Livre blanc

“Sécuriser les échanges d’information par emails ”

BSSI
Conseil & Audit

Octobre 2013

« Sécuriser les échanges d'information par emails »

Par David Isal

Consultant en Sécurité des Systèmes d'Information au sein de l'équipe de BSSI. David intervient sur des missions de gestion des risques notamment dans les domaines réseaux et infrastructures open source.

Synthèse

Ce libre blanc s'adresse aux PME et a pour but de détailler clairement et simplement les risques associés aux échanges de courriels sur Internet, et les moyens cryptographiques pour s'en prémunir. En effet, même si une protection à 100% est impossible à atteindre, utiliser la cryptographie de façon simple et pragmatique permet d'augmenter considérablement le niveau de confiance dans les échanges électroniques.
Après avoir détaillé les risques et les principes de base de la cryptographie, nous verrons comment mettre en place concrètement des solutions de chiffrement des courriels.

Sommaire

1 Introduction 4

2 Comment utiliser la cryptographie pour sécuriser ses échanges d'information ? 6

2.1 Les algorithmes de chiffrement 6

2.1.1 Le chiffrement symétrique 6

2.1.2 Le chiffrement asymétrique 7

2.2 Avantages et limites 9

3 Cas pratique : mettre en place le chiffrement de ses échanges par emails 10

3.1 Projet de mise en place d'un chiffrement symétrique 11

3.1.1 Le choix et la mise en place d'un outil 11

3.1.2 La robustesse des mots de passe 12

3.1.3 Échange de la clé 12

3.2 Projet de mise en place d'un chiffrement asymétrique 13

3.2.1 OpenPGP 13

3.2.2 S/MIME 15

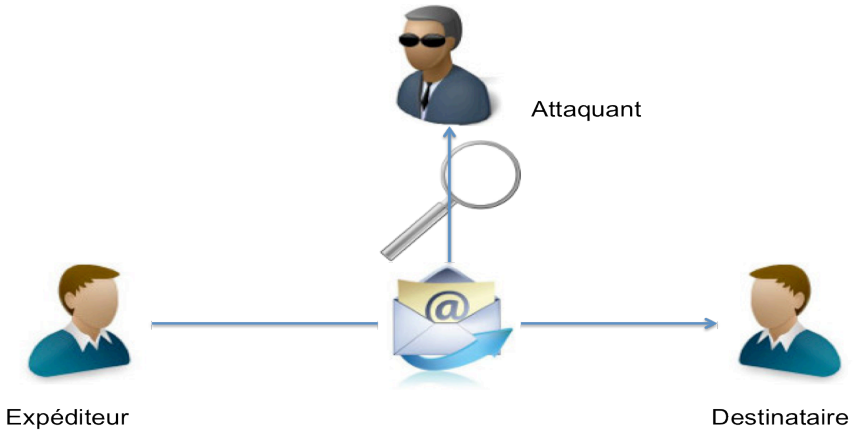
4 Conclusion 18

1 INTRODUCTION

Ce livre blanc s'adresse aux PME et a pour but de montrer en pratique comment sécuriser les échanges emails par Internet. L'envoi de courriels (ou emails) est devenu un acte familier. On en oublie parfois que cette technologie n'est pas sécurisée par défaut. En effet, rien dans la norme de courriels (SMTP) n'est prévu pour sécuriser les échanges entrainant alors différents risques pour les entreprises.

On peut identifier trois catégories de risque :

- ✓ **Perte de confidentialité** : les courriels et pièces jointes associées, quand ils sont envoyés en clair sur Internet, peuvent être facilement lus par des tierces parties. Cela est particulièrement vrai lors de l'envoi d'informations sensibles, documents techniques ou commerciaux.



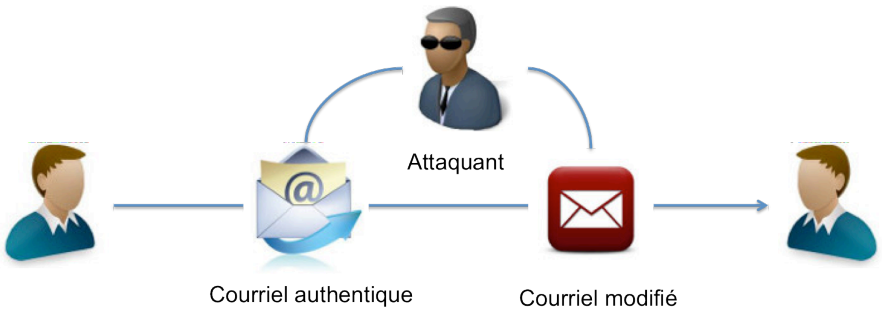
Risque N°1: perte de confidentialité du courriel

- ✓ **Usurpation d'identité** : Un courriel peut être « forgé », c'est à dire fabriqué de toutes pièces, en indiquant une fausse identité pour l'expéditeur. Un attaquant peut alors prendre l'identité d'une personne connue ou inconnue pour déstabiliser l'entreprise.

