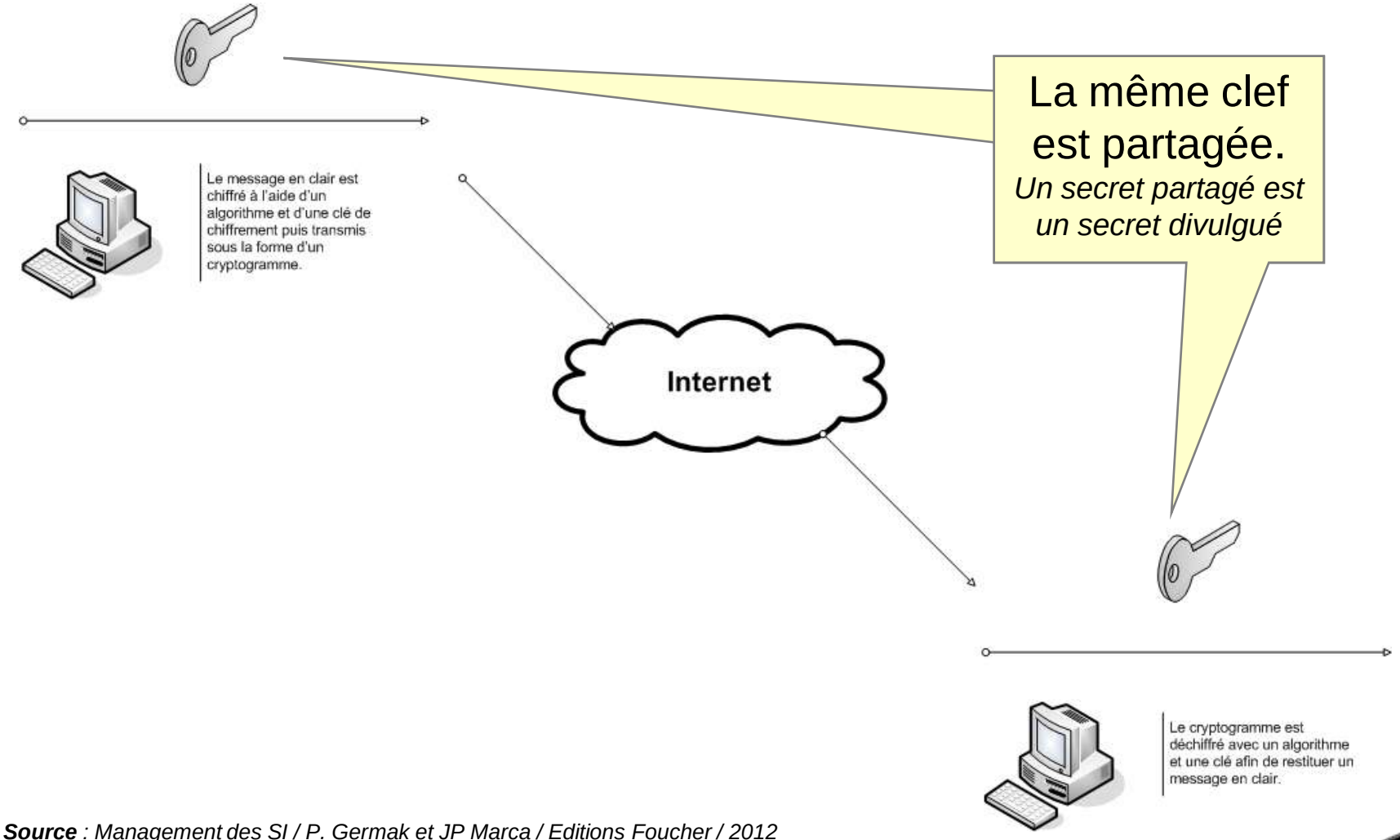
Plan

- **B. Les méthodes et les outils**
  - **Architectures de sécurité**
    - **Chiffrement à clef privée.**
    - Chiffrement à clef publique.
    - Algorithmes de chiffrage.
    - PGP et GnuPG
    - Mise en place d'une architecture PKI. Certification et enregistrement.

Chiffrement à clef privée

- Les algorithmes **à clef privée sont** aussi appelés algorithmes symétriques.
- En effet, lorsque l'on chiffre une information à l'aide d'un algorithme symétrique avec une clef secrète, le destinataire utilisera la même clef secrète pour déchiffrer.
- Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clef privée auparavant, par courrier, par téléphone ou lors d'un entretien privé.
- Les deux utilisateurs utilisent cette même clef pour chiffrer et déchiffrer un message.

