LES DOSSIERS TECHNIQUES

Gestion des secrets cryptographiques

Usages et bonnes pratiques

Mai 2012

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Gabriel	**LEPERLIER**	*Verizon Business*

Les contributeurs :

Annabelle	**TRAVERS-VIAUD**	*Bull*
Manuel	**PRIEUR**	*HP France*
Gérald	**GREVREND**	*Altran*
Rodolphe	**SIMONETTI**	*Verizon Business*
Gilles	**DEFER**	*SOGETI*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

A. Introduction / Généralités

A.1 - La gestion des clés, pourquoi ?

Pour des raisons de sécurité, les systèmes d'information d'aujourd'hui font un usage intensif de cryptographie. Les principaux usages concernent :

- L'authentification pour accéder aux systèmes, aux applications ou aux bases de données ;
- La confidentialité des informations stockées ou transmises, ou des canaux de transit ;
- L'intégrité des informations.

La profusion de clés utilisées rend indispensable une gestion extrêmement rigoureuse. Faute de quoi, certaines seront perdues, corrompues ou dévoilées.

Malgré cette évidence, on constate souvent dans les entreprises que ces clés sont gérées de façon très artisanale, parfois même pas du tout. Par exemple le fait que ces clés ne puissent être utilisées que très occasionnellement par des personnes physiques, ou utilisées uniquement par des systèmes amène souvent ces clés à ne plus être utilisables après expiration ou perte des secrets d'activation, entrainant alors indisponibilité des systèmes ou perte d'information.

De plus, dans la plupart des pays, les entreprises ont des obligations légales vis-à-vis de la conservation de certaines clés utilisées, notamment dans le cadre des enquêtes judicaires.

A.2 - A qui s'adresse ce document ?

Ce document s'adresse à toute personne dont l'activité nécessite de gérer des clés cryptographiques, ou de définir une Politique de Gestion des clés. Par exemple :

- Des concepteurs d'architectures et d'applications, **aucune implémentation ne pouvant *a priori* se passer de sécurisation, certaines font appel à des moyens cryptographiques;**
- Des Maîtrises d'Ouvrage et Maîtrises d'œuvre **à qui revient le rôle de « gardiens du temple », « d'Autorités de Confiance » pour la sécurité des données qui leur sont confiées ;**
- Des auditeurs (internes ou externes), chargés d'évaluer **des systèmes ou des applications faisant usage (ou devant faire usage) de moyens cryptographiques… ;**
- Des Responsable de Petites, Moyennes et Très Petites Entreprises, **éprouvant des besoins de sécurisation de leur SI, mais n'ayant pas nécessairement les moyens (techniques, financiers) ou les ressources pour mettre en place et a fortiori opérer une Infrastructure de Gestion de Clés (IGC)...**

Ce document pourra également être utilisé pour expliquer les principes de base à des personnes ayant à gérer des clés.

A.3 - Définitions

Au sein du présent document, l'expression « secret cryptographique » ou « « secret » doit être entendue comme couvrant :

- Les clés secrètes, utilisées dans les algorithmes de cryptographie symétrique ;
- les bi-clés, composées d'une clé privée et d'une clé publique associée, utilisées dans les algorithmes de cryptographie asymétrique ;
- Les mots de passe et autres séquences alphanumériques complexes ou non, ainsi que par exemple le code PIN des cartes à puces.

Les secrets peuvent avoir de multiples formes, du simple code PIN à 4 chiffres protégeant une carte bancaire, une carte à puce ou dispositif USB contenant une partie d'une clé ayant été « coupée » en plusieurs morceaux, à un ensemble de séquences alphanumériques complexes.

Dans les systèmes les plus sophistiqués, les clés peuvent également revêtir une forme sonore, lumineuse ou électromagnétique, mais la gestion de ces clés est très spécifique et hors du champ d'application de ce document.

L'expression « gestion » de clés cryptographique couvre l'ensemble du cycle de vie d'une clé.

A.4 - Objectifs du document

La multitude de formats, de types d'usages, d'intervenants concernés, rend la gestion des clés cryptographiques particulièrement complexe, ce qui souvent freine la volonté de « bien faire ».

En réalisant ce document, l'objectif du groupe de travail est d'aider les lecteurs dans la compréhension et la mise en œuvre d'une gestion efficace, en présentant :

- Des principes généraux ;
- Des « bonnes pratiques » ;
- Quelques références pour approfondir le sujet sur un volet spécifique.

Ce document a un caractère générique, et devrait être applicable, quels que soient la taille de l'entité concernée, son secteur d'activité, son pays d'implantation. Il n'a pas de vocation normative, et n'est pas non plus un guide d'audit : Il s'agit d'un guide de bonnes pratiques issues de l'expérience des rédacteurs.

B. Inventaire des usages de secrets et risques associés

Au sein d'un S.I., les clés sont utilisées partout. Elles sont largement utilisées par les infrastructures pour la sécurisation des données échangées entre composants, mais aussi celle des données stockées au sein de bases de données ou de fichiers. Les clés et secrets sont également souvent distribués aux utilisateurs du S.I pour leur permettre d'utiliser les services mis à leur disposition en toute confiance. Mais leur omniprésence et l'usage intensif qui en est fait ne doivent pas faire oublier leur sensibilité et les menaces pesant sur leur confidentialité, leur disponibilité et leur intégrité, sans lesquelles la sécurité du S.I. n'est plus assurée.

B.1 - Usage des clés et secrets par les infrastructures

Les systèmes d'informations utilisent des clés pour répondre à différents besoins, parmi lesquels :

- Assurer la confidentialité des informations
- Authentifier une entité responsable d'une action ou initiant cette action (personne, objet...)
- Signer une donnée ou un acte : scellement, attestation, authenticité

Les besoins de sécurité des informations peuvent concerner aussi bien les informations stockées (ou « résidentes ») que les informations échangées (en transit).

B.1.1 - Sécurisation des données résidentes

La première catégorie va consister en l'utilisation de clés pour assurer la protection de données stockées dans un dispositif technique tel qu'un serveur de fichier, une base de données, un HSM (Hardware Security Module) ou des sauvegardes informatiques.

Le premier et principal besoin rencontré est d'assurer la confidentialité des données stockées, c'est-à-dire de se prémunir contre leur divulgation. Cela se fait par la mise en place d'un chiffrement qui va utiliser une clé, un secret qui devra être géré.

Ensuite vont venir les besoins autour de l'authenticité et de l'intégrité des données :

- Assurer l'origine d'une donnée (par exemple par la signature électronique d'un courriel) ;
- Garantir l'intégrité d'une donnée ;
- Horodater un événement ;
- Réaliser une opération de signature électronique afin de prouver une action (approbation, rejet...).

B.1.2 - Sécurisation des données en transit

L'autre grande catégorie d'usage consiste en la protection des informations échangées. Une fois encore le besoin le plus couramment rencontré concerne la protection de la confidentialité de la donnée en transit ainsi que la garantie de son origine et son intégrité. Par exemple, le protocole SSL utilisé pour le commerce électronique permet d'authentifier le serveur émetteur et permet l'établissement d'un trafic réseau à l'aide d'une clé de chiffrement à usage limité dans le temps. Cette fonction est particulièrement utilisée dans le cadre d'échange entre machines dans un environnement Web.

Il est également possible, si le besoin de confidentialité n'est pas requis, de n'utiliser que les fonctions d'authentification de flux et d'intégrité du contenu de ces mécanismes.

Tous ces usages reposent sur des protocoles standardisés ou propriétaires qui s'appuient sur l'utilisation de clés. Celles-ci peuvent être des clés asymétriques, symétriques mais aussi de simples mots de passe.

Les clés asymétriques sont utilisées pour authentifier les deux parties établissant le tunnel, puis échanger une clé éphémère, dite « clé de session » qui ne servira à chiffrer le contenu des échanges que pour la durée de la session établie. Cette clé n'a donc pas vocation à être conservée, voire séquestrée.

Ce principe de génération et d'utilisation d'une clé de session symétrique, sécurisée par une clé asymétrique, est également présent dans de nombreuses implémentations pour la sécurisation de données « résidentes » : chiffrement de champs de bases de données, de fichiers, de contenus de HSM, etc. Les principaux avantages en sont :

- La rapidité des opérations de cryptographie symétrique par rapport aux opérations asymétriques ;

- Le fait de ne pas avoir à « transchiffrer » (déchiffrer puis chiffrer de nouveau) l'ensemble des données ainsi protégées, en cas de changement de clé –asymétrique- de chiffrement ; seule la clé symétrique, chiffrée par la clé asymétrique, est alors « transchiffrée », ce qui est extrêmement rapide.

B.1.3 - Sécurisation en mode « SaaS »

Une gestion de clés intervient également dans le fonctionnement des applications en SaaS ou l'informatique « in the Cloud ».

Cela nécessite la mise en œuvre de mesures de sécurité spécifiques dont la généralisation de l'authentification des composants (surtout des objets logiciels) ou le chiffrement des flux. Il s'agit globalement de la généralisation de moyens de sécurisation mis en œuvre pour sécuriser les échanges entre composants informatiques. Néanmoins, la contractualisation avec le prestataire doit être renforcée afin de clarifier les responsabilités concernant cette sécurisation. Par ailleurs, un secret est utilisé pour authentifier le client de la plate-forme de service. Ce secret doit être géré avec le même soin que tout autre secret.

