N°=d'ordre : 10/PGS-2004/MT

République Algérienne démocratique et populaire

Université des sciences et de la technologie Houari Boumediene

Faculté des mathématiques

Mémoire de post-Graduation spécialisée en mathématiques

Spécialité : Cryptologie

Présenté par :

Monsieur : KHELLAF Hamdane

Sujet :

Gestion des clefs de chiffrement dans un processus de chiffrement en ligne

Soutenu le 24/03/2004

Devant le jury composé de:

M^r : BENTINA Kamel, professeur, USTHB	**Président**
M^r : AISSANI Amar, Professeur, USTHB	**Directeur de Mémoire**
M^r : ZITOUNI Mohamed, Professeur, USTHB	**Examinateur**
M^r : M. BENHAMIDA, DGSCT.	**Examinateur**

Sommaire

I. Introduction ----------1

II. Concepts de fond et de bases. ----------3

1. définition. ----------3
2. les objectifs de la gestion des clefs, ----------5
   menaces et politique.
3. Politique de sécurité et gestion des clefs. ----------6
4. modèles simples d'établissement des clefs. ----------6
5. La distribution Point à point et
   la gestion centralisée des clefs. ----------7
6. Les tiers de confiance. ----------9
7. Les différences parmi les protocoles ----------13
   d'établissement des clefs

III. Les techniques de distribution des clefs confidentielles. ---------15

1. Les couches de clefs et cryptoperiodes. ----------15
2. Les centres de translation des clefs (KTC)
   et les certificats des clefs symétriques. ----------18

IV. Les techniques de distribution des clefs publiques. ----------21

1. Les certificats des clefs publiques. ----------23
2. Les système basés sur l'identité. ----------27
3. Les clefs publiques Implicitement certifiées. ----------29

V. Comparaison des techniques de distribution des clefs. ----------33

VI. Les techniques pour le contrôle de l'usage des clefs. ----------40
1. La séparation des clefs et contraintes d'utilisation. ----------40
2. La séparation des clefs et la menace
de leur usage impropre. ----------40
3. Les techniques pour le contrôle
d'utilisation des clefs symétriques. ----------41
4. La distribution des certificats et révocation. ----------46
5. Révocation de certificat et
CRL (Certificate Révocation List). ----------47

VII. Le cycle de vie des clefs. ----------49
1. Les exigences de la protection
de durée de vie des clefs. ----------49
2. Les exigences de stockage de durée de vie
pour les types divers des clefs. ----------49
3. Cycle de vie de la gestion des clefs. ----------50
4. Initialisation des systèmes et installation des clefs. ----------50
5. Non répudiation et
certification de signatures digitales. ----------51
6. Dépôt des clefs de chiffrement. ----------52

VIII. L'échange des clefs. ----------56

IX. Conclusion. ----------58

I. Introduction

La gestion des clefs est un jeu de techniques destinées à contrôler, distribuer, utiliser et mettre à jour des clefs cryptographiques. Dans notre travail l'intérêt est porté sur les modèles de communications pour la classification, le contrôle basé sur leur utilisation destinée, les techniques pour la distribution des clefs publiques, les architectures de mise à jour des clefs automatisées, et le rôle des tiers de confiance. Les systèmes fournissant des services cryptographiques exigent des techniques pour l'initialisation et la distribution de clefs aussi bien que des protocoles pour la mise à jour en ligne.

Plan du mémoire

Le mémoire est organisé comme suit. Le chapitre 2 fournit les Définitions de bases, classification des clefs cryptographiques, modèles simples pour l'établissement des clefs, et une discussion sur les rôles des tiers de confiance. Le chapitre 3 considère les techniques pour la distribution des clefs confidentielles, les centres de translations des clefs, et les certificats des clefs symétriques. Le chapitre 4 récapitule les techniques pour la distribution et l'authentification des clefs publiques, et les certificats des clefs publiques, les systèmes basés sur l'identité, et les clefs publiques implicitement certifiées. Le chapitre 5 compare les techniques de distribution des clefs. Le chapitre 6

présente les techniques pour contrôler l'utilisation du matériel. Le 7eme chapitre présente le cycle de vie de gestion des clefs. Au dernier chapitre on parle de l’échange des clefs et du protocole Diffie-Hellman

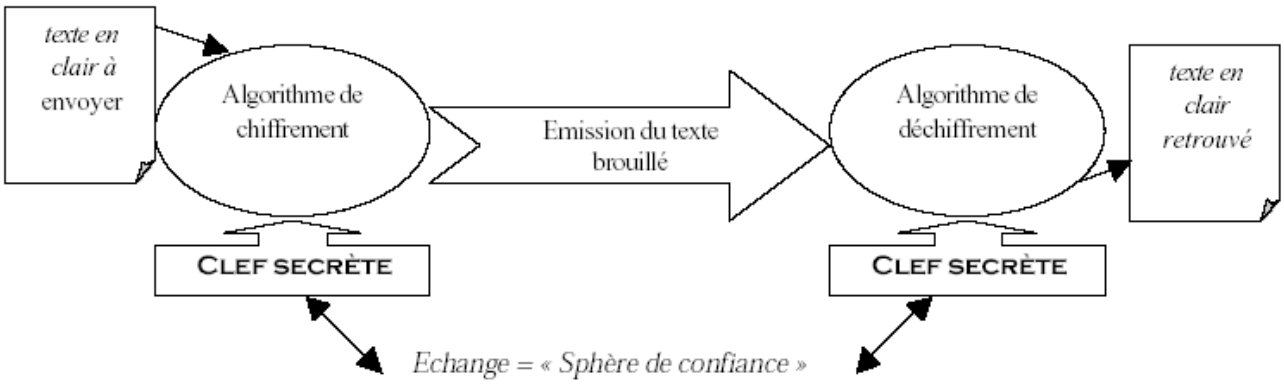
II / Concepts de bases :

Un rapport sécurisé est un état de communication où des entités partagent des données communes sans qu'une tierce personne n'ait accès à ces données. Ces données peuvent inclure des clefs publiques ou secrètes, des valeurs d'initialisation, des paramètres complémentaires non - secrets.

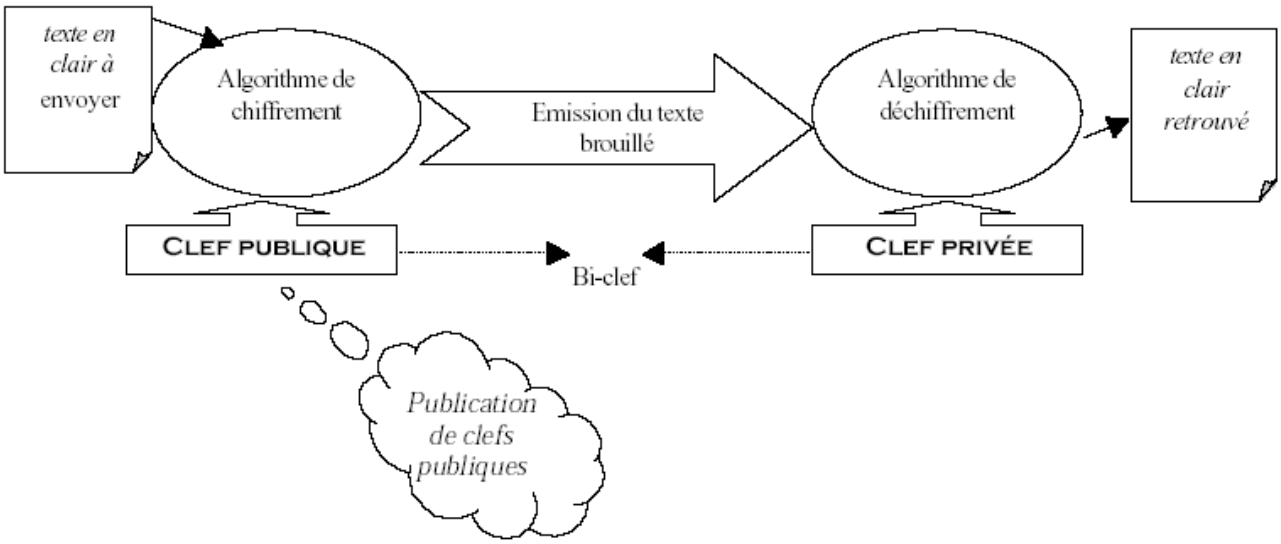
1 / Définition : La gestion des clefs est un jeu de techniques et de procédures portant sur l'établissement et le contrôle des communications sécurisées. Cette gestion des clefs englobe aussi les procédures et les techniques suivantes :

1. l'Initialisation des systèmes d'utilisateurs;
2. Conception, distribution et installation du matériel sécurisé;
3. Contrôle de l'utilisation du matériel sécurisé;
4. Mise à jour, révocation et destruction du matériel sécurisé;

a) Système cryptographique symétrique : c'est un système impliquant deux transformations, une pour l'émetteur et l'autre pour le récepteur dont tous les deux se servent de la même clef (clef symétrique) ou deux clefs facilement calculables l'une a partir de l'autre.



b) Système cryptographique asymétrique : c'est un système impliquant deux transformations liées - une définie par une clef publique (la transformation publique) et l'autre définie par une clef privée (la transformation privée) - avec la propriété qu'il est du point de vue calculatoire infaisable de déterminer la transformation privée de la transformation publique.