Chiffrement à clef privée



***Source** : Management des SI / P. Germak et JP Marca / Editions Foucher / 2012*

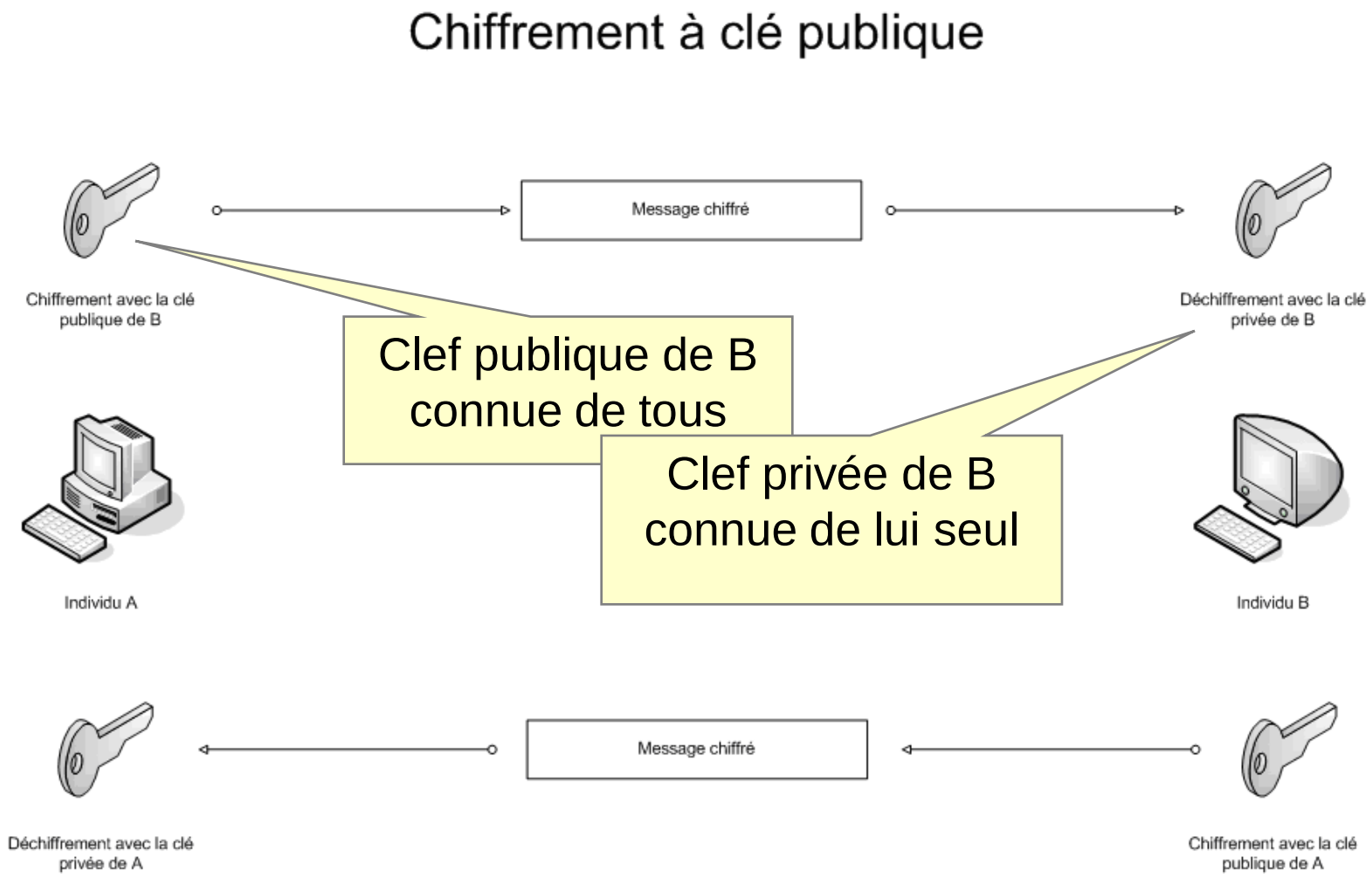
Plan

- ***B. Les méthodes et les outils***
  - ***Architectures de sécurité***
    - *Chiffrement à clef privée.*
    - ***Chiffrement à clef publique.***
    - *Algorithmes de chiffrage.*
    - *PGP et GnuPG*
    - *Mise en place d'une architecture PKI. Certification et enregistrement.*

Chiffrement à clef publique

- La cryptographie **à clef publique** a été inventée par Whitfield Diffie et Martin Hetlman en 1976 pour éviter ce problème d'échange de clef secrète préalable.
- Les algorithmes à clef publique, appelés algorithmes asymétriques, utilisent la clef publique (connue de tous) du destinataire, qui sera à priori le seul à pouvoir le déchiffrer à l'aide de sa clef privée (connue de lui seul).
- Une fois un message envoyé chiffré avec la clef publique du destinataire, nul autre que lui ne peut le déchiffrer, pas même l'expéditeur.

Chiffrement à clef publique



***Source** : Management des SI / P. Germak et JP Marca / Editions Foucher / 2012*

Chiffrement à clef publique

- Outre la confidentialité, ce système assure aussi le principe de non-répudiation.
- La non-répudiation doit reposer dans une preuve de la signature, détenue par le destinataire du document signé, vérifiable par un tiers, inaltérable par l'émetteur signataire.
- Pour conférer cette qualité à sa signature, il suffit que l'émetteur la chiffre avec sa clef privée.
- Le destinataire la déchiffre avec la clef publique du signataire.
- La réussite du déchiffrement apporte la preuve que la signature est authentique.
- Si la signature est constituée par un ***condensat*** du message (résumé numérique obtenu par un algorithme de condensation type *MD5* ou *SHA*), on garantit en plus l'intégrité du message.

Plan

- **B. Les méthodes et les outils**
  - **Architectures de sécurité**
    - Chiffrement à clef privée.
    - Chiffrement à clef publique.
    - **Algorithmes de chiffrage.**
    - PGP et GnuPG
    - Mise en place d'une architecture PKI. Certification et enregistrement.

Algorithmes de chiffrage

A(C)

M → C

B(D)

C → M

- Le message M est transformé en C via un algorithme *A* utilisant une clef de chiffrage C.
- Le message chiffré C est retransformé en M via un algorithme *B* utilisant une clef de déchiffrage D.
- La sécurité ne doit pas dépendre du secret des algorithmes, *A* et *B* mais uniquement du secret des clefs C et D.
- Le code doit être très difficile à casser en partant uniquement des messages cryptés
- Le code doit être très difficile à casser même si l'on dispose d'un échantillon de messages et des messages cryptés correspondants .