Risque N°2: usurpation d'identité

- ✓ **Modification du contenu d'un message** : Un courriel peut être intercepté, modifié, puis relayé à son destinataire. Par exemple, il est techniquement

possible d'intercepter un courriel, de modifier le corps du texte ou les pièces jointes (documents Word…) puis de le relayer normalement. Rien ne garantit que le message que l'on reçoit correspond bien à celui qui a été envoyé par son expéditeur.



Risque N°3: perte d'intégrité: modification du contenu d'un message

Ces risques sont réels, et la sensibilisation de tous les acteurs est essentielle. Ainsi les questions pertinentes à se poser sont les suivantes :

- Quel serait l'impact si une information commerciale confidentielle venait à être connue par un de mes concurrents ? (risque de confidentialité)
- Quel serait l'impact si un message envoyé à un de mes partenaires était modifié à mon insu ? (risque d'intégrité)
- Comment établir une relation de confiance avec mes partenaires commerciaux et les rassurer sur l'authenticité de mes messages ? (risque d'authentification)
- Quel est le coût ou le nombre de jours / hommes nécessaires pour mettre en place une solution simple pour garantir la confidentialité de mes échanges ?

La cryptographie permet de répondre de façon sûre et efficace à ces 3 types de risques : confidentialité, intégrité, authentification. Deux modes d'utilisation de la cryptographie existent. La cryptographie symétrique va permettre de garantir l'intégrité et la confidentialité des échanges sur Internet. La cryptographie asymétrique, elle, va permettre de garantir intégrité, confidentialité, et aussi authenticité des messages grâce à la signature électronique.

Nous allons étudier dans une première partie les principes de base de la cryptographie symétrique et asymétrique. Puis nous nous intéresserons à deux cas pratiques : comment protéger ses emails avec de la cryptographie **symétrique** et **asymétrique**. On verra ainsi qu'on peut mettre en place, pour un investissement en temps relativement réduit, des solutions efficaces qui permettent d'augmenter le niveau de confiance des échanges emails.

2 COMMENT UTILISER LA CRYPTOGRAPHIE POUR SECURISER SES ECHANGES D'INFORMATION ?

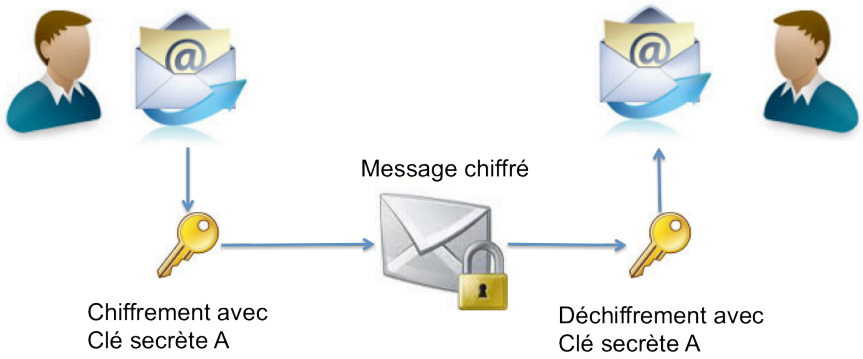
2.1 Les algorithmes de chiffrement

Deux méthodes de chiffrement sont à notre disposition : le chiffrement symétrique et le chiffrement asymétrique. Dans le cas du chiffrement symétrique, on utilise une clé secrète qui est partagée entre les utilisateurs. Dans le cas du chiffrement asymétrique, chaque utilisateur possède une paire de clés, l'une publique, l'autre privée. Il n'y a dans ce cas pas de clé secrète partagée entre les utilisateurs.

2.1.1 Le chiffrement symétrique

La cryptographie symétrique est le moyen le plus simple d'augmenter le niveau de sécurité lors des échanges par courriel. Lors d'un échange par cryptographie symétrique, l'expéditeur et le destinataire partagent une clé secrète. Cette clé va servir au chiffrement du message avant l'envoi, et au déchiffrement du message à sa réception. Cette sécurité simple, mais robuste va permettre de chiffrer des documents confidentiels et de les joindre à un courriel en pièce jointe. Le message du courriel sera en clair et lisible par tous ; mais la pièce jointe sera chiffrée.

Avec le chiffrement symétrique, la confidentialité et l'intégrité des messages sont garanties !



Chiffrement symétrique

Deux algorithmes de chiffrement symétrique sont largement implémentés aujourd'hui : 3DES (triple DES) et AES.

- 3DES est une amélioration de l'ancien algorithme DES. Il est considéré comme plus lent et moins sécurisé qu'AES.

- AES signifie « Advanced Encryption Standard », et cet algorithme a été choisi en 2000 par le NIST américain (National Institute of Standard and Technology) pour servir de référence. C'est aujourd'hui le mécanisme de chiffrement symétrique le plus reconnu, il est donc à privilégier. AES existe en différentes versions, en fonction de la taille de la clé : 128, 192 ou 256 bits. Les implémentations en AES -256 sont à privilégier.

