Les systèmes d'Infrastructure à Clé Publique (PKI)

LIVRE BLANC

Edition de Juin 2015

Ce document de sécurité a été rédigé par **ESSIANE ELLA Justin**, Directeur du Centre PKI de l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC).

Edition de Juin 2015

Publié par ANTIC
B.P. 6170 Yaoundé – Cameroun,
Tél. +237 242 08 64 97 / +237 694 40 58 68
e-mail : pki@antic.cm
Site web : www.antic.cm,

Objet

Le Livre Blanc portant sur les systèmes d'infrastructure à clé publique (PKI=Public Key Infrastructure) que nous publions ce jour est un document qui vise à présenter au lecteur des concepts de base en cryptographie et le mode de fonctionnement de cette technologie de sécurité de manière générale, ainsi que l'usage que l'on peut en faire. Il est écrit à l'intention des utilisateurs des systèmes PKI, des étudiants et autres chercheurs en cryptographie, des communicateurs et des curieux. Pour des notions avancées, le lecteur est prié de prendre l'attache du contact ci-dessus.

Il convient de relever d'entrée de jeu que le présent document ne remplacera jamais le cours de cryptographie des milieux universitaires et écoles de formation spécialisées. Il n'en a d'ailleurs pas l'intention. Il doit être perçu comme l'un des multiples articles écrits sur ce sujet.

Notre intention est de mettre les utilisateurs des certificats actuels et potentiels en confiance parce que nous sommes convaincus que les systèmes PKI que nous leur proposons d'utiliser dans le monde virtuel pour faire leurs échanges sécurisés sont robustes, fiables et faciles d'utilisation. Comme le réseau Internet est en soi non sécurisé, les systèmes PKI ont été conçus pour vous assurer la sécurité nécessaire lorsque vous vous engagez dans des transactions électroniques sur Internet. Il vous suffit juste de communiquer avec un système sécurisé à l'aide d'une PKI et de disposer d'un certificat électronique.

Nous invitons donc tous les lecteurs à bénéficier des opportunités qu'offrent aujourd'hui les systèmes PKI pour évoluer dans le cyberespace sans méfiance ni crainte.

Table de Matières

Introduction Générale

Ce qui nous amène à écrire ce document de sécurité qui porte sur la technologie PKI (Public Key Infrastructure) ou infrastructure à clé publique est le souci que nous partageons à présenter une solution de cybersécurité robuste, fiable et éprouvée qu'il convient de déployer dans les réseaux d'entreprises pour faire face à la recrudescence des actes de cybercriminalité.

Dans l'ensemble, la technologie PKI utilise les moyens de cryptographie pour sécuriser l'information qui circule dans le cyberespace.

En général, il existe plusieurs types de systèmes d'infrastructure à clé publique que l'on peut classer en deux (02) grands groupes :

- le groupe qui permet à l'administrateur du système de générer la paire de clés, d'émettre le certificat et de donner une copie de chaque élément à l'utilisateur final. Dans cette technique, l'administrateur du système a connaissance de la clé privée de l'utilisateur et la protège. En cas de perte, il peut lui procurer une autre copie ;
- et le groupe des PKI où l'utilisateur génère par lui-même la paire de clés, grâce au dispositif technique que le système met à sa disposition, puis l'utilisateur envoie juste la clé publique en ligne à l'opérateur de l'autorité de certification pour l'émission de son certificat. Dans ce deuxième groupe, l'administrateur du système PKI n'a pas connaissance de la clé privée de l'utilisateur. L'utilisateur est donc le seul responsable de la sécurité de sa propre clé privée.

Au moment de conduire une étude de faisabilité d'un système PKI, il conviendrait de faire le bon choix pour la communauté d'utilisateurs. Il ne faudrait pas négliger cet aspect, et toujours se souvenir que la première règle en sécurité c'est que ″l'on ne fait confiance à personne.″

Le document dont la teneur suit décrit les principes de base qui sont communs aux deux groupes des systèmes PKI.

Nous avons pensé qu'il faille commencer par présenter les actes de cybercriminalité perpétrés dans le monde avant de nous attaquer à la notion de cybersécurité. Ce d'autant plus qu'un adage de chez nous stipule que ″Pour contrer efficacement une personne, il faut soit penser comme elle, donc savoir comment elle agit, soit connaître ses limites, mieux ses faiblesses.″

Chapitre 1 : LA DELINQUANCE NUMERIQUE

Introduction : Contexte Général

Les systèmes informatiques se trouvent au centre des systèmes d'information. Ces derniers irriguent l'ensemble du patrimoine de tout organisme. Il s'agit notamment de la propriété intellectuelle, du savoir-faire et de la stratégie de développement. Ils facilitent la diffusion et l'échange d'informations entre entités au sein d'un organisme.

Le constat est que l'information qui circule dans ce réseau est très prisée par beaucoup de gens. Elle confère au système d'information ou cyberespace, une dimension incontournable au sein de l'organisme.

Il convient de relever que l'information représente pour un organisme, un capital précieux et une source fondamentale pour son développement. C'est son bien économique.

L'importance que revêt l'information est diverse et fonction de l'activité qu'exerce l'organisme. Ce dernier devrait dès lors, se doter de tous les moyens pour la protéger. L'on comprend aisément pourquoi elle fait souvent l'objet de tant de convoitises, de la part des concurrents et des hackers ou pirates informatiques. Aujourd'hui, aucune entreprise ne peut plus se passer de l'utilisation d'un système d'information, dans l'accomplissement de ses activités quotidiennes.

Dans tous les secteurs d'activités, les systèmes d'information font désormais partie du fonctionnement des Administrations et Institutions Publiques, de l'activité des entreprises, et du mode de vie des citoyens. Les services qu'ils assurent deviennent tout aussi indispensables que l'approvisionnement en eau, en électricité ou en téléphone.

Pour une compréhension aisée de ce document, l'on entendra par système d'information ou cyberespace, un ensemble de machines connectées entre elles de façon permanente ou temporaire permettant à une communauté de personnes physiques ou morales d'échanger des informations.

Si l'on s'en tient à cette définition, des systèmes aussi variés que le réseau d'un opérateur de téléphonie, le réseau Intranet d'un organisme, le réseau de commandement des forces de maintien de l'ordre… sont des systèmes d'information.

Un système d'information est aussi l'ensemble constitué par un réseau, des machines ou équipements et des données ou informations.

Nous vibrons maintenant à l'heure du commerce électronique, de la gouvernance électronique, de l'économie numérique pour les transactions électroniques de toutes sortes ont droit de cité. Nous sommes, pour tout dire, au pays des merveilles de l'Internet.

Les Administrations, Institutions et Entreprises sont maintenant obligées de dématérialiser les procédures des services qu'elles rendent au public pour épouser l'ère du temps. L'usage de l'Internet devient incontournable à telle enseigne qu'un organisme non connecté de nos jours contribuerait à sa propre mort.

Par ailleurs, l'Internet fournit un cadre privilégié aux transactions électroniques.

Il convient de se rappeler que, l'informatisation du monde telle que nous la vivons a été engendrée par des érudits de la technologie. Dans leur rêve, Internet ne devait être qu'un espace libre et d'échanges, où l'on cherche sans cesse à pousser des limites de la technologie, à apprendre et à partager ses connaissances avec le grand nombre. Ils n'avaient jamais envisagé que le cyberespace deviendrait le supermarché virtuel qu'il est aujourd'hui.

De simple réseau public d'informations, l'Internet est devenu pour de nombreux organismes, un moyen d'accès au système de partage de l'information que l'on offre, suivant les cas, aux collaborateurs, partenaires, clients, grand public ou encore fournisseurs.

La multiplication des moyens d'accès, l'ouverture des réseaux de l'organisme au monde extérieur, la décentralisation des traitements de données… accroissent des menaces et des risques de dénaturation des systèmes, d'altération des données et fragilisent le système d'information. Il devient alors la cible privilégiée d'attaques cybernétiques, qui visent non seulement à prendre connaissance, copier, modifier, effacer l'information, mais aussi à paralyser le système tout entier.

Du fait de leur interconnexion, les réseaux de communications électroniques et les cyberespaces qui constituent Internet, se trouvent exposés à des menaces et aux risques de toutes sortes. Cela met au grand jour la problématique de la sécurité à laquelle il faut rapidement trouver des solutions, afin d'éviter un jour le chaos.

En général, Internet met en relation des individus aux motivations différentes. D'aucuns vont y faire de la recherche ou consulter des e-mails, tandis que d'autres s'y intéressent pour bien mener des activités inavouées. Les pirates informatiques utilisent Internet, pour commettre des infractions (délits et crimes) cybernétiques encore appelées cybercriminalité. Autant Internet nous émerveille par des services fabuleux qu'il nous offre, autant il s'accompagne hélas, d'une prolifération de virus, de vers, de chevaux de Troie, de spywares, de malwares, de botnet... fruit des individus qui sont à la recherche de l'information épique, pour couler des entreprises. L'espionnage industriel visant à intercepter des informations d'adversaires ou de concurrents sont légion sur le net.

Ces pirates d'un genre nouveau utilisent leurs connaissances en informatique pour rechercher, coûte que vaille, l'information et commettre des forfaits prémédités.

1.1. Importance de l'information

La sagesse populaire camerounaise a coutume de dire : "Qui détient l'information, possède le pouvoir." Les Etats-Unis d'Amérique ont parfaitement compris, et ce depuis longtemps, tout l'intérêt stratégique et politique du contrôle absolu de l'information. C'est à juste titre qu'ils ont mis un point d'honneur sur l'"information dominance" qui est "l'aptitude à prendre connaissance des communications secrètes de nos adversaires tout en protégeant nos propres communications", capacité par laquelle les Etats-Unis dominent le monde. Le scandale des écoutes téléphones des hauts responsables d'Etat de par le monde, l'affaire wikileaks qui viennent d'éclater dans ce pays et les actes de cybercriminalité visant les médias comme TV5 monde en disent long.

La recherche effrénée de l'information, voilà la clé de voûte qui conduit des gens à poser des actes répréhensibles.

Les pirates informatiques sont des gens sans foi ni loi. Ils se servent de leurs connaissances en informatique, pour détruire, altérer, accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement des systèmes d'information des organismes. Les motivations sont diverses, fonction de la nature des informations recherchées et de la cible visée.

Pour l'Etat du Cameroun, il s'agit d'un enjeu de souveraineté nationale non marchandable. Il a, en effet, la responsabilité de garantir la sécurité de ses propres systèmes d'information, la continuité de fonctionnement des Institutions et des infrastructures vitales pour les activités socio-économiques du pays, sans oublier la protection des entreprises du secteur privé et des citoyens.

De leur côté, les entreprises doivent protéger, de la concurrence et de la malveillance, leur système d'information qui irrigue l'ensemble de leur patrimoine (propriété intellectuelle et savoir-faire) et porte leur stratégie de développement.

1.2. Les cyberattaques

Internet ne connaît pas les limites géographiques de nos pays. C'est un réseau qui fait du monde entier un village planétaire. Tout ordinateur connecté à ce réseau est potentiellement vulnérable à une ou plusieurs attaques cybernétiques encore appelées cyberattaques.

Une "cyberattaque ou attaque cybernétique" est l'exploitation d'une faille ou vulnérabilité dans un système informatique : système d'exploitation, logiciel ou programme de l'utilisateur à des fins non connues par le propriétaire de l'ordinateur, mais généralement préjudiciable.

Internet n'a jamais été conçu pour être sécurisé. Sur Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques cybernétiques par minute sur chaque machine connectée. Ces cyberattaques sont pour la plupart lancées automatiquement à partir des machines infectées par des virus, chevaux de Troie, vers, etc… à l'insu de leur propriétaire. Il s'agit dans tous ces cas et de bien d'autres de l'action des pirates informatiques.

Les cyberattaques visent, entre autres, les objectifs suivants :

- la désinformation et la déstabilisation ;
- l'empêchement de l'accès à une ressource ;
- la prise de contrôle d'une ressource ;
- la récupération de l'information présente sur le système ;
- l'utilisation d'un système compromis pour rebondir vers un système cible.

Les motivations des cyberattaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations relatives aux secrets industriels ou aux propriétés intellectuelles ;
- glaner des informations à caractère personnel sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- se servir du système de l'utilisateur comme "rebond" pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée ;
- modifier des informations sur le système cible ;
- se venger contre son ancien employeur ou assouvir sa soif de rancœur que l'on nourrit vis-à-vis de son ancien employeur ;
- lancer des défis intellectuels ;
- aiguiser la curiosité pour découvrir le monde des pirates informatiques ;
- rechercher la notoriété : pour être reconnu par la communauté des pirates, il faut réaliser un exploit ;
- attaquer pour le plaisir de gagner de l'argent (cupidité) ;
- défendre une idéologie politique ou religieuse.

L'attaque cybernétique peut aussi être :

- **ludique** : les attaquants sont motivés par la recherche d'une prouesse technique valorisante, cherchent à démontrer la fragilité d'un système et se recrutent souvent parmi des jeunes informaticiens ;
- **terroriste** : lorsque des groupes de hackers organisés veulent frapper l'opinion par un chantage ou par une action spectaculaire amplifiée par l'impact des médias, tel que le sabotage d'infrastructures vitales ;
- **stratégique** : l'attaque massive des systèmes vitaux d'un pays ou d'une entreprise, afin de les neutraliser, de les paralyser, de prendre le contrôle ou connaissance d'informations sensibles ou classées confidentielles, notamment en accédant frauduleusement à des banques de données d'un État, des groupes organisés ou des entreprises.

Les cibles des cyberattaques sont généralement :

- des Etats ;
- des serveurs des bases militaires et des forces de sécurité nationales ;
- des banques ;
- des serveurs des ministères de production de biens et services sollicités par des citoyens ;
- des universités et des laboratoires de recherche ;
- des entreprises concurrentielles ;

- des individus : toi, moi, tout le monde.

1.3. Les pirates informatiques

En réalité il existe de nombreux types de pirates informatiques ou "attaquants", catégorisés selon leur expérience et leurs motivations. Parmi eux, nous allons nous intéresser seulement aux hackers.

1.3.1. Les hackers

Au départ, l'esprit du hacker reposait sur l'exploration des limites d'un système. Trois grands principes fondaient alors sa raison d'être :

- explorer les limites d'un système informatique ;
- apprendre des failles et/ou vulnérabilités du système ;
- partager l'information avec les autres, afin de rechercher l'ensemble des solutions aux failles ou vulnérabilités que l'on a découvertes dans le système.

L'esprit du hacker de départ n'avait donc pas pour but de détruire ou de chercher de l'argent.

Le vocable hacker a eu plus d'une signification depuis son apparition avant les années 1950 jusqu'à nos jours.

A l'origine, ce nom désignait d'une façon méliorative les programmeurs émérites. Ensuite, il servit à décrire les révolutionnaires de l'informatique, qui pour la plupart, sont devenus les fondateurs des plus grandes entreprises informatiques.

Cela a servi à désigner les personnes impliquées dans le piratage des jeux vidéo, en désamorçant les protections de ces derniers, afin d'en revendre des copies.

Le terme hacker est usité de nos jours pour désigner les personnes qui s'introduisent frauduleusement dans des systèmes informatiques.

Aujourd'hui, les hackers n'ont qu'une chose en tête : l'argent.

Tout le monde est susceptible de devenir pirate informatique ou hacker. Ce groupe désigne entre autres tous ceux qui recherchent et trouvent des clés sur Internet, pour désamorcer des applications et autres systèmes informatiques.

1.3.2. Les familles de hackers

Les hackers sont organisés en familles. Il s'agit notamment de la famille :

- **Des white hat hackers** : Ce sont des hackers au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes, des logiciels et autres technologies informatiques. Ils interviennent dans des systèmes pour trouver des palliatifs ou patches aux failles ou vulnérabilités découvertes. Ils sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui : le courrier électronique est un des exemples. Ils cherchent et trouvent des solutions aux problèmes des failles des systèmes ;

- **Des black hat hackers** : plus couramment appelés pirates informatiques, c'est-à-dire des personnes s'introduisant frauduleusement dans les systèmes informatiques dans un but nuisible. Ils testent et découvrent des failles ou vulnérabilités des systèmes, afin de les exploiter. Dans cette famille on retrouve :
  - **Les scripts kiddies** : ou gamins du script, également surnommés crashers, lamers ou encore packet monkeys, pour les singes des paquets réseau. Ce sont des jeunes usagers du réseau utilisant des recettes de piratage trouvées sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques, afin de s'amuser.
  - **Les phreakers** : Ce sont des pirates informatiques qui ne s'intéressent qu'au réseau téléphonique commuté (RTC), afin de téléphoner

gratuitement grâce à des circuits électroniques qualifiées de box, comme la blue box, la violet box ... connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement. On appelle "phreaking" le piratage des lignes téléphoniques.

- **Les carders** sont des hackers qui s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires), pour en comprendre le fonctionnement et en exploiter les failles. Le terme carding désigne le piratage des cartes à puces.
- **Les crackers** désignent des pirates informatiques dont le but est de créer des logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants. Un "crack" est un programme exécutable créé spécifiquement pour modifier (patcher) le logiciel original, afin d'en supprimer les protections.

- **Les hacktivistes** (contraction de hackers et activistes que l'on peut traduire par cybermilitant ou cyberrésistant), sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle, qualifiée généralement de underground, par analogie aux populations souterraines des films de science-fiction.

Les systèmes d'information des organismes constituent donc la cible indiquée de ceux qui convoitent l'information. Depuis quelques années, le phénomène de cybercriminalité grandit, prend des formes diverses et inquiète tout le monde. Le Cameroun n'en est pas épargné. Notre pays était devenu, à un moment donné, une destination déconseillée car ses réseaux, lorsqu'ils ne servaient pas de support de rebond aux attaques cybernétiques, en constituaient une base. D'ailleurs, chacun d'entre nous a déjà été menacé ou victime, plus d'une fois, d'une arnaque par voie électronique :

- vous recevez le courrier d'un individu à qui vous n'avez pas donné votre adresse de courrier électronique ;
- une loterie que vous gagnez sans avoir joué ;
- une fiche de renseignements à servir de la part de votre banque en ligne qui vous demande vos informations à caractère personnel jusqu'à votre numéro de compte ;
- des virus, des vers, des chevaux de Troie qui inondent nos ordinateurs à longueur de journée et ralentissent son fonctionnement ;
- un lien vers un virus ou un ver dans un mail reçu ;
- des disques durs des ordinateurs qui perdent leurs fichiers...