RSA

- Le plus célèbre des algorithmes à clef publique, ***RSA***, est dû à Ron ***R***ivest, Adi ***S***hamir et Leonard ***A***dleman du MIT.
- Les clefs sont constituées de la façon suivante :
  1. Choisir deux (grands) nombres premiers p et q.
  2. Calculer $n=p*q$: les opérations s'effectueront modulo n.
  3. Calculer $\varphi(n)=(p-1)(q-1)$.
  4. Choisir un entier e inférieur à $\varphi(n)$ et premier avec $\varphi(n)$: c'est l'exposant de la clef publique.
  5. Calculer l'inverse d de e pour la multiplication modulo $\varphi(n)$ (il existe et est unique puisque e et $\varphi(n)$ sont premiers entre eux : calcul par l'algorithme d'Euclide). L'entier d est l'exposant de la clef privée.
- La clef publique se compose de l'entier n et de l'exposant e, connus de tous.
- La clef privée est l'exposant d qui doit être tenu secret.

RSA

- Voici comment fonctionnent le codage et le décodage :
  - Le message à transmettre est d'abord transformé en un entier (par exemple par concaténation des codes ascii des caractères qui le composent).
  - On note *m* cet entier qui est censé être inférieur à *n*.
  - Le codage le transforme en $c=m^e \text{ modulo } n$.
  - Pour décoder, il faut connaître *d* et calculer $c^d \text{ modulo } n$.
  - On retrouve *m*.
- Évidemment, quelqu'un qui connaît *n* peut théoriquement retrouver ses deux facteurs premiers *p* et *q* et donc recalculer les éléments de la clef privée.
- La sécurité du système repose sur le fait que la décomposition d'un nombre en produit de facteurs premiers est très coûteuse en temps de calcul : il est virtuellement impossible de décomposer un nombre produit de deux très grands facteurs premiers.
- Cela n'empêche pas les utilisateurs de changer assez souvent de clef par mesure de sécurité.

AES

- ***Advanced Encryption Standard*** ou ***AES*** (soit « standard de chiffrement avancé »), aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique.
- Rappelons que *RSA* est un algorithme de chiffrement asymétrique (ou à clef publique).
- Chiffrement déchiffrement se font avec une seule clef AES, alors qu'on doit utiliser 2 clefs séparées (une clef publique et une clef privée) en RSA.
- La force d'une clef 128-bits AES est approximativement equivalente à une clef 2600-bits RSA mais les deux algorithmes ont une finalité différente :
  - Pour chiffrer ses propres sauvegardes : AES.
  - Pour chiffrer des échanges avec des tiers : RSA
- AES est devenu le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis.
- Il a été également approuvé par la NSA (*National Security Agency*) pour les informations top secrètes.

Algorithmes de chiffrage

- Le chiffre de Vigenere, considéré comme incassable au milieu du XIX siècle, a été a été cassé par le major prussien Friedrich Kasiski en 1863.
- L'algorithme du sac à dos (algorithme de Hellman, Merkle et Diffie) proposé comme une solution à clef publique a été rejeté en quelques années.
- Le DES, algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clefs de 56 bits a été déclassifié en 1999.
- RSA doit utiliser des produits de deux nombres premiers de plus en plus grands, pour garder toujours une longueur d' avance face à la puissance de calcul croissante des ordinateurs qui permet d'explorer toutes les combinaisons dans un temps raisonnable.
- Si un mathématicien découvrait une technique permettant de factoriser sans effort un nombre de n'importe quelle longueur, RSA serait facilement « cassable ».
- L'architecture et la longueur des clefs de AES (128, 192 et 256) sont suffisantes pour protéger des documents classifiés jusqu'au niveau « SECRET ».
- Le niveau « TOP SECRET » nécessite des clefs de 192 ou 256 bits.
- L'AES n'a pour l'instant pas été cassé et la recherche exhaustive (« force brute ») demeure la seule solution (2^{128} opérations pour une clef de 128 bits)
- **Mais le chiffrement absolu n'existe pas.**

Plan

- **B. Les méthodes et les outils**
  - **Architectures de sécurité**
    - Chiffrement à clef privée.
    - Chiffrement à clef publique.
    - Algorithmes de chiffrage.
    - **PGP et GnuPG**
    - Mise en place d'une architecture PKI. Certification et enregistrement.

PGP

- "***Pretty Good Privacy***" (en anglais : "Plutôt bonne intimité") est un logiciel de cryptographie renforcée qui est bien adapté à l'utilisation sur Internet.
- PGP est gratuit, facile d'utilisation, et disponible en français.
- PGP a été créé en 1991 par Philip Zimmermann, un informaticien américain.
- Ayant diffusé son logiciel sur Internet, il a été poursuivi par le gouvernement américain pour trafic d'armes (car la cryptographie est considérée là-bas comme une "arme" interdite d'exportation).
- PGP, utilise à la fois les clefs symétriques ("clef de session" de 128 bits) et les clefs asymétriques ("clef publique" de 512 à 2048 ou 4096 bits qui permet de crypter la clef de session).

PGP

- Lorsqu'un utilisateur chiffre un texte avec PGP, les données sont d'abord compressées.
- Cette compression des données permet de réduire le temps de transmission par tout moyen de communication, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.
- La plupart des cryptanalystes exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement.
- La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse.
- Ensuite, l'opération de chiffrement se fait principalement en deux étapes :
  - PGP crée une clef secrète IDEA de manière aléatoire, et chiffre les données avec cette clef
  - PGP crypte la clef secrète IDEA et la transmet au moyen de la clef RSA publique du destinataire.
- L'opération de déchiffrement se fait également en deux étapes :
  - PGP déchiffre la clef secrète IDEA au moyen de la clef RSA privée.
  - PGP déchiffre les données avec la clef secrète IDEA précédemment obtenue.

