



Cryptographie quantique

Mercredi 15 mars 2006

- Préambule
- Principe d'incertitude d'Heisenberg
- Polarisation de photons
- Cryptographie quantique
- Caractéristiques
- Usages
- Limitations

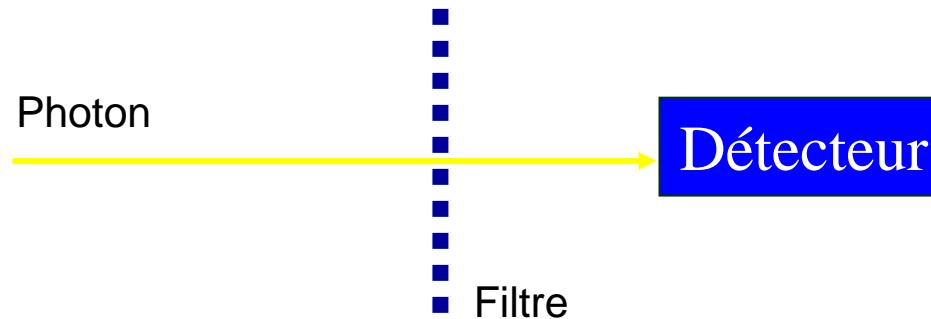
- La présentation n'a pas pour vocation d'exposer toute la théorie de la cryptographie quantique.
- La présentation ne nécessite pas de connaissance particulière de physique quantique.

- A l'échelle normale, il est possible d'effectuer une mesure sans modifier réellement le fonctionnement d'un système.
 - En pratique, toute mesure est perturbatrice mais l'effet peut être rendu négligeable.
- A l'échelle atomique, certaines mesures perturbent le système.
 - Le fait de mesure est donc détectable.

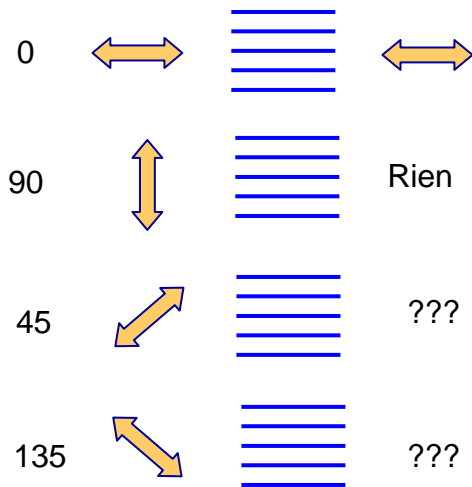
- Le principe d'incertitude affirme que certaines quantités ne peuvent pas être mesurées simultanément.
 - Exemple : Il n'est pas possible de connaître à la fois la position et la quantité de mouvement d'une particule.
- Un état quantique est caractérisé par plusieurs valeurs
 - Impossibilité de connaître toutes ces valeurs
 - La mesure d'une valeur perturbe les autres

- Chaque photon peut être polarisé, c'est-à-dire que l'on impose une direction à son champ électrique. La polarisation est mesurée par un angle qui varie de 0° à 180° .
- Dans le protocole défini par les canadiens CH. Bennett et G. Brassard, la polarisation peut prendre 4 valeurs : 0° , 45° , 90° , 135° .
- Pour les photons polarisés de 0° à 90° , on parle de polarisation rectiligne, pour ceux polarisés de 45° à 135° , de polarisation diagonale :



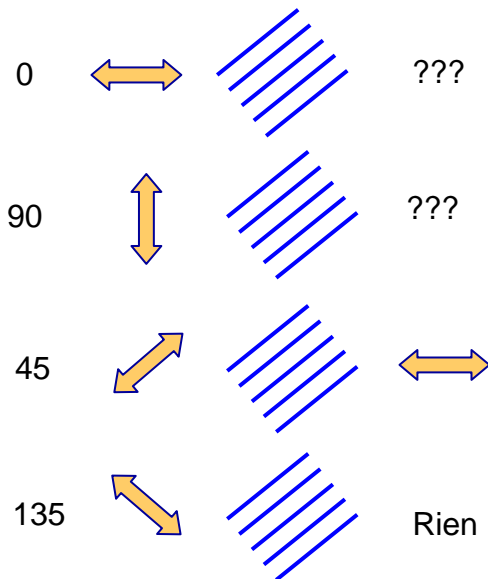


- Pour cela, on utilise :
 - **un filtre polarisant.** Le filtre permet de filtrer les photons en fonction de leur polarisation.
 - **un détecteur de photons.** Le détecteur permet de savoir si un photon a pu passer à travers le filtre.
- Le filtrage n'est pas une mesure, il n'empêche donc pas la détection du photon.