Des citoyens Camerounais peuvent se dire avoir connu cette malheureuse expérience au moins une fois dans leur vie. Nous-mêmes, en tant qu'individu, avons déjà été victime à plusieurs reprises. Des structures dans lesquelles nous travaillons ou celles qui sont à côté de nous ont elles aussi déjà été victimes ou constituent des victimes potentielles de ce genre de délits cybernétiques.

1.3.3. La provenance des cybercriminels

Les cybercriminels ne viennent malheureusement pas que d'ailleurs, nos collègues de service, nos enfants éveillés, nos populations pourraient adhérer à des causes qui dépassent nos frontières géographiques. Ils peuvent se battre pour des causes qui ne concernent pas seulement notre Nation sans que nous ne nous en rendions compte.

Le cyberespace offre des possibilités nouvelles aux camerounais. Nous devons comprendre que les citoyens numériques que nous sommes en train de devenir auront demain une double nationalité : celle se trouvant sur notre carte d'identité nationale ou sur notre passeport et celle des groupes

auxquels nous adhérons à travers Internet ou les réseaux de communications électroniques.

1.4. Les actes de cybercriminalité

Depuis quelques décennies, se développe une nouvelle forme de délinquance numérique : la cybercriminalité. C'est-à-dire tout acte répréhensible ou infraction cybernétique utilisant des réseaux de communications électroniques, des systèmes d'information ou cyberespace, c'est-à-dire des réseaux informatiques et des réseaux de télécommunications.

Il convient de relever qu'en matière de cybercriminalité, il n'y a que deux infractions qui peuvent être qualifiées aujourd'hui : les délits et les crimes cybernétiques. La qualification est fonction du degré des dommages causés par l'acte posé.

1.4.1. La cybercriminalité dans le monde

La cybercriminalité est un fléau des temps modernes. Elle n'épargne aucun pays encore moins un continent. Les actes criminels perpétrés dans les systèmes d'information et les réseaux de communications électroniques sont l'œuvre des individus agissant seuls ou en groupes sur l'Internet.

Si les arnaques via Internet ou cyberattaques explosent, c'est que les cybercriminels sont les AS de l'informatique. Ils s'installent dans votre ordinateur à votre insu, copient, effacent, modifient vos informations, pire encore, enregistrent votre mot de passe au moment où vous vous connectez à votre banque. C'est une porte ouverte pour piller votre compte.

Des cyberattaques majeures motivées par des considérations politiques ou terroristes, contre des systèmes d'information, sont susceptibles d'affecter un système d'information critique. Ces attaques ou incidents majeurs ont de graves répercussions, notamment sur des infrastructures critiques qui fournissent des services à l'ensemble de la société.

Le 11 Août 2003, le virus blaster a été lancé et le 14 Août 2003, en quelques secondes aux Etats-Unis, des centrales électriques se sont fermées privant d'électricité des millions de personnes, certaines étaient calées dans des ascenseurs ou des métros, des centraux téléphoniques étaient aux arrêts, les sources secondaires n'ayant reçu aucune commande de prendre le relai... En quelques temps, toutes les infrastructures critiques reliées à l'Internet ou dépendantes d'électricité ont arrêté de fonctionner. Les gens étaient pris de panique.

Le 1er mai 2007, jour de la fête russe, les hackers d'origine russe ont organisé et lancé une cyberattaque contre l'Estonie. Ils ont remplacé les pages web des sites gouvernementaux par des images insultantes du Premier Ministre Estonien. Le trafic Internet s'est affolé brusquement jusqu'à saturer les serveurs. Les écrans des banques étaient devenus noirs et ne livraient plus aucune information. Tous les services en ligne ne fonctionnaient plus. La cyberattaque avait dégénéré en émeute. Tous les systèmes informatiques étaient bloqués. L'Estonie a été paralysée pendant quelques jours par cette cyberattaque.

A l'origine de l'attaque cybernétique estonienne, un botnet c'est-à-dire un réseau d'un million d'ordinateurs connectés de par le monde. Ces ordinateurs appartenaient à des particuliers, des entreprises et à des institutions publiques, infectés par un cheval de Troie qu'un cybercriminel russe contrôlait à distance. Le Russe faisait faire à ce botnet tout ce qu'il veut. Des millions d'ordinateurs connectés en réseau servaient ainsi l'industrie du logiciel malveillant. Avec la technique du botnet, les jeunes russes ont explosé les serveurs estoniens.

En 2010, le compte bancaire de l'ex-Président français Monsieur Nicolas Sarkozy avait été piraté, preuve que tout le monde peut être victime d'une cyberattaque ou d'une escroquerie sur Internet. Les actes de cybercriminalité ou cyberattaques n'épargnent donc personne.

Le 7 mars 2011, la Présidence de la République Française, le Premier Ministère, le Ministère de l'Economie et des Finances, le Ministère de la Défense ont été l'objet d'attaques cybernétiques. Ces dernières ont également été faites à base des chevaux de Troie, du Botnet et des virus.

Plus récemment encore, les attaques cybernétiques dirigées contre TV5 monde font partie de ces registres. La cyberattaque a handicapé ce média pendant quelques jours.

Bref, il existe plusieurs autres exemples dans le monde que nous n'avons pas cités ici.

1.4.2. La délinquance numérique au Cameroun

Le constat est clair : les actes de criminalité cybernétique en direction des pays de la sous-région Afrique Centrale en général et du Cameroun en particulier sont légion.

C'est ainsi que certains sites nationaux ont été visités par les hackers ces derniers temps. En voici quelques exemples :

- En mai 2008, des hackers ont attaqué le site web du Ministère des Domaines et des Affaires foncières qui donne des informations sur les titres fonciers et autres affaires domaniales aux citoyens camerounais. Ils ont copié et détruit la base des données secondaire contenant certaines informations cadastrales et domaniales. A la sortie, ils ont laissé sur le site web le message suivant "Bonjour, je tiens à vous signaler que votre site a une faille dans la partie login pour accéder à l'administration." avant le black-out total ;
- en février 2009, le site du journal Le Messager a été piraté. Après leur forfait, le texte de revendication et d'engagement politique musulman suivant a été diffusé : "Countries as USA and Israel are terrorists who are killing children and women in Iraq and Palestine but they are now going to see muslim defend their countries";
- En septembre 2008, le site de La Nouvelle Expression, journal bien connu et prisé des camerounais, a été visité par les hackers. Ils y ont substitué l'information par des images publicitaires et un texte qui n'a rien à voir avec la structure ;
- En 2011, Cameroon-Tribune et le Parti des Démocrates Camerounais ont également été attaqués par des hackers ;
- En début Juin 2012, 8 sites institutionnels du Cameroun se sont vu victimes d'effacement par un groupe de hackers "Dz4HaCk" d'Algérie qui les a attaqués ;
- En 2014, le site de l'Assemblée nationale ainsi que celui de la présidence ont subi les assauts des cybercriminels. A chaque fois ceux-ci ont fait faire passer un message d'engagement politique qui leur tenait à cœur.

″Parmi les sites attaqués par les cybercriminels figurent en bonne place les sites institutionnels, preuve que les applications critiques de l'Etat doivent, plus que jamais bénéficier d'une attention particulière. De hautes personnalités ont également subi des pertes de grande valeur lors des cyberattaques dirigées contre leur patrimoine. Vous et moi avions été victimes ou sommes aussi des victimes potentielles. En somme, personne n'est à l'abri des attaques cybernétiques″

1.4.3. Les motivations des cybercriminels

Outre des motivations sus-évoquées, il en existe d'autres qu'affectionnent les cybercriminels. En effet, les agents de sécurité du Ministère des Postes et Télécommunications ont constaté depuis pratiquement cinq ans, que plusieurs applications métiers, réseaux et systèmes du Cameroun, sont devenus des cibles privilégiées des cybercriminels. La probabilité de lancement des cyberattaques contre des services publics est d'ailleurs devenue importante et donc un aspect majeur à intégrer aux stratégies de protection des organismes.

Dans le mode de fonctionnement des cybercriminels, le défi de pirater des infrastructures critiques de l'Etat telles que des hôpitaux, des systèmes de transport public, des services de police, des réseaux d'eau et d'énergie, des services financiers, des services des télécommunications, des Institutions et des infrastructures similaires de service public, ainsi que l'effet paralysant que cela

peut engendrer sur la société, renforcent leur motivation.

Interrompre des services rendus au public, provoquer la panique et ralentir les transactions commerciales représentent quelques-unes des motivations qui animent les cybercriminels, pour tirer le meilleur parti des nouvelles méthodes de piratage qu'ils mettent au point assez régulièrement. Ils prennent le temps de rechercher des moyens d'infiltration d'un système central à travers une application malveillante. En paralysant un système de transport ou en créant une panne de courant électrique en périphérie, les cybercriminels envoient un signal fort à ces Administrations, Institutions et Entreprises Publiques, ou à tout autre organisme victime qui n'adhère pas à leurs opinions politique, personnelle ou religieuse.

De nombreux cybercriminels utilisent leurs talents en matière de piratage pour créer un "boycott moderne". Les "hacktivistes" exploitent des failles ou des vulnérabilités des systèmes ou des protocoles des réseaux. Ils ont pour habitude de détruire des sites Internet et de paralyser les activités des services financiers en ligne. De plus, les cybercriminels s'attaquent à tout, des banques tout comme des marchés boursiers n'en sont pas épargnés. L'ajustement des cours en bourse ou le gel des échanges sur le marché boursier pourraient être à l'origine d'une panique financière mondiale, ce qui aiguise leur motivation.

Les cybercriminels sont aussi motivés par les cyberconflits qu'ils peuvent occasionner au bout d'un clic. Des attaques contre des nations, les réseaux du système de Sécurité ou de Défense et de l'Administration d'un État sont autant d'exemples. Le défi de pirater ces infrastructures critiques à l'échelle d'une Nation et l'effet paralysant que cela pourrait engendrer sur la société toute entière représentent une autre source de motivation.

De nombreux pays n'ont pas suffisamment investi dans des infrastructures critiques, en raison de crédits budgétaires limités ou du manque de connaissances et de sensibilisation en termes de dangers potentiels.

Des attaques distribuées par déni de service (DDoS) sont des cyberattaques qui empêchent l'accès à un service Internet. Elles sont obtenues par saturation des ressources de la cible avec des centaines de milliers de connexions qui bloquent le système. Ces types d'attaques sont en hausse avec Estonia DDoS (2007), Georgia DDoS (2009) et les plus récents Stuxnet, Duqu, Flame qui ont attaqué les systèmes SCADA (Supervisory Control And Data Acquisition, système d'acquisition et de contrôle des données).

La plupart de ces attaques sont basées sur le déni de service distribué (DDoS=Distributed Denial of Service) et cela n'est pas une coïncidence puisque habituellement, les attaques par DDoS sont très efficaces pour créer l'impact escompté. En effet, lorsqu'un site Internet tombe en panne, cela se sait. Ces organismes ne peuvent cacher ce qui s'est produit. Quand ces sites ne fonctionnent pas, tout le monde peut s'en rendre compte. En général, ce type d'évènements est aussi bien couvert par les medias, ce que les "hacktivistes" visent à obtenir puisque cela alerte le public sur leurs intentions.

L'Industrie de la cybermalveillance se répand et représente un chiffre d'affaires affolant. Des partenariats sont noués à chaque instant entre les amateurs et les professionnels, pour organiser une délinquance numérique.

Sur Internet, les comportements les plus irresponsables sont tolérés. On constate que les individus sont "investis d'un pouvoir" qui leur permette d'échapper à l'autorité des nations souveraines. Les hackers et tous les pirates informatiques utilisent leur talent pour abuser du pouvoir que leur donne l'ordinateur.

Face au phénomène de cybercriminalité, tous les pays sont vulnérables. Mais il y en a qui sont plus vulnérables que d'autres. La vulnérabilité peut être due au fait que certains ont beaucoup plus d'ennemis ou qu'ils sont moins équipés ou dépendent plus d'autres.

1.5. Les cibles des cybermenaces

Il devient évident que, faire face aux cyberattaques menaçant les infrastructures critiques ne peut plus être géré seulement au niveau de l'organisation cible. Seule une stratégie de sécurité nationale, exhaustive, comprenant les aspects domestiques et parfois internationaux de la cybersécurité, peut permettre de sécuriser davantage une Nation, contre les menaces à l'encontre de ses industries critiques.

Un conseil de partenariat mondial multilatéral contre les cybermenaces (IMPACT), de l'Union Internationale des Télécommunications, spécialisé dans le domaine de la cybersécurité, permet aux gouvernements et organismes intéressés d'avoir des systèmes capables de détecter, d'analyser des cybermenaces et d'y réagir efficacement. IMPACT permet de mettre en place des systèmes de veille sécuritaire comme le CIRT (Computer Incident Response Team).

Le Centre d'alertes mondial de cet organe est le principal centre de ressources dans la lutte contre les cybermenaces à l'échelle mondial. Ce centre transmet des alertes d'urgence pour faciliter la détection des cybermenaces et le partage des ressources, afin de prêter assistance aux pays membres.

Fort heureusement, certains pays commencent à comprendre les conséquences du manque de protection des réseaux et des installations stratégiques ou critiques, ainsi que le besoin vital de renforcer les moyens de sécurité. Aux États-Unis, le Gouvernement Obama a instauré un programme de cybersécurité qui informe les infrastructures critiques de l'Etat, des risques encourus et annonce que l'économie numérique s'avère vulnérable.

Le CIRT dispose des moyens techniques qui lui permettent de tester et de sonder les sites à distance. Il émet régulièrement des bulletins d'alertes.

La sécurité des systèmes d'information a pour objet de contrer ces menaces par des mesures proportionnées aux risques pouvant peser sur la confidentialité de l'information, son intégrité, sa disponibilité, la possibilité d'en authentifier la source et de la signer.

Si nous considérons le système d'information comme constitué de trois parties essentielles : les équipements (ordinateur), le réseau et le contenu ou l'information, nous dirons que le Cameroun se devait de prendre des mesures appropriées pour sécuriser ses moyens informatiques, ses réseaux de communications électroniques et ses systèmes d'information, bref son cyberespace. En particulier, l'Etat devait se munir des plateformes de sécurité dans tous les secteurs d'activités, pour surveiller en permanence les activités de ses réseaux, protéger les citoyens, le patrimoine de l'Etat et celui des entreprises, sources de revenus de l'Etat. Mais tout doit être fait dans la discipline et suivant l'ordre prévu par la législation en vigueur. C'est le moyen par lequel, l'Etat pourra faire face à la délinquance numérique exponentielle, que nous observons autour de nous.

Chapitre 2 : QUELQUES CONCEPTS DE BASE EN CRYPTOGRAPHIE

Introduction

Les moyens d'échanges d'informations ou de communications actuels reposent principalement sur des réseaux d'ordinateurs interconnectés ou systèmes d'information, qui offrent aux utilisateurs des services multimédias variés. Le vaste déploiement d'Internet à des débits élevés ces derniers temps est à l'origine de la vulgarisation des nouveaux services électroniques. Il s'agit notamment du portail collaboratif, des centres d'appels, du porte-monnaie électronique, des e-services, de l'e-Administration, des applications métiers… Ces derniers émerveillent, changent complètement les habitudes des usagers et améliorent le mode de communications entre Gouvernements et citoyens, en entreprises et dans des ménages. Cependant, des informations privées et confidentielles appelées à circuler librement dans ces réseaux sont souvent confrontées à de sérieux problèmes de sécurité.

En effet, pendant bien longtemps, tout le trafic de communications électroniques passait en clair sur le réseau Internet et sans aucune protection. N'importe qui pouvait l'intercepter, l'analyser, le scruter ou envoyer des données à d'autres personnes en se faisant passer pour une personne qu'elle n'est pas. L'utilisateur n'avait pas les moyens de vérifier l'identité du correspondant à l'autre bout du réseau, ni de se protéger contre un éventuel déni de service c'est-à-dire une attaque qui empêche l'accès à un service Internet.

L'apparition des agents de renseignements cybernétiques et des programmes malicieux tels que les virus, les spywares, les vers, les botnets, les chevaux de Troie… ainsi que la démocratisation de l'Internet ou l'arrivée de l'informatique grand public, ont définitivement changé cette donne. Une première tentative pour sécuriser le web fut l'utilisation des mots de passe qui permettaient d'identifier les utilisateurs, de leur octroyer des droits et par conséquent de leur restreindre l'accès aux serveurs web et à d'autres ressources. Cette solution s'est vue rapidement dépassée, car devenue faible.

Il se posa alors le problème de satisfaction de nouvelles exigences en sécurité, telles qu'une authentification forte et de manière univoque des utilisateurs et des données, l'intégrité des données transmises, la confidentialité des données et de protection contre le déni de service, et enfin la non-répudiation des données transmises. Ces besoins ont été introduits par des applications telles que la messagerie sécurisée, l'e-commerce, les connexions distantes sécurisées… Nous donnons quelques précisions quant aux concepts utilisés, pour une bonne compréhension de la suite du document. Il s'agit des termes suivants :

L'**authentification** peut se définir comme le processus qui permet de vérifier d'une manière certaine l'identité de la personne avec laquelle vous communiquez.

La **confidentialité** est une technique qui permet de garantir le secret des informations transmises en ligne. C'est la preuve que seul le destinataire est capable de lire en clair le message de l'émetteur.

L'**intégrité** permet de s'assurer que les informations reçues n'ont pas été modifiées ou détruites lors de la transmission.

La **non-répudiation** garantit la preuve irréfutable de l'émetteur de l'information qui ne peut nier l'avoir expédié ou le destinataire l'avoir reçu.

En tout état de cause, la cryptographie, c'est-à-dire la technologie qui utilise les mathématiques pour l'écriture et la lecture des messages codés, se présente actuellement comme une solution idoine, qui permet d'assurer aux utilisateurs les services de **confidentialité**, d'**intégrité**, de **non-répudiation** des informations échangées et d'**authentification** forte et univoque des correspondants qui communiquent. Des dispositions sont en train d'être prises pour étendre l'usage de la cryptographie à plusieurs services des réseaux de nouvelle génération. Ces dispositions permettront à coup sûr de minimiser les menaces qui pèsent sur les

systèmes d'information, car le risque zéro n'existe pas.

L'utilisation de la cryptographie est devenue de nos jours, la base de toute solution sécurisant le web. L'idée est d'utiliser un algorithme de chiffrement associé à une ou plusieurs clés : c'est-à-dire une suite de bits quelconque qui sert à chiffrer et/ou à déchiffrer des informations, pour garantir les services d'authentification, de confidentialité, d'intégrité et de non-répudiation. Ces algorithmes de chiffrement étant en général publiquement connus, tout le problème est à la fois, de garantir le secret des clés et la correspondance entre une clé et son propriétaire.