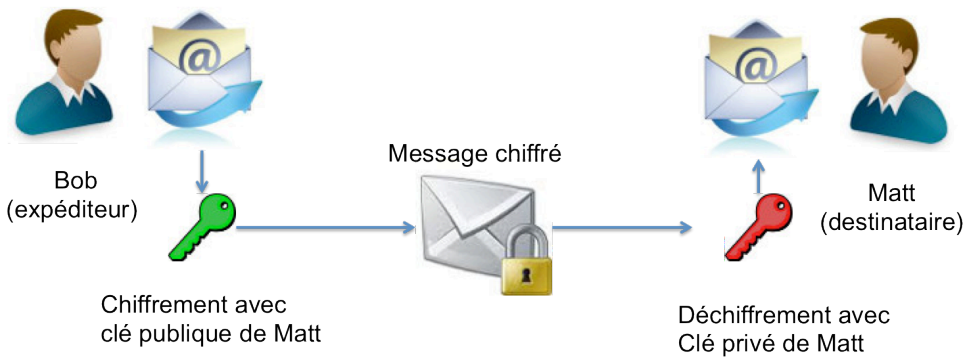
2.1.2 Le chiffrement asymétrique

Avec le chiffrement asymétrique, chaque utilisateur va utiliser une paire de clés (ou bi-clé) : une clé sera publique, l'autre privée. La clé publique peut être mise à disposition de tous sur Internet; tandis que la clé privée doit être tenue secrète. Les deux clés sont liées par des mécanismes cryptographiques, mais il n'est pas possible de déduire la clé privée à partir de la clé publique.

Tout ce qui est chiffré avec la clé publique peut être déchiffré avec la clé privée, et tout ce qui est chiffré avec la clé privée peut être déchiffré avec la clé publique. Cela élimine le problème de l'échange d'une clé secrète entre les utilisateurs.

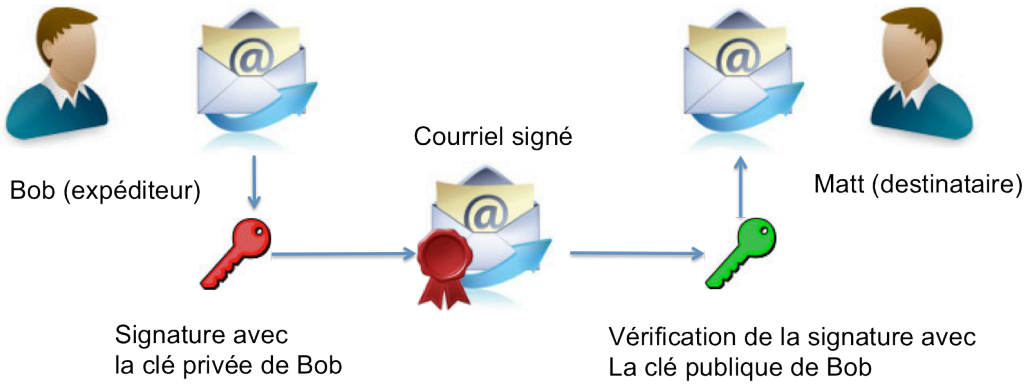
L'algorithme de chiffrement asymétrique le plus connu est appelé RSA, du nom de ses inventeurs Ron Rivest, Adi Shamir et Len Aldeman, qui ont imaginé le principe en 1978.

Chiffrement : l'expéditeur va chiffrer le message à envoyer avec la clé publique du destinataire, disponible sur internet. Le destinataire va déchiffrer le message avec sa clé privée. Le chiffrement garantit la confidentialité et l'intégrité du message.



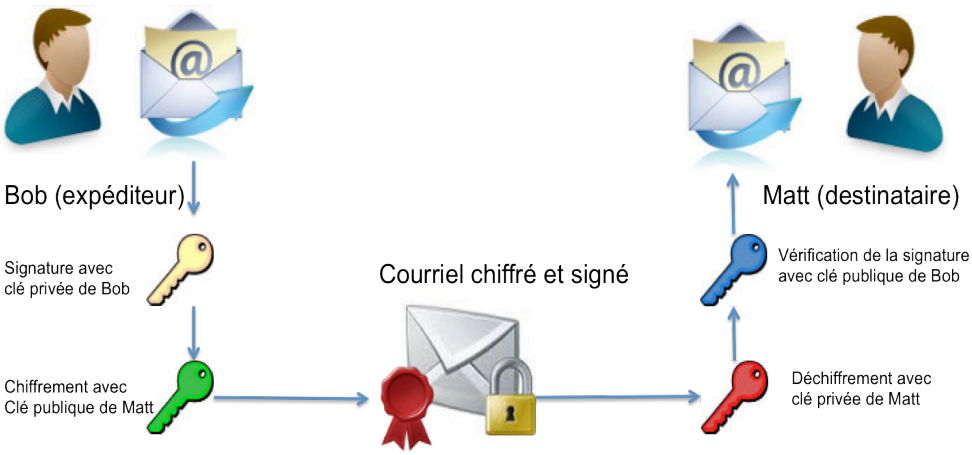
Chiffrement asymétrique

Signature : l'expéditeur va signer le message avec sa clé privée. Le destinataire pourra vérifier la signature avec la clé publique de l'expéditeur disponible sur Internet. Le message sera signé, mais envoyé en clair sur Internet. La signature permet de garantir l'identité de l'expéditeur (authenticité), et également l'intégrité du message. En effet une fois signé, le message ne peut plus être modifié à moins de générer de nouveau une signature.