L'hébergement d'une solution de gestion des clés sur un « cloud » expose à tous les risques que posent ces services, et devrait être évitée autant que possible. Une question importante est de savoir qui a la maitrise des secrets et dans le cas d'une PKI qui a la capacité d'activer la clé privée de l'autorité certification. Le site http://cloudsecurityalliance.org/ (en anglais) propose un ensemble de bonnes pratiques qui peuvent être appliquées. Il est important de prendre le plus grand soin dans la contractualisation de l'externalisation et en particulier sur plusieurs points :

- Définition d'une politique de sécurité spécifique aux SaaS et à l'informatique nébuleuse ;
- Clarification de la juridiction et le cas échéant restriction de celle-ci. Il est important de savoir sur quel territoire physique les traitements informatiques auront lieu afin d'identifier le contexte réglementaire : une localisation sur le territoire américain expose le traitement à toutes les législations locales telles que DMCA ou le Patriot Act par exemple ;
- Le cloisonnement avec les autres clients doit être renforcé ;

- Les clauses habituelles d'un contrat d'externalisation comme une clause d'audit doivent être négociées.

B.2 - Usage des clés et secrets côté utilisateurs

B.2.1 - Différents certificats pour différents usages

Du point de vue utilisateur, le nombre de certificats différents est relativement restreint. Les différentes catégories de certificats utilisateurs et leurs utilisations sont abordées ci-après.

Sont également à prendre en compte les certificats machine et les certificats de personne morale :

- Les certificats machine sont liés à une identité machine et non à l'identité d'un utilisateur physique. Un exemple est un certificat NAC (Network Access Control) utilisé par le poste de l'utilisateur pour se connecter au réseau local de son entreprise.
- Les certificats pour personne morale sont, par exemple, utilisés par le directeur d'un service achat d'une grande structure. Ce certificat, qu'il est pourtant le seul à utiliser, n'est pas à son nom propre mais au nom de sa compagnie.

Dans les deux cas ci-dessus, l'objet du certificat (son CN, son Common Name) ne désigne pas une personne physique contrairement au certificat utilisateur.

Il convient de noter que les usages décrits ci-dessus correspondent à des usages courants (tels que définis dans le RGS par exemple) mais qu'il est tout à fait possible de trouver des certificats spécifiques ou malformés : certificat de chiffrement et de signature par exemple mais sans authentification.

Enfin, ne pas oublier qu'un certificat ne peut pas être utilisé sans la clé privée associée pour pouvoir réaliser certaines opérations cryptographiques comme appliquer une signature numérique par exemple.

B.2.1.A - Certificat de signature

Un certificat de signature est utilisé pour apporter une signature numérique liée à la personne physique porteuse du secret, à savoir la clé privée de signature. La signature numérique est utilisée pour assurer l'intégrité et la non répudiation : le destinataire du document ou du message a la certitude que le document signé n'a pas été modifié et qu'il a bien été émis par l'utilisateur ayant signé le document. L'utilisateur ayant signé le document ne pourra pas non plus nier avoir envoyé le document.

Ce type de certificat peut, dans sa mise en œuvre la plus aboutie, prendre la même valeur légale que la signature manuscrite et permettre d'inverser la charge de la preuve en cas de contestation devant un tribunal. En effet la partie qui conteste la validité de la signature devra apporter la preuve de l'invalidité de la signature. Cela correspond au niveau 3 ★ du RGS : le certificat sera présumé fiable par défaut (a noter que l'ensemble du dispositif doit être 3 ★ pour être habilité 3 ★)

La clé privée de ce type de certificat ne doit pas être séquestrée et elle doit être générée au plus proche de l'utilisateur. Idéalement il doit être généré dans un support cryptographique physique dédié et ne doit pas être exportable en dehors de ce support cryptographique. Si la clé privée venait à être copiée, cela ruinerait les rôles attendus ci-dessus car une personne

physique autre que le porteur légitime pourrait signer des documents au nom du porteur légitime.

B.2.1.B - Certificat d'authentification

Un certificat d'authentification est utilisé pour prouver une identité dans le monde numérique. Il peut être comparé à une carte d'identité : c'est la confiance dans l'autorité qui l'a émise et les protections associées qui garantissent l'identité et la fiabilité de son authentification. Un certificat d'authentification permet de prouver une identité en matière numérique. A l'identique, c'est l'autorité émettrice du certificat qui s'engage sur la fiabilité de l'association entre le certificat, la clé privée associée et l'identité de son porteur.

Les certificats d'authentification sur support physique sont couramment utilisés pour faire de l'authentification forte sur un site internet, activer un conteneur SSO contenant les mots de passe applicatifs du porteur, ou encore utiliser un VPN avec son entreprise par exemple.

Comme pour le certificat de signature, la clé privée ne doit pas faire l'objet d'un quelconque séquestre, et doit être générée au plus proche de l'utilisateur. Idéalement, elle doit être générée dans un support cryptographique physique et ne doit pas être exportable en dehors de ce support cryptographique. Si la clé privée venait à être copiée, cela ruinerait les rôles attendus ci-dessus car une personne physique autre que le porteur légitime pourrait s'authentifier en son nom.

Enfin, comme pour le certificat de signature, il est possible d'obtenir un certificat d'authentification de niveau 3★ c'est-à-dire qui sera présumé fiable par défaut.

B.2.1.C - Certificat d'authentification/signature

Ce certificat permet à son porteur de réaliser des opérations de signature et d'authentification à partir d'une seule et unique clé, et non de deux clés distinctes spécialisées par usage, comme précédemment. Ce certificat ne permet d'atteindre que le niveau 2 ★ au RGS, il ne permet donc pas d'obtenir un certificat présumé fiable par défaut. Il est couramment utilisé dans un but de simplification quand le niveau 3 ★ n'est pas nécessaire, pour compatibilité avec les systèmes existants et non adaptés aux certificats par usage et limiter les coûts.

B.2.1.D - Certificat de chiffrement

Un certificat de chiffrement est utilisé pour chiffrer des données. C'est usuellement le seul type de certificat/clé faisant l'objet d'un séquestre, que ce soit pour satisfaire à un besoin interne ou à une exigence réglementaire. Pour cela, et contrairement aux clés associées aux certificats de signature et de chiffrement, la clé privée de ce type de certificat est générée par l'autorité émettrice qui la fournit ensuite à l'utilisateur. Le chiffrement est couramment mis en œuvre de manière hybride : une clé privée est utilisée pour chiffrer une clé symétrique. Il est possible d'obtenir des certificats de niveau 3 ★. Le séquestre peut être global (l'ensemble des clés privées de chiffrement sont sauvegardées) ou bien une clé de recouvrement globale permet de recouvrer les clés séquestrées.

B.2.2 - Distribution des certificats aux utilisateurs : l'importance des processus

Les processus de distribution des certificats et des clés privées aux utilisateurs sont particulièrement importants. A l'instar identique d'une carte d'identité qui doit être remise avec certitude à leur titulaire et non à un usurpateur, les processus organisationnels mis en œuvre permettent de s'assurer qu'un certificat est bien protégé dès sa création et remis au bon porteur physique.

Actuellement, la robustesse des algorithmes cryptographiques généralement employés est telle que les failles les plus facilement exploitables proviennent de l'exploitation de ces processus de remise. Il est en effet plus facile d'usurper l'identité d'une personne au téléphone pour se faire envoyer la clé privée d'un porteur par recouvrement, ou encore d'observer le porteur taper son code PIN que de calculer une clé privée à partir d'un certificat. Il est donc primordial d'attacher une attention toute particulière à la conception des processus de délivrance et de remise, ainsi qu'à leur mise en œuvre.

B.2.2.A - Le mode décentralisé

Dans ce mode, la génération des clés privées est réalisée côté utilisateur et non à distance par l'Autorité de Certification (AC), Généralement ce mode est utilisé pour les certificats d'authentification et de signature, la clé privée ne devant pas être séquestrée. Le séquestre de ce type de clé puis son transit hors d'un support cryptographique ruinerait la fiabilité attendue : si la clé privée venait à être interceptée, il ne serait plus possible de garantir la fiabilité de la signature et sa non-répudiation par le porteur légitime.

Idéalement, dans ce mode, la génération de la clé privée est prise en charge par un support cryptographique externe. Ce support cryptographique peut prendre la forme d'un token USB (l'apparence d'une clé USB) ou d'une carte à puce. La clé privée ne peut jamais être extraite du support qui l'a générée. En effet, un support cryptographique répondant aux exigences de sécurité doit notamment mettre en œuvre la clé de façon sûre, requérir une authentification par code PIN pour activer la clé au sein du support cryptographique (l'équivalent du code d'une carte bleue ou d'un téléphone portable) et réaliser les opérations cryptographiques directement au sein du support cryptographique sans exposer la clé privée. Ainsi, pour la création d'un certificat signé, la clé privée est générée à l'intérieur du support, une demande de signature est envoyée à la PKI puis le certificat signé est importé dans le token : a aucun moment la clé privée n'est exposée à l'extérieur de son support physique.

La clé privée peut également être générée par le navigateur mais cette méthode est généralement moins sécurisée que la génération dans un support cryptographique, la protection de la clé privée n'étant dans ce cas que logicielle et reposant sur la configuration du navigateur, ou plutôt, de son magasin de certificats. Le navigateur peut néanmoins s'appuyer sur des modules externes et piloter un support cryptographique externe par exemple.

B.2.2.B - Le mode centralisé

Dans ce mode de distribution, la clé privée est générée par l'autorité de certification puis envoyée au porteur. Généralement ce mode est utilisé pour distribuer les clefs de chiffrement.

Ce mode permet le séquestre des clés privées générées, c'est-à-dire leur sauvegarde par l'autorité émettrice. Cette sauvegarde est obligatoire pour permettre à l'entreprise d'avoir accès aux données chiffrées du porteur en cas de départ de celui-ci. Elle est imposée par le législateur, pour garantir l'accès aux données chiffrées en cas de requête judiciaire par exemple.