L'utilisation des certificats numériques permet d'établir de façon fiable et univoque la correspondance entre la clé publique et son propriétaire, de manière qu'un utilisateur puisse faire confiance à un autre, une fois son certificat présenté. Cependant, cette confiance ne peut être établie si l'autorité qui délivre le certificat n'est pas reconnue, comme un tiers digne de confiance.

Il est important de savoir qu'un certificat électronique est un fichier informatique infalsifiable qui lie de manière univoque une entité et une clé. Autrement dit, c'est un document électronique, résultant d'un traitement fixant **les relations** entre **une clé publique**, **son propriétaire** (une personne, une application, un site) et **l'application** pour laquelle il est émis.

Il paraît donc nécessaire actuellement de disposer des produits de sécurité assurant une protection adaptée à des menaces ciblées, qui soient faciles d'emploi, paramétrables, bien documentés et dont les mesures de sécurité auront été évaluées et éprouvées, afin que l'utilisateur puisse les utiliser en toute confiance et même faire son choix en toute connaissance de cause.

2.1. Chiffrement et Déchiffrement d'un message

2.1.1. Notion de chiffrement

Pour assurer la **confidentialité** d'un document électronique, on chiffre le texte du document. Cette opération consiste à appliquer un ensemble de fonctions mathématiques avec des caractéristiques très particulières sur le texte. Cette fonction utilise une variable, la **clé de chiffrement**, qui est une suite de bits quelconque. Une fois le texte chiffré, il devient illisible. Pour obtenir la version lisible, il faut le déchiffrer, c'est-à-dire appliquer d'autres fonctions mathématiques, compatibles avec les premières, en utilisant une autre variable : la **clé de déchiffrement**.

Ces deux types de fonctions mathématiques sont appelés **algorithmes de chiffrement**. La valeur de la clé de déchiffrement dépend de celle de la clé de chiffrement. Seul le possesseur de la clé de déchiffrement peut déchiffrer le texte c'est-à-dire permettre de retrouver le texte chiffré en clair.

Il y a lieu de noter que les algorithmes de chiffrement, c'est-à-dire les formules mathématiques utilisées, sont publics et standardisés. C'est le secret des clés qui permet à ces algorithmes d'assurer le service de confidentialité, d'intégrité, de non-répudiation et d'authentification.

2.1.2. Mécanismes de cryptographie

Les mécanismes de cryptographie mettent en œuvre un algorithme de chiffrement et une valeur secrète appelée **clé**. Pour assurer la sécurité des communications, on utilise généralement les mécanismes de sécurité suivants :

- le **chiffrement** qui assure la confidentialité ;
- la **signature numérique** qui assure l'authentification, l'intégrité et la non-répudiation ;
- et les **fonctions de hachage non réversibles** : c'est-à-dire qu'il doit être extrêmement difficile, voire impossible, d'obtenir le message d'origine à partir de son condensé. Elles assurent l'intégrité et l'authentification.

2.1.3. Les Services de cryptographie

Tout système basé sur la cryptographie doit offrir les services d'authentification, de confidentialité, d'intégrité et de non-répudiation.

a) La confidentialité

Son but est de ne garantir la lecture des informations/données en clair qu'au destinataire légitime. Cela signifie que les données sont chiffrées et qu'elles ne peuvent pas être déchiffrées par une personne ne possédant pas la clé privée gardée secrète.

Ce service s'assure que personne n'avait eu la possibilité de prendre connaissance du message transmis.

Cette fonctionnalité est notamment réalisée par des algorithmes symétriques comme AES, RC2, RC4, DES, 3DES, etc. Ces algorithmes sont appelés symétriques, car ils utilisent la même clé pour chiffrer et pour déchiffrer les messages.

b) L'authentification

Le but de l'authentification est de pouvoir identifier avec beaucoup certitude et de garantie qu'une personne X est bien la personne qu'elle prétend être.

Cette fonctionnalité est notamment réalisée par des algorithmes asymétriques comme RSA, pour le chiffrement et la signature ; et le DSA, pour la signature uniquement. Ces algorithmes sont dits asymétriques, car ils utilisent deux clés dont une utilisée pour le chiffrement des données est différente de celle nécessaire pour réaliser le déchiffrement. Même si ces clés sont liées mathématiquement entre elles, il est quasiment impossible de déduire l'une à partir de l'autre.

L'**authentification** = authenticité + identification

- **Authenticité** : c'est le fait que vous pouvez vérifier que vous communiquez avec l'entité que vous croyez communiquer ;
- **Identité** : vous pouvez vérifier que l'individu avec lequel vous communiquez est bien celui qu'il prétend être et qui se trouve derrière l'entité avec laquelle vous communiquez.

c) L'intégrité

Le but de l'intégrité est de garantir la non altération ou la non modification des données au cours de leur transmission. Ce qui veut dire qu'il est possible de détecter le fait qu'une donnée ait été modifiée ou détruite.

L'intégrité est réalisée par des fonctions de hachage à sens unique comme : MD2, MD5, SHA-1, SHA-2, etc... Ces algorithmes calculent des empreintes numériques. Par cette méthode, deux ensembles différents de données, aussi proches soient-ils, auront des empreintes totalement différentes. Ainsi, pour assurer l'intégrité des données, il faut signer l'empreinte numérique qui est alors appelée **"CONDENSAT"** ou code d'authentification de message, appelé **"MAC"** en anglais. Ces opérations de calcul d'intégrité et de signature sont regroupées en un seul algorithme "**HMAC**".

L'**intégrité** donne la garantie que le message n'a pas été modifié ou détruit pendant la transmission.

d) La non-répudiation

Le but de la non-répudiation est de pouvoir interdire à une personne de réfuter ou de nier une signature qu'elle aura faite. Cela confère à la signature électronique la même valeur que la signature manuscrite. C'est à dire que la signature numérique engage son signataire et qu'en cas de nécessité, un recours à la justice ou à une vérification experte est possible.

Cette fonctionnalité est notamment réalisée par des algorithmes asymétriques de signature comme RSA et/ou DSA.

La **non-répudiation** c'est le fait que l'individu derrière l'entité avec laquelle vous communiquez ne puisse nier être associé ou lié à l'entité émettrice ou réceptrice.

2.1.4. Le principe de chiffrement et de déchiffrement

Un message de texte clair noté M, peut être une suite de bits, un fichier de texte, un enregistrement numérisé de musique, une image ou une vidéo numérique... Mais pour un calculateur, M n'est rien d'autre qu'une suite binaire. Cette suite binaire peut être stockée ou transmise. Le texte chiffré noté : C,

est également une information binaire parfois de la même taille parfois plus grande. On va appeler $E_{KUb}(M)$ la fonction de chiffrement et $D_{KRb}(C)$ la fonction de déchiffrement. L'ensemble est relié par des relations mathématiques de la manière suivante :

C= EKUb(M) et D(EKRb(M))=M

DKRb(C) est la fonction inverse de EKUb(M). Comme le but de ces opérations est de retrouver le message initialement chiffré en clair, la relation DoE( ) = Fonction identité.

Autrement dit

Soient m, n, c ϵ {1,2,……., n-1}

- chiffrement : C = me mod n
- déchiffrement : $m = c^d = m^{ed} = m^{k(p-1)(q-1)+1} = m*m^{k(p-1)(q-1)}$
  = m (mod n) avec e*d mod f(n) = 1

2.1.5. Algorithmes à clés

Un algorithme cryptographique est une fonction mathématique utilisée pour le chiffrement et le déchiffrement des données.

Pour chiffrer un message en clair, on le traite avec un algorithme de chiffrement qui donnera le texte chiffré. Pour le déchiffrer, on le traite avec un algorithme de déchiffrement qui redonnera un message clair. Les algorithmes de chiffrement actuels utilisent une **clé**.

La clé peut prendre une des valeurs binaires parmi un grand nombre de valeurs possibles. L'ensemble des valeurs possibles d'une clé est appelé **espace de clés.** Le chiffrement et le déchiffrement dans un algorithme à clés sont notés:

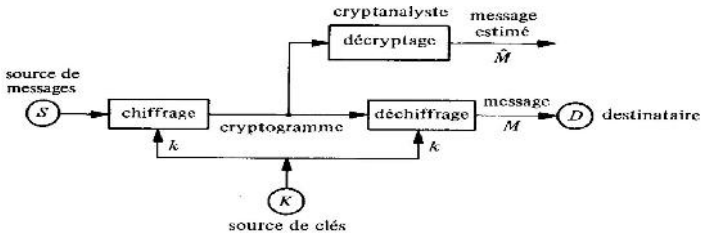
C=E_k(M) et M=D_k(C)

Comme le but de toutes ces opérations est de retrouver le message en clair à partir de la version chiffrée de ce message, l'identité suivante doit être vérifiée :

D_k(E_k(M))=M.

La sécurité des données chiffrées repose entièrement sur les deux éléments suivants :

- L'invulnérabilité de l'algorithme de chiffrement ;
- La confidentialité de la clé.



Principe de fonctionnement d'un système cryptographique

Il existe actuellement deux types de chiffrements : le chiffrement à clé symétrique ou à clé secrète et le chiffrement asymétrique ou à clé publique.

Le principal inconvénient d'un cryptosystème à clé secrète réside dans la distribution des clés.

En effet, le chiffrement symétrique repose sur l'échange d'un secret : les clés. Pour échanger la clé de chiffrement/déchiffrement, il faut établir un canal sûr, afin d'éviter la copie ou le détournement de cette clé par une tierce personne. Pour un groupe de n personnes utilisant un cryptosystème à clé secrète, il est nécessaire de distribuer n x (n-1)/2 clés, ce qui est fastidieux à l'échelle **humaine.**

Nombre d'acteurs	**3**	**10**	**20**	**100**
Nombre de clés nécessaires	**3**	**45**	**190**	**4950**

Mesures à prendre :

- Changer fréquemment de clés pour qu'elles ne soient pas découvertes ;
- Générer des clés sécurisées ;
- Distribuer des clés de manière sécurisée.

2.2. Cryptographie à clés asymétriques

Dans le cadre de ce Projet, nous nous abstiendrons de parler profondément du chiffrement symétrique. Nous ne développerons que l'aspect relatif au chiffrement asymétrique, parce que c'est ce chiffrement qui est mis en exergue dans un système PKI, implémenté dans ce projet.

Principe

Les expressions, chiffrement asymétrique, algorithme à clé publique, cryptographie à clé publique désignent la même technique. Cette

technique repose sur le fait que la clé de chiffrement soit différente de la clé de déchiffrement. De plus, la clé de chiffrement ne peut pas être calculée à partir de la clé de déchiffrement. L'ensemble clé privée/clé publique est appelé bi-clé. Lorsqu'on chiffre un message avec une clé publique on ne peut le déchiffrer qu'avec une clé privée et vice versa.

La figure ci-dessous décrit le processus de chiffrement et de déchiffrement d'un message à l'aide d'une clé publique, d'une clé privée et d'un algorithme.

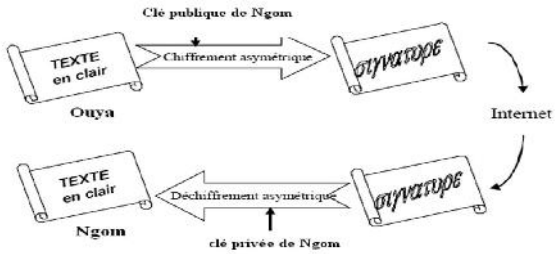


Figure 2 : chiffrement avec algorithme asymétrique

Les algorithmes à clé publique permettent d'assurer la confidentialité d'un message. Dans ce cas, la procédure à suivre est la suivante:

- L'émetteur du message doit récupérer la clé publique k1 du destinataire, qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire LDAP, avec laquelle il va chiffrer le message préalablement en clair M. Puis, il va envoyer le message chiffré résultant C, au destinataire.
- Le destinataire peut déchiffrer le message chiffré reçu C, avec sa clé privée k2, qu'il est le seul à connaître, afin de retrouver le message clair M d'origine.

Seule la personne possédant la clé privée k2 correspondant à la clé publique k1 pourra décrypter le message chiffré reçu C, afin de retrouver le message clair M d'origine. Cela garantit la confidentialité du message envoyé.

Ce système est basé sur une fonction facile à calculer dans un sens, appelée fonction à trappe à sens unique E_{ke}, "one way trapdoor function", mais qui est mathématiquement impossible à inverser à l'heure actuelle, sans la clé privée D_{kd} appelée trappe.

Le problème consistant à se communiquer la clé de déchiffrement n'existe plus. Les clés publiques peuvent maintenant être envoyées librement.

Le chiffrement à clé publique est une technique qui permet à des personnes éloignées de s'échanger des messages chiffrés, sans pour autant partager un secret en commun.

M --→ $E_{ke}(m)$= C est facile à calculer, mais C ---→ $D_{Kd}(m)$ = m est difficile si l'on ne connaît pas la clé D_{kd}

Confidentialité	$D_{Kd}(E_{ke}(m)) = m$
Authentification et Intégrité	$E_{ke}(D_{Kd}(m)) = m$
Confidentialité et Authentification	$D_{Kd}(E_{ke}(m))= E_{ke}(D_{Kd}(m)) = m$

D et E doivent être des nombres suffisamment grands pour éviter l'attaque au dictionnaire.

RSA = Rivest – Shamir – Adleman

2.2.1. Principe de Génération des clés

Le Principe de Génération des clés s'explique grâce à la théorie RSA de la manière suivante :

L'on choisit des grands nombres premiers p, q et n avec n = p*q

$f(n) = (p^{-1}) * (q^{-1})$

L'on choisit également e ϵ [1, f(n) – 1] tel que pgcd(e, f(n)) = 1

et d ϵ [1, f(n) – 1] tel que e*d mod f(n) = 1

- clé publique
- (d, n) : clé privée

2.3. Fonction de hachage

Une fonction de hachage est une fonction mathématique qui, à partir d'un texte, génère **un nombre caractéristique de ce texte** appelé empreinte.

Toute modification du texte entraîne une modification de son empreinte.

Principe

La fonction de hachage reçoit un message de taille quelconque et produit un code de longueur fixe, appelé condensé de message ou résumé de message.

Pour qu'un algorithme puisse être utilisé comme fonction de hachage, il doit répondre aux critères suivants :

- **être cohérent** : obtenir le même condensé du même texte en plusieurs essais.
- **être aléatoire** : si on change un seul caractère du message, on n'aboutit pas au même condensé ou résumé de message.
- **être unique** : deux messages différents ne doivent jamais produire le même condensé.
- **être non réversible** : le résumé ne permet pas de remonter au message initial.

Suivons l'application de la fonction de hachage en informatique, en mathématique et en cryptographie.

En informatique, une fonction de hachage à sens unique convertit une suite de bits de taille quelconque en une suite de bits de taille fixe. Le résultat d'une fonction de hachage s'appelle une empreinte numérique. Deux suites de bits identiques donneront deux empreintes identiques alors que deux suites de bits différentes donneront deux empreintes numériques différentes, mais peuvent aussi donner deux empreintes numériques identiques, bien que la probabilité de se trouver dans ce cas soit infiniment petite. Cette fonction est très utile dans la comparaison des fichiers. Au lieu de les comparer octet par octet, il suffit de calculer leur empreinte numérique et de comparer le résultat obtenu.

En mathématique, une fonction de hachage à sens unique est facile à calculer dans un sens, mais l'inverse est actuellement très difficile à calculer voire impossible dans un temps raisonnable dans l'autre sens.

En cryptographie, une fonction de hachage à sens unique est une fonction qui permet de calculer facilement une empreinte numérique de taille fixe à partir d'une suite de bits de taille quelconque et dont l'inverse est actuellement très difficile à calculer. C'est-à-dire, étant donné une suite de bits et son empreinte numérique, il est très difficile de trouver une autre suite de bits différente donnant la même empreinte numérique. Les fonctions de hachage à sens unique utilisées en cryptographie ont la particularité suivante : si l'on modifie un seul bit du message d'origine, alors la fonction de hachage produit une empreinte numérique différente.

2.3.1. Fiabilité des fonctions de hachage à sens unique

Pour un usage cryptographique, il est recommandé d'utiliser des fonctions de hachage à sens unique qui génèrent des empreintes numériques d'une taille d'au moins 128 bits qui demanderont 2^64 calculs à une attaque de type anniversaire. Etant entendu que des empreintes numériques d'une taille de moins de 128 bits n'offrent pas une sécurité suffisante.

Les algorithmes les plus utilisés sont MD2, MD4, MD5, SHA, SHA-1, SHA-2 et RIPEMD-160.

Les algorithmes des condensés de message MD2, MD4 et MD5 furent développés par Ronald Rivest, pour l'utilisation des signatures numériques. Les trois algorithmes produisent un condensé de message de 128 bits. Bien qu'il existe une ressemblance entre leurs structures, le MD2 est assez différent de MD4 et de MD5. En terme de vitesse de chiffrement, le MD2 est le plus lent ; MD4 est rapide tandis que MD5, ou MD4 avec ceinture de sécurité, est légèrement plus lent que MD4 mais plus sécurisé. MD2 s'applique beaucoup plus aux ordinateurs à 8 bits, tandis que MD4 et MD5 s'appliquent aux ordinateurs à 32 bits.

Il est évident que des collisions existent dès lors que la taille de l'espace des messages est supérieure à la taille des espaces des empreintes numériques, qui est fixe, soit 2^{128} dans le cas de MD5.

Le paradoxe des anniversaires donne une idée du nombre d'empreintes à calculer pour obtenir une

collision avec une probabilité de 50%. En effet, dans une assemblée de 100 "personnes prises au hasard", la probabilité que deux d'entre elles partagent la même date d'anniversaire (jour et mois) peut être supérieure à 50 %. Il est possible de prouver que la taille de l'espace des messages aléatoires à hacher pour obtenir une probabilité de collision est proportionnelle à la racine carrée de la taille de l'espace des empreintes numériques. Une empreinte de 16 bits est donc vulnérable à une attaque du type anniversaire en effectuant 2^8 opérations de hachage sur des messages aléatoires.

Pour un usage cryptographique, on suggère des tailles d'empreintes numériques supérieures ou égales à 160 bits, ce qui demande des calculs de l'ordre de plus de 2^{80} pour une attaque de type anniversaire.

Mais avec la technologie quantum, ces barrières sont aisément franchies.

2.4. Certificats numériques

2.4.1. Problématique des clés

Nous venons de décrire les mécanismes qui permettent d'assurer les quatre services d'un système cryptographique à savoir : la confidentialité, l'authentification, l'intégrité et la non-répudiation, au moyen d'un couple : clé privée/clé publique, et des algorithmes de chiffrement. Il y a néanmoins un problème qui se pose.

Soient les trois utilisateurs suivants : Ouya, Ngom et Eugène.