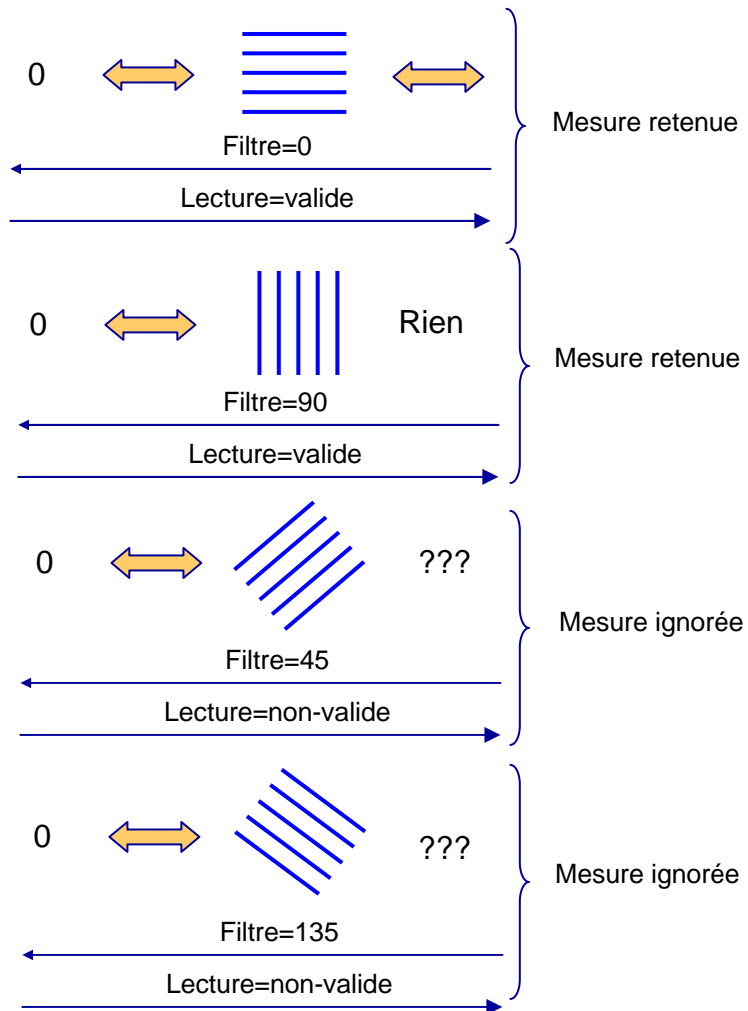
- Si un photon polarisé à 0° rencontre un filtre polarisant orienté à 0° , il traverse ce filtre polarisant et est enregistré par le détecteur placé juste après.
- Si un photon polarisé à 90° rencontre le même filtre, il est immédiatement stoppé, et le détecteur n'enregistre rien.
- Si le photon est polarisé diagonalement (45° ou 135°), une fois sur deux, il traverse le filtre, et une fois sur deux, il est stoppé.
- Si on peut distinguer entre une polarisation à 0° et à 90° , il est impossible de distinguer en même temps entre une polarisation à 45° et à 135° !

Détection de polarisation diagonale



- De la même façon, on peut utiliser un filtre polarisant orienté à 45° : il laisse passer les photons polarisés à 45° , stoppe ceux polarisés à 135° , et se comporte aléatoirement avec ceux à 0° et 90° !