Objectif Cryptographique	Type d'algorithme	
	clef publique	clef symétrique
Confidentialité	Chiffrement	Chiffrement
Authentification de l'origine	Signature	MAC
Accord de clef	Diffie-Hellman	différentes méthodes
authentification d'entité	1. signature 2. déchiffrement 3. personnalisé	1. MAC 2. chiffrement

Table 2 : Type d'algorithmes utilisés pour des objectifs spécifiques.

2 / Les objectifs de la gestion des clefs, menaces et politique :

La gestion des clefs joue un rôle fondamental en cryptographie comme la base pour la garantie de la sécurité cryptographique fournissant confidentialité, authentification d'entité, authentification de l'origine des données, Intégrité des données et signatures digitales. Le but d'une bonne conception cryptographique est de réduire les problèmes les plus complexes à la gestion appropriée et la bonne garde d'un petit nombre de clefs cryptographiques, et en fin de compte il faut sécuriser le soft et le hard (applications et matériels) par un isolement physique ou commandes procédurales, (par exemple, pièces garanties (cage faraday) avec équipement isolé), Le grand nombre d'individus est réduit au minimum en concentrant la confiance sur un petit nombre d'éléments contrôlés et dignes de confiance.

La sécurisation d'un environnement de communications implique au moins deux parties (un expéditeur et un récepteur) en temps réel. Dans un environnement de stockage, il peut y avoir seulement une simple partie, qui stocke et récupère des données aux points distincts du temps.

L'objectif de la gestion des clefs est de maintenir des communications sécurisées de manière à résister aux menaces appropriées, comme :

1. Compromission de confidentialité des clefs secrètes.

2. Compromission d'authenticité des clefs secrètes ou publiques. Les exigences d'authenticité incluent la connaissance ou la vérifiabilité de la vraie identité de la partie avec la quelle une clef est associée ou partagée avec.

3. Utilisation non autorisée des clefs secrètes ou publiques. Les exemples incluent l'utilisation d'une clef qui n'est plus valable, ou pour d'autres buts.

En pratique, un objectif complémentaire est la conformité à une politique de sécurité appropriée.

3 / Politique de sécurité et gestion des clefs :

On fournit d'habitude la gestion des clefs dans le contexte d'une politique de sécurité spécifique. Une politique de sécurité définit explicitement ou implicitement les menaces auxquelles un système est destiné à faire face. La politique peut affecter la rigueur des exigences cryptographiques, selon la sensibilité de l'environnement en question aux types divers d'attaque. La politique de sécurité spécifie aussi :

1. Les pratiques et procédures a suivre comportant aspects technique et administratif, automatisé et manuel;

2. Les responsabilités et la responsabilité de chaque partie impliquée;

3. Les types de rapports (information de protocole d'audit) a tenir.

4/ Modèles simples d'établissement des clefs:

Le problème de distribution des clefs suivant a contribué à des models d'établissement de clefs plus efficaces.

a) Le problème de distribution de clefs [n^2] :

Dans un système à (n) utilisateurs impliquant les techniques à clefs symétriques, si chaque paire d'utilisateurs a besoin de communiquer secrètement, alors chaque paire doit partager une clef distincte secrète.

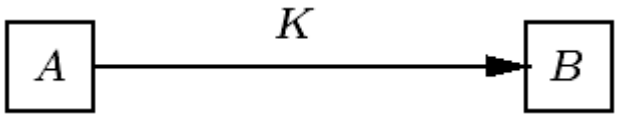
Dans ce cas, chaque partie doit avoir (n – 1) clefs secrètes; le nombre complet des clefs dans le système qui peuvent êtres sauvegardées, est alors [n (n - 1) /2], ou approximativement (n^2). Comme la taille d'un système augmente, ce nombre devient inadmissible ment grand.

Dans des systèmes basés sur les techniques a clefs symétriques, la solution est d'utiliser les serveurs de clefs centralisés : un réseau star-like ou spoked-wheel est mis au point, avec le tiers de confiance. Cela met le problème de distribution de clefs (n^2), aux dépends de l'exigence d'un serveur de confiance en ligne. Les techniques a clefs publiques offrent une solution supplémentaire.

5 / La distribution Point à point et la gestion centralisée des clefs :

1. / La distribution point a point :

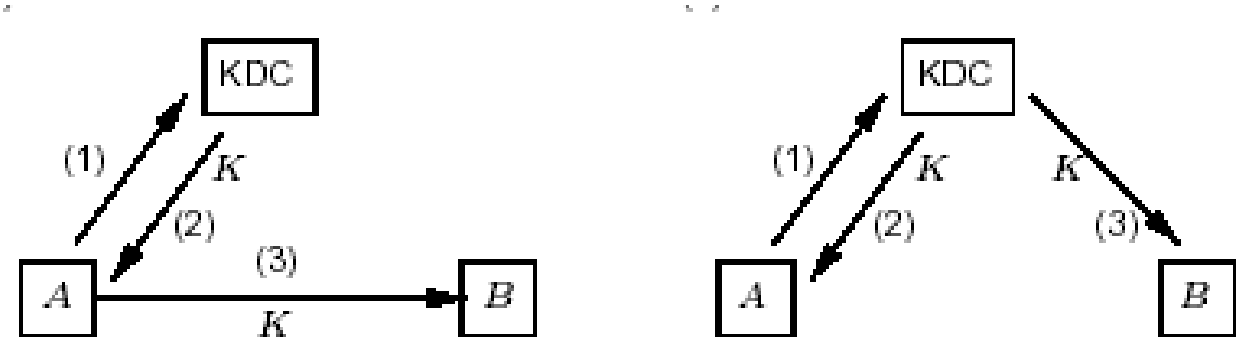
Les communications point a point et la gestion centralisée des clefs, employant les centres de distribution des clefs KDC ou les centres de translation des clefs KTC , sont les exemples simples des modèles de distribution des clefs par rapport au systèmes a clefs symétriques. Ici "simple" implique l'implication au maximum d’un tiers. Ceux-ci sont illustrés dans la figure décrite ci-dessous.



[a] Distribution de clefs point a point

2. / Les centres de distribution des clefs (KDC) :

Les KDC sont des protocoles de distribution des clefs entre des utilisateurs qui partagent des clefs distinctes avec le KDC, mais non entre eux. Un protocole de base KDC procède comme suit. À la demande de A pour le partage d'une clef avec B, le KDC *T* produit ou acquiert autrement une clef K, et l'envoie ensuite chiffrée sous K_{AT} à A, avec une copie de *K* (pour B) chiffré sous K_{BT}. Alternativement, *T* peut communiquer *K* (chiffrée sous K_{BT}) à B directement.