PGP et GnuPG

PGP

Le texte en clair est crypté avec la clef de session

Emetteur A

Texte chiffré

La clef de session est cryptée avec la clef publique de B

Message crypté = texte chiffré + clef de session cryptée

Récepteur B

Envoi via réseau

Réseau

Clef de session à durée de vie limitée

Clef publique de B

Clef privée de B

Clef privée de B utilisée pour déchiffrer la clef de session

Clef de session utilisée pour déchiffrer le texte transmis

Texte chiffré

Texte en clair d'origine

PGP

- Cette méthode de chiffrement associe la facilité d'utilisation du cryptage de clef publique à la vitesse du cryptage conventionnel.
- Le chiffrement conventionnel symétrique est environ 1000 fois plus rapide que les algorithmes de chiffrement asymétriques à clef publique, mais n'est pas adapté aux échanges.
- Le chiffrement à clef publique résoud le problème de la distribution des clefs.
- Utilisées conjointement, ces deux méthodes améliorent la performance et la gestion des clefs, sans pour autant compromettre la sécurité.

GnuPG

- ***GnuPG*** (ou *GPG*, de l'anglais ***GNU Privacy Guard***) est l'implémentation *GNU* du standard OpenPGP défini dans la RFC 48802.
- Le projet est initié à la fin des années 1990 dans le but de remplacer la suite PGP par une alternative en logiciel libre.
- Il est distribué selon les termes de la *GNU GPL.*
- Le risque principal de *GnuPG*, comme pour tous les procédés de chiffrement à clef publique, est que la clef privée doit être enregistrée quelque part.
- Si c'est sur une clef *USB* que l'on garde avec soi, les risques de perte, de vol ou de copie existent. Si elle se trouve sur le disque dur d'un ordinateur, on est alors exposé aux risques classiques du piratage. Notons qu'une phrase (ou mot) de passe, optionnelle mais pouvant protéger la clef privée, limite alors les risques.
- Depuis sa version 2.0, *GnuPG* peut être installé sur une carte à puce. La clef privée est alors protégée par le code *PIN* de la carte, ce qui permet d'en améliorer sensiblement la confidentialité.

Plan

- ***B. Les méthodes et les outils***
  - ***Architectures de sécurité***
    - *Chiffrement à clef privée.*
    - *Chiffrement à clef publique.*
    - *Algorithmes de chiffrage.*
    - *PGP et GnuPG*
    - ***Mise en place d'une architecture PKI. Certification et enregistrement.***

Retour sur le chiffrement à clef publique

- Le chiffrement des données est complexe à mettre en œuvre.
- Il nécessite des boîtiers spécialisés et/ou des logiciels de chiffrement à toutes les extrémités du réseau, ainsi que des échanges de clefs.
- Ces échanges reposent sur une infrastructure technique et des procédures d'exploitation et d'administration qui permettent de délivrer et de stocker des certificats numériques de manière sécurisée (Infrastructure à clef publique ou **PKI – Public Key Infrastructure**).
- Un certificat électronique est un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.
- Ces certificats permettent d'accéder aux clefs publiques.
- Problème : Peut-on faire confiance à l'organisme qui distribue les clefs ?

Certificats numériques

- Comment Juliette peut-elle être certaine que la clé publique qu'elle reçoit est bien celle de Roméo et vice-versa ?
- La solution est de passer par un **tiers de confiance** reconnu par tous deux, et qui va leur fournir des **certificats**.
- Un certificat est un document électronique (un fichier) qui atteste qu'une clé publique est bien liée à une organisation ou une personne.
- Il ne contient que des éléments publics.
- Sa diffusion ne pose donc évidemment aucun problème de sécurité.
- Le tiers de confiance est un organisme indépendant qui atteste de la véracité, via sa signature électronique, des informations contenues dans le certificat.
- Un tel organisme est désigné sous le nom d'**Autorité de Certification** (**AC**).

Certificats numériques

- Un certificat contient généralement :
  - la clé publique de l'entité (utilisateur, serveur);
  - un nom et d'autres champs permettant d'identifier cette entité (société, service) ;
  - les dates de début et de fin de validité du certificat ;
  - un numéro de série ;
  - le nom de l'organisation qui contresigne le certificat ;
  - la signature des données du certificat par l'Autorité de Certification (AC).

Certificats numériques

- Le Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique le définit ainsi : « ***Certificat électronique*** *: un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire* » ;

- Avec cette autre précision : « *les données de vérification de signature électronique sont les éléments, tels que des clefs cryptographiques publiques, utilisés pour vérifier la signature électronique*. »

- On le voit au travers de ces définitions, le **certificat numérique** est l'instrument qui va remplir un double rôle : permettre le chiffrement avec des clefs et attester l'identité du signataire.

- Un autre point à noter est l'indication de « clefs cryptographiques publiques », ce qui veut dire que système de chiffrement doit impérativement être asymétrique.

Certificats numériques

- L'usage du certificat électronique de signature permet :
  - l'authentification de l'émetteur : confirmation que le document est bien envoyé par la personne identifiée ;
  - l'intégrité des données transmises : cohérence entre les données envoyées et celles reçues ;
  - la non-répudiation des messages : ('ensemble de ces fonctionnalités offre l'assurance que ni la transaction elle-même, ni les informations transmises lors de cette transaction ne pourront être contestées ultérieurement par l'émetteur.
- L'usage du certificat électronique de chiffrement permet :
  - la confidentialité : protection contre toute tentation de piratage et préservation de la confidentialité des échanges.

Certificats numériques

- Lors d'une authentification à clef publique, le récepteur du message doit connaître la clef publique de son interlocuteur.
- Mais il doit pouvoir en vérifier la validité auprès d'un tiers de confiance, dans la mesure où une usurpation d'identité serait possible.
- Le vérificateur doit s'adresser à une autorité de certification, une instance fiable et indépendante chargée de gérer les clefs publiques des interlocuteurs de confiance.
- L'autorité de certification procure un certificat numérique contenant le nom de l'interlocuteur et la clef publique de confiance.
- La norme gérant les certificats numériques est appelée X.509 de l'Union Internationale des Télécommunications.