- La transmission de photons polarisée n'est pas suffisante
 - Impossible de savoir si la valeur lue est correcte
- Il faut que l'émetteur indique si la lecture est bonne
- Utilisation d'un canal technique pour :
 - Le récepteur envoie le filtre utilisé
 - L'émetteur indique si avec le filtre utilisé, la valeur lue est correcte (une fois sur deux en moyenne).



- Emission d'un photon polarisé à 0°
- La validité de la détection dépend du filtre
- Principe identique pour les autres valeurs

- Convention :
 - Bit 0 → polarisation à 0° ou 45°
 - Bit 1 → polarisation à 90° ou 135°

Bit à émettre	0	0	1	1	1	0	0
Polarisation du photon	45	0	90	90	135	45	0
Filtre utilisé	45	45	0	0	0	0	0
Détection	Oui	Non	Non	Non	Non	Oui	Oui
Bit reçu	0	1	1	1	1	0	0
Filtre transmis	Diagonal	Diagonal	Droit	Droit	Droit	Droit	Droit
Réponse	OK	KO	OK	OK	KO	KO	OK
Bit retenu	0	X	1	1	X	X	0

- Ajout de bits de contrôle (CRC ou similaire)
- Impossibilité pour un observateur de reproduire les photons avec la bonne polarisation

- La distance de transfert est limitée
 - Réseau fibré :
 - 2002 : 67 km
 - 2004 : ~100 km
 - Espace libre :
 - 1992 : 30 cm
 - 1996 : 1,6 km
 - 2002 : 23,4 km
- Impossibilité de mettre des répéteurs
 - Perturbations
 - Considérés comme des espions

Source : Séminaire d'Introduction à l'Information Quantique (ENST 2004)

- Quelques kbits
- Suffisant pour la transmission d'une clé

- Utilisation pour les échanges de clés
 - Emission de photons avec une polarité aléatoire mais connue par l'émetteur.
- Transfert de OneTimePassword
- Pas d'utilisation réelle pour les transferts de données
 - Trop lent
 - Les données transitent en clair (on sait qu'elles sont interceptées mais trop tard)
- Pas d'authentification intégrée
- Pas de chiffrement de messages
 - Mode connecté obligatoire

- Générateurs/détecteurs non parfaits
 - Erreurs pouvant être assimilées à de l’espionnage
 - Réparation des erreurs en détectant l’espionnage (probabilités)

- Attaque man-in-the-middle
 - Interception du canal technique
 - Le destinataire ne doit faire la demande que lors de la réception du photon
 - Comment être sûr que c’est le bon destinataire ???

- Encore très théorique (même si quelques startup)

- Société de service et éditeur de logiciels spécialisé dans la sécurité logique et les réseaux
- Produits : Gamme Security BOX[®]
- Actionnaire : ARKOON (100%)

- Adresse : 3 place Renaudel
69003 LYON
Tél : 04 78 14 04 10 Fax : 04 78 14 04 11
Web : <http://www.securitybox.net>

- Philippe PERRET
Directeur technique
philippe.perret@msi-sa.fr



Le cryptage de mail et de documents

La cryptologie : une science d'origine millénaire

Cryptographie, cryptanalyse, chiffrement, ... : un peu de vocabulaire

Les différents types de chiffrement, la signature électronique :
intégrité & authentification, les certificats

Contexte de mise en oeuvre

XVI^e siècle avant JC : Le premier document chiffré (XVI^e siècle avant JC) est une tablette d'argile retrouvée en Irak, suppression consonnes et modification orthographe des noms

X^e à VII^e av JC : La technique grecque : chiffrement par transposition, utilisation d'une scytale (bâton de Plutarque) et d'une bande de cuir sur laquelle est inscrit le message ; le déchiffrement nécessite un bâton de même diamètre

200 ans av JC : Les premiers vrais systèmes de cryptographie : chiffrement par substitution. (César : substitution mono alphabétique i.e. décalage lettre dans alphabet ; le carré de Polybe : lettres dans un tableau ; code crypté = coordonnées)

1379 : Gabriel de Lavinde écrit un recueil de codes et clés (nomenclateur), utilisé plusieurs siècles par les diplomates