Signature électronique

Chiffrement et signature : l'expéditeur signe le message avec sa clé privée, puis chiffre le message avec la clé publique du destinataire. Le destinataire devra d'abord déchiffrer le message avec sa clé privée, puis vérifier la signature du message avec la clé publique de l'expéditeur.



Signature + chiffrement d'un message

Remarque : Les schémas ci-dessus sont corrects pour expliquer les principes généraux de la cryptographie asymétrique. Néanmoins la réalité est légèrement plus complexe. En effet chiffrer entièrement un message avec un mécanisme asymétrique est très consommateur en ressources de calcul. Voilà pourquoi en pratique on utilise un mode dit « hybride » :

Signature : une empreinte du message est généré (par exemple avec l'algorithme sha-1), et c'est cette empreinte qui est chiffré avec la clé privée, puis jointe au message. Le destinataire déchiffre l'empreinte avec la clé publique, génère une empreinte et vérifie que les eux empreintes sont identiques.

Chiffrement : une clé symétrique, appelée clé de session, est utilisée pour chiffrer le message. Cette clé de session est chiffrée avec la clé publique du destinataire et jointe au message. Le destinataire déchiffre la clé de session avec sa clé privée puis déchiffre le message avec la clé de session.

2.2 Avantages et limites

Les besoins couverts par la cryptographie à clé secrète (symétrique) et la cryptographie à clé publique (asymétrique) peuvent être résumés dans le tableau suivant :

	Confidentialité	Intégrité	signature
Cryptographie à clé secrète	✔	✔	✖
Cryptographie à clé publique	✔	✔	✔

Les avantages et limites des deux solutions peuvent se résumer dans le tableau suivant :

	Avantages	Limites
Cryptographie à clé secrète	✔ Déploiement logiciel simple et rapide ✔ Une seule clé à générer pour les échanges ✔ outils open source disponibles ✔ Assure la confidentialité et l'intégrité des messages de	✖ Ne permet pas la signature électronique ✖ Nécessite l'échange de la clé secrète de façon sécurisée entre les correspondants ✖ Pas de granularité dans le choix des correspondants : tout le monde partage la clé

	façon robuste ✔ Pratique pour envoyer rapidement un message chiffré à un groupe de personnes	secrète
Cryptographie à clé publique	✔ Élimine le problème de l'échange d'une clé secrète entre les utilisateurs ✔ Couvre toutes les catégories de risques : confidentialité, intégrité, signature des messages ✔ Permet la révocation de la clé d'un utilisateur en cas de compromission d'une clé privée ✔ outils open source disponibles	✖ Nécessite une mise en place légèrement plus complexe ✖ Nécessite d'émettre une paire de clés par utilisateur et de gérer ces clés

3 CAS PRATIQUE : METTRE EN PLACE LE CHIFFREMENT DE SES ECHANGES PAR EMAILS

Quelle que soit la méthode (symétrique ou asymétrique) et le logiciel choisis, mettre en place un projet de chiffrement nécessite un minimum de réflexion avant sa réalisation pratique. La démarche proposée est la suivante :

- ✓ Identifier les risques qui pèsent sur les échanges électroniques. Quels sont les documents sensibles et leurs destinataires (partenaires, fournisseurs, clients) ? Il faut lister les informations à protéger lors des échanges. Par exemple on peut décider que tous les échanges d'information avec une société tierce seront chiffrés, pour la réalisation d'une mission ou de façon habituelle ;

- ✓ Définir et diffuser une politique d'utilisation du chiffrement. Les collaborateurs doivent être sensibilisés au risque et impliqués dans la mise en place du chiffrement. Les règles de sécurité peuvent par exemple être intégrées dans un Plan d'Assurance Qualité (PAQ) ;

Une fois les risques identifiés, la politique d'utilisation du chiffrement défini et les collaborateurs sensibilisés, on peut procéder au déploiement de l'outil. Celui-ci peut être symétrique ou asymétrique.

3.1 Projet de mise en place d'un chiffrement symétrique

Mettre en place un projet de chiffrement symétrique est certainement la façon la plus rapide de sécuriser ses échanges par courriel ; il faut procéder au choix d'un outil, choisir la clé secrète, puis échanger celle-ci de la façon la plus sécurisée possible.

3.1.1 Le choix et la mise en place d'un outil

Des outils open source qui implémentent le standard AES sont disponibles, et permettent donc une utilisation totalement gratuite. Le même outil de chiffrement doit être installé chez l'expéditeur et le destinataire des échanges.

On peut citer par exemple les outils open source suivants:

- AxCrypt, gratuit et disponible pour Windows, qui implémente AES -128. Une fois installée AxCrypt s'intègre directement à Windows : il suffit d'un clic-droit sur un fichier pour procéder au chiffrement ou au déchiffrement.

- 7zip, gratuit et disponible pour Windows, qui implémente AES -256. 7zip, une fois l'application installée, permet d'ouvrir une fenêtre qui propose la compression et le chiffrement des fichiers par glisser-déposer.