Le séquestre est également utilisé pour permettre d'accéder les données chiffrées suite à la perte du support cryptographique.

Le standard PKCS#12 est utilisé pour protéger la clé privée et le fichier est protégé par un mot de passe. Ce fichier peut alors être envoyé par email à l'utilisateur, mis à disposition sur une plateforme de téléchargement ou encore être injecté dans le navigateur ou le support cryptographique du porteur par le client PKI de l'utilisateur.

Ce mode est évidemment moins sécurisé que le mode décentralisé car la clé privée est transportée en dehors d'un support cryptographique et transite d'une manière ou d'une autre sur un réseau mais certains mécanismes permettent néanmoins d'assurer le stockage et le transport sécurisés de ces clés. Ainsi les séquestres sont protégés par HSM et certains tokens mettent en œuvre des canaux sécurisés SSL directement entre la puce cryptographique et le séquestre : le stockage et le transport sont ainsi sécurisés. Enfin, il y a deux modes de séquestre différents : une copie de chaque clé privée peut être réalisée ou deux clés privées sont utilisées (une clé privée individuelle et une clé paître de recouvrement).

B.2.2.C - Face à Face

Aux modes de génération de la bi-clé, centralisé ou décentralisé, il est possible d'associer le mode de remise du certificat, avec ou sans face-à-face.

Le mode avec face-à-face consiste à faire remettre le support cryptographique de main à main à l'utilisateur par un opérateur et sur présentation de justificatifs d'identité. Ce mode de remise est obligatoire pour obtenir des certificats de niveau 3 ★. Il est possible d'utiliser ce mode de remise même pour des certificats de niveau inférieur à 3 ★.

B.2.3 - Stockage et mise en œuvre des certificats et clés associées

B.2.3.A - Magasins de certificats du système d'exploitation

Sur un poste pourvu d'un système d'exploitation de Microsoft (Windows), les certificats sont stockés dans des "magasins", ce sont en fait des conteneurs logiciels de certificats. Les magasins Microsoft sont de trois types : magasins utilisateurs, ordinateur ou de service. Il s'agit dans le cas présent du magasin utilisateur : chaque utilisateur se connectant sur un poste sous Windows accédera à son magasin personnel lié à sa session.

Le magasin utilisateur est partagé/accédé facilement par les applications Microsoft : un certificat utilisateur sera accessible indifféremment dans Internet Explorer, Outlook et le reste de la suite MS Office par exemple.

Il convient de noter que le navigateur web internet explorer permet la génération de clés privées dans le magasin de l'utilisateur.

B.2.3.B - Supports cryptographique physiques et individuels

Ces supports cryptographiques individuels prennent la forme de clés USB (couramment appelés "tokens") ou de cartes à puce au format ISO 7816 de type « carte bancaire », le point essentiel résidant dans le fait qu'ils sont tous équipés d'une puce cryptographique quelle que soit leur forme. Ces supports cryptographiques sont les plus sécurisés mais les plus couteux. Idéalement ils peuvent être accompagnés d'un clavier de saisie du code PIN, évitant que le code PIN ne soit saisi directement sur le clavier de l'ordinateur et où il peut être intercepté par une application malveillante, de type « keylogger ».

La plupart du temps, les clés privées générées à l'intérieur d'un tel support ne peuvent pas être exportées hors du support de par la conception même de la puce. Le fait que seul l'utilisateur connaisse le code permettant d'activer la clé privée contenue au sein du support cryptographique assure la non-répudiation des opérations réalisées grâce à cette clé : l'utilisation de la clé privée a nécessairement eu lieu avec le token et avec le code PIN.

L'utilisation d'un support cryptographique certifié 3 ★ est obligatoire pour pouvoir mettre en œuvre des certificats de niveau 3 ★ du RGS.

B.2.3.C - Magasins tiers

Ces magasins sont des magasins propriétaires et dédiés pour chaque application. Les certificats dans ces magasins ne sont pas visibles ni utilisables en dehors de l'application elle-même. Firefox par exemple utilise son propre magasin de certificats : les certificats dans le magasin Windows n'y apparaissent pas.

Ce cloisonnement peut amener certains problèmes pratiques. Par exemple, si le certificat utilisateur émis par l'administration fiscale pour permettre la télé-déclaration des impôts est généré par Firefox, l'année suivante vous ne pourrez pas vous connecter sur le site des impôts en utilisant Internet Explorer car le certificat n'apparaîtra pas.

B.3 - Inventaire des risques portant sur ces clés et secrets

B.3.1 - Introduction : pourquoi l'identification des risques en préambule à la gestion des clés ?

La "gestion des clés" a pour objectif premier la protection des clés et secrets de l'organisme contre les atteintes pouvant les impacter.

Ces atteintes peuvent par exemple être faites de divulgations, mais aussi de pertes involontaires, potentiellement dommageables à l'entreprise. Il suffit d'imaginer la perte des clés de son domicile, ou de son coffre-fort... Et dans le cas des clés cryptographiques, pas d'appel au serrurier possible, sauf si un Séquestre a été implémenté.

L'inventaire des risques portant sur ces biens d'un type un peu particulier peut être dressé suite à la réalisation formelle d'une évaluation des risques, plus couramment appelée "analyse de risques".

Cette identification des risques permet d'identifier les scénarios "catastrophe" pouvant impacter ce que l'on souhaite protéger - des clés et des secrets dans le cas présent-, en mesurant la gravité de ces scénarios à partir de leur impact sur l'activité de l'entreprise.

B.3.2 - Identification des risques

B.3.2.A - Identification des biens essentiels et des biens supports

La protection des clés et secrets leur est due à deux titres :

- au titre de "bien informationnel" (au sens du mot "asset" des normes ISO/IEC 2700x) ; les clés et secrets doivent être identifiés comme bien informationnel ou données à protéger ;

- au titre d'éléments de sécurité, sur lesquels reposent en grande partie des mécanismes de sécurité, qui sont justement, eux, chargés de protéger les biens informationnels du SI !

Pour pouvoir lister l'ensemble des menaces et des risques portant sur les clés et secrets utilisés par un organisme, il est nécessaire dans un premier temps d'en établir l'inventaire :

- **les biens dits "sensibles"** : les données et informations que l'on veut protéger vis-à-vis de la divulgation, de la corruption et/ou de l'indisponibilité :;

- Clé privée d'authentification[*]/signature dont clé de diversification pour secret d'authentification (clé de session, OTP...), d'une personne physique ou d'un serveur ou d'une application
- Clé privée de signature d'une Autorité : Autorité de Certification, d'Horodatage, de Gestion de Preuve, de Création d'Attestation
- Clé de déchiffrement d'une personne physique ou d'un serveur/application
- Clé symétrique (hors clé de session) d'une personne physique ou d'un serveur/application
- Code PIN, secret d'activation d'une personne physique ou d'un serveur/application
- Mot de passe associé à un identifiant lié à une personne physique ou à un compte générique,
- Auxquelles on peut ajouter les secrets "fugaces" ou "fugitifs" tels que : OTP, clés de session (établissement d'un tunnel SSL, etc)

- **les biens dits "de support" :** Une clé cryptographique ou un secret étant par nature une donnée, une information, elle ne peut exister sans son support : ce support peut être :

- un support au format papier :
    - courrier : courrier de transmission d'un code PIN ou d'un mot de passe...
    - document archivé : formulaire d'enregistrement d'un code d'activation, du mot de passe du compte "root" d'un serveur...
- un support électronique en transit :
    - mail de transmission d'un mot de passe, d'un fichier PKCS#12...
    - échange téléphonique : transmission d'un mot de passe par une hot-line à un utilisateur…
    - échange réseau : échange protocolaire d'éléments de calcul d'une clé de session, transmission d'un fichier PKCS#12 entre composants applicatifs d'une Autorité de Certification...
- un support de type "humain" :
    - code PIN ou d'un mot de passe retenu par la mémoire de son porteur
- un support matériel :
    - bande de sauvegarde, CD-Rom (sauvegardes et archives de systèmes)
    - mémoires flash (clés USB de stockage...)
    - carte à puce / puce cryptographique,
    - HSM.
- un support logiciel :
    - magasin de certificats,

[*] serveur au sens serveur applicatif assurant/mettant à disposition un service, tel que : serveur Web, serveur d'application, serveur de messagerie...

- code logiciel : mot de passe codé "en dur" dans l'application ou inclus dans le paramétrage, code d'activation de clé pour une application ;
- conteneur de mots de passe utilisé dans le cadre du SSO,
- enveloppe cryptographique, de type PKCS#12,

Note : le support logiciel est stocké sur un ou plusieurs supports matériels (de même type ou différents).