1467 : Leone Battista Alberti invente le système de substitution polyalphabétique appliqué à l'aide d'un disque : changement d'une lettre par celle d'un autre alphabet avec changement multiple d'alphabet au cours du chiffrement ; puis le surchiffrement codique (chiffrement du texte déjà chiffré) utilisé bien après

1518 : Jean Trithème expose le procédé stéganographique consistant à remplacer chaque lettre du texte par un groupe de mots, le texte crypté ressemblant à un poème ; repris et modifié par Blaise de Vigenère (1586) dont le principe ne sera décrypté qu'en 1854)

1854 : Charles Wheatstone invente le chiffrement de Playfair basée sur une substitution digrammatique (remplacement d'un couple de lettre adjacentes par un autre couple dans une grille qui constitue la clé de chiffrement)

1883 : le hollandais Auguste Kerckhoffs publie un livre sur la cryptologie exposant les règles à respecter pour un bon système cryptographique dont la principale est que la sécurité d'un système de doit pas reposer sur le secret de la méthode de cryptage (toujours vrai aujourd'hui)

1893 : Etienne Bazeries réussit à décrypter, 3 siècles après, les documents de Louis XIV chiffrés par ce qu'on appelle le Grand Chiffre

Seconde guerre mondiale : la machine Enigma, inventée pour les civils (1919) et reprise par les militaires sur le principe de substitution d'une lettre par une autre mais la substitution change d'une lettre à l'autre (au moyen de fiches et de rotors : la position de départ des fiches et des rotors ainsi que l'ordre des rotors constituant la clé de chiffrement => 10^{16} possibilités)

Guerre Amérique – Japon : Philipp Johnston utilise la langue Navajo comme moyen de cryptographie (indéchiffrable pour les étrangers du fait de sa méconnaissance et de sa grammaire très particulière). Problème : les mots usuels de l'armée n'existaient pas en Navajo => création d'une table de correspondance par association d'idée pour la rendre mémorisable (bombardier => buse, bombe => œufs dans la langue navajo). Ainsi « les parleurs de code » (windtalkers) navajo prirent part à la campagne du pacifique.

- Cryptographie : terme générique désignant l'ensemble des techniques permettant de chiffrer (crypter) des messages
- Cryptologie : (science du secret) : science qui étudie les aspects scientifiques de ces techniques : cryptographie et cryptanalyse
- Chiffrement : fait de coder un message de façon à le rendre secret ; réalisé à l'aide d'une clé de chiffrement
- Déchiffrement : opération inverse réalisé à l'aide d'une clé de déchiffrement
- Cryptogramme : message chiffré par opposition au message initial (message en clair)
- Décryptement (décryptage) : fait d'essayer de déchiffrer illégitimement un message (que la clé soit connue ou non) ; lorsque la clé n'est pas connue, on utilisera des techniques de cryptanalyse (crypto-analyse, cassage) pour décrypter le message.

Les différents types de clés symétrique / asymétrique / clé de session

Chiffrement symétrique

(chiffrement à clé secrète)

- Principe :
 - Utilisation de la même clé pour le chiffrement et le déchiffrement
- Algorithmes de chiffrement symétrique :
 - DES, 3DES, AES, Blowfish, Idea
- Avantages :
 - performance de temps de calcul
- Inconvénients :
 - nécessite un échange préalable de la clé (distribution sécurisée), communication avec plusieurs interlocuteurs nécessite autant de clés que de niveau de confidentialité distincts

Chiffrement asymétrique

(chiffrement à clés publiques)

- Principe :
 - Les clés existent par paire : une clé publique (échangée par canal non sécurisé) pour chiffrer, une clé privée pour déchiffrer
- Algorithmes de chiffrement asymétrique :
 - RSA, ElGamal, courbes elliptiques
- Avantages :
 - plus d'échange de la clé (pas de secret en commun)
- Inconvénients :
 - moins efficace en temps de calcul, assurance que la clé publique appartient bien à la personne à qui l'on souhaite communiquer les données chiffrées ?