Nous avons considéré qu'un utilisateur connaissait la clé publique d'un autre utilisateur simplement en consultant un Annuaire LDAP, un serveur de clés ou un serveur Web par OCSP et la considérait comme vraie. Mais, rien ne garantit que la clé publique de **Ngom** que l'utilisateur **Ouya** a récupéré soit la bonne. N'oublions pas que tout cela fonctionne de manière électronique sur Internet sans contact direct, donc sans moyen visuel de reconnaissance ou de vérification de l'individu supposé propriétaire de la clé. Le pirate **Eugène** peut très bien avoir modifié les données de l'Annuaire LDAP ou du serveur Web qui contiennent la clé publique de **Ngom** en la remplaçant par la sienne. Une fois cette mascarade commise, **Eugène** pourra désormais lire les courriers confidentiels destinés à **Ngom** et signer des messages en se faisant passer pour **Ngom**.

Ce sera donc une conséquence que l'utilisateur **Ouya** croit détenir la clé publique de **Ngom,** alors que c'est celle d'**Eugène** qu'il détient. En effet, si **Ouya** envoie un message chiffré à **Ngom**, il va le chiffrer avec la clé publique d'**Eugène**. Si celle-ci est en fait la clé publique d'**Eugène**, alors **Eugène** pourra déchiffrer le message destiné à **Ngom** avec sa clé privée.

Une autre possibilité est que l'utilisateur **Eugène** pourra envoyer un message signé à **Ouya** avec une signature générée avec sa clé privée en se faisant passer pour **Ngom**. **Ouya** qui recevra le message vérifiera la signature du message avec ce qu'il croit être la clé publique de **Ngom**. La vérification sera correcte, donc **Ouya** pensera que le message vient de **Ngom**.

Eu égard à ce qui précède, il a fallu créer un mécanisme supplémentaire de vérification : **le certificat électronique** qui permet d'assurer la validité de la clé publique.

2.4.2. Définition de certificat électronique

Un certificat électronique est un fichier informatique infalsifiable qui lie de manière univoque une entité et une clé. En quelque sorte, c'est l'équivalent d'une carte identité ou d'un passeport du monde réel dans le monde virtuel. Un passeport contient des informations concernant son propriétaire : nom, prénom, adresse, la signature manuscrite, la date de validité, ainsi qu'un tampon et une présentation (forme, couleur, papier) qui permettent de reconnaître que ce passeport n'est pas un faux, qu'il a été délivré par une autorité bien connue et habilité à le faire.

Un certificat électronique contient les informations équivalentes. Le format reconnu actuellement est le **format X.509 V3.** Ce petit fichier

ou structure de données contient au moins les informations suivantes :

*Un champ TBS qui sera signé et qui contient toutes les informations suivantes:
*Le numéro de version du certificat (v1, v2 ou v3):
*Nom de l'autorité ayant délivré le certificat :
*Noms & Prénoms de la personne à qui appartient le Certificat (subject) :
*Son service :
*Son adresse électronique :
*Sa clé publique :
*Les dates de validité du certificat :
*Des informations optionnelles :
*L'algorithme asymétrique et la fonction de hachage utilisés pour la signature :
*Une signature électronique de l'empreinte:
*etc.

En d'autres termes, un **certificat** est un document électronique, résultant d'un traitement fixant **les relations** entre **une clé publique**, **son propriétaire** (une personne, une application, un site) et **l'application** pour laquelle il est émis.

- **Pour une personne**, le certificat prouve l'identité au même titre qu'une carte d'identité, dans le cadre fixé par l'autorité de certification qui l'a validé ;
- **Pour une application,** le certificat assure que celle-ci n'a pas été détournée de ses fonctions ;
- **Pour un site,** le certificat offre la garantie, lors d'un accès vers celui-ci, que l'on est bien sur le site auquel on veut accéder.

Un certificat électronique permet à son propriétaire de faire 3 choses :

- une authentification forte ;
- le chiffrement/déchiffrement des données envoyées en ligne ;
- la signature électronique et la vérification des signatures.

2.4.3. Principe d'émission d'un certificat électronique

Afin de mieux comprendre le principe d'émission d'un certificat électronique ou numérique, nous allons considérer deux utilisateurs : Ouya et Ngom.

L'utilisateur **Ouya** veut certifier que sa clé publique lui appartient. Il envoie cette clé publique dans le serveur de clés d'une autorité de certification, ainsi que différentes informations le concernant (nom, e-mail, etc..).

L'autorité d'enregistrement vérifie des informations fournies par l'utilisateur **Ouya**, à partir du formulaire servi. L'autorité de certification ajoute au certificat : son propre nom, le nom de l'utilisateur, la période de validité, la clé publique de l'utilisateur **Ouya**, l'algorithme de chiffrement, l'usage que l'on peut faire de ce certificat et surtout sa signature numérique.

Cette signature est calculée à partir des informations du certificat. L'autorité de certification calcule un résumé en appliquant une fonction de hachage connue, comme RSA. Puis, l'autorité de certification signe ce résumé en lui appliquant sa clé privée.

Lorsque l'utilisateur **Ngom** veut envoyer un message à l'utilisateur **Ouya**, il **télécharge** le certificat de celui-ci à partir d'un serveur de certificats du système PKI (Public Key Infrastructure). Il calcule le résumé du certificat. Puis, applique la clé publique de l'autorité de certification, auteur du certificat à la signature électronique et envoie donc le message à l'utilisateur **Ouya**. A la réception, l'utilisateur **Ouya** fait le travail inverse. Si la quantité obtenue est égale au résumé par comparaison bit par bit, l'utilisateur **Ouya** est sûr qu'il est entrain de communiquer avec l'utilisateur **Ngom**.

2.5. Signature électronique

2.5.1. Définition de signature électronique

Une signature électronique ou digitale est un condensé de message ou empreinte **chiffrée au moyen de la clé privée de son auteur** et joint à un document. Une telle signature va permettre de garantir l'authentification de l'origine du document électronique et son intégrité. Pour obtenir une signature électronique, on effectue une empreinte (ou un condensé) à l'aide de l'algorithme (SHA-2

par exemple), et on chiffre l'empreinte obtenue. Elle combine l'utilisation du chiffrement à clé publique et une fonction de hachage non réversible. Cela implique certaines propriétés :

- une signature ne peut être falsifiée,
- une signature donnée n'est pas réutilisable par un autre document,
- la modification d'un document signé altère la signature de ce document,
- une signature ne peut être reniée par son auteur.

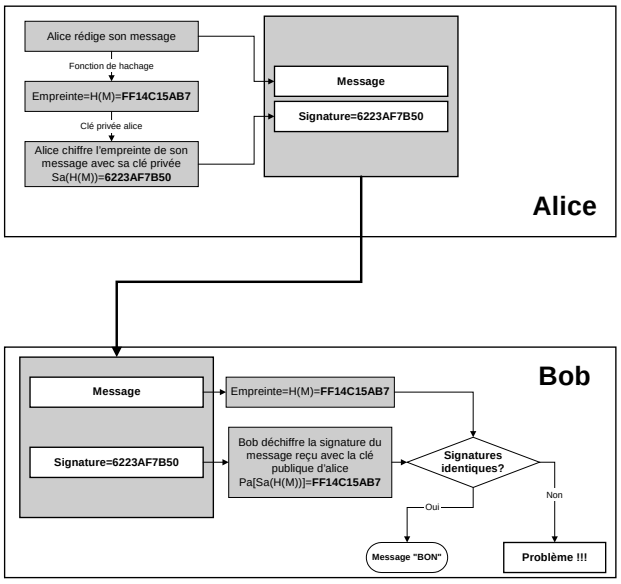


Schéma de principe

Principe

L'un des principaux avantages du chiffrement asymétrique est qu'il offre une méthode de signature électronique. Cette méthode permet au destinataire de vérifier l'authenticité du message, l'identité de l'expéditeur, l'origine et l'intégrité du message signé. Ainsi, les signatures électroniques à clé publique garantissent l'authentification de l'émetteur et l'intégrité des données. Elles fournissent également la fonctionnalité de non-répudiation, afin d'éviter que l'expéditeur prétende n'avoir jamais envoyé des informations.

2.5.2. Signature électronique simple

L'émetteur signe le message en clair M à l'aide de sa clé k2, puis il va envoyer le message en clair M et le message signé résultant C au destinataire. Ainsi, le destinataire n'a qu'à récupérer la clé publique k1 de l'émetteur avec laquelle il va déchiffrer le message signé reçu C pour obtenir un message M1.

Pour vérifier la signature électronique, le destinataire doit comparer le message M1 qu'il vient d'obtenir avec le message en clair M. Si les deux sont identiques, alors la signature électronique est vérifiée.

Seule la personne possédant la clé privée k2 correspondant à la clé publique k1 peut chiffrer le message en clair C qui pourra être déchiffré avec la clé publique k1. Un destinataire qui aura récupéré la clé publique k1 de l'émetteur pourra ainsi être sûr que le message a bien été signé avec la clé privée k2 de l'émetteur. Cela garantit bien l'authentification de l'émetteur et l'intégrité du message envoyé.

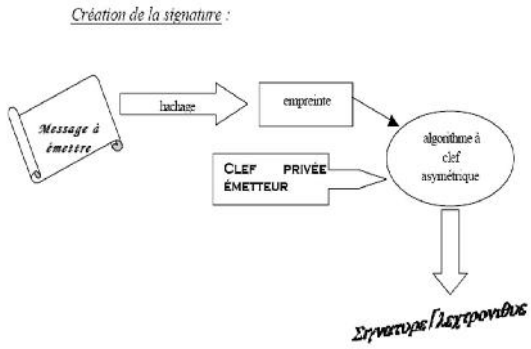


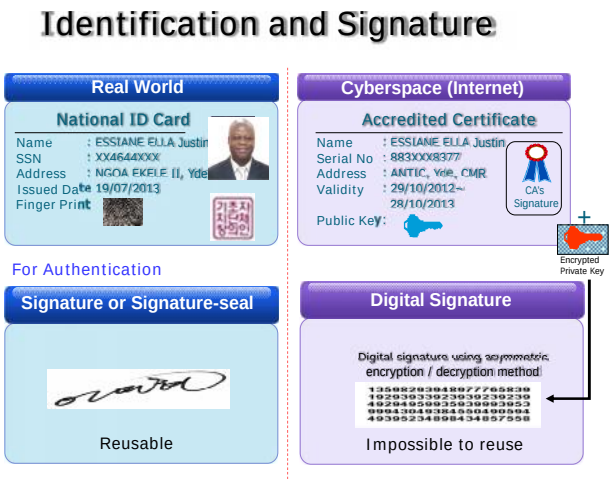
Schéma de principe

2.5.3. Signature numérique sécurisée

En général, la signature numérique simple n'est jamais utilisée en pratique, car le processus est lent et produit un volume important de données. Il est lent car l'obtention de la signature se fait en chiffrant l'ensemble du texte original, et le résultat comprend le texte en clair et la signature : ce qui donne un volume de données égal au double de la taille du texte en clair.

En pratique, on utilise la signature numérique sécurisée qui s'appuie sur les fonctions de hachage à sens unique. Plutôt que de signer tout le message, seule l'empreinte numérique du message est signée. D'après les propriétés des fonctions de hachage à sens unique, cela revient exactement au même que de signer le message lui-même.

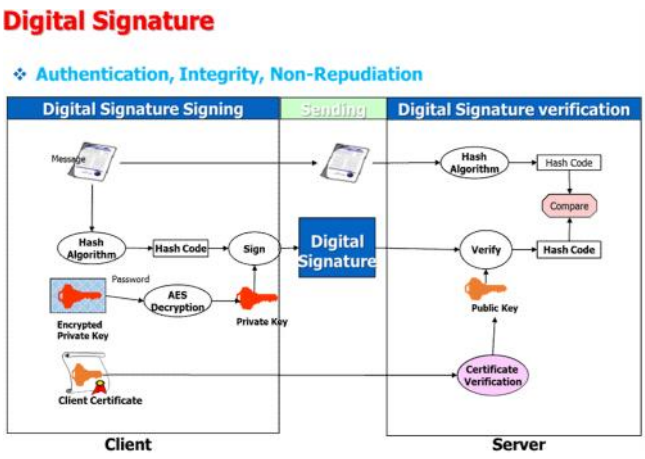
En général, comme le chiffrement asymétrique est 1000 fois plus lent que le chiffrement symétrique, il est seulement utilisé pour chiffrer des messages courts de quelques centaines de bits au plus, comme une empreinte numérique ou une clé de session.

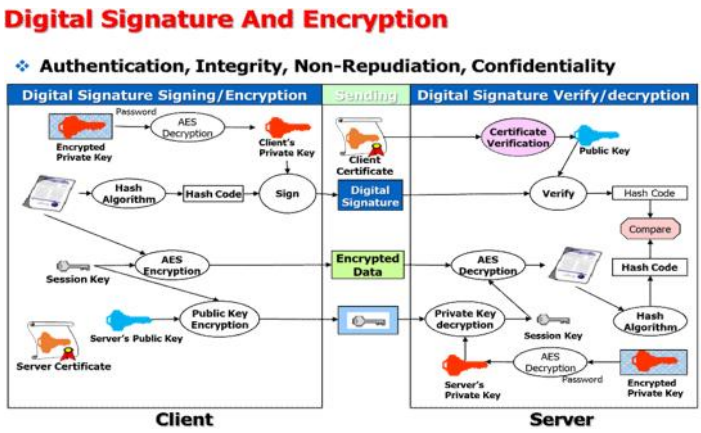


2.5.4. La signature d'un certificat électronique

Un certificat est signé, au sens signature électronique du terme. Pour ce faire, on effectue une empreinte ou un condensé du certificat, à l'aide d'un algorithme de hachage SHA-2 dans le cadre de ce projet, et on chiffre l'empreinte obtenue. Le chiffrement s'effectue avec la clé privée de l'autorité de certification, qui possède elle-même son propre certificat.

La signature électronique est calculée sur les différentes informations contenues dans le certificat électronique, comme dans le cas d'un message électronique explicité précédemment.





La signature électronique est l'empreinte des informations chiffrées de l'autorité de certification qui a délivré le certificat électronique.

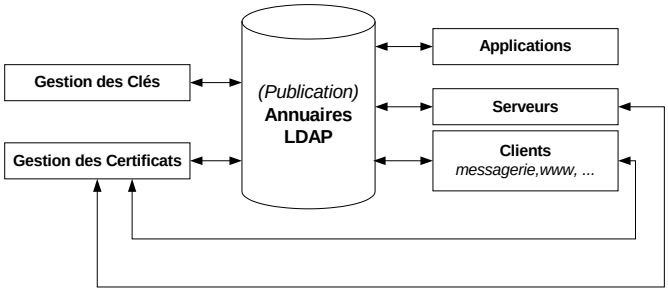
Dans la pratique, un certificat numérique permet de chiffrer les données que l'on envoie en ligne lors de la transaction électronique, d'émettre une signature électronique et de réaliser une authentification forte et formelle de l'individu avec lequel vous communiquez en ligne.

2.6. Formats et standards

Le certificat s'appuie sur un protocole normalisé X.509 de (ITU-T X.509) international Standard V3 apparu en 1996 selon la RFC 2459. Il permet d'associer à la clé des informations spécifiques à l'entité physique ou morale, à laquelle elle se rapporte. Des informations supplémentaires à savoir : numéro de version, numéro de série, algorithme de signature, période de validité, propriétaire du certificat, le signataire du certificat, l'usage que l'on peut faire de la clé contenue dans le certificat… sont contenues dans le certificat X.509 v3. La publication des certificats, donc «a fortiori» des clés publiques, est faite en utilisant des structures d'annuaires de type LDAP (Lightweight Directory Access Protocol), suivant la RFC 2251.

Les certificats révoqués sont regroupés dans des listes, la CRL (Certificate Revocation List) qui est constituée des structures de données signées par l'autorité de certification et dont le format est défini par le protocole X.509 V2 CRL, suivant la RFC 2459. Ce format peut permettre une distribution des CRL via des annuaires LDAP.

Certaines implémentations telles que celles de Netscape par exemple, font également apparaître la notion de fingerprint de certificat. C'est une empreinte MD5 ou RSA du certificat, qui permet de vérifier que celui-ci est bon.



Les extensions introduites dans la norme X.509 V3 permettent de spécifier un certain nombre d'informations en fonction de l'usage prévu du certificat.

version	Indique à quelle version du protocole X.509 correspond ce certificat
Serial number	Numéro de série du certificat (propre à chaque autorité de certification).
Signature Algorithm	Algorithme utilisé pour la signature
issuer	Nom de l'Autorité de Certification qui a émis ce certificat
validity	Période de validité du certificat (date de début et date de fin de validité)
subject	Nom du propriétaire du certificat
Subject public key info	Clé publique contenu dans le certificat
X.509 v3 Extensions	Extensions génériques optionnelles, introduites avec la version 3 de X.509
Basic Constraints	indique s'il s'agit du certificat d'une Autorité de Certification ou non, c'est-à-dire permettant d'émettre des certificats ou non.
Key Usage	Donne une ou plusieurs fonctions de sécurité auxquelles la clé publique est destinée. Ce champ permet de spécifier plusieurs services de sécurité pour lesquels le certificat peut servir
subjectAltName	Ce champ contient un ou plusieurs noms alternatifs pour le porteur de certificat, exprimé sous diverses formes possibles**.**
issuerAltName	Ce champ contient un ou plusieurs noms alternatifs pour l'AC qui a généré ce certificat, exprimé sous diverses formes possibles.
CRL Distribution Points	adresse de la CRL permettant de connaître le statut de ce certificat

2.6.1. Les formats

Les formats standards les plus utilisés sont les suivants :

- RSA PKCS#1 : RSA Cryptography Standard
- ANSI X9.62 : The Elliptic Curve Digital Signature Algorithm (ECDSA)
- FIPS PUB 180-1 : Secure Hash Standard (SHA-1)
- FIPS PUB 180-2 : Secure Hash Standard (SHA-2)
- FIPS PUB 46-3 : Data Encryption Standard (DES)
- TTAS.KO-12.0001/R1 : Digital Signature Algorithm (KCDSA)
- TTA.KO-12.0011/R1 : Hash Function Algorithm Standard (HAS-160)
- TTAS.KO-12.0004 : 128-bit Symmetric Block Cipher (SEED)

2.6.1.1. Format ASN.1

La définition du certificat dans le standard X.509 v3 utilise le langage ASN.1 (Abstract Syntax Notation). Ce format permet de décrire des types de données indépendants d'une architecture particulière. Elle figure dans le document intitulé Internet Public Key Infrastructure –X.509 Certificate and CRL Profile, disponible sur le site de l'IETF (Internet Engineering Task Force). Un fichier source aura l'extension **".asn".** Elle utilise une représentation en classe d'objet pour caractériser les différents certificats.