- TrueCrypt, gratuit et disponible pour Windows, Linux, MacOS. TrueCrypt est l'un des outils open-source les plus avancés disponibles sur internet et sa documentation est très claire et didactique. De plus c'est un logiciel certifié CSPN par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). TrueCrypt implémente AES mais aussi d'autres algorithmes moins connus comme TwoFish et Serpent. TrueCrypt possède deux modes de fonctionnement : d'une part il permet de chiffrer une partition entière ; d'autre part il permet de créer un « conteneur » chiffré qui apparaît comme un fichier sur le disque. C'est cette dernière option qui nous intéresse pour les échanges par courriel. En effet, une fois monté, le conteneur apparaît comme une partition sur le disque, où l'on peut simplement copier les fichiers que l'on souhaite chiffrer. Une fois démonté, le conteneur est un fichier (chiffré) tout ce qu'il y a de plus normal, ce qui permet de l'envoyer par courriel en pièce jointe. Pour cela la taille du conteneur doit être inférieure à la taille maximale autorisée pour les courriels (25Mo pour Gmail).

AxCrypt et 7zip sont des outils très simples d'utilisation. TrueCrypt, s'il peut paraître un peu plus complexe au départ, permet une utilisation pratique et ergonomique, puisqu'on peut travailler avec une partition chiffrée qui peut ensuite être envoyée par courriel.

3.1.2 La robustesse des mots de passe

La sécurité d'un système se mesure à son maillon le plus faible. Si le mot de passe utilisé est un mot de passe faible (constitué de moins de 8 caractères ou d'un mot courant du dictionnaire), il peut être décodé en quelques minutes par la méthode d'attaque dite « brute-force » : un logiciel va essayer toutes les combinaisons de mot de passe possible.

La méthode recommandée est de créer un « fichier de mot de passe ». Il s'agit d'un simple fichier texte dans lequel on va stocker un mot de passe fort, c'est-à-dire du texte aléatoire composé de lettres minuscules, majuscules, chiffres et caractères spéciaux.

La longueur du mot de passe doit être de 22 caractères au moins pour un chiffrement en AES -128, et de 43 caractères au moins pour un chiffrement en AES -256.
Cela n'est pas un problème dans le cas de l'utilisation d'un fichier de mot de passe, puisqu'on n'a plus à le connaître par cœur ; se pose cependant la question du stockage du fichier.

Il est conseillé de le stocker sur clé USB : cela évite qu'il soit accessible trop facilement en cas de compromission de l'ordinateur. Il est également important de sauvegarder ce mot de passe. Le moyen de sauvegarde le plus sûr est de l'imprimer et de le stocker sous format papier.

3.1.3 Échange de la clé

Une fois le mot de passe généré se pose le problème de l'échange de la clé. En effet, le mot de passe doit être connu de l'expéditeur comme du destinataire. Il est hors de question d'envoyer le mot de passe en clair sur internet puisqu'il pourrait être intercepté et cela reviendrait à une sécurité nulle.

Le mot de passe doit donc être échangé par un autre canal de communication que l'internet. Les différents modes d'échange d'une clé secrète sont :

- Par téléphone (voix)
- Par téléphone (SMS)
- Au format papier par courrier postal
- Lors d'une rencontre physique entre les interlocuteurs, au format papier ou par clé USB

La méthode, la plus fiable et sûre, est d'échanger la clé en main propre lors d'une rencontre avec son interlocuteur.

3.2 Projet de mise en place d'un chiffrement asymétrique

Dans le domaine du chiffrement à clés publiques, deux standards différents sont disponibles : OpenPGP et S/MIME ; la différence fondamentale entre ces deux standards est la question de la validité de la clé publique.

En effet un problème critique se pose lorsqu'on télécharge la clé publique d'un utilisateur : comment être certain que cette clé publique correspond bien à la bonne personne ?

Pour répondre à ce problème, le standard S/MIME propose d'utiliser une IGC (infrastructure de gestion de clé), qui est un tiers de confiance, reconnu par les parties prenantes de l'échange électronique, et qui va valider l'authenticité de la clé publique. On utilise alors un certificat de clé publique au format x509. Le certificat sera signé, donc authentifié, par une autorité de certification.

Le format de certificats OpenPGP, de son côté, laisse le soin à l'utilisateur de déterminer lui-même s'il peut faire confiance à une clé publique. En effet le certificat de clé publique va être signé, donc authentifié, par d'autres utilisateurs. On choisit ou pas d'accorder sa confiance aux personnes qui ont signé la clé.

Il n'y a pas de bonne ou de mauvaise solution : les deux standards sont valables, s'ils sont utilisés correctement. En général les IGC sont utilisées dans les grandes organisations tandis que OpenPGP est destiné à un usage individuel ; mais techniquement les deux solutions sont valables et peuvent êtres utilisées dans une PME.

La mise en place d'un projet de chiffrement asymétrique nécessite le choix de la méthode (OpenPGP ou S/MIME), puis le déploiement de l'outil et la création des paires de clés des utilisateurs, et enfin la publication des clés publiques.