La clé de session (combiné chiffrement symétrique / asymétrique)

- Principe :
 - Chiffrement symétrique du document ; la clé de chiffrement est générée aléatoirement (clé de session)
 - Chiffrement de la clé de session (asymétrique) avec la clé publique du partenaire

- La signature électronique :
 - Garantir l'authenticité de l'expéditeur
 - Vérifier l'intégrité du message reçu
 - Fonction de non répudiation (expéditeur ne peut nier avoir transmis le message)

- La fonction de hachage
 - Principe :
 - ✓ Obtenir un condensé du message (haché), associant un et un seul haché au texte clair (toute modification entraîne la modification du haché) et à sens unique (impossible de retrouver le texte clair à partir du haché)
 - ✓ le haché est « l'empreinte digitale » du document
 - Les algorithmes de hachage
 - ✓ MD5 (Message Digest)
 - ✓ SHA (Secure Hash Algorithm)

- Vérification de l'intégrité du message
 - Expédition : hachage du message & transmission du document et de son haché
 - Réception : hachage du document reçu, comparaison avec le haché accompagnant le document reçu
 - Si le message ou le haché a été falsifié durant la communication, les 2 empreintes ne correspondront pas

Le hachage permet de vérifier que l'empreinte correspond bien au message reçu mais pas qu'il a été envoyé par celui que l'on croit être l'expéditeur

- Le scellement des données : garantir l'authentification du message
 - Expédition : Le haché est chiffré à l'aide de la clé privée (sceau) de l'expéditeur et transmis (document & haché chiffré) au destinataire
 - Réception : déchiffrement du sceau à l'aide de la clé publique du destinataire, hachage du document reçu et comparaison entre les 2
 - Le mécanisme de création de sceau est appelé scellement

■ Chiffrement asymétrique :

- basé sur le partage d'une clé publique via annuaire LDAP, site WEB, email

Problème : garantie que la clé est celle de l'utilisateur associé ?

■ La réponse : les certificats

- association de la clé publique à une entité (personne, machine, ...) i.e. carte d'identité de la clé publique délivrée par une autorité de certification ou une infrastructure locale PKI
- Structurés (standard X.509 v3) en 2 parties : les informations (CA, propriétaire, email, validité, clé publique & objet d'utilisation, algorithme de chiffrement du certificat) & la signature de l'autorité

■ Principe :

- Certificat est signé par l'autorité (hachage + chiffrement avec clé privée)
- A réception du certificat d'un destinataire ("clé publique"), possibilité de vérifier la validité du certificat via la comparaison entre le hachage du certificat reçu & le déchiffrement de la signature (sceau) de l'autorité à l'aide de sa clé publique

■ Les différents types de certificats

- Certificats signés par une infrastructure locale PKI :
 - ✓ Intéressant pour authentification, protection des échanges internes...
 - ✓ ... et des échanges externes (basé sur la connaissance des tiers dans une relation établie) ; approbation de l'autorité et intégration dans les tiers de confiance (expliquer!)
- Certificats signés par un organisme de certification :
 - ✓ Préférables pour échanges avec des utilisateurs anonymes (cas site WEB sécurisé), valables et plus simples (?) pour authentification et protection des mails
 - ✓ Le certificateur assure que le certificat appartient à l'organisation (utilisateur / organisation) à laquelle il est censé appartenir ; attention cependant à la classe du certificat (classe 1 : généralement anonyme – téléchargement ; classe 2 : vérification identité sur pièce ; classe 3 : vérification identité de visu (présence physique))

■ Les contextes d'utilisation

- Le certificat client (stocké sur le poste de travail ou sur une carte à puce) : authentification auprès d'un ordinateur, protection des mails, ...
- Le certificat serveur : authentification de l'URL, protection des échanges (SSL), authentification du client (souvent non utilisée)
- Le certificat VPN : chiffrement des flux de communication point à point (IPSec)

■ Contexte

– Stratégie :

- ✓ Innovation : produits, procédés de fabrication, approches des marchés
- ✓ Qualité & valorisation de l'image des produits
- ✓ Internationalisation
- ✓ Multiplication des échanges de compétences, tant en interne qu'avec nos partenaires

– Partage & circulation de l'information : gage de performance et d'efficacité ...