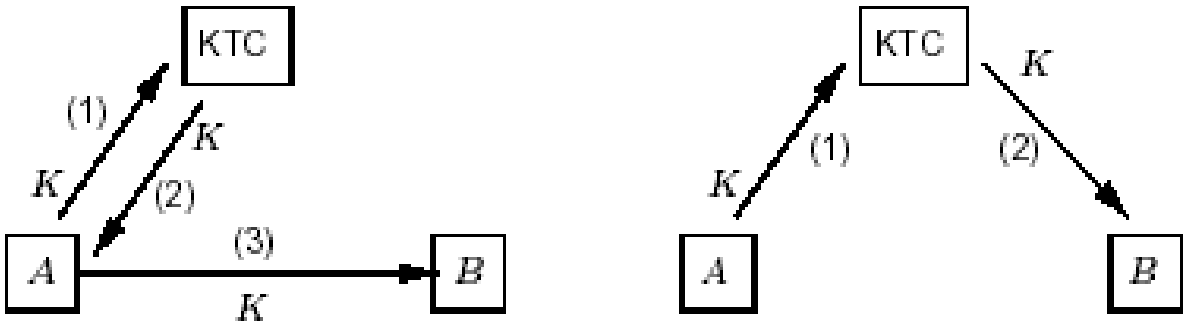


[b] Centre de distribution des clefs

3. / Les centres de translation des clefs (KTC) :

Les suppositions et les objectifs des KTC sont comme pour les KDC ci-dessus, mais ici une des parties (par exemple, A) fournit la clef de session plutôt que Le centre de confiance. Un protocole de base KTC procède comme suit. A envoi une clef *K* au KTC *T* chiffré Sous K_{AT}. Le KTC déchiffre et re-chiffre *K* sous K_{BT}, rend ensuite cela à A (pour retransmettre à B) ou l'envoie à B directement.

Les KDC fournissent la génération centralisée des clefs, tandis que les KTC permettent la génération distribuée des clefs. Tous les deux sont des techniques centralisées dans lesquelles ils impliquent un serveur de confiance en ligne.



[c] Centre de translation des clefs

Remarque : (avantages et inconvénients de la gestion centralisée des clefs) la gestion Centralisée des clefs impliquant les tierces parties (KDC ou KTC) offrent l'avantage de l'efficacité du stockage des clefs, chacune des parties a besoin de maintenir seulement une clef secrète à long terme avec le tiers de confiance.

6 / Les tiers de confiance :

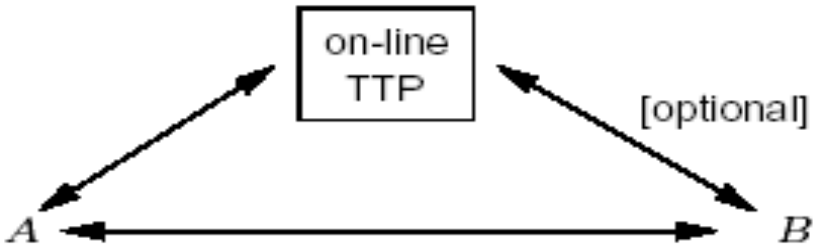
Ci-dessous, les tiers de confiance sont d'abord classifiés sur leurs interactions en temps réel avec d'autres entités. Les fonctions de gestion des clefs fournies par des tierces parties sont alors discutées.

a/ Les Tierces parties: In-Line, On-Line et Off-Line : un point de vue de communications, trois catégories de tierces parties *T* peuvent être distinguées

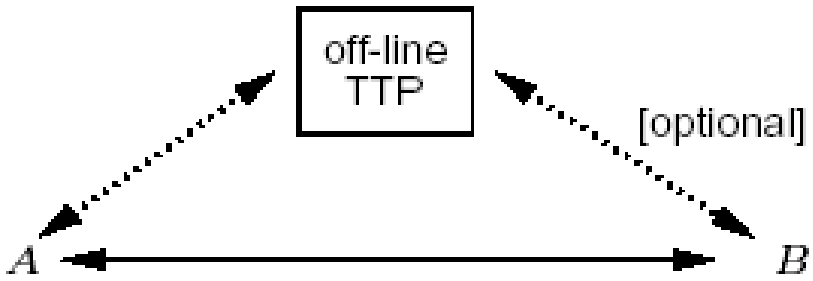
basées sur l'emplacement relatif et à l'interaction avec les parties de communication A et B

1. In-line (En vigueur) : *T* est un intermédiaire, servant comme moyen de temps réel d'une communication entre A et B.

2. On-line (En ligne) : *T* est impliqué en temps réel pendant chaque instance de protocole (communicant avec A ou B ou les deux), mais A et B communiquent directement plutôt que par *T*.



3. Off-line (En mode autonome) : *T* n'est pas impliqué dans le protocole en temps réel, mais prépare l'information a priori, qui est disponible à A ou B ou tous les deux et utilisée pendant l'exécution de protocole.



Les tierces parties en vigueur sont d'un intérêt particulier quand A et B appartiennent à des domaines de sécurité différents ou ne peuvent pas réciproquement agir directement d'une autre manière en raison des mécanismes de sécurité non-interoperable.

Les exemples d'un tiers In line (en vigueur) incluent un KDC ou un KTC qui fournit les chemins de communications entre A et B est données par les schémas ci-dessus, L'exemple du tiers Off-line (autonome) est une autorité de certification produisant des certificats des clefs publiques et leur placement dans une liste d'adresses publique (LDAP *Lightweight Directory Access Protocol*), ici, la liste d'adresses peut être un tiers en ligne, mais l'autorité de certification ne l'est pas.

Remarque : (pour et contre : On-line, In-line, Off-line) les protocoles avec les tiers autonomes [off-line] d'habitude impliquent moins d'échanges de messages en temps réel et n'exigent pas la disponibilité en temps réel des tierces parties. La révocation des privilèges (par exemple, si une clef secrète est compromise) est plus facilement traitée par des tierces parties en vigueur [in-line] ou en ligne [on-line].

b/ Les fonctions d'un tiers liées aux certificats des clefs publiques :

Les rôles potentiels joués par les tierces parties dans un système de gestion des clefs impliquant les certificats des clefs publiques sont inscrites ci-dessous. Leur rapport est illustré dans **la Figure 3**

1. Autorité de certification (CA) - responsable de l'établissement et de l'authenticité de clefs publiques.

2. nom. de serveur - responsable de gérer

3. L'autorité d'enregistrement - responsable pour autoriser des entités, distingué par des noms uniques.

4. Le générateur de clef - crée des paires de clefs publiques / privées (des clefs symétriques ou des mots de passe), Cela peut faire partie de l'entité utilisateur.

5. Liste d'adresses des certificats - une base de données de certificat ou serveur accessible par les utilisateurs. Le CA peut fournir des certificats (et entretenir) la base de données, ou les utilisateurs peuvent gérer leurs propres entrées de base de données (sous un contrôle d'accès approprié).

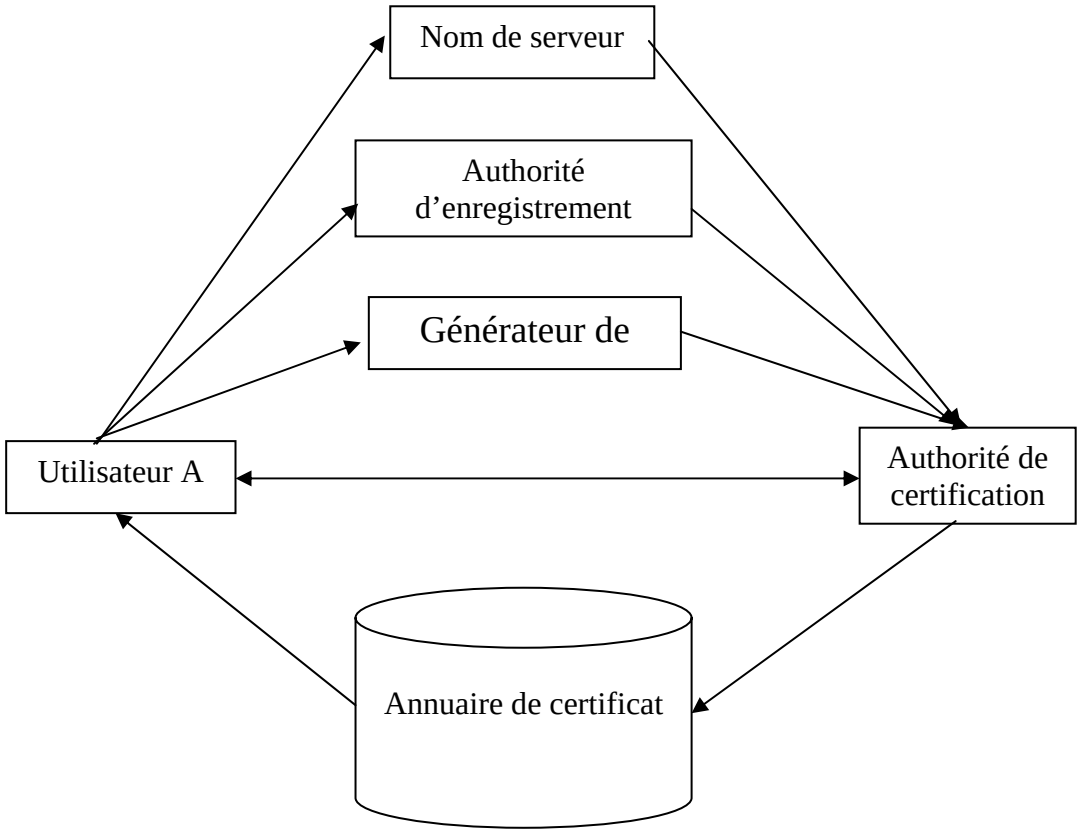


Figure 3 : les services des tiers reliés aux certification des clefs publiques.

c/ D'autres fonctions de base de tierces parties :

1. Le serveur de clef (le serveur d'identification) - facilite l'établissement des clefs entre d'autres parties.

2. La facilité de gestion des clefs - fournit quelques services incluant le stockage et archivage des clefs. Renforcement de cycle de vie, mise à jour et révocation des clefs.