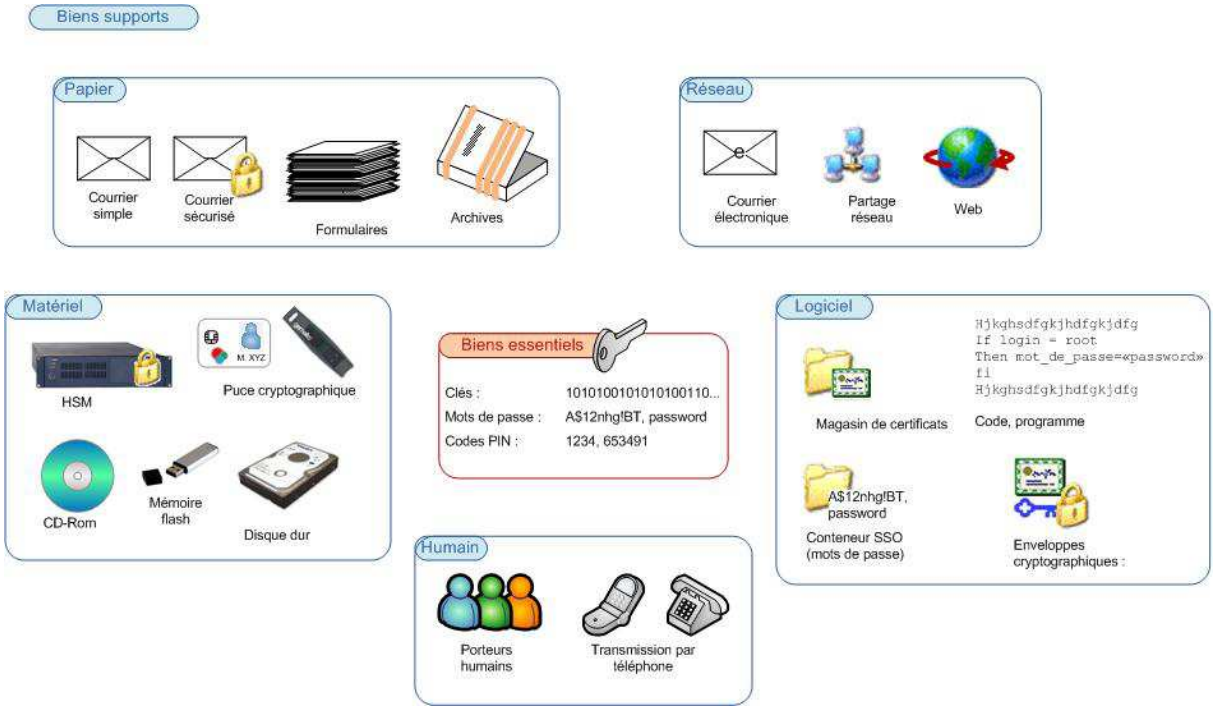


Figure 1 : Biens sensibles et biens supports en gestion de clés

Note : l'ensemble de ces biens support est contenu au sein d'autres biens supports, comme par exemple : le site géographique, les locaux, et est entouré d'autres biens, comme par exemple le personnel !

Les risques pesant sur ces autres biens sont donc également à prendre en compte, même si, dans la majorité des cas, ils seront partagés avec l'ensemble du Système d'Information ! Aussi, ne sont-ils pas traités spécifiquement dans le présent document.

	Papier		Electronique en transit			Humain	Support matériel				Support logiciel		
	Courrier	Archive	Mail	Téléphone	Réseau	Mémoire humaine	Bandes, CD-Rom	Mémoire flash	Puce crypto	appliance crypto	Code applicatif	Magasin de certificats	Conteneur SSO
Clé privée auth*/sign			X*		X*		X*	X	X			X	
Clé privée auth/cachet			X*		X*		X*	X		X		X	
Clé privée de signature d'une Autorité							X			X		X	
Clé de déchiffrement			X*		X*		X*	X	X			X	
Clé de déchiffrement			X*		X*		X*	X		X		X	
Clé symétrique (hors clé de session)			X				X	X	X				X
Clé symétrique (hors clé de session)			X				X			X	X	X	
Code PIN, secret d'activation	X	X	X	X		X					X		X
Mot de passe	X	X	X	X	X	X					X		X
OTP, clés de session					X								

X* : secret usuellement sous forme chiffré
X : secret usuellement "en clair"

Figure 2 : Exemple de matrice identifiant les relations « Biens supports/biens sensibles »

B.3.2.B - Identification des besoins de sécurité et des menaces

Les besoins de sécurité relatifs à ces biens sensibles et de support sont évidemment, à minima, les besoins DIC:

- la **confidentialité** => une clé ou un secret doit en principe rester... secret, comme son nom l'indique. Ce besoin de confidentialité ne concerne bien évidemment que les parties secrètes des bi-clés asymétriques (« clés privées ») ;

- **l'intégrité** => la perte d'intégrité d'une clé ou d'un secret implique l'impossibilité d'utiliser celui-ci ;

- la **disponibilité**, => l'impossibilité d'accéder à une clé ou un secret ne permet pas d'activer le mécanisme de sécurité auquel celui-ci est lié.

Ce sont ces besoins, pour chacun des biens, qu'il convient de protéger : s'il est assez évident qu'il faut protéger la confidentialité d'un secret, la question de la préservation de sa disponibilité est souvent éludée lors de la mise en place de solutions requérant des secrets. Pourtant, sans accès possible au secret ou à la clé nécessaire, impossible d'accéder aux données ou fonctions protégées !

La confidentialité est usuellement considérée de façon binaire : ou un élément est secret, ou il est divulgué. Il peut être nécessaire dans certains cas d'identifier des niveaux successifs de confidentialité. Par exemple, le secret peut être considéré comme « moins » corrompu s'il a été divulgué auprès d'un effectif restreint et identifié de personnes qu'auprès d'un large public. Cependant, dans la majorité des cas, le fait qu'un élément ne soit plus connu que par son détenteur seul, suffira à le déclarer corrompu et justifiera la prise de mesures adéquates (mise en opposition du secret concerné, et utilisation d'autres secrets…).

En revanche, en matière de disponibilité, il est nécessaire de distinguer les indisponibilités définitives (perte irrémédiable du secret) des indisponibilités passagères. Et au sein de celles-ci, il est nécessaire de définir une échelle d'impact (sur l'activité) en fonction de la durée de l'indisponibilité ; une disponibilité sous 2 heures n'aura pas les mêmes impacts sur l'activité de l'organisme qu'une disponibilité sous 3 jours, voire plus, ce qui s'avère possible lorsqu'un secret est par exemple détenu par un porteur humain.

La prise en compte de l'intégrité est elle aussi souvent binaire ; soit le secret est intègre -et peut être utilisé, soit il a été modifié/corrompu, et il est alors inutilisable. Ce dernier cas est assimilé à une indisponibilité définitive.

La mesure de l'impact d'une perte d'intégrité d'un secret pourra prendre en compte la détection de celle-ci ; si la rupture d'intégrité peut être détectée aussitôt, alors il pourra éventuellement être possible d'y remédier plus vite (restauration, etc.), et surtout, cette perte d'intégrité ne se doublera pas d'une indisponibilité lors d'un cas d'utilisation "en urgence".

Les menaces pouvant impacter chacun de ces types de supports varient bien entendu en fonction de la nature de celui-ci. Il est évident que les risques relatifs à la gestion des ressources humaines seront plus importants dans le cas d'un secret détenu par un seul porteur et sans que celui-ci l'ait noté (cas d'un support "humain"), que dans le cas d'un support numérique, même si, dans les deux cas, ce type de risques rentre en jeu.

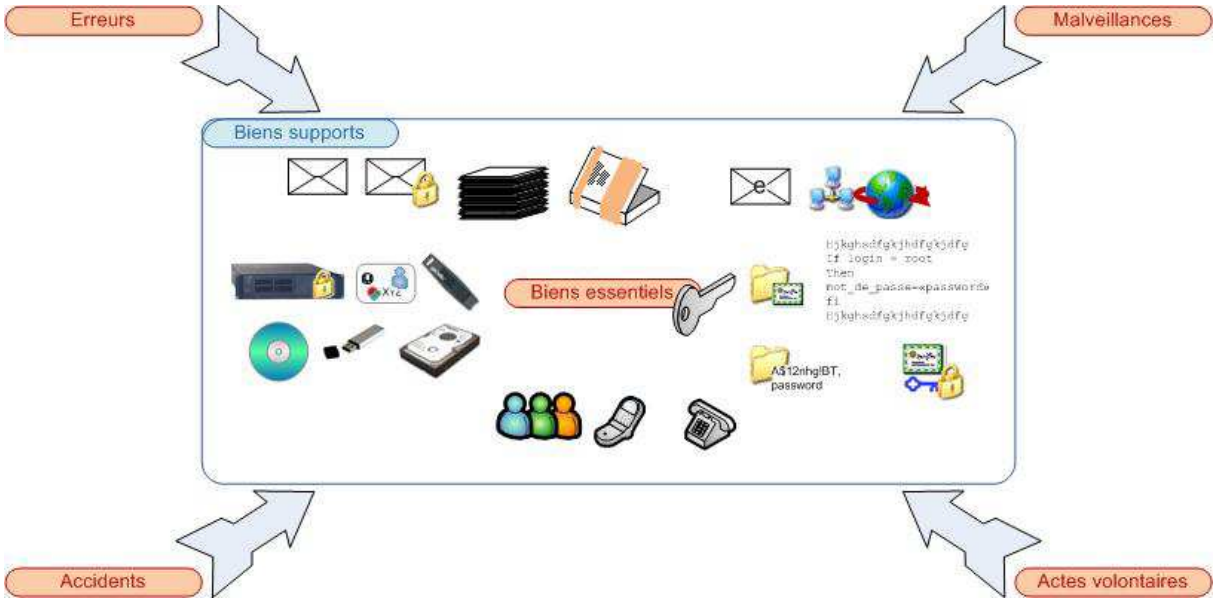


Figure 3 : Biens et menaces en gestion de clés

Au sein du catalogue de menaces possibles, certaines peuvent immédiatement être identifiées comme impactant la sécurité des secrets ! Par exemple, les menaces de type "Perte ou oubli de document ou de media" ou "vol physique", font immédiatement survenir des craintes quant à la confidentialité et à la disponibilité des éléments secrets contenus sur ces documents ou média.

De même pour les menaces "Perte d'un support papier", "Perte d'un matériel "Départ d'une personne" ou "Influence sur une personne" : leur implication est directe dans la sécurité des secrets confiés à des porteurs humains...