– ... si confiance dans cette information : intégrité & confidentialité

■ 2 medium de diffusion de l'information

– Extranet fournisseurs : intégration des fournisseurs de plus en plus en amont du processus innovation

– Mail sécurisé : Échanges quotidiens et plus informels d'informations (externe / interne) : finance, juridique, stratégie, communication & publicité, ...

■ Enjeux majeurs : compétitivité, réglementation, cohésion sociale, ...

■ Solution

– Principes :

- ✓ TCC (UGS), surcouche fonctionnelle de WSS : base documentaire pour partage de documents, conferencing, synchronisation avec les outils R&D (CAO, PLM)
- ✓ Utilisateurs avertis de toute publication via email (lien vers document)
- ✓ Architecture documentaire modélisée (& normalisée) afin de cloisonner l'accès à l'information selon le besoin d'en connaître des utilisateurs (internes & externes)
- ✓ La gestion des droits délégués au plus près de la connaissance des utilisateurs : droits d'administration délégués aux Responsables BE ; droits d'accès délégués aux Chefs de projets

– Sécurité : authentification et confidentialité

- ✓ Mise en oeuvre d'un certificat serveur (Global Sign, CA) : authentification URL et chiffrement SSL 128 bits (mais dépendant du poste client)
- ✓ Authentification utilisateur login/mot de passe : politique de mot de passe & règles contractuelles fournisseurs

■ Bilan et évolution à étudier

- Une solution intuitive et très facilement appréhendée
- Authentification du client (option du sous protocole Handshake du protocole SSL) via la signature du client à l'aide de sa clé privée (certificat client nécessaire)

■ Solution & principes

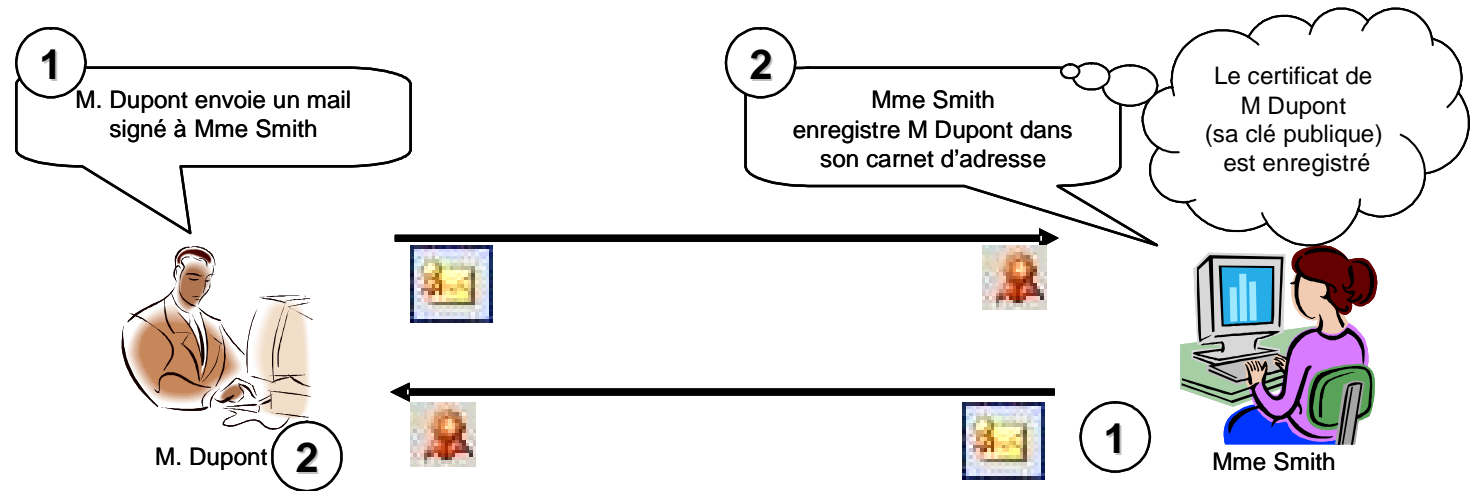
- Serveurs Exchange 5.5 (e/c évolution Exchange 2003) / client Outlook 2003
- Solution standard S/MIME sur le principe du chiffrement des différentes parties du message (mail & PJ), chacune à l'aide d'une clé de session (3DES) ; les clés de session sont chiffrées avec la clé publique du destinataire (RSA)
- Signature pour authentification message via clé privée de l'expéditeur (SHA1)
- Choix de certificats personnels externalisés (GlobalSign, certification authority)