2.6.1.2. Format DER

Le passage de cette définition abstraite d'un certificat numérique en mode X.509, à un fichier exploitable par des applications, se fait en appliquant les règles de codage DER (Distinguished Encoding Rules), qui sont un sous-ensemble de règles BER (Basic Encoding Rules) décrites dans les recommandations ITU-T X.208 (International Telecommunications Union).

Les éléments ASN.1 encodés avec DER sont des triplets tar/longueur/valeur représentés par une suite d'octets. Les fichiers sont au format ".der" ou ".ber", le premier appelé (identifier octet) comporte trois champs :

8	7	6	5	4	3	2	1
Classe		Composé	Numéro de tag				

Où les différentes Classes (bits 8 et 7) sont:

00	Universel	Identique pour toutes les applications, définies dans X.208
01	Application	Spécifique à une application
10	Privé	Spécifique à une entreprise
11	Dépendant du contexte	Spécifique à un type structuré

Pour les numéros de tag supérieurs à 30, le numéro de tag 31 $(11111)_2$ est utilisé, pour indiquer que le numéro de tag est contenu dans le ou les octets suivants en base 128, avec le bit 8 à 1, sauf pour le premier octet. L'octet suivant indique la longueur, en octets, de la suite des octets à interpréter en tant que valeur. Si la longueur est supérieure à 127, le bit 8 est mis à 1, les bits de 1 à 7 indiquant le nombre d'octets à lire pour déterminer la longueur. Le dernier octet de la longueur est suivi des octets représentant la valeur encodée.

La commande suivante permet de visualiser un certificat X.509 en format (.der) :

```
openssl x509 –inform DER –in toto-07.der –noout –text
```

2.6.1.3. Format PEM

Le format DER des certificats numériques se prête mal aux applications du type courrier électronique, car il contient des octets qui pourraient être mal interprétés par certains logiciels de transfert de messages. Le format PEM (Privacy Enhanced Mail) y remédie en utilisant l'encodage Base 64. Un fichier quelconque au format PEM aura une extension ".pem", mais l'on préférera lui donner une extension spécifiant le type de données contenues pour un certificat signé ".crt". Un certificat numérique au format PEM commence par la balise :

```
-------BEGIN CERTIFICATE----------
```

et se termine par la balise :

```
--------END CERTIFICATE-----------
```

La longueur des lignes, exception faite de la dernière, est de 64 caractères ; lesquelles n'utilisent que les 64 caractères [A-Za-z0-9/+] qui devraient résister aux manipulations des logiciels de courrier électronique.

2.6.2. Les standards PKCS

L'évolution de l'utilisation de la cryptographie est également liée au développement de plusieurs standards.

PKCS (Public Key Cryptographic Standards) est un ensemble de standards, pour la mise en œuvre des PKI : coordonnés par RSA. Ces standards définissent les formats des éléments de cryptographie suivants :

- PKCS#1: RSA Cryptography Specifications version 2 (RFC 2437)
  - Spécifie le chiffrement RSA, le décryptage, la signature et des vérifications primitives
  - Spécifie que le chiffrement a été fait à base de l'Algorithme RSA et la signature électronique a été utilisée
  - Spécifie la méthode de codage utilisée pour ces schémas
  - Spécifie la syntaxe ASN.1 pour la clé publique/clé privée à base de RSA
- PKCS#2: inclus dans PKCS#1
- PKCS#3: Diffie-Hellman key Agreement standard Version 1.4
- PKCS#4: inclus dans PKCS#1
- PKCS#5: Password-Based Cryptography Standard. Specifies an encryption scheme based on password for private key protection
- PKCS#6: Extended-Certificate Syntax Standard Version 1.5
- PKCS#7 : Cryptographic Message Syntax Standard Version 1.5 (RFC 2315)
- PKCS#8: Private Key Information Syntax Standard. Specifies a syntax for storage private key
- PKCS#9: Selected Attribute Types Version 2.0
- PKCS#10: Certification Request Syntax Version 1.7 or Certificate Signing Request (CSR) (RFC 2314)
- PKCS#11: Cryptographic Token Interface Standard. Specifies an API (Cryptoki) to be

an interface between applications and all kinds of portable cryptographic devices(ex : Smart Card, PCMCIA. etc)

- PKCS#12: Personal Information Exchange Syntax Standard. Specifies a transfer syntax for private keys and certificate.
- PKCS#13 : Elliptic Curve Cryptography Standard Version 1.0
- PKCS#14 : Pseudorandom Number Generation Standard Version 1.0
- PKCS#15 : Cryptographic Token Information Format Standard. Specifies the format of private key and certificate stored on cryptographic devices.

Le format PKCS#12 permet de rassembler dans un seul fichier, une paire de clé, clé privée/clé publique, le certificat électronique correspondant, le certificat signataire, toute la chaîne de certificats signataires jusqu'au certificat racine. Ce format est très utile pour installer un certificat utilisateur dans un client du Web ou dans un client de Messagerie. Un fichier au format PKCS#12 aura comme extension ".p12".

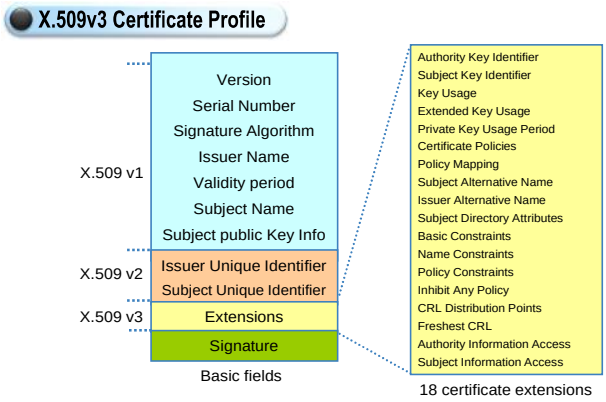
Des Informations à caractère personnel sont protégées par mot de passé ou chiffrement à l'aide de la clé publique et ne peuvent être décryptées ou déchiffrées que par usage de la clé privée correspondant à la clé publique utilisée pour le chiffrement.

2.7. Les Profils

2.7.1. Le Profil du Certificat X.509 V3

Les champs suivants sont renseignés par le logiciel de l'autorité de certification :

- **version** : version du certificat X.509
- **serialNumber** : numéro de série unique du certificat
- **signature** : identifiant de l'algorithme de signature de l'Autorité de Certification
- **issuer** : nom de l'Autorité de Certification émettrice du certificat
- **validity** : dates d'activation et d'expiration du certificat
- **subject** : nom du propriétaire du certificat
- **subjectPublicKeyInfo** : identifiant de l'algorithme d'usage de la clé publique contenue dans le certificat, et valeur de la clé publique
- **extensions** : les extensions du certificat définies dans le document de Déclaration des Pratiques de Certification de l'autorité de certification



2.7.2. Le Profil de la CRL

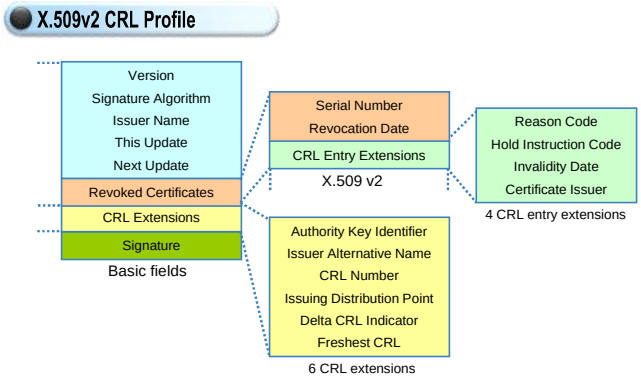
Les CRL contiennent les champs de base tels que spécifiés dans la recommandation X 509 CRL V2.

Ces champs sont les suivants :

- **version** : version de la liste de certificats révoqués X.509.
- **signature** : identifiant de l'algorithme de signature de l'AC
- **issuer** : nom de l'Autorité de Certification émettrice
- **thisUpdate** : date d'émission de cette CRL
- **nextUpdate** : date limite d'émission de la prochaine CRL
- **revokedCertificates** : liste d'enregistrement de certificats révoqués
- **userCertificate** : numéro de série unique du certificat révoqué
- **revocationDate** : date de la révocation
- **crlEntryExtensions** : extensions propres à cette révocation (motif de révocation,

comportement souhaitable face à cette révocation…)

- **crlExtensions** : extensions générales de la CRL



Cette spécification technique définit le profil d'une liste de certificats révoqués. Elle est établie suivant la RFC 3280 et basée sur des dispositions de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité et sur les textes réglementaires subséquents.

Dans le cadre de ce projet, nous avons jugé utile de mettre en exergue le profil de la CRL.

Les standards relatifs au profil de la CRL sont :
[X.509] ITU-T Recommendation X.509 (2000), Information technology - Open Systems Interconnection - The Directory: public-key and attribute certificate frameworks;
[RFC2119] IETF RFC 2119 (1997), Key Words for use in RFC to Indicate Requirement Levels ;
[RFC2459] IETF RFC 2459 (1999), Internet X.509 Public Key Infrastructure Certificate and CRL Profile ;
[RFC3280] IETF RFC 3280 (2002), Internet X.509 Public Key Infrastructure Certificate and CRL Profile ;

La légende utilisée

Les termes suivants, utilisés dans la spécification technique du profil CRL sont compatibles avec la RFC 2119 to status of the implementation of accredited certification authorities and subscribers software

1) Must (Symbol : M)
   Must use
2) Recommend (Symbol : R)
   To consider the security and interoperability, it is recommended to use
3) Optional (Symbol : O)
   Considering the situation, if necessary can be used optionally
4) Not recommend (Symbol : NR)
   To consider the security and interoperability, it is not recommended to use
5) Must not (Symbol : X)
   Must not use
6) Not mentioned (Symbol : -)
   Not mentioned in this specification

Abbreviation

1) CA : Certification Authority
2) CRL : Certificate Revocation List
3) OID : Object Identifier
4) DN : Distinguished Name
5) SHA : Secure Hash Algorithm

Conclusion

La cryptographie se trouve aujourd'hui à la base de toute solution fiable qui apporte la confiance dans les transactions électroniques. Elle résout de façon définitive le problème d'échange de clés entre entités qui désirent communiquer en toute sécurité.

Chapitre 3 : L'INFRASTRUCTURE A CLE PUBLIQUE

Introduction

Une Infrastructure à clé publique est un ensemble de moyens logiciels, matériels et de composants cryptographiques mis en œuvre par des personnes, combinés avec des politiques et des pratiques requises qui permettent de générer des clés, de créer, de gérer, de conserver, de renouveler, de distribuer, de suspendre, de réactiver, de changer des informations à caractère personnel et de révoquer les certificats électroniques basés sur la cryptographie asymétrique.

De nos jours, l'infrastructure à clé publique est par excellence la solution technologique basée sur la cryptographie asymétrique qui présente moins d'inconvénients. Elle utilise la clé publique et la clé privée dans son fonctionnement.

Différentes solutions permettent d'implémenter une PKI à l'aide des logiciels Open Source. Il s'agit notamment le PyCA, Oscar, IDX-PKI, NewPKI, OpenCA… Des solutions existent également parmi les logiciels propriétaires.

3.1. Généralités

Une infrastructure à clé publique PKI (Public Key Infrastructure) a pour but de résoudre le problème crucial de la distribution et de la sécurité des clés publiques. Elle fournit des certificats garantissant le lien entre une entité et sa clé publique. Chaque entité : personne, serveur, etc... Possède une paire de clés : une clé privée et une clé publique. L'utilisateur peut s'authentifier et/ou signer numériquement des documents avec sa clé privée, afin qu'on puisse l'identifier et même vérifier sa signature. Le principe dans un échange est qu'un utilisateur doit distribuer sa clé publique auprès de tous ses partenaires et même de tout le monde capable d'échanger des informations avec lui en toute confiance. Même si le réseau n'est pas sécurisé.

L'arrivée d'une PKI dans un environnement permet la levée des réseaux tels que la ligne spécialisée, le réseau VPN, les tunnels et autres IPSec. Tous ces réseaux n'assurent que le service de la confidentialité, alors que la PKI vous garantit les quatre services de sécurité que sont : la confidentialité, l'authentification, l'intégrité et la non répudiation.

Une PKI utilise des certificats au format X.509 v3 selon la norme internationale RFC 2510/2511. Elle a pour but d'établir la confiance entre plusieurs personnes échangeant des messages, en leur fournissant les services de sécurité suivants : l'authentification, la confidentialité, l'intégrité et la non–répudiation.

3.2. Les Composantes d'une PKI

Une infrastructure à clé publique est composée d'entités qui doivent fournir un certain nombre de services. Certaines de ces entités sont des composantes obligatoires : ce sont l'autorité de certification, l'autorité d'enregistrement et le service de publication des certificats, les autres sont complémentaires.

Les principaux services fournis par la PKI sont :

- L'enregistrement des utilisateurs
- La publication des certificats valides et révoqués des utilisateurs
- L'identification et l'authentification des utilisateurs
- L'archivage des certificats

Elle est constituée de :

- Une autorité de certification (CA)
- Une autorité d'enregistrement (RA)
- Un opérateur de certification (OC)
- Un annuaire de publication de certificats (DS pour LDAP et/ou Autorité de validation OCSP)
- Une autorité d'horodatage (TSA)
- Éventuellement, un service de séquestre de clés (KMI)

3.2.1. Autorité de certification (CA = Certification Authority)

Généralement appelée CA en anglais ou AC en français, l'Autorité de Certification est une entité

tierce, digne de confiance, et reconnue comme telle par la communauté des utilisateurs de certificats. Elle délivre et gère le cycle de vie des certificats électroniques avec les clés publiques qui leur sont associées et les listes des certificats révoqués, CRL, selon les recommandations de la norme X.509.

L'Autorité de Certification est assujettie aux dispositions de l'Autorité de Certification Racine qui elle-même est soumise aux Lois et Règlements en vigueur dans un pays. C'est le cas avec les dispositions de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun et l'ensemble des textes subséquents, ainsi qu'aux normes et directives édictées pour les Etats de la CEMAC en vigueur et aux Conventions internationales ratifiées par le Cameroun, et qui touchent l'application, l'élaboration, l'interprétation et la validité des politiques de certification et le document de Déclaration des Pratiques de Certification.

L'autorité de certification est accréditée auprès d'une Autorité de Certification Racine. Elle possède à cet effet un certificat signé par l'Autorité de Certification Racine qui possède un certificat auto-signé. L'Autorité de Certification Accréditée utilise sa clé privée pour signer des certificats qu'elle délivre aux utilisateurs ou demandeurs de certificats. Elle génère des certificats associés aux clés publiques des utilisateurs et garantit l'intégrité et la véracité des informations qu'ils contiennent. L'autorité de certification accréditée les signe avec sa clé privée.

L'intégrité de la clé publique et la confidentialité de la clé privée de l'Autorité de Certification Accréditée sont fondamentales pour la sécurité d'une PKI. Des dispositions fiables sont généralement prises pour garantir la sécurité à la clé privée de l'autorité de certification.

Avec la prolifération des actes de piratage sur Internet, l'on note une multitude de CA. Preuve qu'il s'agit d'une technologie fiable, solide, bien organisée.

Il convient de relever que n'importe quelle entité peut se déclarer Autorité de Certification. Cependant, pour être qualifié et servir de preuve en Justice en cas de problème, toute autorité de certification qui émet des certificats électroniques doit être garantie par la loi de son pays, disposer d'une police d'assurance pour faire face aux dommages qui pourraient être causés du fait de l'utilisation ou des erreurs contenues dans les certificats émis par votre autorité de certification.

Une CA peut être organisationnelle, spécifique à un corps de métiers ou encore institutionnelle. Mais elle doit être accréditée par une autorité de certification racine.

Selon le crédit accordé à une CA, les certificats délivrés auront un champ d'application plus ou moins important : limité à l'intérieur d'un organisme, échanges inter-organismes, etc...

En délivrant un certificat électronique, l'Autorité de Certification Accréditée se porte garant de l'identité de l'entité qui se présentera avec ce certificat. Par rapport aux entités, personnes ou applications, qui utilisent ses certificats, l'ACA joue le rôle de **tiers de confiance**.

Le niveau de garantie offert par l'ACA dépend du mécanisme de signature, c'est-à-dire les moyens mis en œuvre pour s'assurer de l'identité des demandeurs de certificats, ainsi que la sécurité mise en œuvre pour protéger la clé privée de la CA, etc.

En somme, une Autorité de Certification Accréditée est responsable vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et de la validité des certificats qu'elle émet. A ce titre, elle édicte la Politique sur les Certificats qu'elle émet et le document de Déclaration des Pratiques de Certification aux différentes composantes de l'Infrastructure à Clé Publique qui lui sont rattachées.

La garantie apportée par l'Autorité de Certification Accréditée vient non seulement de la qualité de la technologie mise en œuvre, mais aussi

du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.

Une Autorité de Certification a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (émission, diffusion, renouvellement, suspension, réactivation, révocation,...) et s'appuie pour cela sur une infrastructure technique : l'infrastructure à Clé Publique (PKI).

Les prestations de l'Autorité de Certification Accréditée sont le résultat de différentes fonctions cryptographiques, notamment la sécurisation des applications et la gestion du cycle de vie des bi-clés et des certificats.

La CA possède une base de données interne dans laquelle elle stocke le statut de tous les certificats qu'elle a créés. Cette base de données locale est propre à la CA et donc distincte du dépôt de publication des certificats.

3.2.2. Autorité d'Enregistrement (RA = Registration Authority)

Généralement appelée RA en anglais ou AE en français, elle sert d'intermédiaire entre l'utilisateur et la CA. L'Autorité d'Enregistrement (RA) applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par l'Autorité de Certification et clairement énoncées dans le document de Déclaration des Pratiques de Certification. Son but est d'établir que le demandeur a bien l'identité et les qualités qui seront indiquées dans sa demande de certificat.

La RA traite les demandes de certificats avec diligence. Après en avoir vérifié la recevabilité ainsi que la complétude des dossiers, elle rend compte à l'Autorité de Certification et apporte la preuve en cas de litige et systématiquement pour des cas de demande de suspension ou de révocation.

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et le bénéficiaire. Qu'elle soit ou non directement en contact physiquement avec le bénéficiaire, elle reste dépositaire de ses informations à caractère personnel.

Sa responsabilité ne peut être engagée que par l'Autorité de Certification. En effet, l'Autorité de Certification a un devoir de contrôle et d'audit des Autorités d'Enregistrement placées sous son autorité.