D'autres n'ont a priori qu'une incidence plus éloignée vis-à-vis de la gestion des secrets, comme par exemple les menaces liées au terrorisme ou au vandalisme. Pourtant, elles aussi peuvent être à prendre en compte, notamment vis-à-vis de la disponibilité de secrets, en fonction de l'environnement (urbain ou non...) et de l'activité de l'organisme (sensible ou non).

Il n'est donc pas possible d'écarter a priori l'une ou plusieurs des menaces potentielles identifiées. A chaque menace doit être associée une probabilité de survenue ; celle-ci dépend intimement du contexte et de l'activité de l'organisme... Cette évaluation est à faire par chaque organisme en fonction de son propre contexte.

Il est également possible de prendre en compte le potentiel d'attaque de l'agent menaçant :

- faibles capacités,

- capacités importantes,

- capacités illimitées.

Il est évident qu'un organisme aux activités sensibles devra prendre en compte des agents menaçants avec des capacités potentiellement importantes, voire illimitées (attaque par un état, par exemple), ce qui ne sera pas le cas d'une société à l'activité sans enjeu direct vis-à-vis de la sûreté nationale...

Suivant la nature de la menace, de son intention (malveillante ou non), de son potentiel d'attaque, les dégâts causés peuvent être plus ou moins importants, l'activité de l'entreprise

plus ou moins compromise, et par conséquent, les mesures à mettre en place pour contrer ces risques diffèreront.

B.3.2.C - Identification des risques résiduels après application des mesures usuelles

Les menaces potentiellement à l'origine de scénarios de risques impactant les secrets sont principalement liées à la nature de leur support (matériel, logiciel, humain, papier…)

A chaque type de support correspondent des menaces spécifiques :

- support matériel :
    - détérioration, détournement,
    - perte,
    - espionnage,
- support logiciel :
    - espionnage par analyse
    - suppression
- support humain :
    - départ volontaire ou non, disparition,
    - oubli,
    - divulgation,
- support papier :
    - perte,
    - destruction,
    - copie illicite,
- support « réseau » :
    - écoute passive, interception, modification non détectée,
    - indisponibilité du réseau.

B.3.2.D - Illustration par des scénarios commentés

Les scénarios de risques identifiés comme pouvant survenir majoritairement sont les suivants :

Scénario 1 : compromission d'une clé de signature.

Une telle clé peut par exemple appartenir à une personne physique ou un organisme, une application (Métier, d'Archivage) ou une Autorité (de Certification, d'Horodatage).

La compromission d'une telle clé entraîne des risques d'utilisation frauduleuse :

- signature frauduleuse de documents métiers (factures, mails, voire prescriptions médicales, actes notariés…) engageant la personne détentrice de la clé, et/ou son entreprise ;
- scellement frauduleux d'archives déposées dans un SAE (Système d'Archivage Electronique) et remise en cause de leur caractère probatoire (notion de valeur « probatoire ») ; atteinte à la réputation et à l'image du tiers de confiance archiveur ;

- signature frauduleuse de certificats électroniques, entraînant ainsi l'utilisation d'autres clés usurpées, de jetons d'horodatage ; dans tous les cas, atteinte majeure à l'image de l'Autorité ainsi corrompue.

L'atteinte potentielle à l'image de l'organisme ainsi usurpé, à la sécurité des personnes et des biens lui appartenant ou à ses clients, est évidente.

Scénario 2 : Perte d'une clé utilisée pour le chiffrement de données

Une telle clé peut par exemple appartenir à :

- une personne physique, ayant utilisé une clé de chiffrement pour assurer la confidentialité de ses données ou des messages qui lui sont transmis ;
- un organisme, ayant mis en œuvre des fonctionnalités de chiffrement au sein de ses applications et systèmes critiques : chiffrement de données stockées en bases, comme par exemple des données personnelles ou des données de santé (Dossier Patient…), chiffrement de données stockées au sein d'un système de type « coffre-fort » ; chiffrement des boites de messagerie…

L'accès aux données ainsi protégées est compromis : si le système de chiffrement ne permet pas de mécanisme « bris de glace » (accès possible aux données en urgence, nécessaire, par exemple, dans le domaine de la Santé), alors il peut être impossible de réaliser des actions nécessitant la connaissance de ces données : les conséquences en milieu hospitalier en sont par exemple aisément imaginables.

La compromission des clés de chiffrement est bien sûr, outre leur indisponibilité ou corruption, l'autre grand risque les menaçant.

Scénario 3 : compromission de clés ou de secrets d'authentification

Les services d'authentification (forte ou non !) basés sur la présentation d'éléments secrets (mots de passe, OTP (« One-Time-Password »), clés privées…) sont actuellement très répandus au sein des SI des entreprises et organismes de toute taille. Si beaucoup des applications protégées relèvent d'un niveau de sensibilité pouvant être qualifié de « standard », il n'en est pas moins nécessaire d'assurer l'imputabilité de l'authentification à son auteur, c'est-à-dire au titulaire de l'élément secret présenté.

De récents cas d'usurpation d'accès, par connaissance par exemple de mots de passe de « collègues », ont récemment défrayé la presse et ses chroniques judiciaires ces dernières années ou derniers mois, en raison notamment de leurs conséquences économiques ou financières, sans commune mesure avec la « faiblesse » -présumée- des systèmes d'authentification mis en œuvre.

B.3.3 - Particularités selon le domaine d'activités

Il est bien évident que dans des domaines où des intérêts vitaux de l'Etat sont en jeu, les menaces à prendre en compte, et surtout le potentiel d'attaque de l'agent menaçant, doivent être revus à la hausse.

Par ailleurs, d'autres réglementations peuvent également s'appliquer, comme notamment PCI-DSS (*Payment Card Industry Data Security Standard*) relatives à la conservation et à l'utilisation des **données de cartes bancaires**, ces réglementations peuvent inclure des dispositions relatives à la protection des données, et peuvent entraîner à la fois l'utilisation de techniques ou d'outils cryptographiques complémentaires, et la nécessité de protéger les secrets associés, ainsi que d'autres données préalablement non considérées comme des « secrets ».

Le domaine de la **Santé** est lui aussi concerné par la protection des données ; la mise en conformité vis-à-vis des dispositions relatives à la protection des données médicales, et notamment le « Décret Confidentialité » (« Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique ») entraine, directement ou non, la nécessité d'utiliser des techniques ou des mécanismes cryptographiques, dont le chiffrement, mais pas uniquement.

Quant au secteur de la **Défense**, précurseur en la matière, il s'est doté depuis de nombreuses années d'une organisation à la hauteur de ses enjeux :

- service "du Chiffre" : règles de transmission des informations classifiées (dont peuvent faire partie les clés et secrets)

Face à ces enjeux militaires, figurent également les **enjeux civils**. Le rôle de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est de promouvoir un référentiel cohérent et exhaustif sur lequel peuvent s'appuyer/auquel doivent se conformer les administrations de l'Etat.

Au sein de ce référentiel, l'on trouve notamment :

- l'annexe B_1 du RGS « Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » Version 1.20,
    - ce document décrit les règles minimales à respecter pour l'utilisation de mécanismes cryptographiques (algorithmes, tailles de clés) suffisamment robustes en fonction de l'usage et la durée d'utilisation prévus pour ces clés ;
- les dispositions relatives à la certification et à la qualification des produits de sécurité, donc par exemple les dispositifs d'authentification (cartes à puce cryptographiques) destinés à contenir les clés privées des utilisateurs :
    - ces certifications et qualifications permettent de garantir un niveau minimal de sécurité, mais surtout l'implémentation correcte des mesures de sécurité
    - elles peuvent être réalisées conformément aux Critères Communs (ISO 15408) ou à la Certification de Sécurité de Premier Niveau (CSPN) mise en place par l'ANSSI.

C. La couverture de ces risques : Les mesures de sécurité préconisées

Afin de couvrir les risques encourus pas les clés et secrets cryptographiques, il convient de mettre en place un ensemble de mesures d'ordre techniques et organisationnelles.

Aussi il existe déjà un certain nombre de modèles de gestion des clés et secrets qu'il convient de connaitre, au moins dans les grands principes.

C.1 - Aspects techniques

La première protection qu'une bonne gestion des clés se doit d'apporter à son infrastructure est la qualité intrinsèque des clés générées. Afin de permettre au lecteur de choisir les algorithmes et les tailles de clés appropriés, des organismes étatiques comme le NIST, la NSA (aux Etats-Unis), l'ANSSI (en France) ou le BSI (en Allemagne) fournissent des recommandations.

A ce titre, le site de BlueKrypt©, Keylength.com, rassemble ces recommandations dans des tableaux synthétiques, dont voici un exemple concernant l'ANSSI :

Ce papier [5] correspond aux recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il représente l'expression du gouvernement français en termes de qualité cryptographique.

Date	Symétrique	Asymétrique	Logarithme discret GF(p) Clef	Logarithme discret GF(p) Groupe	Logarithme discret GF(2^n) Clef	Logarithme discret GF(2^n) Groupe	Courbe elliptique GF(p)	Courbe elliptique GF(2^n)	Hash
2010 - 2020	100	2048	200	2048	200	2048	200	200	200
> 2020	128	4096	200	4096	200	4096	256	256	256

Les tailles de clef sont exprimées en bit. Ces résultats garantissent une sécurité minimale.
Cliquer sur une valeur pour la comparer avec les autres méthodes.

Remarques et algorithmes recommandés pour les systèmes symétriques:

La taille recommandée pour les systèmes symétriques est de 128 bits.
La taille minimale des blocs de chiffrement par bloc est de 64 bits (128 bits après 2020).
Il est recommandé d'employer des algorithmes par bloc et non des algorithmes de chiffrement par flot.
Algorithme de chiffrement: AES-CBC (FIPS 197)
Algorithme d'authentification et d'intégrité: CBC-MAC "retail" avec AES et 2 clefs distinctes.