7/ Les différences parmi les protocoles d'établissement des clefs :

Un nombre énorme de protocoles d'établissement des clefs est disponible. pour choisir parmi ceux-la pour une application particulière, beaucoup de facteurs à part ceux de la sécurité cryptographique peuvent être appropriés.

Dans des applications de gestion des clefs choisies, des protocoles hybrides impliquant les deux techniques symétrique et asymétrique offrent la meilleure alternative.

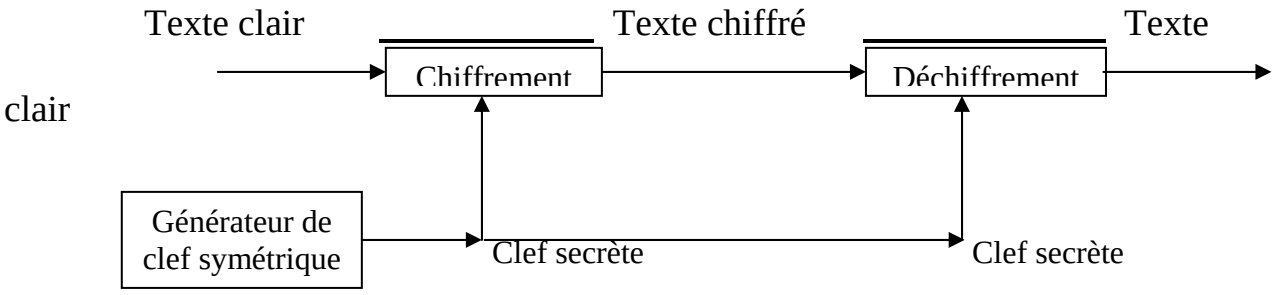
a/ Les techniques a clefs publiques contre les techniques a clefs symétriques (dans la gestion des clefs) : Avantages primaires offerts par les techniques a clefs publiques (contre les techniques a clefs symétriques) pour des applications liées a la gestion des clefs incluent :

1. La gestion des clefs simplifiée. Pour chiffrer des données pour une autre partie, seulement la clef publique de chiffrement de cette partie qui doit être obtenue. Cela simplifie la gestion des clefs seulement comme l'authenticité des clefs publiques est exigée, pas leur secret.

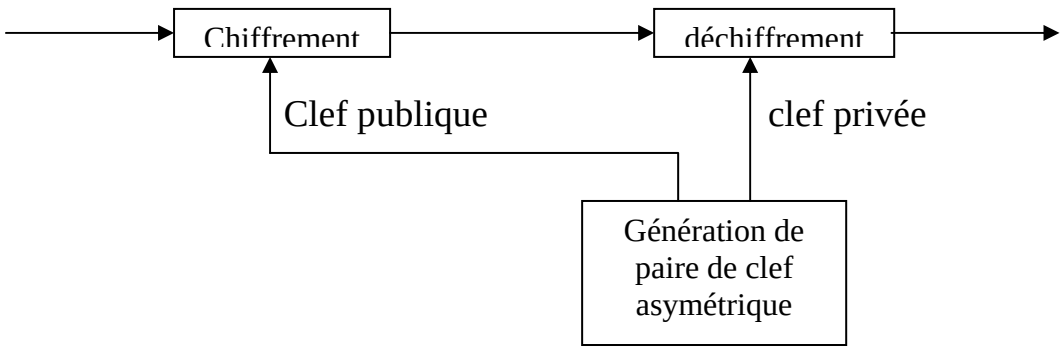
2. un Serveur en ligne de confiance n'est pas exigé. Les techniques a clefs publiques permettent a un serveur en ligne de confiance à être remplacé par un serveur de confiance off-line autonome.

3. Fonctionnalité augmentée. La cryptographie à clef publique offre des fonctionnalités qui ne peuvent pas être produites rentablement par des techniques symétriques (avec les tiers de confiance ou du matériel sûr et personnalisé).

La figure **4** compare la gestion des clefs pour le chiffrement a clefs symétrique et a clefs publique. Le canal par paires sûr dans la **figure 4 (a)** est souvent un serveur de confiance avec lequel chaque partie communique. Le canal par paires authentique dans la **figure 4 (b)** peut être remplacé par un annuaire publique sur lequel des clefs publiques sont disponibles via des certificats; la clef publique dans ce cas est typiquement employé pour chiffrer une clef de données symétrique.



[a]



[b]

4/ Gestion des clefs symétriques et publique.

III / Les techniques de distribution des clefs confidentielles :

Des techniques et des protocoles divers sont disponibles pour distribuer des clefs cryptographiques dont la confidentialité doit être préservé (et les clefs privées et les clefs symétriques). Ceux-ci incluent l'utilisation des clefs et les certificats des clefs symétriques.

1 / Couches des clefs et Cryptoperiodes :

La table 2 peut être employé pour classifier des clefs basées selon l'utilisation. La classe "confidentialité" Peut être sous-classifié à la nature de l'information étant protégée : données utilisateur contre Verrouillage de matériel. Cela suggère une schistosité naturelle clef comme suit :

1. Clefs principales (de base) - des clefs au plus haut niveau de la hiérarchie, eux-mêmes sont cryptographiquement non protégées. Elles sont distribuées manuellement ou installées au commencement et protégées par des commandes procédurales et un isolement physique ou électronique.

2. Les clefs de chiffrement de clef – Les clefs symétriques ou les clefs de publiques de chiffrement employées pour le transport de clefs ou le stockage d'autres clefs. Ceux-la aussi peuvent être appelez des clefs de transport de clefs et peuvent être elles-mêmes chiffrées sous d'autres clefs.

3. Les clefs de données - utilisées pour fournir des opérations cryptographiques sur les données utilisateur (par exemple, le chiffrement, l'authentification). Celles-ci sont généralement des clefs symétriques de court terme; cependant, la signature

des clefs privées asymétrique peut aussi être considérée comme des clefs de données, et celles-ci sont d'habitude des clefs a terme long.

Les clefs à une couche sont utilisées pour protéger des articles à un niveau inférieur. Cette contrainte est destinée à rendre les attaques plus difficiles et à limiter l'exposition résultante de la compromission d'une clef spécifique.

Note (la protection des clefs de chiffrement de clefs) la compromission d'une clef chiffrement des clefs (et de plus, une clef principale comme cas spécial) affecte toutes les clefs protégées. Par conséquent, des mesures spéciales sont employées pour protéger les clefs principales, incluant une limitation d'utilisation et d'accès, et la protection du matériel.

Exemple : (les couches des clefs avec les clefs de base et les clefs de chiffrement des clefs) chaque terminal ***X*** partage une clef de chiffrement de clefs K_X avec un noeud de confiance centrale **C**, et que **C** stocke une liste chiffrée de toutes les clefs de chiffrement des clefs sous une clef principale K_M. **C** peut fournir alors une clef de session aux terminaux ***X*** et ***Y*** comme suit. **C** obtient une valeur aléatoire ***R*** (Probablement d'une source externe) et définit la clef de session pour être $S = D_{K_M}(R)$, le déchiffrement de ***R*** sous K_M. En employant le K_M, **C** déchiffre la liste des clefs pour obtenir K_X, calcule ***S*** de ***R***, ensuite chiffre ***S*** sous K_X et le transmet à ***X***. ***S*** est analogiquement transmis à ***Y*** et peut être récupéré, et par ***X*** et par ***Y***.

a) Cryptoperiods, les clefs de long terme et les clefs de court terme :

Définition : La cryptoperiode est la période d'une clef pour laquelle la clef est valable pour l'utilisation par des parties légitimes.