3.2.1 OpenPGP

Avec le standard OpenPGP, le certificat de clé publique est authentifié par la signature d'un ou plusieurs utilisateurs. C'est ce qu'on appelle le « Web Of Trust » (toile de confiance). Si l'on accorde sa confiance à l'un ou plusieurs des signataires, on peut considérer que le certificat, et donc la clé publique, est authentique. Le signataire d'une clé publique est appelé « introducer » (introducteur). Si l'on accorde sa confiance au signataire il est appelé « trusted introducer » (introducteur de confiance).

Le « Web Of Trust » donne lieu à des « key signing party », c'est à dire des réunions où chacun apporte son certificat, vérifie l'identité de ses interlocuteurs et signe leur clé publique. C'est donc un mode de validation des clés publiques totalement décentralisé.

Cependant prenons l'exemple concret de deux interlocuteurs de deux entreprises partenaires qui souhaitent communiquer de façon sécurisé. Si les deux interlocuteurs se font déjà mutuellement confiance, il n'est pas besoin de procéder à une « key signing party ». Il suffit d'émettre un certificat public, de le télécharger sur un serveur, et d'informer son interlocuteur, par email ou téléphone, de la validité de cette clé.

Un certificat de clé publique OpenPGP contient notamment les informations suivantes :

- La clé publique elle-même
- Les informations d'identité de l'utilisateur
- La date de validité de la clé publique
- Eventuellement une ou plusieurs signature d'utilisateurs qui authentifient le certificat

Le standard de chiffrement OpenPGP est implémenté avec différents logiciels, pour tous les systèmes d'exploitation :

- GnuPG (aussi appelé GPG) disponible pour Linux
- GPGTools disponible pour MacOS X
- Gpg4win disponible pour Windows

Chaque utilisateur qui souhaite participer à l'échange sécurisé soit suivre les étapes suivantes :

- Installer l'un des logiciels de la liste ci-dessus qui implémente OpenPGP ;
- Générer une paire de clé (clé publique, clé privée). Lors de la génération une phrase de passe est demandée. C'est le mot de passe qui protégera la clé privée, il doit donc être un mot de passe fort d'au moins 20 caractères. La longueur recommandée de la clé est de 2048 bits ;
- Uploader son certificat de clé publique sur un serveur de clé. Ce processus peut être proposé automatique par le logiciel au moment de la création de la paire de clé. Différents serveurs de clé sont disponibles sur internet. On peut utiliser par exemple hkp://keys.gnupg.net ;
- Télécharger la clé publique de son interlocuteur. Pour cela il suffit de rechercher son nom et prénom sur le serveur de clé. Si l'on est sûr de l'authenticité de la clé on peut procéder à sa signature ;
- Enfin, utiliser son client de messagerie pour chiffrer et signer les courriels. Des problèmes d'intégration peuvent se poser avec Outlook ; c'est pourquoi il est recommandé d'utiliser le logiciel libre Thunderbird qui est parfaitement compatible avec OpenPGP.

Ces différentes étapes permettent de mettre en place simplement la sécurisation des échanges électroniques ; bien entendu, le mode de validation de la clé est à adapter en fonction de l'évaluation de la menace, i.e. des potentiels attaquants qui pourraient intercepter le courriel. Si l'on souhaite réellement valider une clé publique de la façon la plus sure possible, rien ne remplace une rencontre physique qui permet de valider l'identité de son interlocuteur et de signer sa clé.

3.2.2 S/MIME

Le standard S/MIME consiste en l'utilisation du courriel sécurisé (chiffré et signé) avec des certificats au format X509. La différence de ces certificats avec le standard OpenPGP est qu'ils sont signés par une autorité de certification.

Chaque utilisateur qui fait parti de l'échange électronique, doit faire confiance à une même autorité de certification. Cette autorité de certification (aussi appelée AC) signe les certificats de clé publique des utilisateurs et les authentifie.

Un certificat x509 comporte notamment les champs suivants :

- Le numéro de série du certificat
- Le nom de l'autorité de certification qui a émis le certificat
- La date de validité du certificat
- Le nom du détenteur du certificat
- L'algorithme utilisé pour la clé publique
- La signature de l'autorité de certification qui a émis le certificat

Toute la question de la confiance repose donc sur le choix de l'autorité de certification. Deux options sont possibles : soit les correspondants décident de faire confiance à une tierce partie pour émettre et valider leurs certificats. Ce peut être une AC, nationale ou internationale, reconnue. Soit l'une des deux parties décide d'implémenter en interne une autorité de certification et d'émettre et de signer des certificats pour les échanges électroniques.

Une infrastructure qui permet de créer et gérer des autorités de certification, pour émettre, signer, ou révoquer des certificats x509, est appelée IGC (Infrastructure de Gestion de Clé) ou PKI (Public Key Infrastructure).

1ère option : externaliser le service d'autorité de certification

L'avantage de faire confiance à une autorité de certification externe, est d'une part un gain en termes de coût et de maintenance ; et d'autre part le fait qu'on s'adresse à une entreprise spécialisée qui va donc apporter un niveau honorable de sécurité pour son IGC.

Différentes sociétés proposent des solutions d'IGC « dans le Cloud », en mode SaaS (Software As A Service). On peut citer par exemple Symantec, ou Keynectis. L'IGC Keynectis bénéficie d'une certification critères communs EAL4+, le plus haut niveau de certification, par l'ANSSI.