Remarques et algorithmes recommandés pour les systèmes asymétriques:

Pour le chiffrement, les exposants publics doivent être strictement supérieurs à 2^{16}=65536.
Les exposants secrets doivent être de la même taille que le module.
Algorithme de chiffrement: RSAES-OAEP (PKCS#1 v2.1)
Algorithme de signature: RSA-SSA-PSS (PKCS#1 v2.1)
Algorithme de signature: ECDSA avec P-256, P-384, P-521, B-283, B-409 ou B-571 (FIPS 186-2)
Courbes elliptiques GF(p): P-256, P-384 et P-521 (FIPS 186-2)
Courbes elliptiques GF(2^n): B-283, B-409 et B-571 (FIPS 186-2)

Algorithme recommandé pour les fonctions de hachage: SHA-256 (FIPS 180-2)

Source BlueKrypt©, www.keylength.com/fr/5/

Ces recommandations peuvent également concerner le multi-contrôle auquel doivent être soumises les clés :

- Il est nécessaire de définir le nombre de personnes nécessaires aux différentes étapes de la vie des clés (Création, activation, suppression…). Ce nombre de personnes minimum peut être défini suite à l'analyse de risques.
- En aucun cas, ce nombre de personnes ne doit être égal à 1 ; il se doit donc d'être au moins égal à 2. Un nombre égal à 3 semble adapté aux petites structures, ce nombre pouvant être porté à 5 pour les structures plus importantes.

Il est également nécessaire de respecter le cycle de vie des clés de chiffrement ou secrets :

- Demande : La demande de génération et d'attribution des secrets doit faire partie d'un processus formel, incluant les approbations par les responsables compétents.
- Création : La création des secrets se doit d'être tracée et les journaux d'enregistrement des événements conservés. Il doit être possible de savoir qui a généré quoi, et de quelle manière.
- Distribution : Il se peut qu'un processus de distribution des secrets soit nécessaire afin de s'assurer notamment que les secrets sont remis aux bons destinataires, sans compromission.
- Activation : Dans certains cas, une activation formelle des secrets ou de la ressource matérielle ou logicielle supportant ces derniers est nécessaire. Cette activation se doit d'être sous multi-contrôle.
- Désactivation : A l'instar de l'activation, des procédures de désactivation peuvent s'avérer nécessaire. Même cette désactivation peut nécessiter d'être placée sous multi-contrôle.
- Révocation : Tout secret doit pouvoir être révoqué ; il peut y avoir plusieurs raisons à cela, comme le départ d'un employé, la compromission avérée ou suspectée des secrets, etc.
- Expiration : Tout secret se doit d'avoir une date d'expiration. Cette date d'expiration doit être calculée au plus juste en fonction du besoin et conforme aux recommandations évoquées ci-dessus.
- Mise sous séquestre : Afin de se prémunir contre la perte de secrets, ce qui pourrait avoir des conséquences graves en matière de disponibilité, un service de mise sous séquestre peut être disponible. Correctement protégés, les secrets peuvent être recouvrés en cas de sinistre.
- Recouvrement : Un autre moyen de se prémunir contre la perte de secrets est le recouvrement à savoir une opération qui consiste à régénérer les clés à partir d'une clé autre que l'on aura précieusement gardée et protégée.
- Destruction : Un processus de destruction sécurisée des clés ou secrets doit être mis en place afin de garantir qu'en cas de compromission ou tout simplement en fin de vie, ces secrets seront correctement détruits sans possibilité d'être recouvrés.

C.2 - Aspects organisationnels

La deuxième protection qu'une bonne gestion des clés doit apporter à son infrastructure est la mise en place d'une gestion centralisée, centralisation de la fonction et des données. Cette gestion centralisée pourrait être matérialisée par une ou plusieurs personnes, ROC soutenus par des piliers de nature autant documentaire, qu'organisationnelle ou encore physique.

C.2.1 - Le ROC ou Responsable des Opérations Cryptographiques

L'expérience montre qu'il est indispensable de désigner formellement un responsable de la gestion des clés ainsi que des secrets et matériels associés à celles-ci, ce responsable pouvant avoir un ou plusieurs adjoints.

Une dénomination possible pour ce poste serait « Responsable des Opérations Cryptographiques », en charge de faire respecter les procédures définies en la matière, un 'policier' directement responsable de la mise en œuvre et de la protection des données et/ou matériels impliqués.

Pourquoi ?

- Parce que la traçabilité sur tout le cycle de vie d'un secret est à ce prix.
- Parce que le doute sur l'intégrité de la clé, du secret d'activation ou encore du HSM n'est pas une option.

Dans les petites structures, le RSSI peut remplir la fonction de ROC.

C.2.2 - Les piliers du ROC

Les piliers sont à la fois les outils à la disposition du ROC pour mener à bien sa mission, mais aussi les fondements de sa fonction, ce sur quoi il peut s'appuyer pour faire prévaloir ses prérogatives.

C.2.2.A - Politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) traduit les orientations prises par la direction générale en matière de sécurité des systèmes d'information. Celle-ci est souvent basée sur des standards reconnus tels ISO 27001 et ISO 27002. Elle couvre les objectifs de sécurité identifiés par l'Analyse de Risques.

C.2.2.B - Organisation de la sécurité de l'information

L'organisation de la sécurité de l'information consiste à définir le cadre de gestion de celle-ci et les rôles de ses principaux protagonistes. Il s'agit également de contrôler la mise en œuvre de la sécurité des systèmes d'information. Le Responsable des Opérations Cryptographiques doit être identifié comme un acteur essentiel de cette organisation, il peut être placé directement sous un Directeur des Systèmes d'Information (DSI), un Responsable de la Sécurité des Systèmes d'Information (RSSI) ou encore un Directeur Technique.

C.2.2.C - Gestion des biens

Le Responsable des Opérations Cryptographiques s'appuie sur une gestion rigoureuse et centralisée des actifs critiques. Il est souvent responsable de l'inventaire de ces actifs critiques nécessaires au bon fonctionnement du système d'information de l'entreprise.

C.2.2.D - Sécurité physique & Contrôle d'accès

La PSSI définit les niveaux de sécurité physiques ainsi que les contrôles d'accès à utiliser dans le cadre de la gestion des ressources cryptographiques.

Le plus souvent sont utilisés des contrôles à multiples facteurs ainsi que le partage des secrets afin d'assurer le niveau de sécurité attendu.

C.2.2.E - Cérémonie des clés

La cérémonie des clés encadre les modalités de génération et de conservation des clés et secrets cryptographiques, comme par exemple la génération du bi-clé de l'Autorité de Certification (AC) et de son certificat destiné à signer les certificats qu'elle émettra.

La cérémonie des clés est le plus souvent suivie de la mise en service de ces clés. Dans le cas d'une Autorité de Certification, l'objectif est de permettre la production des certificats en volume.

C.2.2.F - Gestion de l'exploitation

Le ROC est le garant d'une exploitation sécurisée des ressources cryptographiques et des secrets associés. Il doit assurer en particulier une parfaite *traçabilité* lors de manipulation de ces ressources et secrets.

C.2.2.G - Gestion des incidents liés à la sécurité de l'information

Le responsable des opérations cryptographiques est en particulier en charge de la révocation des certificats associés aux clés en cas de compromission suspectée ou avérée, et en particulier pour les AC. Cette gestion des incidents liés au chiffrement peut faire partie d'un Plan global de Réponses aux Incidents du SI.

C.2.2.H - Gestion du PCA/PRA

Dans le cadre de la continuité ou de la reprise d'activité, le responsable des opérations cryptographiques est le plus souvent impliqué dans la réactivation des ressources faisant usage de moyens cryptographiques. Lors d'incidents majeurs il est l'acteur principal d'un éventuel recouvrement des clés.

C.2.2.I - Conformité PSCE

La certification *Prestataire de service de certification électronique* (PSCE) au sens du décret n° 2001-272 du 30 mars 2001 désigne toute personne physique ou morale qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique.

Le PSCE peut délivrer des *certificats qualifiés*, c'est-à-dire conformes à des exigences réglementaires et normatives.

Le certificat qualifié est un certificat à usage exclusif de signature électronique. Un document signé avec un certificat qualifié est présumé fiable et inverse ainsi la charge de la preuve en cas de litige.

C.3 - Modèles actuels de gestion de clés

C.3.1 - Modèle « PKI »

Il s'agit du modèle le plus connu et probablement le plus utilisé car il est à la base de la distribution massive des certificats X.509, de l'utilisation du protocole SSL et du commerce en ligne.

Il s'agit d'un modèle hiérarchisé de gestion de clés asymétriques, et qui garantit l'association entre une bi-clé et une identité.