La RA a pour rôle de vérifier l'identité du futur sujet du certificat. Pour cela, l'Autorité d'Enregistrement assure les tâches suivantes:

- la prise en compte de la vérification des informations à caractère personnel du futur sujet de certificat, celles de son organisme de rattachement et la constitution du dossier d'enregistrement correspondant ;
- le cas échéant, la prise en compte et la vérification des informations à caractère personnel du futur mandataire, de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- la prise en compte et de vérification des informations du futur responsable pour une authentification serveur et du serveur informatique, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de la PKI suivant l'organisation de cette dernière et les prestations offertes ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du bénéficiaire ou, le cas échéant, du mandataire, y compris lors des échanges de ces données avec les autres fonctions de la PKI, notamment celles respectant la législation relative à la protection des informations à caractère personnel.

Conformément aux dispositions de la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, toute Administration Publique qui désire gérer une RA sera sous la CA de l'ANTIC et devra respecter

les dispositions de la Déclaration des Pratiques de Certification de la CA.

Une RA a pour tâche principale de recevoir et de traiter les demandes de création, de renouvellement, de suspension, de réactivation, de changement d'informations et de révocation des certificats.

Pour ce faire, elle doit:

- assurer le contrôle des données identifiant le demandeur de certificat et son mandataire de façon univoque ;
- valider les demandes d'émission, de renouvellement, de suspension, de réactivation et de révocation des certificats;
- assurer, lors de l'émission d'un nouveau certificat, l'estampillage de la période de validité du certificat, et que ce dernier est en mesure d'assurer la fonctionnalité d'identification, de signature et/ou de chiffrement.

Après vérification des demandes servies par les utilisateurs potentiels, l'Opérateur de l'Autorité d'Enregistrement RA transmet les informations nécessaires à l'établissement du certificat à sa CA de rattachement. Une RA travaille donc en étroite collaboration avec l'opérateur de certification. Elle possède un bi-clef certifié pour s'authentifier et pour accomplir les tâches de sécurité qui lui incombent.

Pour être efficace, l'Opérateur d'une RA doit être assisté de deux (02) staffs qui ne sont pas nécessairement des ingénieurs. L'un qui distribue les demandes de certificats et réalise l'identification des demandeurs de certificats. L'autre qui explique et indique l'adresse URL, ainsi que le numéro de série, sans lesquels, il sera impossible à l'utilisateur de générer sa paire de clé et de terminer la procédure de certification.

Pour devenir une autorité d'enregistrement, un organisme doit faire sécuriser au moins une application par une autorité de certification. Ensuite signer un protocole d'accord de partenariat avec son CA. Suivre la formation adéquate. Accepter de se conformer au document de déclaration des pratiques de certification et se faire auditer dans une fréquence prévue dans le document de déclaration des pratiques de certification.

L'ensemble des fonctionnalités mises en jeu pendant le processus de création de certificats, leurs statuts (obligatoires ou non) et leurs responsables respectifs sont représentés ci-dessous.

Autorité d'enregistrement	Autorité de certification accréditée
Enregistrement : collecte des informations sur les demandeurs de certificats	Certification : signature des certificats
Authentification du demandeur de certificat	Production des supports physiques
Vérification des attributs	Personnalisation des supports physiques
Remise du certificat	Publication des certificats

3.2.3. L'Opérateur de certification

L'Autorité de Certification Accréditée est le tiers de confiance dont la signature apparaît sur le certificat de l'utilisateur. Elle est responsable du processus de certification de bout en bout.

Pour son fonctionnement, une Autorité de Certification Accréditée délègue à l'Opérateur de Certification toutes les opérations d'administration du système nécessitant l'usage de la clé privée de la CA : **création et distribution sécurisée** des certificats, **renouvellement**, **suspension, réactivation, changement des informations** et **révocation** des certificats électroniques**, production** de cartes à puces… L'Opérateur de la CA gère, en collaboration avec celui de l'autorité d'enregistrement RA, le cycle de vie des certificats, suivant les dispositions du document de la politique de certificats définie et celles du document de Déclaration des Pratiques de Certification.

Cependant, elle assure un contrôle de l'opérateur de Certification.

Pour des raisons de sécurité, l'Opérateur de Certification n'est en général pas connecté au réseau en permanence. En effet, la compromission de la clef privée de la CA étant le risque majeur dans une PKI, tout doit être fait pour l'éviter. Cela entraîne en particulier que le transfert des requêtes

entre la RA et l'Opérateur de Certification ne doit pas se faire de manière automatique.

3.2.4. Services de publication des certificats et des CRL

Ces services ont pour rôle de mettre à la disposition de la communauté d'utilisateurs des certificats électroniques et/ou la liste des certificats révoqués (CRL) contenant des clés publiques associées. La CRL devrait être publiée à chaque fois qu'un nouveau certificat est révoqué ou selon la fréquence définie dans le document de Déclaration des Pratiques de Certification (CPS) de l'autorité de certification.

Cette fréquence peut changer d'une autorité de certification à l'autre.

L'annuaire LDAP permet de publier la CRL toutes les 24 heures. Cependant une autorité de validation à base de l'OCSP permet de donner le statut des certificats instantanément.

Les services de publication (CRL et OCSP) sont régulièrement disponibles et maintenus à jour.

En pratique, pendant l'opération de certification, le demandeur de certificat reçoit dans son support de stockage 5 fichiers :

- un fichier qui montre le chemin de certification ;
- un fichier contenant une clé privée de signature ;
- un fichier contenant une clé privée de déchiffrement ;
- un fichier contenant un certificat de vérification de la signature numérique ;
- un fichier contenant un certificat de chiffrement.

Selon l'usage du certificat, il peut être intéressant de le publier ou non.

La publication des clés et certificats de signature n'est pas forcément utile, car, le certificat de signature est toujours joint à la transaction signée.

Par contre, il est intéressant de publier les certificats de chiffrement. Lorsqu'un utilisateur veut envoyer des données confidentielles à un autre utilisateur, il lui faut être en possession de la clé publique de ce dernier. Pour éviter un échange préalable, les certificats doivent être accessibles à tous les utilisateurs.

Néanmoins, même si la publication n'est pas obligatoire, elle est souvent réalisée en pratique.

L'autorité de certification accréditée est souvent responsable de la publication et du stockage des certificats. Ceux-ci sont placés dans un dépôt (repository) ou serveur de certificats. Le format de certificats X.509 V3 s'adapte naturellement aux annuaires X.500, puisque la norme X.509 exige que certains champs du certificat respectent le nommage X.500.

En pratique, la quasi-totalité des dépôts sont implémentés sous forme d'annuaires ; ces derniers sont naturellement accédés au travers du standard LDAP (Lightweight Directory Access Protocol).

A quels utilisateurs faut-il laisser l'accès au dépôt ?

Un dépôt totalement libre d'accès peut laisser la possibilité à un tiers de prendre connaissance de la structuration de l'autorité de certification. C'est ce qui explique que dans la pratique, les dépôts sont d'un accès semi-public.

Ils sont par exemple ouverts pour les utilisateurs «internes» de l'entreprise, mais à accès restreint pour les utilisateurs «externes».

Il est aussi possible de limiter les fonctions de recherche dans le dépôt en exigeant le nom précis d'une personne pour donner accès à son certificat.

3.3. La gestion du cycle de vie des certificats

L'Autorité de Certification est responsable de la gestion du cycle de vie du certificat, notamment pour les fonctions d'émission, de renouvellement, de suspension, de réactivation, de changement d'information et de révocation.

L'émission des certificats étant déjà traitée par ailleurs, nous allons focaliser notre attention sur les autres fonctions du cycle de vie du certificat.

3.3.1. Renouvellement

De manière générale, la durée de vie d'un certificat varie entre un et deux ans pour un certificat utilisateur et entre trois et vingt ans pour le certificat d'une autorité de certification accréditée.

Si la demande de renouvellement est effectuée alors que la période de validité du certificat précédent est expirée, le processus de demande est assez souvent identique à celui de la création d'un nouveau certificat. L'utilisateur se doit de justifier à nouveau son identité et ses attributs. Ceci n'est toutefois pas obligatoire : il est possible que le document de déclaration des pratiques de certification d'une autorité de certification dispose qu'au moment de l'enregistrement d'un secret entre l'utilisateur et la CA, ce secret pourrait être utilisé pour réaliser le renouvellement du certificat sans réaliser les vérifications d'identification.

L'utilisateur peut aussi signer la demande avec sa clé privée, ce qui garantit son identité et ses attributs. Dans ce cas, la CA établit alors un nouveau certificat toujours avec période de recouvrement avec l'ancien certificat.

Ce processus de renouvellement du certificat peut être soit manuel (demande à renouveler par l'utilisateur avant la fin de validité de son certificat), soit automatique.

3.3.2. Suspension

La suspension d'un certificat est une opération qui consiste à révoquer le certificat de manière temporaire.

Le principe consiste à placer dans la CRL l'identifiant du certificat suspendu et à le retirer dans le cas où la suspension est levée.

3.3.2.1. Comment suspendre un certificat en utilisant les delta CRL ?

Lorsque la CA utilise les delta CRL pour notifier la révocation des certificats, il se pose un problème pour la suspension. En effet, il n'est pas possible via une delta CRL de notifier qu'un certificat qui avait été révoqué est à nouveau valide.

Dans ce cas, c'est à la publication de la CRL suivante que sera rétablie la situation. Il suffit donc que le certificat révoqué n'apparaisse plus dans la CRL et il sera à nouveau considéré comme valide.

3.3.2.2. Procédure

1. La CA publie une CRL ;
2. La CA publie une delta CRL notifiant la suspension du certificat.
3. Un utilisateur habilité lève la suspension de ce certificat.
4. Ce n'est qu'avec la publication de la CRL opérée à fréquence fixe que le certificat est à nouveau considéré comme valide.

Ce procédé provoque un temps de latence pendant lequel l'utilisateur ne peut utiliser son certificat, alors que la suspension a été levée.

D'autres mécanismes, tels que la création de CSL (Certificate Suspension List) contenant les identifiants des certificats suspendus, sont aussi possibles. Mais ils ne sont pas implémentés en pratique pour le moment.

3.3.3. Révocation

Dans la pratique, certains mécanismes doivent être prévus pour invalider un certificat avant sa date de fin de validité, c'est à dire pour le révoquer.

Plusieurs causes sont susceptibles de déclencher une révocation :

- une suspicion ou une compromission réelle de la clé privée ;
- une modification des informations contenues dans le certificat (changement de nom après mariage, évolution de fonction…) ;
- un dysfonctionnement du support du certificat ou une perte des données d'activation (code PIN pour une carte à puce) ;
- un changement de l'état de l'art cryptographique…

Seules les personnes dûment habilitées doivent pouvoir révoquer un certificat. Comme pour la demande de certificat, la demande de révocation est souvent adressée à la RA. Une fonction dédiée peut toutefois être mise en place pour gérer les révocations. Après authentification du demandeur, la demande est transmise à la CA qui va entreprendre son traitement.

La CA dispose de plusieurs méthodes pour répercuter la révocation d'un certificat :

3.3.3.1. La révocation par annuaire positif

La CA retire du dépôt, dans lequel elle publie l'ensemble des certificats émis, chacun des certificats révoqués. Ainsi, lorsque les applications accèdent au dépôt, seuls y figurent les certificats valides. Cette implémentation est à l'heure actuelle peu utilisée.

3.3.3.2. La révocation par publication de listes négatives

La CA publie des CRL (Certificate Revocation List), qui sont des listes contenant les identifiants de chacun des certificats révoqués et non expirés. Les CRL sont généralement publiées dans le dépôt de certificats, mais elles peuvent également l'être dans un dépôt dédié (un dépôt de CRL).

L'application récupère périodiquement une copie de la dernière CRL émise par la CA. Lorsqu'elle cherche à vérifier la validité d'un certificat, elle peut ainsi vérifier si le certificat en question est dans cette liste (cf. plus bas le paragraphe portant sur la validation).

La fréquence de publication des CRL doit être paramétrée en fonction de la politique de sécurité retenue. En règle générale, la CRL est publiée à fréquence fixe (une fois par jour, une fois par heure…) par la CA.

Le plus souvent, la CRL devient rapidement un fichier volumineux et sa manipulation une opération lourde. Pour pallier ce problème, la CRL complète n'est pas publiée à chaque fois qu'un certificat est révoqué. Des optimisations de la CRL ont été mises au point :

• Les **CRL Distribution Point** consistent à partitionner la CRL de manière à obtenir des fichiers de taille moindre, qui soient faciles à récupérer.

Pour ce faire, chaque certificat contient les références de la partition dans laquelle il se trouve, afin que les applications puissent récupérer la CRL de la partition idoine.

• La **delta CRL** permet de fournir la liste des certificats dont le statut a changé depuis l'émission de la dernière CRL.

Dans ce cas, la CA publie également la CRL à intervalles réguliers, alors que la publication de la delta CRL est beaucoup plus fréquente (par exemple dès qu'un certificat a été révoqué).

Ceci permet d'optimiser le délai de prise en compte des révocations par les applications.

Le mécanisme des delta CRL est toutefois aujourd'hui très peu implémenté.

3.4. Gestion des certificats et des clés des composantes d'une PKI

La spécificité et la criticité des certificats d'une Autorité de Certification Accréditée (et plus généralement des certificats de l'ensemble des composants de l'infrastructure) suppose une organisation particulière de la gestion de leur cycle de vie.

Ainsi, les opérations relatives à la gestion du cycle de vie des clés de CA sont usuellement réalisées au cours de «Key Ceremonies» qui s'apparentent à des cérémonies notariées (réalisées en effectifs restreints devant témoins, éventuellement filmées, etc.). Par exemple la Key Ceremony associée à la création d'un certificat de CA regroupera les procédures de génération du bi-clés, de génération du certificat correspondant, de clonage éventuel du bi-clé sur un HSM de sauvegarde ou mis en coffre, de génération et de partage des secrets liés à l'activation de la clé privée, etc… On réalisera des Key Ceremonies notamment pour la création, le renouvellement, la suspension, la réactivation et la révocation d'un

certificat de l'autorité de certification racine ou d'une CA accréditée.

Les actions associées à la révocation d'un certificat de CA accréditée doivent permettre une prise en compte rapide par les utilisateurs. Or, la publication d'une ARL (Authority Revocation List) lors d'une Key Ceremony ne permet pas de bloquer totalement l'utilisation des certificats car la plupart des applications standards ne permettent pas nativement de vérifier la publication éventuelle d'une ARL. Il est donc en général nécessaire de notifier l'ensemble des administrateurs d'application et des porteurs de certificat.

On peut également placer dans la CRL les références de l'ensemble des certificats émis par la CA (cette dernière opération peut poser néanmoins certains problèmes pour la récupération de la CRL qui atteint alors une taille largement plus importante qu'à l'accoutumée).

Le renouvellement de la clé d'une CA accréditée fait également l'objet d'une organisation spécifique. En effet, une clé privée de CA doit rester valide tant que tous les certificats qu'elle a signés ne sont pas expirés (dans le cas contraire lesdits certificats ne pourraient plus être considérés comme valides). On met alors en œuvre un processus de renouvellement avec période de recouvrement (roll-over).

3.5. La validation des certificats

Lorsqu'un certificat est présenté à une application pour réaliser une opération de chiffrement, d'authentification d'un utilisateur, de vérification de la signature d'un document…, l'application doit s'assurer de la validité de ce certificat.

Cette opération englobe plusieurs vérifications qui peuvent être réalisées ou non. Il convient de faire le choix lors de la sécurisation de l'application. Ces vérifications sont notamment :

- Vérification de la période de validité du certificat telle qu'elle est mentionnée dans le certificat lui-même ;
- Vérification de la signature présente dans le certificat, à l'aide de la clé publique de la CA émettrice. Ceci implique de détenir au préalable ou de récupérer par un moyen sûr le certificat de la CA concernée ;
- Vérification du chemin de certification. En effet, l'application doit, pour accepter le certificat, avoir confiance en la CA émettrice. Si le certificat de la CA émettrice a été émis lui-même par une autre CA, il faut remonter la «chaîne de certification» jusqu'à un certificat de CA «connue» et «de confiance». Cela implique aussi la vérification de la validité (date de validité et statut de non révocation) de chaque certificat de CA se trouvant dans la «chaîne de certification». Au sommet de la chaîne, doit se trouver une CA dans laquelle l'application place sa confiance, et dont le certificat auto-signé aura été remis au préalable à l'application par un moyen sûr.
- Vérification du statut du certificat. Cette opération consiste à vérifier que le certificat n'est ni révoqué ni suspendu.

Utilisateur	**ACA**	**CA Racine**
Identité : Utilisateur	Identité : ACA	Identité : RCA
Clé Publique de chiffrement	Clé publique de signature	Clé publique de signature
Usage : chiffrement	Usage : certification	Usage : certification
Identité du signataire : ACA	Identité du signataire : RCA	Identité du signataire : RCA

Figure : Chaîne de certification

Ces vérifications peuvent être réalisées de différentes manières en fonction des services offerts par la PKI et de l'implémentation retenue. Elles peuvent être faites soit par l'application sécurisée elle-même, soit par une «interrogation» de l'infrastructure PKI.

3.5.1. Contrôle par l'application

Les contrôles réalisables de manière «autonome» par l'application sont essentiellement la vérification des dates de validité, la vérification de la signature et dans certains cas, la vérification du chemin de certification.

3.5.2. Contrôle par la PKI

Les contrôles décrits plus haut sont réalisables en interrogeant les services de la PKI, soit par récupération ou interrogation de CRL, soit par interrogation d'un module supplémentaire de la PKI.

3.5.2.1. Accès aux CRL

Les CRL permettent uniquement d'assurer le contrôle de la non révocation et de la non suspension du certificat. Le principe consiste à récupérer en local la CRL, ou l'une de ses variantes, pour opérer cette vérification. Plusieurs stratégies sont envisageables en fonction du niveau de sécurité désiré :

- l'application va périodiquement chercher la dernière CRL publiée : c'est le pull ;
- l'ACA transmet à l'application chaque nouvelle version de la CRL et des delta CRL : On parle de push.

En fonction de la fréquence de récupération des CRL, le temps de latence pour la répercussion des informations sera plus ou moins long et le service plus ou moins dégradé.