Fonctionnement d'une architecture PKI

- **L'entité finale** ou entité d'extrémité (EE : End Entity) : l'utilisateur ou le système qui est le sujet du certificat
- **L'autorité d'enregistrement** (AE/RA) : exécute les vérifications d'usage sur l'identité de l'utilisateur. Fait la demande de certificat et donne le certificat signé à l'utilisateur.
- **L'autorité de certification** (AC/CA) : signe les demandes de certificat (CSR) et les listes de révocation (CRL)
- **L'autorité de dépôt** (AD/Repository) : stocke les certificats numériques et les listes de révocation (CRL).
- **L'autorité de séquestre** (AS/Key Escrow) : stocke de façon sécurisées les clefs de chiffrement qui ont été engendrées par l'IGC, pour pouvoir les restaurer le cas échéant.

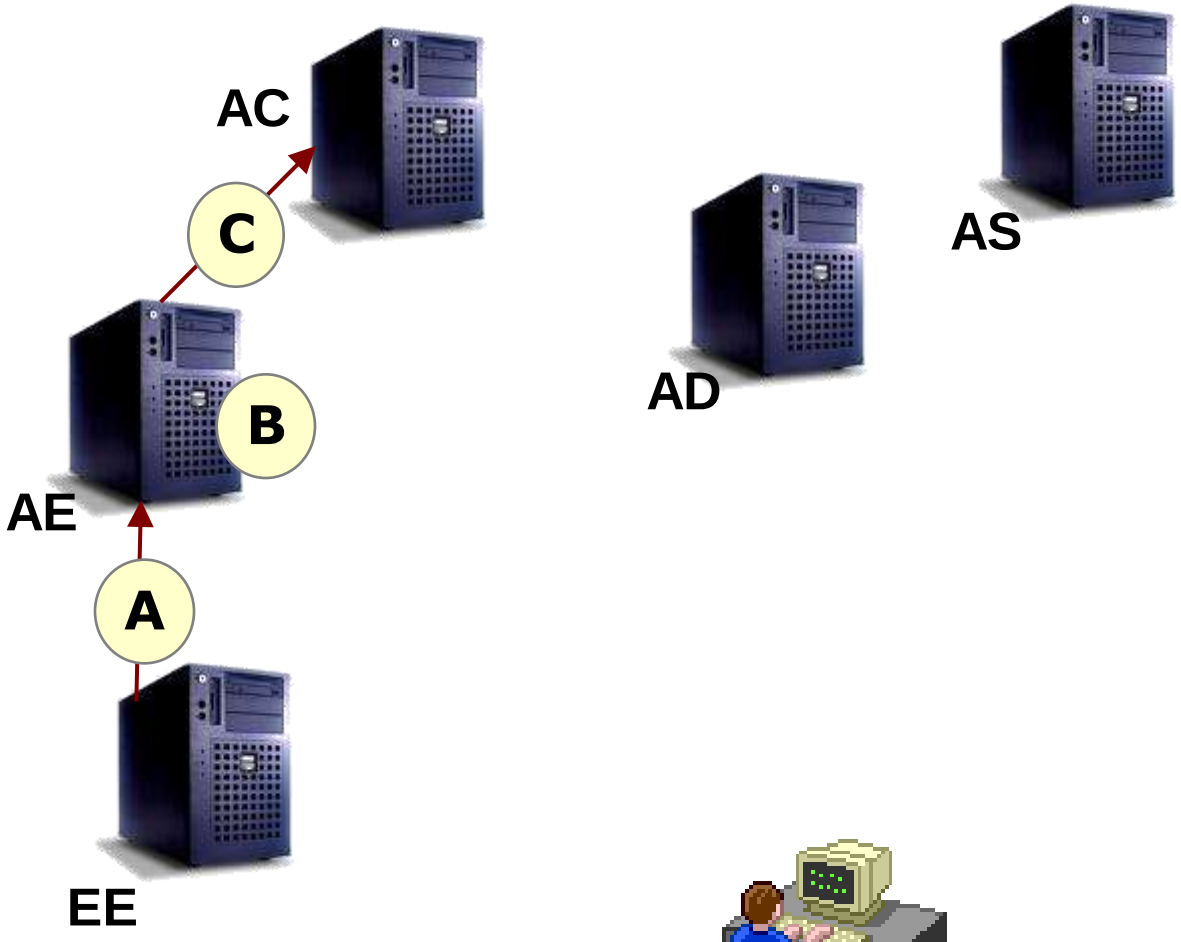
Fonctionnement d'une architecture PKI

A. Le serveur EE a fait une demande de certificat à AE en remplissant un formulaire et en fournissant les justificatifs.

B. EE ne requiert pas directement son certificat auprès de l'AC, de même qu'un citoyen s'adresse à la mairie pour obtenir un passeport qui sera délivré par la Préfecture.
L'AE d'une PKI vérifie le lien entre le sujet et sa clé publique.
L'AE peut être :

- une agence commerciale d'une banque ou d'un opérateur ;
- le correspondant RH d'un employé d'une entreprise ;
- un simple site web, à condition que l'AE dispose de moyens complémentaires pour vérifier l'identité du sujet : adresse e-mail, authentifiant et mots de passe transmis par une voie tierce telle que le courrier postal…