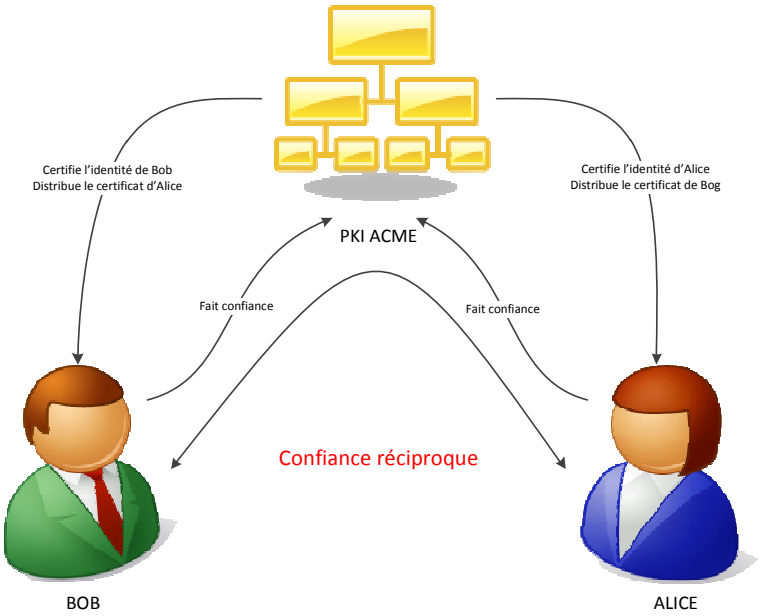
Chaque membre de l'organisation dispose d'une clé privée qu'il garde secrète et de la clé publique associée. Cette clé publique est diffusée au sein d'un certificat électronique qui joue le rôle de pièce d'identité car elle contient l'identité du porteur. Il est important de noter que l'identité peut désigner aussi bien une personne physique qu'une machine ou tout autre composant.

L'authenticité de ce certificat (et donc de l'association entre l'identité et la clé publique) est garantie la signature électronique apposée par l'Autorité de Certification (AC), qui peut elle-même être certifiée par l'AC de niveau supérieur, dans une logique hiérarchique.

Cette hiérarchie est dominée par une AC dite Racine, qui est signée par elle-même ou éventuellement Cross Certifiée à savoir signée réciproquement par une autre AC Racine, et à laquelle l'utilisateur est invité à faire confiance s'il souhaite utiliser les certificats émis par les AC certifiées par cette AC Racine.

Lorsque l'usage d'un certificat doit être interdit avant sa fin de validité naturelle (suite à un vol ou une fin d'activité), celui-ci sera révoqué.

A partir du moment où une personne fait confiance à une AC en important son certificat dans son navigateur (dans le magasin de certificats de ce dernier), elle reconnaît comme valides tous les certificats émis par cette AC ou par une AC de niveau inférieur et qui ne sont pas révoqués : l'utilisateur acceptant le certificat d'une AC Racine, reconnait ensuite automatiquement comme valides tous les certificats sous cette Autorité.



Les niveaux de services et surtout les processus que met en œuvre la PKI pour contrôler la validité d'une identité avant de délivrer un certificat sont décrits dans un document public

appelé Politique de Certification. Il s'agit d'un contrat entre la PKI et ses clients, utilisateurs, « consommateurs » des certificats délivrés aux porteurs. Cette politique permet à l'utilisateur de savoir jusqu'à quel point et pour quels usages, il peut faire confiance en un certificat émis par une PKI donnée. En particulier, la PKI peut restreindre les domaines fonctionnels d'utilisation des certificats qu'elle émet en fonction de leur cible d'utilisation (authentification, chiffrement, signature électronique).

Il est très important de noter que la PKI se limite à garantir le lien entre une identité et une clé publique via le certificat. La gestion des habilitations (droits d'accès applicatifs) est de la responsabilité des applications utilisatrices et non de la PKI.

La diffusion des certificats peut être réalisée suivant plusieurs modes, généralement via publication au sein d'un annuaire.

Avantages

- Fonctionnement hiérarchique maitrisé
- Système organisé et contractualisé via des politiques
- bien documentée et standardisée (X.509)
- interopérable
- ne nécessite que la possession du certificat d'AC (et d'une liste de certificat révoqués à jour) pour prouver l'identité d'un tiers

Inconvénients

- organisation qui peut être complexe à mettre en œuvre
- fonctionnement assez rigide (il est nécessaire de respecter les processus d'enregistrement et de gestion de l'opérateur de PKI)
- l'utilisateur doit faire confiance dans le fait que l'opérateur de la PKI se limitera à son périmètre d'activité

Les services d'une PKI peuvent être mis en place via le déploiement d'une offre logicielle, ou sous forme d'offre de service auprès d'opérateurs de certification dits tiers de confiance.

Nature des coûts

- Achat des licences et matériels spécifiques
- Coût d'exploitation et de support (révocations, renouvellement, gestion des oublis du support de stockage)
- Coût organisationnel de la gestion des processus de distribution des identités (enregistrement des utilisateurs, renouvellement des identités…)
- Coût éventuel du support de stockage de l'identité (type carte à puce)

C.3.2 - Modèle PGP

Il s'agit d'un modèle du type « les amis de mes amis sont mes amis » c'est à dire d'un réseau de confiance. Pretty Good Privacy a été inventé en 1991 par Philip Zimmermann.

Il n'y a pas de composant centralisé qui garantit l'association entre une identité et une clé selon une politique publiée, c'est l'utilisateur qui ajoute manuellement des identités dans sa

base personnelle d'identités valides. Cette base est appelée un « keyring » ou cercle de confiance.

Lorsque l'utilisateur ajoute une identité à son cercle, il peut faire confiance à celui-ci et reconnaître également son « keyring ». Son domaine de confiance est alors étendu au « keyring » tiers qui peut lui aussi habiliter d'autres « keyrings » et ainsi de suite.

En l'absence de centralisation du contrôle des identités, il n'y a pas de processus de contrôle ni aucun contrat de service. C'est à chacun des utilisateurs à être vigilant sur les identités auquel il accorde sa confiance.

Pour avoir l'assurance qu'une clé (et l'identité associée) ajoutée au keyring est valide, il faut que l'utilisateur ait la maitrise de ce processus (par exemple lors d'une rencontre physique en face à face ou via la réception par un autre canal qui garantit la validité des données échangées).

Le fonctionnement de PGP a été standardisé dans la RFC 4880.

Avantages du modèle

- principe de fonctionnement simple
- l'absence de serveur centralisé rend l'infrastructure légère
- présent sur le marché depuis longtemps
- seul l'utilisateur a connaissance de sa clé privée (en général mais pas obligatoire)

Inconvénients du modèle

- Nécessite un face à face (ou équivalent) pour vraiment reconnaître une identité
- Le niveau d'assurance sur la validité d'une identité est plus faible que dans une gestion « PKI » et repose sur la confiance que l'utilisateur met dans la rigueur de gestion de « amis »
- N'offre aucun niveau de service et d'engagement sur la fiabilité des données
- Problématiques de révocation
- Peu interopérable

Le modèle PGP est actuellement diffusé en solution propriétaire par la société PGP corporation ou en logiciel libre via OpenPGP (sans compter toutes les applications qui supportent PGP via des bibliothèques de compatibilité).

Nature des coûts

- Achat des licences (hors logiciel libre) et matériels spécifiques
- Coût d'exploitation et de support (dans un contexte d'entreprise)
- Coût organisationnel de la gestion des processus de distribution des identités (absence de mécanisme centralisé et intégré)
- Coûts cachés liés aux risques découlant de l'absence de gestion centralisée des identités (absence de vérification formelle de l'identité)
- Coût éventuel du support de stockage de la clé (type carte à puce)

C.3.3 - Solutions propriétaires ou fermées

Il s'agit ici de l'ensemble des solutions propriétaires mises en œuvre par certains éditeurs pour répondre à des besoins de gestion de clé.

Par nature, leur fonctionnement est fermé et non connu. Il s'agit parfois d'un fonctionnement dérivé de celui d'une PKI X.509 mais sans utiliser de certificat ou sans être interopérable. Les technologies utilisées (algorithmes et implémentation) ne sont généralement par diffusées ce qui ne permet pas d'en évaluer le niveau de sécurité et la fiabilité.

Par exemple, il peut s'agir d'une solution où un serveur central conserve l'ensemble des clés et des identités. Lorsqu'une entité a besoin de correspondre avec une autre entité, elle sollicite ce serveur qui lui fournit la clé pour joindre son correspondant. L'authenticité du fonctionnement dépend des mécanismes d'authentification mis en place pour accéder au service centralisé.

Celui-ci dispose de toutes les clés de tous les utilisateurs. En cas d'intrusion sur ce serveur, toutes les identités sont compromises.

Avantages

- Peut être plus efficace dans certains contextes métiers (environnements fermés) par exemple en s'affranchissant des processus de distribution des clés
- Fonctionne aussi bien pour des clés asymétriques que des clés symétriques

Inconvénients

- Technologies par définition non interopérables
- Le fonctionnement est caché et peut plus difficilement être évalué par le client
- Les algorithmes utilisés peuvent être « maison » et ne pas avoir été évalués
- Requiert de faire 100% confiance à un éditeur
- En cas d'incident de sécurité, l'ensemble des identités sont compromises

Nature des coûts

- Achat des licences et matériels spécifiques
- Coût d'exploitation et de support
- Coûts cachés liés au manque de maitrise de la solution (dépendance au fournisseur, risque de porte dérobée)
- Coût éventuel du support de stockage de la clé (type carte à puce)

Ce type de solution se retrouve parfois dans des logiciels répondant à des besoins métiers tels que le monde médical pour l'échange de données entre médecins et laboratoires.

Certaines solutions de chiffrement d'Entreprise utilisent parfois ce modèle (ce qui n'interdit pas d'utiliser une PKI X.509 pour l'authentification des utilisateurs auprès du service de chiffrement).

C.3.4 - Modèle non structuré

Il s'agit de l'autre modèle le plus couramment rencontré où il n'y a aucune organisation de gestion, aucun processus. Chaque utilisateur se débrouille comme il le peut.

Il s'agit du modèle que l'on retrouve quand le chiffrement symétrique est utilisé pour diffuser les clés ou les « passphrase » (par exemple en cas de chiffrement d'un fichier zip en vue d'un envoi par mail).