La Cryptoperiodicité peut servir a :

1. Limiter l'information (lié à une clef spécifique) disponible pour la cryptanalyse;

2. Limiter l’exposition dans le cas de la compromission d'une clef simple;

3. Limiter l'utilisation d'une technologie particulière par rapport à sa durée de vie (de fonctionnement);

4. Limiter le temps disponible pour des attaques de cryptanalyse du point de vue des calcul intensifs (dans des applications ou la protection de clefs de long terme n'est pas exigée).

En plus de la hiérarchie des clefs ci-dessus, les clefs peuvent être classifiées sur des considérations temporel comme suit.

1. Clefs de long terme : Celles-ci incluent des clefs principales (de base), souvent des clefs de chiffrement des clefs.

2. Clefs de court terme. : Celles-ci incluent les clefs établies par la clef de transport, et souvent utilisées comme clefs de données ou clefs de session pour une session de communications simple.

En général, les applications de communications impliquent les clefs de court terme, tandis que les applications de stockage de données exigent des clefs de long terme.

Les clefs Diffie-Hellman sont une exception dans quelques cas. Les Cryptoperiodes limitent l'utilisation des clefs a des périodes fixées, après les quelles ils doivent être remplacés.

2 / Les centres de translation des clefs et les certificats des clefs symétriques :

De plus à la gestion des clefs centralisée discutée plus loin, cette partie prend en considération les techniques impliquant les centres de translation des clefs, incluant l'utilisation des certificats des clefs symétriques.

a) Les centres de translation des clefs :

Un centre de translation des clefs (KTC) *T* est un serveur de confiance qui permet a deux parties A et B, ne partageant pas directement le matériel de sécurité, a établir des communications sûres par l'utilisation des clefs de long terme K_{AT} et K_{BT} qu'ils partagent respectivement avec *T*. A peut envoyer un message confidentiel M à B (l'utilisation du Protocole **qui suit).** Si M est une clef *K*, cela fournit un protocole de transfert de clef; ainsi, un KTC fournit la translation des clefs ou des messages.

Protocole 1 : protocole de translation de Message en utilisant un KTC

RÉSUMÉ : A agit réciproquement avec un serveur de confiance (KTC) *T* et la partie B.

RÉSULTAT : A transfert un message secret M (ou la clef de session) à B.

1. Notation : E est un algorithme de chiffrement symétrique. M peut être une clef de session *K*.
2. A et T partagent la clef K_{AT}. De la même façon B et *T* partagent K_{BT}.

3. protocole de Messagerie

$$A \longrightarrow T : A,\ E_{KAT}(B, M) \qquad (1)$$

$$A \longleftarrow T : E_{KBT}(M, A) \qquad (2)$$

$$A \longrightarrow B : E_{KBT}(M, A) \qquad (3)$$

4. Actions du protocole.

(**a**) A chiffre M (avec l'identification du destinataire) sous K_{AT}, et l'envoie à *T* avec son propre identificateur (pour permettre à *T* de chercher K_{AT}).

(**b**) En déchiffrant le message, *T* défini ce qui est destiné pour B, cherche la clef (K_{BT}) du destinataire indiqué et re-chiffre M pour B.

(**c**) T rend le message transmis pour A pour l'envoyer a (ou le poster dans un site publique pour) B; alternativement, *T* peut envoyer la réponse à B directement.

Seulement A ou B ont besoin de communiquer avec *T*. Comme une alternative au protocole comme cité, A peut envoyer le premier message à B directement, que B retransmettrait alors à *T* pour la translation, avec *T* répondant directement à B.

b) Les certificats des clefs symétriques :

Les certificats des clefs symétriques fournissent le moyen pour un KTC pour éviter l'exigence du maintien d'une base de données de secrets d'utilisateur sûre (ou faisant un double d'une telle base de données pour des serveurs multiple).

Comme auparavant, associé à chaque partie, B est un clef K_{BT} partagé avec *T*, qui est maintenant incorporé dans un certificat de clef symétrique E_{KT} (K_{BT}; B) chiffré sous une clef principale (de base) symétrique K_T connu seulement à *T*. (un

paramètre de durée de vie (de fonctionnement), L pourrait aussi être inclus dans le certificat comme une période de validité.) le certificat sert comme note de *T* à lui-même (qui seul peut s'ouvrir) est donné à B, pour que B puisse par la suite le présenter à *T* précisément quand il est nécessaire d'accéder à la clef symétrique de B qui est K_{BT} pour la translation de message. Plutôt que de stocker toutes les clefs d'utilisateur, *T* n'a maintenant besoin que de sauvegarder K_T.

Les certificats des clefs symétriques peuvent être utilisées dans le Protocole suivant**,** en changeant seulement le premier message comme ci-dessous,

Où $SCert_A = E_{KT}(K_{AT}; A)$, $SCert_B = E_{KT}(K_{BT}; B)$:

$$A \longrightarrow T : SCertA, E_{KAT}(B; M); SCertB \qquad (1)$$

Une base de données publique peut être établie avec une entrée spécifiant le nom de chaque utilisateur et son certificat de clef symétrique correspondant. Pour construire le message (1), A récupère le certificat de clef symétrique de B et inclut avec cela son propre certificat. *T* effectue la translation comme auparavant, recouvrant K_{AT} et K_{BT} de ces certificats.

IV / Les techniques de distribution des clefs publiques :

Les protocoles impliquant la cryptographie a clef publique sont typiquement décrits, supposant a priori la possession des clefs publiques de parties appropriées. Cela permet l'acquisition de telles clefs.

Des alternatives pour la distribution des clefs publiques explicites avec authenticité vérifiable, incluant les clefs Diffie-Hellman sont citées :

1. La distribution point a point sur un canal sécurisé (sur) : Les clefs publiques authentique d'autres utilisateurs sont obtenues directement de l'utilisateur associé par l'échange personnel, ou sur un canal direct, provenant à cet utilisateur, et qui garantit par des procédures l'intégrité et l'authenticité. Cette méthode est appropriée si elle est employée rarement, ou dans de petits systèmes fermés.

2. La méthode la plus appropriée est d'échanger des clefs publiques et les informations associées sur un canal électronique non sur et fournit l'authentification de cette information en communiquant un HASH (utilisant une fonction de hachage) via un canal indépendant a largeur de bande étroite.

Les inconvénients de cette méthode incluent : le besoin d'acquisition non automatisée de clef avant la garantie des communications avec chaque nouvelle partie (Timing chronologique); et le coût du canal sur.

3. Accès direct à un fichier de confiance publique (enregistrement de clef publique) : Une base de données publique, l'intégrité en qui nous faisant confiance, peut être faite pour contenir le nom et la clef publique authentique de

chaque utilisateur de système. Cela peut être mis en oeuvre comme un enregistrement de clef publique opéré par une partie de confiance. Les utilisateurs acquièrent des clefs directement de cet enregistrement.

4. Utilisation d'un serveur de confiance on-line. Un serveur en ligne de confiance fournit l'accès à un fichier publique stockant des clefs publiques authentiques. dans les transmissions signées, la confidentialité des clefs publiques n'est pas exigée. La partie requerrante possède une copie de la signature d'authenticité des clefs publiques, permettant ainsi la vérification de chaque transmission.

5. Utilisation d'un serveur off line (autonome) et de certificats : Dans un processus ancien, chaque partie A contacte une partie autonome de confiance a mentionné comme une autorité de certification (CA).

Pour enregistrer sa clef publique et obtenir la signature de vérification de la clef publique du (CA) (permettant la vérification des certificats d'autres utilisateurs), Le CA certifie la clef publique de A en la liant à une chaîne Identifiant A, créant ainsi un certificat**.**

Les parties obtiennent des clefs publiques authentiques en échangeant les certificats ou en les ex tractant d'une liste d'adresses publique (**LDAP**).

6. Utilisation des systèmes garantissant implicitement l'authenticité des paramètres publiques : Dans de tels systèmes, incluant les systèmes basés sur l'identité et ceux utilisant implicitement des clefs certifiées, selon les conceptions algorithmiques, modification des résultats des paramètres publiques, l'échec non compromettant des techniques cryptographiques.