C. AE transmet la demande (CSR) à AC.



Fonctionnement d'une architecture PKI

D. L'AC est l'entité morale qui signera et délivrera les certificats en son nom,
Par exemple :

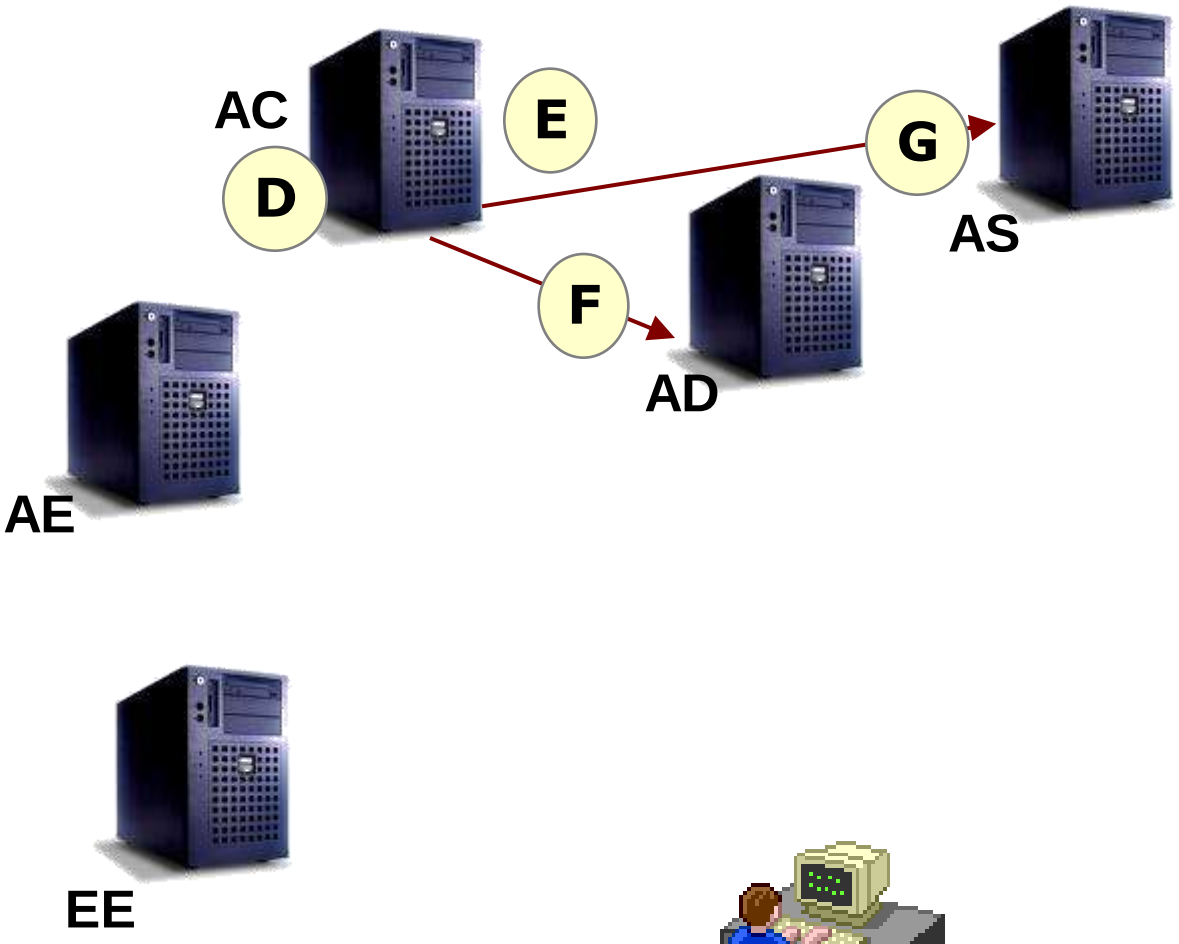
- une grande entreprise pour délivrer des certificats à ses employés ;
- un opérateur de services (Globalsign, Symante0verisign) pour ses clients ;
- une banque pour ses clients particuliers ou entreprises ;
- une administration.

L'AC veille à l'application de la politique de certification adoptée pour la PKI.
La paire de clefs peut être générée en divers lieux (EE, AE ou AC selon le cas).
Considérons le cas le plus sécurisé (AC).