Il s'agit aussi tout simplement du modèle des mots de passe d'accès au réseau d'Entreprise et des « passphrase » en général.

Pour obtenir un bon niveau d'assurance sécurité, ce modèle nécessite des moyens organisationnels très lourds pour assurer la correspondance entre les identités et les clés (par exemple des listings stockés dans un coffre contenant la liste des destinataires de messagerie associés à la « pass-phrase » utiliser pour leur envoyer un email contenant une pièce jointe chiffrée sans s'appuyer sur une PKI).

Avantage

- simple à comprendre et à mettre en place
- Rapide à mettre en œuvre sur de petits périmètres

Inconvénients

- Peut devenir très complexe en cas de volonté de disposer d'un niveau de fiabilité élevé ou si le nombre d'acteurs augmente
- Absence de garantie de fonctionnement et de structure de contrôle

Nature des coûts

- Support des utilisateurs qui perdent leur mot de passe ou leur clé
- Coût de fonctionnement lié au fait que chaque relation 1 à 1 demande une clé gérée manuellement
- Coûts cachés liés au manque de sécurité des processus de distribution et de gestion qui induit des risques de fuite d'information, de vol d'identité et de panne
- Nécessite de nombreux processus manuels

D. ANNEXES

D.1 - Glossaire acronymique

AC (Autorité de Certification)
Dans le cadre d'une PKI, entité qui délivre des certificats électroniques.

AES (Advanced Encryption Standard)
Algorithme de chiffrement symétrique, standardisé par le NIST.

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
Autorité française en matière de sécurité des systèmes d'information. Rattachée au Secrétaire général de la défense et de la sécurité nationale.

BCP (Business Continuity Plan): Voir PCA.

CA (Certification Authority) : Voir AC.

COM (Cryptographic Operations Manager) : Voir ROC.

CC (Critères Communs, Common Criteria)
Standard international (ISO/IEC 15408)pour la sécurité des systèmes d'information, dont le nom exhaustif est "Common Criteria for Information Technology Security Evaluation". Standard d'évaluation le plus utilisé à ce jour. En France, l'ANSSI délivre des certificats basés sur ce standard.

CEI (Commission Electrotechnique Internationale) : Voir IEC.

Cryptographie : Technique ayant pour but de rendre inintelligible un message aux yeux de ceux à qui il n'est pas destiné.

CSPN (Certification de Sécurité de Premier Niveau)
Label de l'ANSSI obtenu au terme d'une expertise moins pointue que celle des Critères Communs.

DMCA (Digital Millennium Copyright Act)
Loi américaine de 1998 ayant pour but d'établir une législation de la propriété intellectuelle adaptée à l'information numérique.

DRP (Disaster Recovery Plan) : Voir BCP.

HSM (Hardware Security Module)
En français, Dispositif de Sécurité Matériel. Coffre-fort numérique permettant de créer, stocker et contrôler l'usage sécurisé de composants critiques, tels que des clés cryptographiques.

IEC (International Electrotechnical Commission)
Organisme de normalisation couvrant des domaines complémentaire à ceux de l'ISO, tel que les ondes électomagnétiques pour le Wi-Fi (ISO/CEI 8802-11).

IETF (Internet Engineering Task Force)
Groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards pour Internet. L'IETF produit la plupart des nouveaux standards d'Internet.

IGC (Infrastructure de Gestion de Clé) : Voir PKI.

ISO (International Standards Organisation)
Organisation Internationale de Normalisation.

ITU (International Telecommunication Union)
Organisme de normalisation dépendant de l'ONU. Cet organisme a notamment produit la norme des certificats électronique (X.509).

NIST (National Institute of Standards and Technology)
Institution américaine ayant pour but de promouvoir l'économie en développant les technologies.

OSI (Open Systems Interconnection)
Norme ISO 7498, servant de référence pour décrire l'interconnexion réseau entre systèmes ouverts.

OTP (One Time Password)
Solution d'authentification forte reposant sur des mots de passe à usage unique.

Patriot Act : Loi américaine de 2001 visant à faciliter la lutte contre le terrorisme.

PCA (Plan de Continuité d'Activité)
Organisation de l'entreprise pour assurer la continuité de l'activité en cas de désastre (notamment panne informatique majeure). Le PCA est à la fois le nom d'un concept, d'une procédure et du document qui la décrit.

PCI-DSS (Payment Card Industry - Data Security Standard)
Directives de sécurité imposées par l'industrie des cartes bancaires (VISA, AMEX, MASTERCARD, JCD et DISCOVERY) à toute entité manipulant des données de cartes de paiement.

PGP (Pretty Good Privacy)
Logiciel de chiffrement et de signature de données, développé par Philip Zimmermann en 1991 et téléchargeable librement sur Internet.

PIN (Personal Identification Number)
Code confidentiel composé exclusivement de chiffres, utilisé avec des terminaux ayant peu de touches (Distributeurs de billets, téléphone mobile, …).

PKCS (Public-Key Cryptographic Standards)
Ensemble de spécifications liées à la cryptographie, publiées par les laboratoires RSA. Certaines spécifications sont devenues standard de fait.

PKI (Public Key Infrastructure).
En français **IGC**, ensemble de composants physiques, logiciels, procédures et documents visant à gérer le cycle de vie des certificats numériques et éléments connexes.

PRA (Plan de Reprise d'Activité)
Organisation des services informatiques pour assurer la remise en service des infrastructures et des applications en cas de panne majeure.

PSCE (Prestataire de Services de Certification Electronique)
Dans le contexte des marchés publics français, toute entité qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique.

PSSI (Politique de Sécurité des Systèmes d'Information)
Plan d'actions défini pour maintenir un niveau de sécurité conforme à la stratégie de l'entreprise.

RFC (Request for Change)
Documents de l'IETF décrivant les aspects techniques d'Internet. Certaines RFC deviennent ensuite des standards.
A ne pas confondre avec la définition ITIL (Request for Change).

RGS (Référentiel Général de Sécurité)
Ensemble de règles de sécurité qui s'imposent aux autorités administratives françaises dans la sécurisation de leurs systèmes d'information.

ROC (Responsable des Opérations Cryptographiques)
Responsable de la gestion des clés de chiffrement ainsi que des secrets et matériels associés à ceux-ci.

RSA (Rivest, Shamir and Adleman)
Algorithme de cryptographie asymétrique, devenu un standard incontournable. Le nom est l'initiale de ses auteurs.

SaaS (Software as a Service)
Concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence.

SAE (Système d'Archivage Electronique)
Environnement de gestion du cycle de vie du document, de sa création à sa destruction.

SSL (Secure Sockets Layer)
Protocole de sécurisation, très utilisé avec les pages Web. S'appelle désormais TLS (Transportation Layer Security), mais l'acronyme SSL reste très utilisé.

SSO (Single Sign-On)
Méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques.

UIT (Union Internationale des Télécommunications) : Voir ITU.

VPN (Virtual Private Network)
Technique d'interconnexion de réseaux locaux permettant de chiffrer les communications pour en conserver la confidentialité.

X.509 Norme de PKI de l'ITU. La structure des certificats est définie plus spécifiquement par la RFC 5280 de l'IETF.

D.2 - Bibliographie - Pour aller plus loin …

D.2.1 - Normes et standards :

- UIT/SG17 Identity management framework

- IEEE - P1619.3 Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data

- ISO 11770 "Key Management" :

- ISO/IEC 11770-1 : 1996 : Gestion de Clés - Partie 1 : Cadre général
- ISO/IEC 11770-2 : 2008 : Gestion de Clés - Partie 2 : Mécanismes utilisant des techniques symétriques
- ISO/IEC 11770-3 : 2008 : Gestion de Clés - Partie 3 : Mécanismes utilisant des techniques asymétriques
- ISO/IEC 11770-4 : 2006 : Key management - Part 4 : Mechanisms based on weak secrets
- ISO/IEC 11770-5 : (projet) : Key management - Part 5 : Group key management

- ISO 11568 - Banking -- Key management (retail)
  - ISO 11568-1 : 2005 - Part 1: Principles
  - ISO 11568-2 : 2005 - Part 2: Symmetric ciphers, their key management and life cycle
  - ISO 11568-3 (Projet) : Part 3: Key life cycle for symmetric ciphers
  - ISO 11568-4 : 2007 Part 4: Asymmetric cryptosystems -- Key management and life cycle

ISO 15782-1:2009 Certificate management for financial services -- Part 1: Public key certificates
ISO 15782-2:2001 Banking -- Certificate management -- Part 2: Certificate extensions

D.2.2 - Documentation sur les modèles de gestion de clés :

- "Certificateless Public Key Cryptography" - Sattam S. Al-Riyami and Kenneth G. Patersony - 21/10/2003

D.2.3 - Documents de bonnes pratiques existants :

D.2.3.A - D'ordre générique :

- Annexe RGS_B_2 : titre : RGS 1.0 - Annexe B2 - Gestion des clés cryptographiques - Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques.
  Version 1.10 du 24/10/2008

D.2.3.B - D'ordre sectoriel :

Finances :
IEEE - P1619.3 Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data
Management:
- Part 1 : General (révision en 2007).
- Part 2: Best Practices for Key Management Organization (édité en 2002)
- Part 3 : Applicationy-Specific Key Management Guidance (édité en 2002

D.2.3.C - Documentation/préconisations d'éditeurs de logiciels et matériels cryptographiques

- SafeNet "An Enterprise Guide to Understanding Key Management" – 08/2009
- SafeNet "Applying Enterprise Security Policy and Key Management" – 08/2009
- RSA "Managing lifecycle of keys with RSA Key Manager.pdf" - 2007

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.fr

Téléchargez les productions du CLUSIF sur

www.clusif.fr