Les sections suivantes discutent les susdites techniques dans le plus grand détail. Figure 7 au chapitre 5 fournit une comparaison de l'approche basée sur les certificats, les systèmes basés sur l'identité, et l'utilisation des clefs publiques implicitement certifiées.

1 / Les certificats des clefs publiques :

Les certificats des clefs publiques sont un moyen par lequel des clefs publiques peuvent être stockées, distribuées ou expédiées sur des médias.

L'objectif est de rendre la clef publique d'une entité disponible à d'autres, tel que son authenticité (c'est-à-dire, son statut comme la vraie clef publique de cette entité) et la validité est vérifiable.

Définition :

Un certificat de clef publique : est une structure de données se composant d'une partie données et d'une partie signature. La partie données contient les données texte-clair incluant, comme un minimum, une clef publique et une chaîne identifiant la partie (l'entité sujette) pour être associé avec celle-la. La partie signature se compose de la signature digitale d'une autorité de certification sur la partie donnée, ainsi attacher l'identité de l'entité sujette à la clef publique indiquée.

L'autorité de Certification (CA) : est un tiers de confiance dont la signature sur le certificat répond a l'authenticité de la clef publique attachée à l'entité sujette. La signification de cet attachement (par exemple, en quoi la clef peut être utilisée) doit être fournie par des moyens complémentaires.

Dans le certificat, La chaîne qui identifie l'entité soumise doit être un nom unique dans le système (un nom distingué), que le CA associe typiquement avec une entité réelle. Le CA exige sa propre signature de paire de clef, dont la clef publique authentique est disponible à chaque partie en s'inscrivant comme un utilisateur autorisé du système. Cette autorité de certification de clef publique permet à n'importe quel utilisateur de système, a travers l'acquisition et vérification de certificat, pour acquérir transitivement la confiance en l'authenticité de la clef publique dans n'importe quel certificat signé par cette CA.

Des exemples d'information complémentaire que la partie donnée d'un certificat pourrait contenir inclut :

1. Une période de validité de la clef publique;
2. Un numéro de série ou identificateur de clef identifiant le certificat ou la clef;
3. Information complémentaire sur l'entité soumise (par exemple, rue ou adresse de réseau);
4. Information complémentaire sur la clef (par exemple, algorithme et utilisation destinée);
5. Mesures de qualité liée à l'identification de l'entité soumise, la génération de la paire de clef ;
6. Information facilitant la vérification de la signature (par exemple, une signature d'algorithme);
7. Le statut de la clef de publique (certificats de révocation) ;

a) Création des certificats des clefs publiques :

Avant la création d'un certificat de clef publique pour une entité soumise A, l'autorité de certification doit prendre des mesures appropriées (quant au niveau de sécurité exigé, et les procédures de gestion usuelles), pour vérifier l'identité revendiquée de A et le fait que la clef publique à être certifiée est en réalité celle de A. Deux cas peuvent être distingués.

Cas 1 : la partie de confiance créée la paire de clef. Elle l'assigne à une entité spécifique et inclut la clef publique et l'identité de cette entité dans le certificat. L'entité obtient une copie de la clef privée correspondante sur un canal (authentique et privé) sure après avoir prouver son identité (par exemple, en montrant un passeport). Toutes les parties employant par la suite ce certificat délèguent essentiellement confiance à cette vérification antérieure d'identité par la partie de confiance.

Cas 2 : l'entité créée sa propre paire de clefs, et transfère secrètement la clef publique à la partie de confiance avec une façon qui préserve l'authenticité (Par exemple, sur un canal sure). Sur vérification de l'authenticité (la source) de la clef publique, la partie de confiance crée le certificat de la clef publique comme ci-dessus.

b) Utilisation et vérification des certificats des clefs publiques :

Le processus complet par lequel une partie B emploie un certificat de clef publique pour obtenir la clef publique authentique d'une partie A, peut être récapitulée comme suit :

1. Acquérir la clef publique authentique de l'autorité de certification.

2. Obtenir une chaîne d'identification qui identifie uniquement la partie destinée A.

3. Acquérir sur quelque canal sans sécurité (par exemple d'une base de données centrale publique de certificats, ou de A directement), un certificat de clef publique correspondant à l'entité A, et étant d'accord avec la chaîne d'identification précédente.

4. (a) Vérifier la date et l'heure actuelles contre le temps de validité de la période dans le certificat, faisant confiance a une horloge locale;

(b) Vérifier la validité actuelle de la clef publique du CA;

(c) Vérifier la signature sur le certificat de A, employant la clef publique du CA;

(d) Vérifier que le certificat n'a pas été révoqué.

5. Si tous les contrôles succèdent, acceptent la clef publique dans le certificat comme la clef authentique de A.

c) Certificats d'attribut :

Les certificats des clefs publiques lient une clef publique et une identité et incluent des champs de données complémentaires nécessaire pour clarifier cette liaison, mais ne sont pas destinés pour la certification d'information complémentaire. Les certificats d'attribut sont semblables aux certificats des clefs publiques, mais spécialement dessinés pour permettre les spécifications d'information (attributs) autre que les clefs publiques (mais lié a un CA, entité, ou une clef publique), tel qu'il peut aussi être transmis avec une façon vérifiable.

Attribuer des certificats peut être associés à une clef publique spécifique en liant l'information attribuée à la clef par la méthode avec laquelle la clef est identifiée, par exemple, par le numéro de série d'un certificat de clef publique correspondant.

Les certificats d'attribut peuvent être signés par une autorité de certification d'attribut, créés en conjonction avec une autorité d'enregistrement d'attribut et distribué en conjonction avec un service de renseignements d'attribue**.** Plus généralement, n'importe quelle partie avec une clef de signature et l'autorité appropriée reconnaissable peut créer un certificat d'attribut. Une demande doit certifier l'information d'autorisation liée à une clef publique. Plus spécifiquement, cela peut être utilisé, par exemple, limiter la responsabilité résultante d'une signature digitale, ou contraindre l'utilisation d'une clef publique (par exemple, aux transactions de valeurs limitées, certains types, ou pendant certain Heures).

2/ Les systèmes basés sur l'identité :

Les systèmes basés sur l'identité ressemblent aux systèmes ordinaires a clefs publique, impliquant une transformation privée et une transformation publique, mais des utilisateurs n'ont pas de clefs publiques explicites comme auparavant. Au lieu de cela, la clef publique est effectivement remplacée par l'information d'identité de l'utilisateur publiquement disponible (par exemple, nom du réseau ou l'adresse de la rue). Chaque Information publiquement disponible qui identifie uniquement un utilisateur et peut être indéniablement associé à l'utilisateur, peut servir comme l'information d'identité.

Définition : Un système cryptographique basé sur l'identité est un système asymétrique où l'information d'identification publique d'une entité (nom unique) joue le rôle de sa clef publique et est employé comme entrée par une autorité de confiance T (avec la clef privée de T) pour calculer la clef privée correspondante de l'entité. Après le calcul, T transfère la clef privée de l'entité à l'entité sur un canal sûr (authentique et privé). Cette clef privée est calculée non seulement de l'information de l'identité de l'entité, mais doit aussi être une fonction de quelques informations privilégiées connues seulement à T (clef privée de T). C'est nécessaire de prévenir la contrefaçon et l'imitation, c'est essentiel que seul T soit capable de créer des clefs privées valables correspondant à l'information d'identification de données.

Le système de données authentiques publiquement disponibles doit être incorporé dans les transformations cryptographiques du système basé sur l'identité, analogues à la clef publique de l'autorité de certification dans les systèmes basés sur le certificat**. Figure 7 (b)** illustre La conception d'un système basé sur identité.

Remarque : (l'authenticité dans les systèmes basés sur l'identité) les systèmes basés sur l'identité diffèrent des systèmes a clefs publiques en cela l'authenticité des données publiques spécifiques d'utilisateur n'est pas explicitement Vérifiée, comme il est nécessaire pour les clefs publiques d'utilisateur dans les systèmes basés sur certificat. La redondance inhérente des données publiques d'utilisateur dans les systèmes basés sur l'identité, ensemble avec l'utilisation des systèmes de données publiques authentiques, protègent implicitement la contre contrefaçon; si

des données publiques d'utilisateur incorrectes sont utilisées, les transformations cryptographique échouent facilement.