E. AC crée une clef privée et le certificat (qui contient la clef publique)

F. AC transmet le certificat à AD

G AC transmet la clef privée à AS

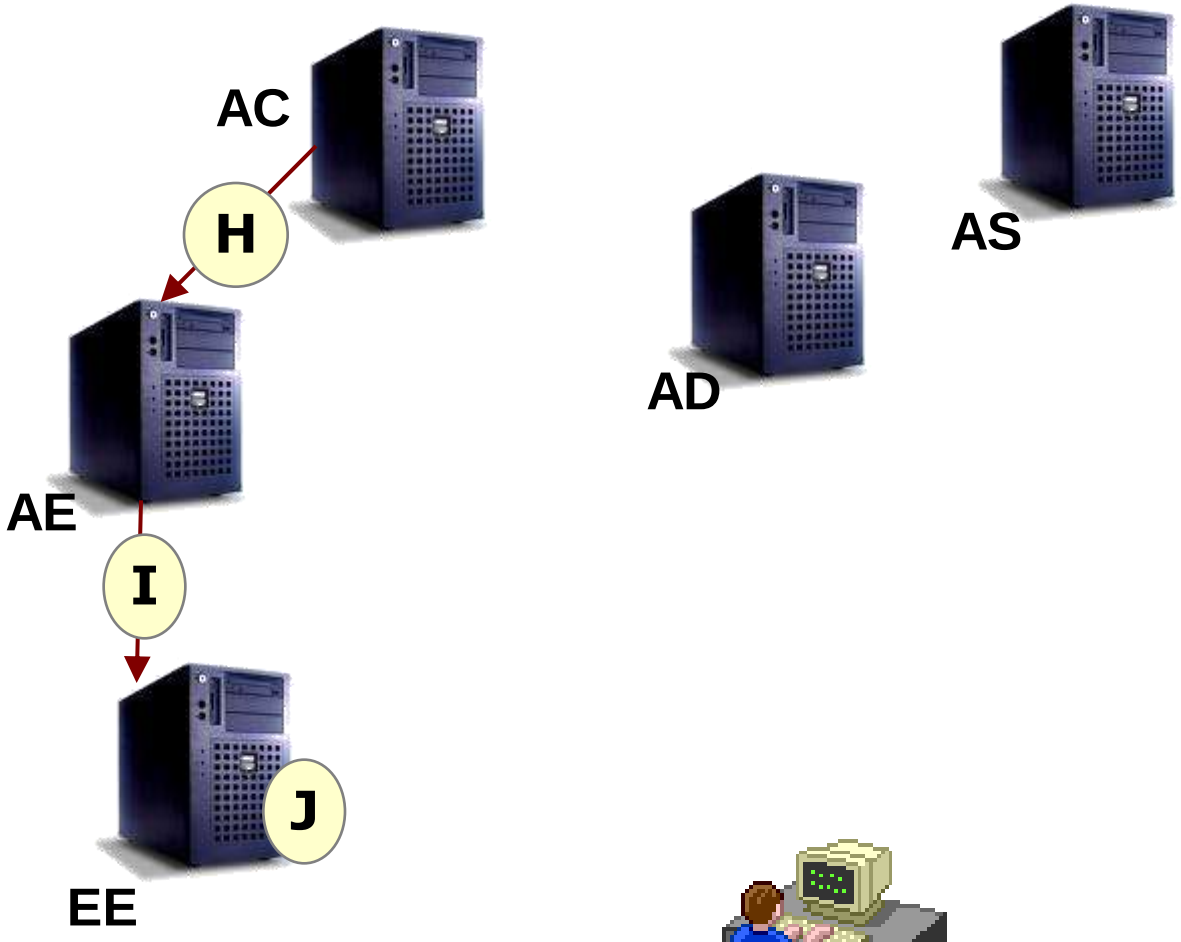


Fonctionnement d'une architecture PKI

H. AC transmet le certificat signé (CRT) ainsi que la clef privée à AE.

I. AE retransmet le certificat signé (CRT) ainsi que la clef privée à AEE

J. EE est en mesure de communiquer ce certificat (et la clef publique associée) à toute entité utilisatrice qui en fait la demande.



Architectures de sécurité

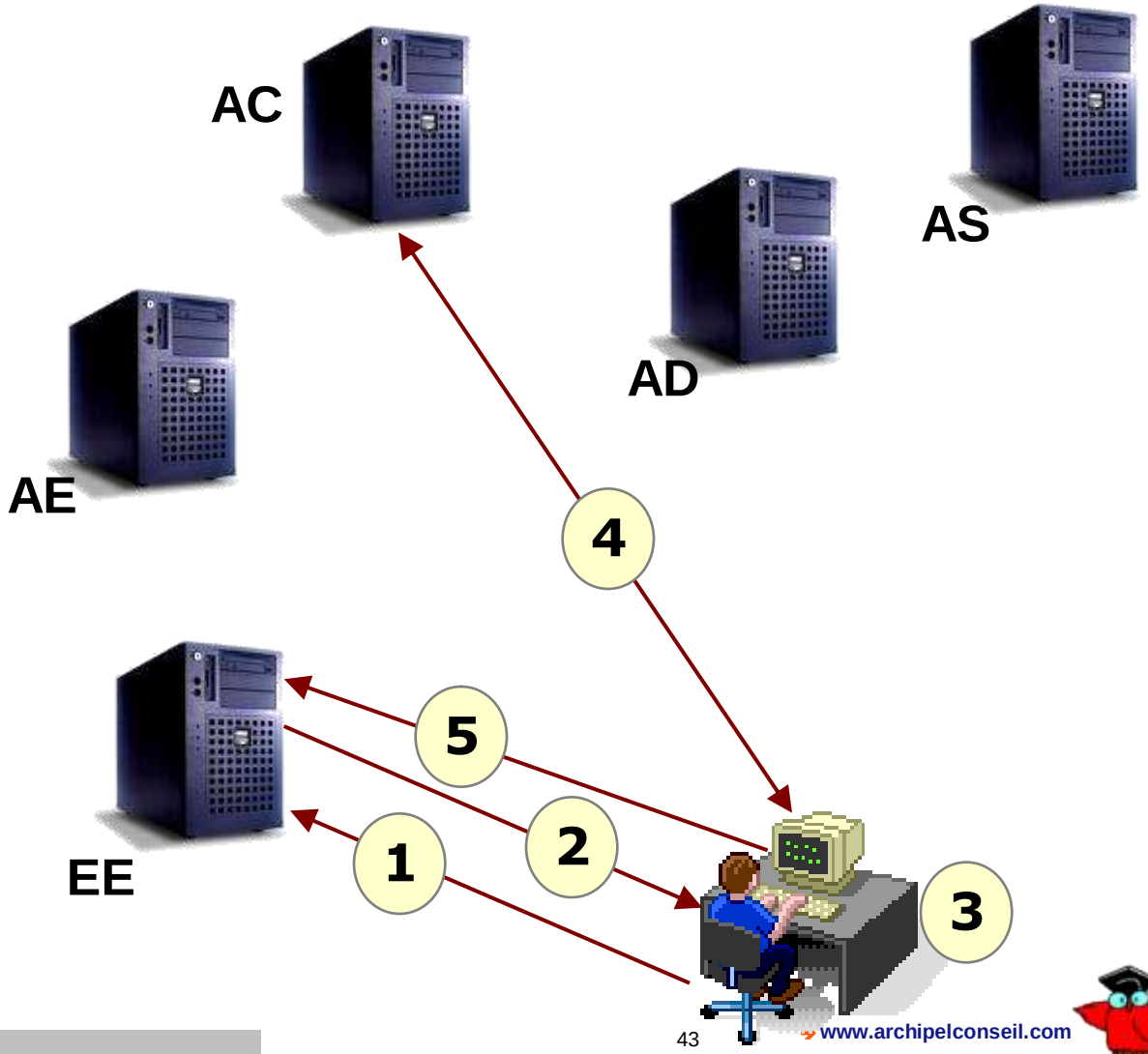
Fonctionnement d'une architecture PKI

1. L'utilisateur demande au serveur de prouver son identité

2. Le serveur EE montre un certificat signé

3. L'utilisateur vérifie le certificat du site :
   - il regarde la date de validité du certificat;
   - Il vérifie que l'adresse du serveur correspond bien à l'adresse indiquée par le certificat;
   - Il fait confiance à l'AC (4) concernée quant à la vérification des informations associées au site lors de la création du certificat;
   - Il vérifie que le certificat a bien été scellé par cette AC :
     - Il utilise la clef publique de l'AC pour déchiffrer l'empreinte cryptée du certificat,
     - Il calcule l'empreinte du certificat,
     - Il compare les empreintes.