Cela permet de bénéficier d'une IGC « clé en mains » et de pouvoir émettre des certificats électroniques pour ses clients et partenaires.

Le standard S/MIME est largement implémenté dans les clients de messagerie électronique. Ainsi Outlook, par exemple, permet d'intégrer facilement des certificats X509 pour sécuriser ses échanges de courriel.

2ème option : déployer une autorité de certification en interne

Cette option permet de maitriser de bout en bout son infrastructure et d'être indépendant d'un fournisseur externe de solution. Elle nécessite en échange un investissement en temps de travail un peu plus conséquent.

Plusieurs IGC open source, et donc totalement gratuites, sont disponibles sur le marché. On peut citer par exemple EJBCA, qui bénéficie du niveau de certification critères communs EAL4+ par l'ANSSI.

EJBCA propose un tutoriel qui permet de l'installer facilement sous Linux Ubuntu, ainsi que d'un forum de support destiné aux utilisateurs.

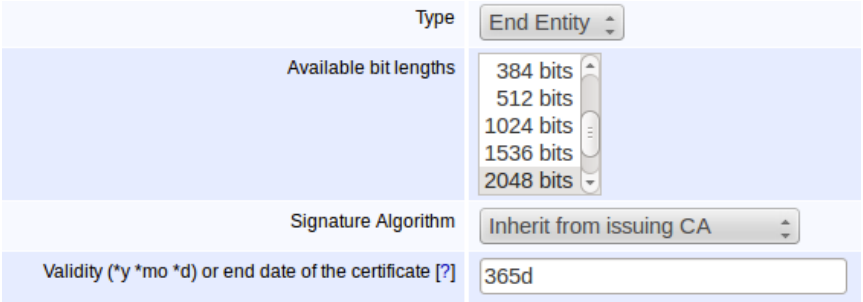
Sans vouloir réécrire un tutoriel, puisque celui-ci est disponible en ligne sur le site d'EJBCA, nous allons voir en quelques étapes-clé comment implémenter cette solution :

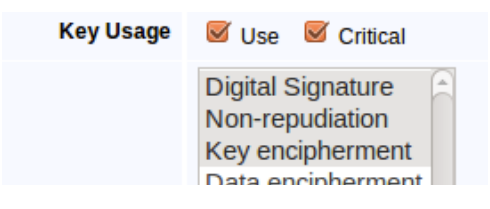
1) installer EJBCA sur une machine Ubuntu déconnectée du réseau, en suivant le tutoriel disponible sur le site d'EJBCA. Une IGC est une infrastructure critique, elle est garante de la validité des certificats. Sa sécurité est donc critique, et le meilleur moyen de la garantir est encore de la déconnecter totalement du réseau.

2) créer à l'installation une seule autorité de certification qui sera autosignée.

3) Une fois l'IGC installé, il faut créer des profils de certificat. Le profil de certificat va indiquer quel sera l'usage du certificat, dans notre cas la sécurisation du courrier électronique avec S/MIME. Pour cela, dans l'interface d'administration, dans « CA functions », créer un « certificate profile » qu'on pourra appeler « smime » avec les caractéristiques suivantes :

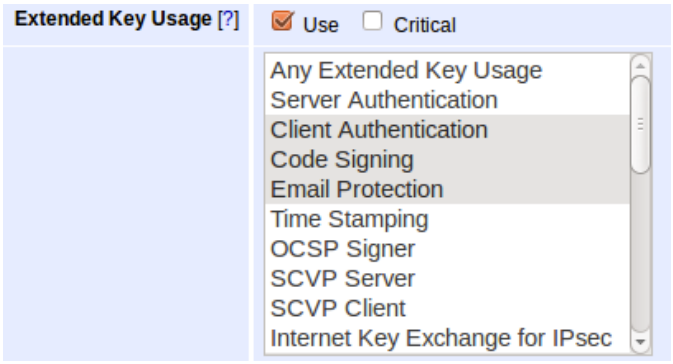
Taille de la clé, 2048 bits, durée de validité : indiquer 365 jours



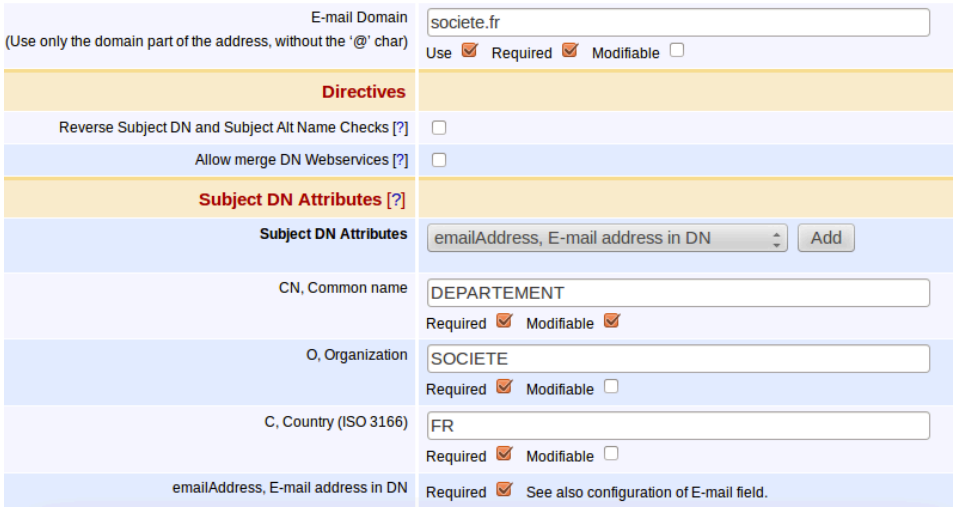


Key Usage :