Plus spécifiquement ; la vérification de signature échoue, l'authentification d'entité Échoue, le chiffrement a clef publique résulte en texte indéchiffrable.

La motivation qu'il y'a derrière les systèmes basés sur l'identité est de créer un système cryptographique modélisant un système de courrier idéal où la connaissance du nom d'une personne a elle seule suffit pour permettre au courrier d'être envoyer et que cette seule personne peut lire, et de permettre la vérification des signatures que cette seule personne à pu produire. Dans un tel système cryptographique idéal :

1. Les utilisateurs n'ont besoin d'échanger ni les clefs symétriques, ni les clefs publiques;

2. Des répertoires publiques (les fichiers des clefs publiques ou de certificats) n'ont pas besoin d'être tenus; et

3. Les services d'une autorité de confiance sont nécessaires seulement pendant une phase d'installation (pendant la quelle les utilisateurs acquièrent des paramètres de système publique authentique).

3/ Les clefs publiques Implicitement certifiées :

Une autre variété de systèmes a clefs publiques c'est les systèmes asymétriques avec les clefs publiques implicitement certifiées. Ici les clefs publiques explicites d'utilisateur existent, mais elles doivent être reconstruites

plutôt que de les transportées par les certificats a clefs publiques selon les systèmes basés sur certificat.

Pour d'autres avantages, voir la **Remarque 4**. Les systèmes avec des clefs publique implicitement certifiées sont conçus tel que :

1. Les clefs publiques des entités peuvent être reconstruites (par d'autres parties) de données publiques (qui remplace essentiellement un certificat).

2. Les données publiques dont une clef publique est reconstruite incluent :

(a) Le publique (c'est-à-dire, système) de données associées à une partie de confiance T;

(b) L'identité de l'entité d'utilisateur (ou information identifiante, par exemple, nom et adresse);

(c) Données publiques complémentaires par utilisateur (données publiques de reconstruction).

3. L'intégrité d'une clef publique reconstruite n'est pas directement vérifiable, mais une clef publique correcte peut être récupérée seulement de données publiques d'utilisateur authentiques.

Quant à l'authenticité des clefs publique reconstruites, la conception de systèmes doit garantir :

1. Le changement ou bien de l'identité d'un utilisateur ou bien des données publique de reconstruction aboutit au rétablissement d'une clef publique corrompue, que cause le démenti de service, mais non l’exposition cryptographique.

2. Du point de vue calculatoire c'est infaisable pour un adversaire (sans la connaissance des données privées de T) pour calculer une clef privée correspondante à la clef publique de n'importe quelle partie, ou construire une identité d'utilisateur correspondante et reconstruction de données publique pour lequel une clef privée peut aussi être calculer. Des clefs publiques reconstruites sont ainsi implicitement authentifiées par construction.

Remarque 4: (les applications des clefs implicitement certifiées) les clefs publiques Implicitement certifiées peuvent être employées comme un moyen de remplacement pour la distribution des clefs publiques (par exemple, les clefs Diffie-Hellman) dans les divers protocoles d'accord des clefs, ou en conjonction avec les protocoles d'identification, les plans de signatures digitales, et les plans de chiffrement a clefs publiques.

Les classes des clefs publiques implicitement certifiées :

Deux classes de clefs publiques implicitement certifiées peuvent être distinguées :

1. Clefs publiques basées sur l'identité (Classe 1). La clef privée de chaque entité A est calculée par une partie de confiance T, basé sur l'information d'identification de A et la clef privée de T; c'est aussi une fonction de données publiques de reconstruction spécifiques d'un utilisateur A, qui sont fixées a priori par T. La clef privée de A est alors secrètement transférée par T à A.

2. Clefs publiques auto certifiées (Classe 2). Chaque entité A calcule elle-même sa clef privée et sa clef publique correspondante. Les données publiques de

reconstruction de A sont calculées par T comme une fonction de clef de publique (transféré à T par A), L'information d'identification de A et la clef privée de T.

La classe 1 exige plus de confiance en tiers, qui a l'accès aux clefs privées des utilisateurs. Cela diffère de la Classe 2, comme souligné par le terme "self" dans "self-certifié", qui se réfère à la connaissance de cette clef étant limitée à l'entité elle-même.

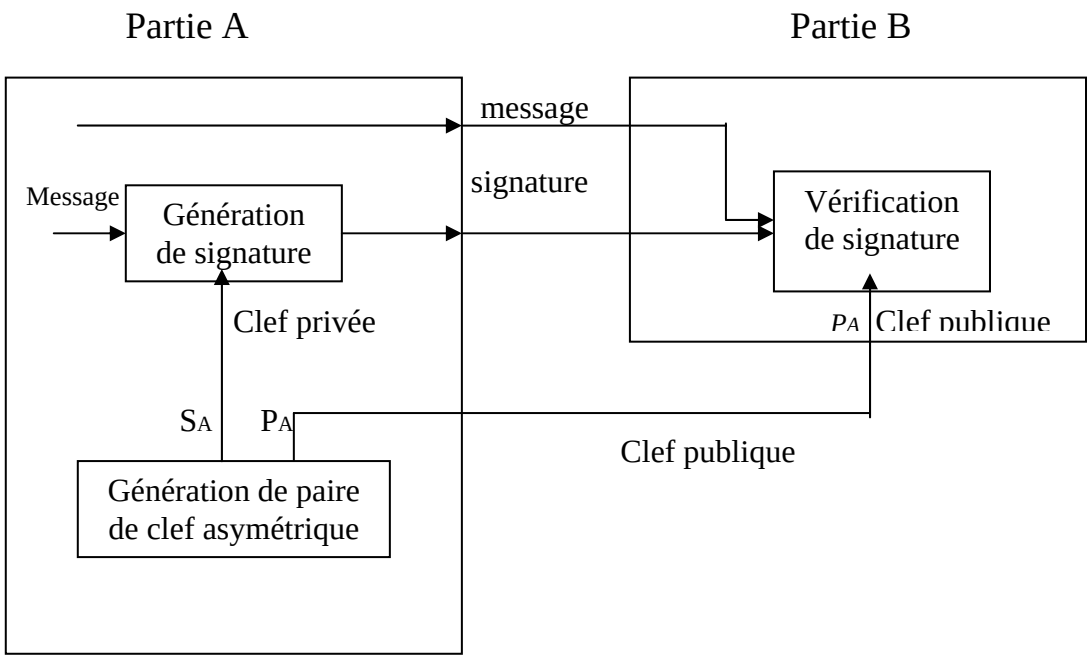
V / Comparaison des techniques de distribution de clefs :

La figure 7 illustre les classes correspondantes des systèmes de signature asymétriques, l'opposition des systèmes a clefs publiques (avec des clefs publiques explicites), les systèmes basés sur l'identité (la clef publique est a l'information d'identité de l'utilisateur) et les systèmes avec des clefs publiques implicitement certifiées (une clef publique explicite est reconstruite des données publiques d'utilisateur). Les différences principales sont comme suit :