5. Il accède au serveur EE



Fonctionnement d'une architecture PKI

Signature d'un certificat par une Autorité de certification

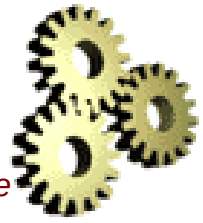
Certificat

Nom : J. Surfe

Clef publique :

Autorité de certification : BP

Signature de l'autorité de certification :



Signature

Clef privée de l'autorité de certification

Vérification de la validité du certificat par l'utilisateur

Certificat

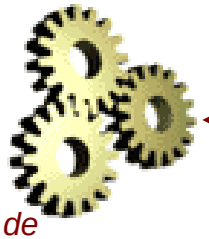
Nom : J. Surfe

Clef publique :

Autorité de certification : BP

Signature de l'autorité de certification :

Clef publique de l'autorité de certification



Vérification de signature

OK ?

But d'une architecture PKI

- Les infrastructures à clefs publiques (ICP ou PKI) assurent une prise en charge intégrale de la gestion des clefs.
- Objectif : Conformément à ce que nous avons dit dans les diapositives précédentes, délivrer des certificat numériques qui offrent les garanties suivantes lors des transactions électroniques :
  - Confidentialité : seul le destinataire légitime du message pourra le lire
  - Authentification : l'identité de l 'émetteur est garantie
  - Intégrité : Garantie qu'un message expédié n'a pas altéré accidentellement ou intentionnellement ;
  - Non-répudiation : l'auteur du message ne peut pas renier son message.

But d'une architecture PKI

- **Sécurisation des échanges Web**
- Aujourd'hui, les certificats les plus couramment utilisés sont les certificats serveurs, c'est-à-dire des certificats garantissant le lien entre un nom de serveur (www.ma-banque.fr) et sa clé publique.
- Un tel certificat est utilisé pour que des utilisateurs puissent authentifier le serveur avant de lui envoyer des informations confidentielles.
- Ils permettent en outre de mettre en place, via un protocole adéquat (SSLv3, TLS) une connexion sécurisée (chiffrée) permettant de sécuriser les échanges.
- Ce type de certificat est largement utilisé par les sites d'achat en ligne.
- Des serveurs peuvent également utiliser des certificats pour s'authentifier mutuellement et échanger des données de manière sécurisée.
- Quand des certificats utilisateurs sont déployés, d'autres usages sont possibles.

But d'une architecture PKI

- **Authentification forte des utilisateurs**
- Les certificats utilisateurs permettent l'authentification des utilisateurs, aussi bien en local, que pour un accès distant ou nomade en faisant appel aux techniques de RPV.
- Ils peuvent être utilisés pour autoriser l'accès à un réseau filaire ou Wi-Fi (802.1X).
- La sécurité de l'authentification ainsi obtenue est largement supérieure au couple classique identifiant / mot de passe, procédé très répandu mais qui n'offre qu'une faible sécurité.
- L'usage de la PKI permet une authentification multi-facteurs :
  - quelque chose que l'utilisateur possède : la carte à puce dans laquelle est stockée la clé privée ;
  - quelque chose que l'utilisateur connaît : le code PIN nécessaire pour débloquer l'usage de la clé secrète par la carte.
- A noter que l'authentification est la plupart du temps mutuelle puisque le serveur fournit également un certificat qui permet au client de l'authentifier.

But d'une architecture PKI

- **Messagerie sécurisée**
- **Horodatage**
- **Télé-procédures administratives**
- Au-delà de ces utilisations classiques, l'apparition en France des télé-procédures administratives a offert aux PKI une nouvelle occasion de montrer leur intérêt.
- Les télé-procédures les plus connues étaient TéléTVA pour la déclaration de la TVA et TéléIR pour la déclaration des revenus, regroupées aujourd'hui dans le portail fiscal www.impots.gouv.fr (12 millions de déclarations IR et 85% des impôts pour les professionnels)
- Le certificat avait alors deux fonctions :
  - d'une part permettre au serveur de l'administration d'authentifier le télédéclarant, comme si le déclarant présentait sa pièce d'identité avant d'accéder à son dossier fiscal ;
  - d'autre part permettre au déclarant de signer électroniquement sa déclaration, comme il le faisait auparavant avec une signature manuscrite.

Architecture PKI

- les infrastructures à clefs publiques nécessitent une approche organisationnelle très attentive à la formation des utilisateurs et à leur appropriation des mécanismes de protection de la confidentialité des échanges.
- Ce type d'infrastructure peut servir de base robuste à un déploiement de la signature électronique dans une organisation ou un réseau.
- Malheureusement, du fait de l'absence de normes, ce sont des solutions propriétaires, incomplètes et peu compatibles entre elles, ce qui limite leur adoption.

Quelques offres commerciales d'infrastructure à clef publique

Editeur	Offre
Baltimore Technologies	Unicert
Entrust Technologies	Entrust/PKI
Keynectis	PKI/offre initiale
TrustyCom	TrustyKey
Sagem	Xelios

Offre open source openPKI

Editeur	Offre
www.openssl.org	openssl