Extended Key Usage :



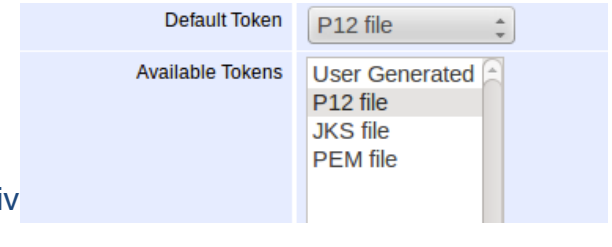
4) Il faut ensuite créer un profil pour les « end entity ». Ce qui est appelé « end entity » est en fait la personne pour qui le certificat va être émis. Pour cela, dans « RA functions », créer un « end entity profile » avec les caractéristiques suivantes :



Le champ « email domain » est à remplacer par le domaine sur lequel sera utilisé l'email.

Le champ « departement » est à remplacer par le nom de votre département, le champ « société » est à remplacer par le nom de votre société.

Pour le mode distribution, indiquer « P12 » :



Cela signifie que les certificats seront distribués au format PKCS12. Le format PKCS12 est un format de fichier qui est chiffré, et qui contient la clé privée et la clé publique de l'utilisateur. Ce fichier, une fois émis, devra être distribué à chaque utilisateur final dont on souhaite sécuriser le courrier électronique.

5) Une fois les profils de certificat et d'utilisateur créés, on peut passer au cœur du sujet, qui consiste à émettre des certificats pour les utilisateurs. on peut ajouter un utilisateur en cliquant sur « add end entity ». Il faut indiquer un mot de passe pour l'utilisateur. Ce mot de passe est critique et doit être un mot de passe fort d'au moins 20 caractères : c'est celui qui protègera le fichier PKCS12 et la clé privée de l'utilisateur.

Les fichiers PKCS12 peuvent êtres retirés dans l'interface « public web » dans « create keystore », pour êtres distribués aux utilisateurs.

Chaque PKCS12 doit être distribué à l'utilisateur concerné, ainsi que son mot de passe. On peut distribuer ce fichier par email, puisqu'il est chiffré, néanmoins il est toujours préférable de le remettre en main propre sur clé USB.

6) une fois les certificats distribués aux utilisateurs, il faut les intégrer à la messagerie. Outlook par exemple, est conçu en standard pour fonctionner avec S/MIME. Il faut procéder à la distribution des clés publiques des correspondants avec qui l'on souhaite communiquer. Ces clés étant publiques par définition on peut les mettre à disposition sur un site web ou bien les transmettre par courriel. Il faut également distribuer aux utilisateurs la clé publique de l'autorité de certification qui a émis et signé les certificats.

Une fois ces étapes suivies, on dispose donc d'une autorité de certification en interne qui va permettre d'émettre des certificats pour le chiffrement et la signature S/MIME.

4 Conclusion

L'affaire PRISM nous rappelle que la majorité des communications électroniques mondiales sont écoutées voire déchiffrées, et vient semer le doute sur la protection réelle apportée par la cryptographie.

S'il est vrai qu'il est difficile pour une PME de garantir la confidentialité de ses échanges contre un Etat disposant de moyens conséquents, le chiffrement des messages permet cependant de se prémunir contre un ensemble de risques : concurrents, intermédiaires malveillants, cybercriminels, etc.

Chiffrer ses messages électroniques est une bonne pratique à adopter, qui équivaut à envoyer un courrier dans une enveloppe scellée, ce qui est toujours préférable à une carte postale, quand on communique des informations sensibles.

Cependant il faut garder à l'esprit que le chiffrement ne prémunit pas à coup sûr contre le piratage : dans le cas d'une communication chiffrée, ce sont les « end point », c'est à dire les ordinateurs d'où partent et où finissent les échanges, qui vont devenir une cible privilégiée pour les attaquants. Sécuriser ses échanges électroniques doit donc s'inscrire dans une démarche globale de sécurité du système d'information.

Sources :

http://www.axantum.com/axcrypt/

http://www.7-zip.org/

http://www.truecrypt.org/

http://www.hsc.fr/ressources/cours/pki/index.html.fr

http://www.pgpi.org/doc/pgpintro/

http://www.symantec.com/verisign/managed-pki-service/

http://www.keynectis.com/fr/securite-identite/cloud-pki

http://www.ejbca.org/

Livre Blanc :

« Sécuriser les échanges d'information par emails»

BSSI
Conseil & Audit

Pour plus d'information,

contact@bssi.fr

Suivez notre veille sur twitter : @BSSI_Conseil
et n'hésitez pas à vous inscrire à notre newsletter sécurité hebdomadaire