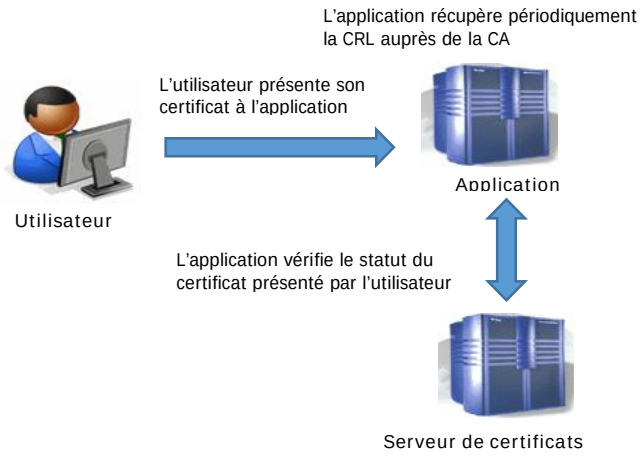


Figure : Vérification de la validité d'un certificat par l'application

3.5.2.2. Mise en place d'une Autorité de validation (VA)

Cette solution consiste à intégrer un module technique supplémentaire dans la PKI, la VA. Les applications vont alors interroger ce composant tiers pour connaître le statut d'un certificat. Par l'envoi d'un message de réponse signé, la VA assure la validité du certificat.

Le concept d'Autorité de validation est né avec l'avènement du protocole OCSP (Online Certificate Status Protocol), qui est devenu un standard.

OCSP repose sur un modèle client-serveur. L'application héberge un client qui interroge le serveur OCSP, appelé OCSP Responder. A cet effet, la requête OCSP est postée par le client via un protocole de transport tel que HTTP, LDAP ou SMTP vers un serveur OCSP (OCSP Responder). Ce dernier formate une réponse, signée électroniquement, faisant état du statut du certificat, à savoir «valide», «révoqué» ou «inconnu».

3.5.2.2.1. Les différentes versions d'OCSP

Le module Online Certificate Status Protocol (OCSP) version 1 selon la norme RFC 2560 travaille uniquement avec l'identifiant du certificat. L'application fournit à l'OCSP Responder l'identifiant du certificat. Le seul service assuré est par voie de conséquence la vérification des informations de non- suspension et de non-révocation du certificat présenté.

OCSP version 2 (en cours de normalisation) pourra utiliser directement le certificat. L'application fournira le certificat lui- même à l'OCSP Responder, qui sera alors en mesure de vérifier comme OCSP version 1 les informations de non-suspension et de non-révocation, mais également les dates de validité, le statut de la CA ayant signé le certificat ainsi que la chaîne de certification.

D'autres évolutions de ce protocole devraient voir le jour, comme SCVP (Simple Certificate Validation Protocol) qui utilise XML.

Deux types d'implémentation sont possibles pour l'OCSP Responder :

- **Utilisation des CRL**

L'OCSP Responder récupère les CRL, ou ses dérivés, en local avec la même problématique de stratégie de récupération (pull/push) que dans le cadre de la vérification de la validité des certificats par les applications.

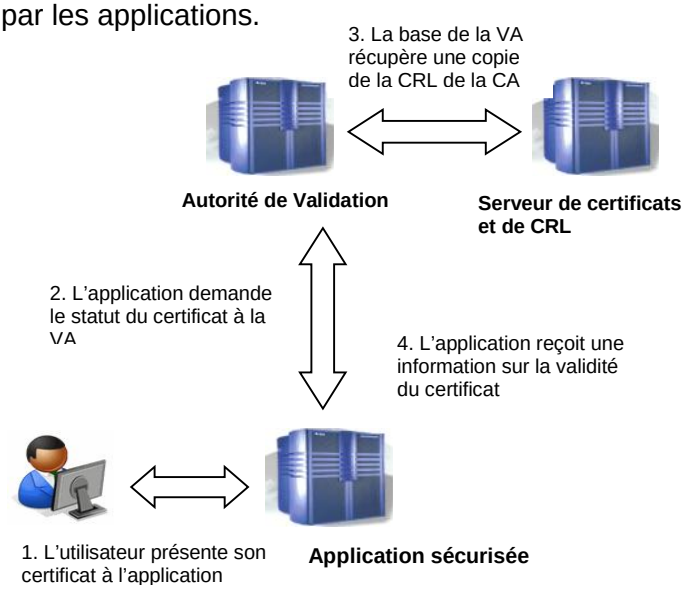


Figure : Vérification de la validité d'un certificat par une Autorité de Validation avec CRL

- **Consultation directe de la base de données de la CA**

Afin de mettre en place un véritable service de validation en temps réel du statut des certificats, l'agent de l'autorité de validation peut directement consulter le statut des certificats dans la base de données de la CA.

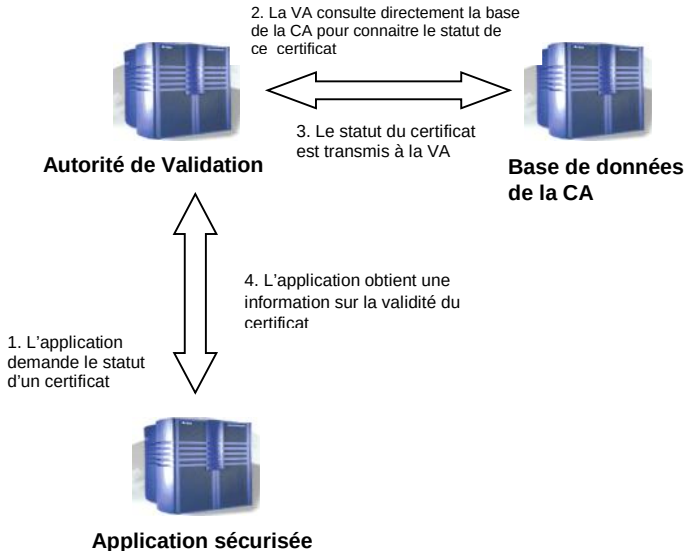


Figure : Vérification de la validité d'un certificat par une autorité de validation avec consultation de la base de données de la CA

L'utilisation d'une VA présente principalement les intérêts suivants :

- les applications sont «déchargées» en grande partie de la tâche de validation des certificats ;
- les applications sont certaines d'obtenir une information sur la validité du certificat qui soit la plus récente possible ;
- les applications obtiennent une réponse **signée électroniquement** par la VA, ce qui peut constituer un élément de preuve sur la validité du certificat en cas de contestation ultérieure sur la validité d'un échange.

Le choix de la méthode de validation est à la charge de l'applicatif et sera fonction du niveau de criticité de l'application.

3.6. Services de recouvrement, d'horodatage et de notariat

Les fonctionnalités et modules techniques des PKI que nous venons de présenter participent directement à la gestion du cycle de vie des certificats et l'exploitation par les applications.

D'autres services peuvent être également mis en place pour compléter les offres de la PKI. Il s'agit notamment des services de recouvrement, ou encore des services d'archivage et d'horodatage qui apportent la preuve irréfutable de la non-répudiation.

3.6.1. Le Service de recouvrement

En pratique, il conviendrait d'éviter la perte de données chiffrées. Sur le plan juridique, il y a nécessité de mettre à disposition de la justice les données chiffrées. A cet effet, la PKI peut rendre des services de sauvegarde et de recouvrement des clés privées de chiffrement, et/ou des services de séquestre de ces clés, grâce à l'intégration d'un module supplémentaire.

En revanche, il ne doit jamais être envisagé de service de recouvrement de clé privée de signature.

Pour réaliser ce service, un module hautement sécurisé placé sous la responsabilité d'une autorité digne de confiance et bien identifiée, qui peut être

la CA ou une tierce partie de confiance dédiée, est en charge de la sauvegarde des clés privées de chiffrement et de l'accès à ces données par des personnes autorisées.

Lorsque le bi-clé est généré au sein de l'Infrastructure de Confiance, la clé privée est directement transmise à l'organe prévu à cet effet. C'est la solution la plus fréquemment retenue.

Lorsque le bi-clé est généré en local sur le poste de l'utilisateur, la clé privée doit être transmise à l'Infrastructure de Confiance pour pouvoir bénéficier de ce service. Ce transfert se fait préférablement hors ligne, mais il peut également se dérouler après la remise du certificat à l'utilisateur à travers un échange sécurisé.

Des solutions alternatives peuvent être utilisées :

- Chaque chiffrement peut être réalisé deux fois, une fois avec la clé publique du destinataire, et une fois avec la clé publique d'une autorité de recouvrement dédiée ;
- L'autorité de recouvrement peut se contenter de sauvegarder de manière sécurisée les clés symétriques utilisées par chaque chiffrement.

Les processus organisationnels liés au recouvrement sont complexes à mettre en place. Il faut s'assurer de l'habilitation du demandeur d'un recouvrement, éventuellement informer le porteur de la clé correspondante…

Le service de recouvrement est délicat. Pour des raisons de sécurité, il ne devrait pas être autorisé à un Mandataire ou à un commissionnaire de le solliciter pour un organisme, quelle que soit la raison, afin d'éviter d'éventuelles situations de compromission.

3.6.2. Le Service d'horodatage

L'importance du service d'horodatage dans les transactions temporelles n'est plus à démontrer. Il permet d'associer une date / heure réputée fiable à un document ou à une transaction électronique.

Il est aussi souvent utilisé pour prouver l'antériorité d'un message ou d'une transaction par rapport à un évènement, à l'instar de la révocation ou de la suspension d'un certificat.

L'horodatage se doit de satisfaire deux impératifs :

- S'appuyer sur une **source de temps reconnue** par tous les acteurs impliqués dans la transaction :

  Une des sources les plus utilisées par les systèmes d'horodatage est le GPS, précis à 1 µs. D'autres sources peuvent être utilisées, notamment l'horloge parlante téléphonique (précise à 20 ms), les stations LF comme l'émetteur France Inter (précise à 1 ms), le CDMA utilisé dans les réseaux de téléphones mobiles UHF (précis à 100 µs) ou le NTP à précision variable.

  Dans le cas du Cameroun, la source de temps utilisée par l'ANTIC est le GPS.

  Le fait que la source de temps soit reconnue de tous les acteurs concernés est en pratique souvent plus important que la précision intrinsèque de cette horloge.

- S'associer **de façon irrévocable** au document ou à la transaction :

  Cette association, pour être incontestable, doit s'appuyer sur un mécanisme de signature par une "Autorité d'Horodatage", ou Time Stamping Authority (TSA) reconnue des différents acteurs, c'est-à-dire respectant une politique d'horodatage conforme à l'état de l'art, utilisant un certificat contrôlable... Le fichier signé par cette autorité comprend une trace du document ou de la transaction visée et le jeton d'horodatage lui-même. Lorsque la transaction a déjà été signée par son "propriétaire", l'autorité d'horodatage vient la contre-signer avec sa propre clé de signature.

  Les jetons d'horodatage signés par l'autorité d'horodatage ne peuvent être falsifiés ou

contrefaits sauf dans le cas éventuel de compromission de sa clé de signature qui pourrait être utilisée de manière illicite avant la révocation du certificat associé.

La norme RFC 3161 "Internet X 509 Public Key Infrastructure Time Stamping Protocol", décrit le format d'échange avec une autorité d'horodatage (TSA).

3.6.3. Le Service de notariat

Le Service de notariat consiste à archiver des informations, après les avoir horodatées et signées, dans le but de retrouver le séquencement des échanges, et d'exhiber les preuves de la réalité et/ou du contenu de ces échanges. Le notariat permet d'offrir une fonction de non-répudiation complète.

L'archivage consiste à stocker des informations dans un lieu sûr et sur des supports sécurisés, afin de pouvoir y accéder ultérieurement.

Le Service de notariat peut être réalisé soit au niveau de chacune des applications, soit au niveau d'un service d'horodatage et d'archivage, qui stocke l'ensemble des informations qui lui sont transmises.

Le Service de notariat peut aussi être réalisé hors ligne, dans ce cas, les autres modules demandent au module d'archivage de conserver un élément. Il peut être réalisé en ligne, dans ce cas, les éléments transitent obligatoirement par ce module qui, après horodatage et archivage, les transmet au(x) destinataire(s)).

3.7. Interconnexion des systèmes PKI

Dans le domaine de la sécurité, l'établissement d'un lien de confiance entre deux parties repose sur la confiance placée par chaque partie en la signature de l'autorité de certification se trouvant sur le certificat de l'autre partie.

Avant qu'une autorité de certification ne puisse générer et signer des certificats pour le compte d'entités utilisatrices, notamment les autorités de certification accréditées, elle doit elle-même générer et signer son propre certificat pour représenter sa propre identité.

Une CA ayant signé son propre certificat est appelée Autorité de Certification Racine (Root Certification Authority).

L'ensemble des entités utilisatrices ainsi que les applications sécurisées reconnaissant l'Autorité de la CA racine constitue un domaine de sécurité. Un tel domaine peut être implémenté pour couvrir un pays, une organisation, une société, une communauté d'intérêt…

La mise en œuvre de ces concepts d'interconnexion de PKI permet de créer de vastes domaines de confiance sur des réseaux ouverts comme Internet. Dans le commerce électronique, un utilisateur détenant un certificat délivré par une banque pourra commercer avec un vendeur qui détient un certificat fourni par une autre banque, pourvu que les banques en question aient interconnecté au préalable leurs PKI, et en évitant de diffuser à l'ensemble des utilisateurs les certificats racines des AC de chaque banque.

Toutefois, la mise en place d'une interconnexion des PKI n'est pas une simple opération technique : pour que cette connexion ait un sens, il faut garantir la compatibilité entre les politiques de sécurité mises en œuvre par chaque CA participante.

Pour cette raison, la mise en place en pratique de la certification hiérarchique ou de la certification croisée est réalisée dans le cadre d'initiatives très encadrées par une loi, des traités ou des conventions imposant des règles de fonctionnement strictes.

De manière générale, l'interconnexion des PKI doit reposer sur la compatibilité des politiques de certification, des stratégies de sécurité et les documents de Déclaration des Pratiques de Certification que nous allons décrire maintenant.

3.7.1. Architecture hiérarchisée

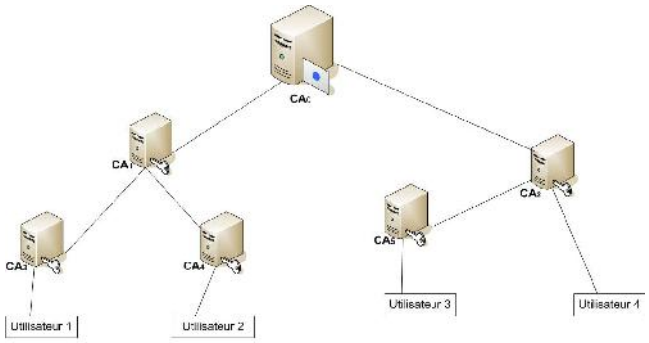
La norme X.509 V3 propose le concept de la hiérarchisation des autorités de certification. C'est ici que nait également la notion d'accréditation.

Dans le cas d'une relation hiérarchisée, une CA dite racine délivre un certificat à une ou plusieurs autres CA, qui elles-mêmes peuvent délivrer un certificat à d'autres CA et ainsi de suite.

Chaque CA délivre des certificats aux CA filles et éventuellement aux utilisateurs. En général les CA feuilles délivrent uniquement des certificats aux

utilisateurs. On peut donc établir des relations de confiance hiérarchiques de la manière suivante.

Au sommet de cette arborescence, on trouve les CA racines dont le certificat est signé avec leur propre clé privée (certificat auto-signé). L'architecture hiérarchique évite qu'une seule entité soit responsable des certificats et donc augmente la fiabilité et réduit le risque de compromission des clés privées des CA. Pour valider un certificat utilisateur ayant déposé sa demande au niveau de CA4 par exemple, il faut les certificats de signature de la RCA0, de la CA1 et de la CA4. On appelle cela une chaîne de certification.



Architecture hiérarchique d'une PKI

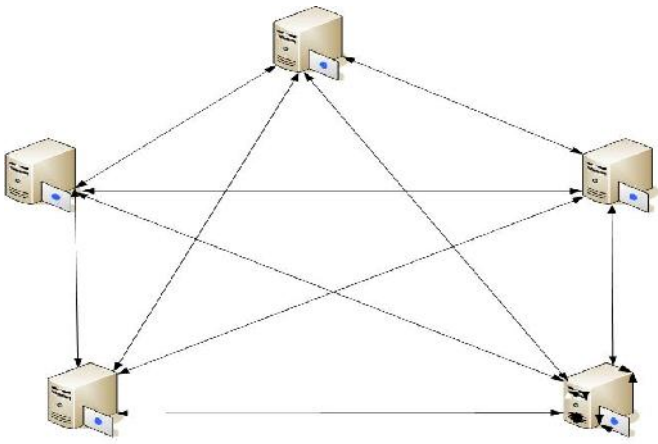
3.7.2. Architecture croisée

Une certification est dite croisée lorsque deux autorités de certification racines se font mutuellement confiance. Dans ce cas, une certification croisée est opérée entre les deux entités : chaque autorité de certification racine signe de façon bi-latérale la clé publique de l'autre autorité de certification racine, reconnaissant ainsi la confiance accordée à l'autre autorité de certification racine.

Tous les utilisateurs dépendant de l'une des CA racines reconnaissent ainsi les certificats émis par l'autre CA racine.

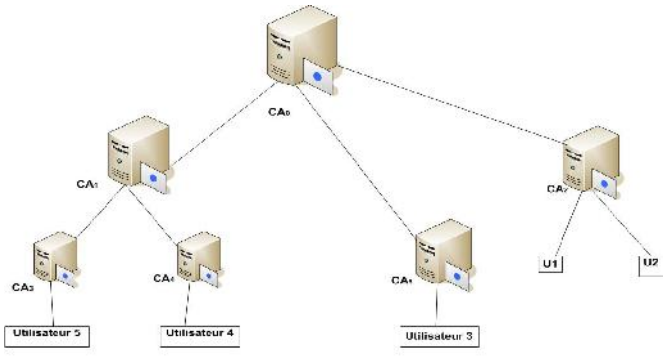
Ainsi un utilisateur certifié par la CA1 de RCA1 pourra vérifier le certificat d'un autre utilisateur certifié par la CA2 de RCA2 en toute confiance et sécurité.

La certification croisée est très utile si le nombre de RCA voulant se faire mutuellement confiance est limité. Le problème se pose pour une communauté de n autorités de certification racines distinctes, avec n grand, voulant certifier chacune les n-1 certificats des autres RCA.


Architecture croisée

3.7.3. Architecture à pont

C'est une structure proposée pour résoudre le problème de complexité de la certification croisée. Dans cette structure, plusieurs autorités de certification racines distinctes (par exemple appartenant à plusieurs entreprises) veulent se faire mutuellement confiance, alors elles font confiance à une seule CA pont (ou bridge CA) qui va établir des chemins de confiance c'est-à-dire des branches de certificats entre différentes PKI. Chaque CA racine de chaque PKI établit un certificat croisé avec la CA pont (bridge CA) puisque que la bridge CA ne délivre de certificat qu'aux CA qu'elle accrédite. Seules les CA doivent avoir des certificats délivrés par la bridge CA. La CA bridge ne délivre pas de certificats aux utilisateurs finals mais aux RCA.