■ Processus d'obtention / renouvellement des certificats

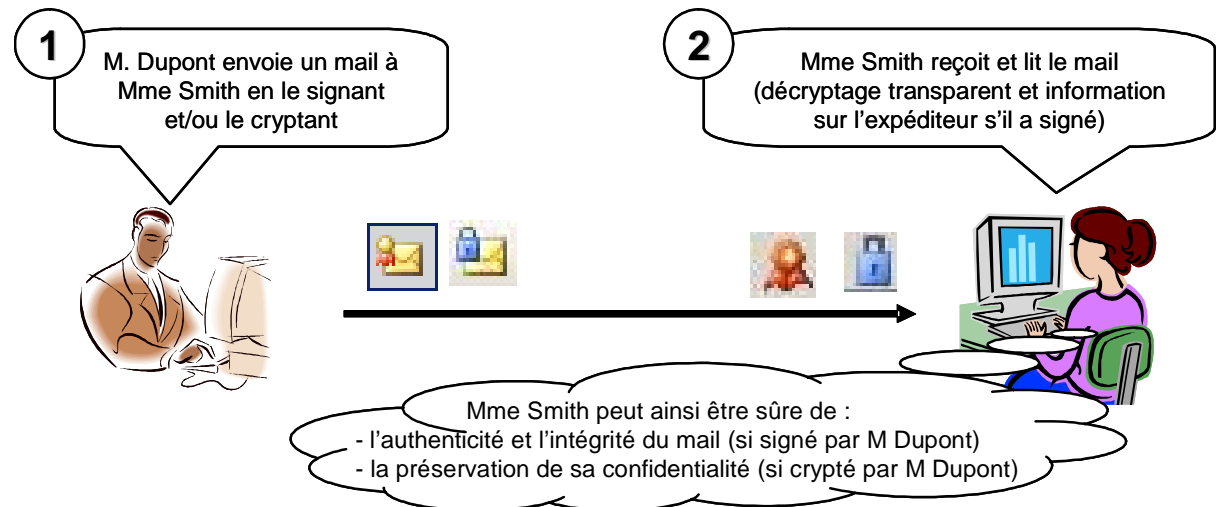
- Administrateur interne (autorité de certification) par délégation de GlobalSign
- Processus :
 1. Utilisateur : signature « subscriber's agreement » et copie passeport
 2. Administrateur interne : demande de certificat de travail (contrôle appartenance au Groupe) et demande de certificat (on line)
 3. Utilisateur : réception d'un mail de GlobalSign et installation du certificat (guide interne d'aide à l'installation)(Renouvellement annuel avec validation administrateur / révocation si départ utilisateur)

■ Initialisation & échanges de mails sécurisés

Etape 1 : la transmission de la clé publique



Etape 2 : la transmission de mails chiffrés



- Un premier retour d'expérience
 - Les freins
 - ✓ s/mime & certificats pas ou mal pris en charge par certains clients de messagerie
 - ✓ Concepts pas forcément aisés à expliquer (clés publiques, chiffrement, signature)
 - ✓ Obtenir des partenaires qu'ils se procurent un certificat (note créée à cet effet)
 - ✓ L'utilisateur doit lui-même gérer ses clés publiques et veiller à sauvegarder sa clé privée (+ procédure de séquestre en cours)
 - ✓ Quelques soucis d'installation des certificats (changement de matériel)
 - Les avantages :
 - ✓ Les actions de sensibilisation créent la demande de la solution
 - ✓ Utilisation quasi transparente pour les utilisateurs
 - ✓ Stockage sécurisé dans les archives de messagerie
- Des solutions complémentaires sans doute nécessaires
 - Containers sécurisés mais manipulations utilisateurs, coûts et...
 - ...une problématique plus forte de réglementation selon les outils / pays (exportation, importation, utilisation) dans un contexte international