Architecture à pont

Chapitre 4 : LA POLITIQUE DE CERTIFICATION ET LE CADRE LEGAL

Introduction

Le Cameroun a mis en place un cadre juridique qui encadre la gestion technique de la PKI. Or, le système PKI n'offre pas seulement la solution technologique, il intègre également des règles de sécurité et des procédures organisationnelles, régissant la délivrance et l'utilisation des certificats. Ces procédures et règles sont d'une importance capitale et permettent de mesurer la confiance que l'on peut accorder aux certificats qui seront délivrés par la PKI. La confiance est une conséquence de la satisfaction de l'utilisateur.

En effet, l'infrastructure technique aura beau être parfaitement sécurisée et protégée, les certificats n'auront aucune valeur si les processus organisationnels ne sont pas rigoureusement définis et appliqués. Lorsque les procédures de vérification d'identité des demandeurs de certificats prévues ne sont pas appliquées complètement, cela pourrait poser un problème crucial et constituer une faille de sécurité qu'il sera difficile de résoudre.

Dans ce chapitre, nous décrivons les principaux processus à formaliser et les documents associés. Ensuite nous décrivons comment la loi camerounaise relative à la cybersécurité et à la cybercriminalité se propose de fixer un cadre pour la reconnaissance de la signature électronique, grâce aux certificats qualifiés et à la signature avancée.

4.1. Processus et Classes de certificats

4.1.1. Processus organisationnels

Lors de l'étude de faisabilité de tout projet PKI, il convient de mener une réflexion pour formaliser les processus organisationnels nécessaires à la gestion des certificats, ainsi que des processus nécessaires à la gestion de la PKI elle-même.

Cette réflexion doit permettre de définir les responsabilités de chacun des acteurs intervenants autour de la PKI (CA, RA, VA, TSA, utilisateur…)

Principaux processus relatifs au cycle de vie des certificats destinés aux utilisateurs

Phase d'initialisation

- Enregistrer une demande de certificat
- Authentifier une demande de certificat
- Générer le certificat (ou le récépissé contenant le numéro de code et l'adresse URL qui vont permettre à l'utilisateur de finaliser la procédure initiée par l'opérateur de la RA)
- Distribuer le certificat (et la clé privée dans certains cas)

Phase d'utilisation

- Vérifier le statut d'un certificat

Phase de révocation ou de suspension

- Enregistrer une demande de suspension ou de révocation
- Suspendre un certificat
- Réactiver un certificat suspendu
- Révoquer définitivement un certificat

Phase de renouvellement

- Enregistrer une demande de renouvellement
- Renouveler un certificat
- Publier et distribuer le nouveau certificat

Gestion du support matériel (carte à puce)

- Enregistrer une demande de déblocage du PIN Code
- Débloquer le PIN Code

Principaux processus relatifs au cycle de vie des composantes de la PKI

- Création de l'Autorité de Certification
- Création de l'Autorité d'Enregistrement centralisée, déléguée ou locale
- Fin d'activité d'une Autorité de Certification
- Renouvellement des certificats des composantes de l'infrastructure (CA, RA, TSA, VA…)
- Compromission des clés des composantes de l'infrastructure (CA, RA, TSA, VA…)…

4.1.2. Classes de certificats

Avant l'implémentation de la solution technique du système PKI, une réflexion doit être conduite pour définir le bouquet de certificats qui seront

utilisés. En effet une organisation peut décider pour diverses raisons d'émettre plusieurs types de certificats, avec des caractéristiques différentes. On parle généralement de classes de certificats. Les différences entre les classes de certificats porteront le plus souvent sur :

- le niveau des contrôles réalisés lors du processus d'enregistrement et de distribution des certificats ;
- le support utilisé pour stocker ces certificats ;
- les usages possibles du certificat (signature, chiffrement…) ;
- les différents porteurs de certificats ;
- les applications utilisatrices des certificats.

Il est possible de définir un certificat de «haute-sécurité», stocké sur une carte à puce, avec deux authentifications de l'utilisateur en «face à face» physique lors de l'enregistrement et de la remise du certificat. A l'opposé, un certificat de faible sécurité serait basé sur un enregistrement et une distribution entièrement automatisés et serait stocké sur le disque dur du poste de travail ou une clé USB.

Les résultats de ces réflexions sont notamment consignés dans deux documents qui sont à la base du fonctionnement de la PKI : la Politique de Certification (PC) ou Certification Policy (CP) et la Déclaration des Pratiques de Certification (DPC) ou Certification Practice Statement (CPS).

4.2. La Politique de Certification (PC)

La Politique de Certification (PC) est un ensemble de règles qui indiquent les conditions d'utilisation d'un certificat pour une communauté donnée ou pour des applications ayant des besoins de sécurité communs.

Les principaux rôles de la PC sont donc de :

- définir le périmètre d'utilisation des certificats ;
- spécifier les obligations et définir les responsabilités des utilisateurs et de chacune des entités composantes de la PKI ;
- déterminer le niveau des contrôles d'authentification et de vérification des attributs.

Ainsi, la PC indique les garanties offertes par les certificats émis par l'Infrastructure de Confiance, ainsi que les conditions d'utilisation de ces certificats. Elle ne traite pas des pratiques mises en œuvre pour atteindre ces garanties : c'est le rôle de la DPC.

La politique de certification est un document de «haut niveau». Elle peut être définie indépendamment des contraintes organisationnelles de l'environnement de mise en œuvre auquel elle s'applique. Ainsi, une PC peut être la même pour plusieurs entreprises d'un même pays ayant des exigences de sécurité d'un niveau semblable.

Traitant de la répartition des responsabilités entre les différentes composantes de l'Infrastructure de Confiance, la PC est structurante pour le déploiement et l'exploitation de la PKI.

La RFC 3647 qui est la norme la plus récente donne une recommandation pour l'élaboration le plan type d'une Politique de Certification.

Avant sa mise en application effective par la PKI, la PC peut être soumise à une validation juridique ou gouvernementale et à un audit de sécurité qui déterminent sa cohérence. Ce mode de validation est fortement conseillé.

Dès lors qu'elle s'applique à un environnement ouvert, dans lequel une relation contractuelle lie la CA et les utilisateurs des certificats, la PC doit être rendue public : les utilisateurs peuvent ainsi s'assurer que les politiques mises en œuvre au sein de la PKI sont dignes de confiance. Les autorités de certification publient souvent sur leur site Web les politiques de certification qu'elles appliquent.

Il est aussi possible de référencer la PC auprès d'un organisme tiers comme l'ANTIC. Cet établissement public administratif délivre alors un identifiant unique (OID) qui peut être repris dans un champ du certificat. Cela permet à l'utilisateur d'identifier de manière unique la PC appliquée par la CA émettrice du certificat, puis de déterminer s'il lui fait ou non confiance.

La publication des PC est également nécessaire lorsque deux CA souhaitent se faire mutuellement confiance, dans le cadre d'une certification croisée. Par la consultation et la comparaison de leurs PC respectives, elles peuvent déterminer les garanties offertes par l'autre protagoniste et décider de la confiance à lui accorder.

Contraintes juridiques

Un certain nombre d'aspects juridiques doivent être pris en considération au moment de la rédaction de la PC, car ils ont une incidence forte sur les processus organisationnels de l'entreprise.

En particulier au moment de la demande de certificat par un utilisateur, l'entreprise récupère un certain nombre d'informations à caractère personnel sur le demandeur. Un texte régit la protection de la vie privée face à la collecte de données personnelles : la loi relative à la cybersécurité et à la cybercriminalité.

Par ailleurs la PC doit préciser les durées de conservation des données liées au fonctionnement de la PKI (dossiers d'enregistrement, listes de révocation des certificats…).

La conservation sur des périodes très longues pose des problèmes techniques et organisationnels considérables. Il convient de vérifier quelles sont les durées adéquates d'un point de vue juridique en fonction de l'usage des certificats.

4.3. Déclaration des Pratiques de Certification (DPC)

La Déclaration des Pratiques de Certification (DPC) décrit les pratiques usuelles mises en œuvre pour atteindre les garanties sur les certificats, énoncées dans la PC. Ce document répond à la question du «comment», alors que la PC répondait plutôt à la question du «quoi».

La DPC est donc la déclaration de la part des entités de la PKI (CA, RA, TSA, VA…) des détails de leur système de confiance et des procédures employées pour réaliser l'ensemble des tâches dont elles sont responsables : création et exploitation des certificats, création et exploitation des listes de révocation...

Ce document, dont la rédaction est placée généralement sous la responsabilité de la CA, est donc l'adaptation de la PC aux contraintes humaines, matérielles et organisationnelles de l'autorité de certification. De ce point de vue, il est logique que la diffusion de ce document soit limitée, contrairement à la PC qui était diffusée à très large échelle.

4.4. Reconnaissance légale de la signature électronique

La cryptographie à clé publique est la technologie qui permet de mettre en application la législation nationale pour ce qui est de la signature électronique.

La loi camerounaise relative à la cybersécurité et à la cybercriminalité traite de la signature électronique et son application dans le cyberespace camerounais apportent les bases juridiques à la dématérialisation des échanges : une signature électronique ne pourra plus désormais être désavouée sous le seul prétexte qu'elle est électronique et non manuscrite.

En d'autres termes, les parties d'un échange dématérialisé seront donc affranchies d'un accord contractuel préalable définissant une convention de preuve, comme c'était le cas jusqu'à maintenant.

Signature électronique et législation

Le Parlement Européen avait adopté une directive sur la signature électronique le 13 décembre 1999. La loi française correspondante a été votée le 13 mars 2000, entraînant une mise à jour du code civil de ce pays. La République de Corée avait adopté une loi sur la signature électronique. La loi camerounaise relative à la cybersécurité et à la cybercriminalité qui traite de la signature électronique a été votée le 21 décembre 2010.

Désormais, la signature électronique a la même valeur juridique que la signature manuscrite au Cameroun et il n'est plus possible d'invoquer la

non-validité de la signature électronique pour renier une transaction.

L'arrêté n°00000014/MINPOSTEL du 27 Juin 2012 fixe les critères de qualification des certificats et les caractéristiques techniques du dispositif de création des signatures électroniques.

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve de contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Ce texte fait apparaître trois notions importantes :

- La signature électronique sécurisée : une telle signature doit permettre d'identifier le signataire, doit pouvoir être réalisée par des moyens que le signataire puisse garder sous son contrôle exclusif, et doit garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable. Les technologies de cryptographie à clé publique, sous réserve qu'elles soient mises en œuvre dans un cadre rigoureux, répondent déjà à ces critères.

- Le dispositif sécurisé de création de signature électronique : il s'agit d'un dispositif qui doit faire l'objet d'une certification par un prestataire agréé par les services du Premier Ministre.

- Le certificat électronique qualifié : un tel certificat doit être émis par un Prestataire de Service de Certification (PSC) préalablement accrédité, et doit comporter un certain nombre d'éléments (certains obligatoires, d'autres optionnels), tels que le nom du signataire ou son pseudonyme, les données de vérification de signature électronique, la période de validité du certificat, les conditions d'utilisation du certificat, etc. Le certificat qualifié sera, sauf à apporter la preuve du contraire, «présumé fiable» par les tribunaux (ce qui n'en fait pas forcément un certificat "universel" accepté par tous : son utilisation peut en effet éventuellement être restreinte à un cadre contractuel spécifique).

La capacité d'un Prestataire de Service de Certification à émettre des certificats qualifiés sera évaluée par des organismes de qualification, a priori accrédités au Cameroun par la CamRootCA de l'ANTIC. Cet audit sera réalisé suivant une méthode et par rapport à un référentiel de bonnes pratiques disponible en ligne dans le site web www.rootca.cm de la CamRootCA.

LES TELEPROCEDURES

Le Ministère des Finances (MINFI) a entamé un vaste programme de dématérialisation progressive des échanges entre l'administration fiscale et les administrés. Dans le cadre de cette initiative, le projet ″Télédéclaration″ a eu pour première étape visible la déclaration en ligne de la TVA par les entreprises et les citoyens. L'un des moyens proposés pour la déclaration en ligne consiste schématiquement à remplir un formulaire électronique et à le déposer sur le site Internet de la Direction Générale des Impôts du MINFI. Pour le moment, cette procédure n'est pas encore sécurisée et donc ne s'accompagne pas encore de la signature électronique du représentant de l'entreprise déclarante ou du déclarant.

Normalement, le déclarant doit disposer d'une clé privée et d'un certificat de la clé publique correspondante. Ce certificat devrait être délivré au préalable par une Autorité de Certification (CA) accréditée par l'ANTIC. Cet agrément, qui est délivré à l'issue d'un audit de la CA par l'ANTIC, permet de vérifier que la PC appliquée par la CA répond bien au niveau de sécurité et de qualité de service souhaité par le MINPOSTEL.

Le MINPOSTEL devrait mettre à la disposition des prestataires de certification du Cameroun une Politique de Certification «de référence» qui définit les minima et les maxima à respecter.

Actuellement, il n'y a que l'Autorité de Certification Gouvernementale qui est référencée

dans le secteur public et aucune dans le secteur privé.

CONCLUSION GENERALE

Dans un avenir proche, l'usage de la technologie PKI dans les échanges est appelé à s'intensifier du fait notamment de sa robustesse, de sa fiabilité et de son organisation. Tout organisme sérieux, utilisant des réseaux intranet/Iternet aujourd'hui devrait disposer d'un prestataire de cryptographie. La question sera combien cela va-t-il me coûter pour décider finalement s'il conviendrait de mettre en place une autorité de certification et donc de prendre des dispositions nécessaires pour ce faire, ou sécuriser ses applications par une autorité de certification déjà accréditée et en qui l'on porte sa confiance.

Dans le présent document, nous avons voulu démontrer que la technologie des systèmes PKI permet de gérer la sécurité dans les grands réseaux Intranet et surtout permet la réalisation des échanges électroniques sécurisés sur Internet :

- Elle permet à un utilisateur, grâce à son certificat, de réaliser des échanges sécurisés avec un grand nombre de serveurs sans que ceux-ci aient besoin de connaître l'utilisateur au préalable. Seule l'Autorité d'Enregistrement aura vérifié une fois pour toute l'identité de l'utilisateur pour le compte de toute la communauté.

- Elle offre, sous la forme d'une solution de sécurité unique, une panoplie de fonctions répondant à tous les besoins de sécurité des échanges électroniques. A cet effet, elle assure les services d'authentification, de confidentialité, d'intégrité et de non-répudiation.

- Grâce à l'utilisation de standards et aux mécanismes de certification croisée, hiérarchique ou à pont. Il est possible de créer des domaines de sécurité de très grande taille sur Internet, bien que de tels domaines de sécurité soient ingérables en pratique avec des solutions traditionnelles.

- Elle permet de réaliser la dématérialisation des procédures pour moderniser les

échanges et les processus de l'entreprise dans un contexte légal approprié.

Une large utilisation des PKI paraît maintenant inéluctable. Il reste à adopter et à mettre en œuvre le planning de sécurisation des applications dans lequel la généralisation de l'utilisation des certificats sera un principe sacré.

La technologie des systèmes PKI est déjà disponible et opérationnelle dans plusieurs pays dont le Cameroun. Il est donc possible et même nécessaire dès maintenant de solliciter son utilisation dans votre plateforme.

Les enjeux liés à la mise en place de ces systèmes PKI sont multiples :

- Capacité à engager une démarche de dématérialisation progressive d'un grand nombre de procédures de votre organisme, cela vise comme objectif l'apport immédiat des gains de productivité.

- Possibilité de simplifier une partie significative de la gestion de la sécurité réalisée aujourd'hui au niveau de chaque application, tout en augmentant le niveau de sécurité pour l'authentification et la confidentialité.

- Possibilité de mieux formaliser, de rationaliser et d'homogénéiser tous les processus d'enregistrement des utilisateurs du système d'information.

Pour leurs besoins e-Business ou de commerce électronique, certaines entreprises ou communautés d'intérêt économique ont par ailleurs entamé la mise en œuvre d'infrastructures complètes, intégrant tous les services d'une PKI, et qui seront en mesure de gérer plusieurs dizaines ou plusieurs centaines de milliers de certificats. Ces projets font généralement suite à une initiative stratégique de la Direction Générale.

Il est nécessaire de s'accommoder à l'environnement sécuritaire en intégrant dans ses habitudes la nouvelle donne, celle d'utiliser les certificats dans les échanges à faire sur Internet. C'est vrai que l'on n'est jamais suffisamment sécurisé. Il est préférable de prendre des dispositions de sécurité même modestes pour son système d'information que de le laisser ouvert sans aucune restriction. L'on ne connaît la valeur de la cybersécurité que lorsqu'on est victime d'une cyberattaque.

La sécurité coûte chère, la non sécurité encore plus.

BIBLIOGRAPHIE

La sécurité des systèmes d'information : un enjeu majeur pour la France, Pierre Lasbordes, 2005, Pp 160 ;
Hacking/Security hand book, NZEKA Gilbert, pp 275;
La signature électronique dans le droit de la preuve, Preuve et signature électronique, Valérie Sédallian, mai 2000 ;
Les PKI : vers une solution globale de sécurité, Solucom, novembre 2001, pp 63 ;
Usage et gestion actuels des certificats électroniques, Chakib Bekara & Maryline Laurent Macknavicius, 2004 ;
Fonctionnement des PKI, Hervé Schauer Consultants, 1999, pp 175 ;
La sécurisation des transactions électroniques dans un réseau IP, Justin ESSIANE ELLA, pp 195, 2006 ;
Formation Sécurité des Réseaux : Support instructeur Eric BERTHOMIER, Mars 2005
Guide de la sécurité des systèmes d'information à l'usage des directeurs (2e éd) Robert Longeon et Jean-Luc Archimbaud CNRS, Paris. ISBN 2-910986-21-7 (1999), 100p.
Menace sur Internet DESTOUCHE. Édition Michalon. ISBN 2-84186-101-5
Intelligence stratégique sur Internet REVELLI. Dunod. ISBN 2-10-003621-1 (04/1998), 212 p.
Sécurité et qualité des systèmes d'information. GUINIER. Masson. ISBN 2-225-82686-2 (01/1992), 300 p.
Cyberwars espionage on the Internet. GUISNEL. Plenum. ISBN 0-306-45636-2 (08/1997), 295 p.
Cryptographie appliquée. (2e éd.). SCHNEIER. ITPS. ISBN 2-84180-036-9 (11/1996), 896 p.
Certificats, Jean-Luc Archimbaud, 22 Décembre 2000