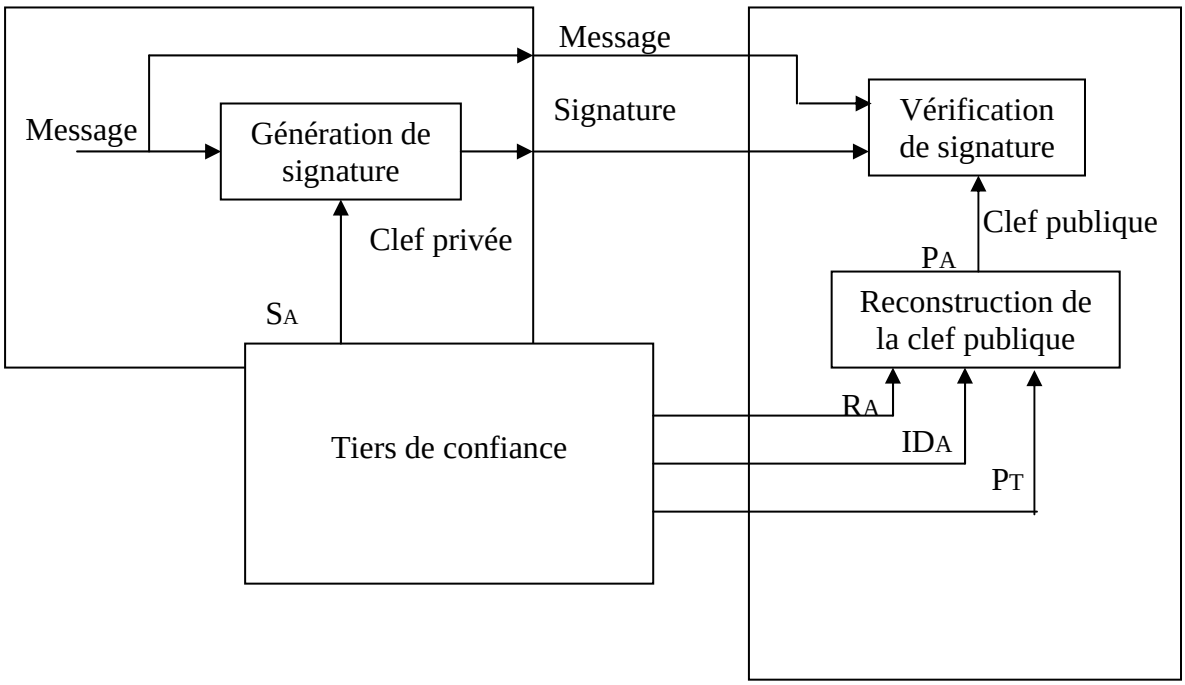
1. Les systèmes à clefs publiques basés sur certificat ont des clefs publiques explicites, tandis que les systèmes basés sur l'identité ne le sont pas; dans les systèmes implicitement certifiés des clefs publiques explicites sont reconstruites.

La clef publique explicite dans les systèmes a clefs publique (Figurent 7 (a)) est remplacé par :

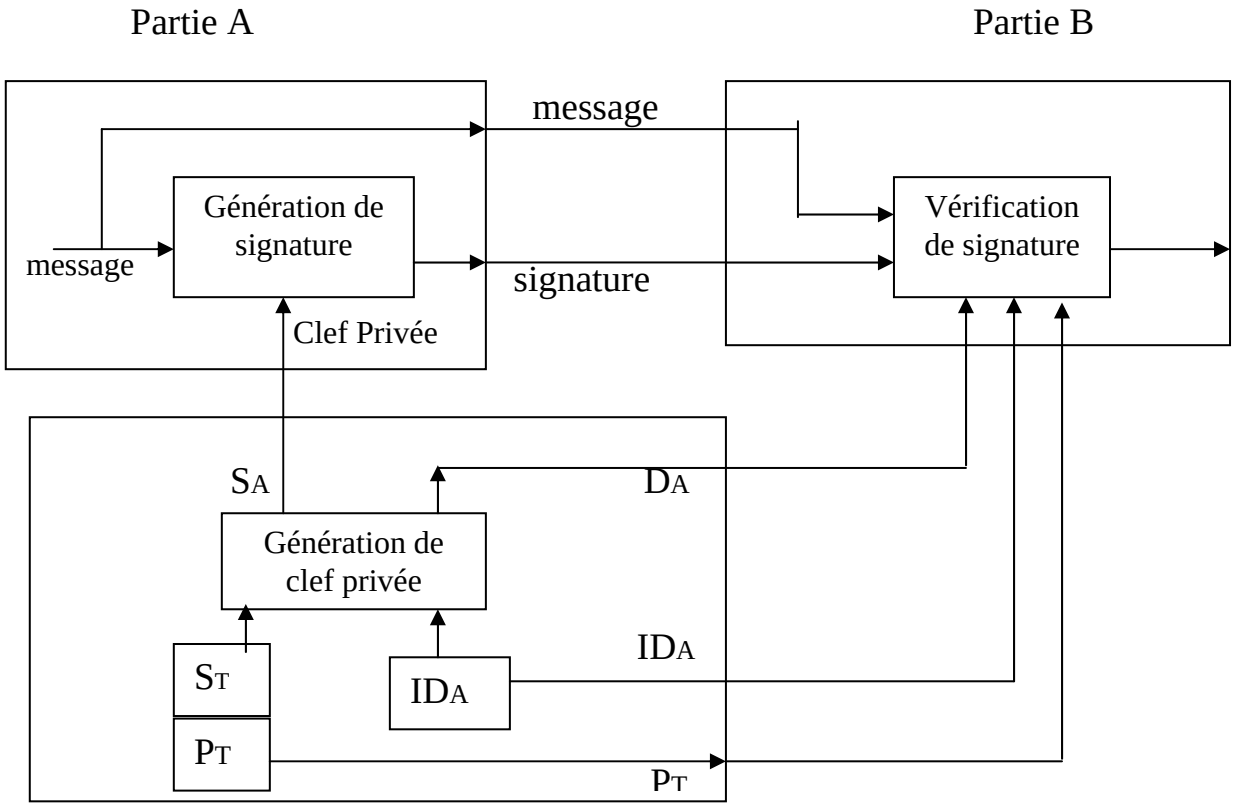
(a) Le triplet (D_A; ID_A; P_T) pour les systèmes basés sur l'identité (Figure 7 (b)). ID_A est une chaîne d'identification pour A, D_A est une donnée publiques complémentaire (définie par T et liée a ID_A et la clef privée de A) et P_T consiste en la clef publique de confiance (ou Paramètres de système) d'une autorité de confiance T.



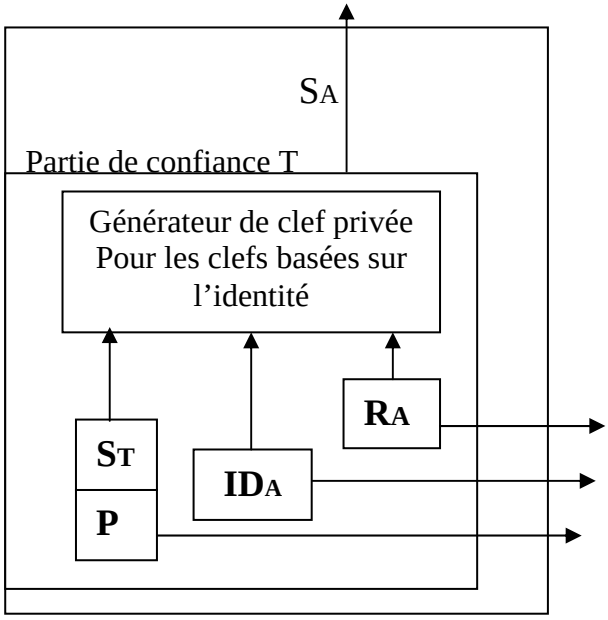
7 [a] Systéme a clefs publiques.



7(b) Systeme basé sur l'identité.



[c] Systeme a clefs publiques implicitement certifiées.



ST, PT : les clefs privée et publique de T.

[d] Clefs publiques basées sur l'identité.

Figure 7 : La gestion des clefs dans ces différentes classes des systèmes a signatures asymétriques.

b) Le triplet (R_A; ID_A; P_T) pour les systèmes avec des clefs publiques implicitement certifiées (Figure 7 (C). Dans ce cas, une clef publique explicite P_A est reconstruite de ces paramètres. Les données publique de reconstruction R_A jouent un rôle analogue aux données publiques D_A dans Figure 7 (b).

2. L'authenticité des clefs publiques peut (et doit) être explicitement vérifiée dans les systèmes basés sur certificats, mais pas dans les systèmes basés sur l'identité ou implicitement certifiés.

3. L'autorité de confiance n'a pas besoin de connaître les clefs privées des utilisateurs dans les systèmes a clefs publiques basés sur certificats ou systèmes implicitement certifiés avec des clefs publiques certifiées par soi-même; mais le contraire dans les systèmes basés sur l'identité et dans les systèmes implicitement certifiés avec des clefs basées sur l'identité.

4. C'est semblable aux systèmes basés sur l'identité, les clefs publiques implicitement certifiées (des deux classes) dépendent de l'information d'identification d'une entité et dans ce sens sont aussi "Basé sur l'identité". Cependant, les systèmes basés sur l'identité évitent entièrement les clefs publiques explicites, tandis que les clefs publiques implicitement certifiées ne sont pas limitées aux identités d'utilisateur et peuvent être explicitement calculées (et ainsi plus facilement employées en conjonction avec des arrangements ordinaires des clefs publiques).

5. Les deux classes de clefs publiques implicitement certifiées (**Figurent 7 (c**)) diffèrent dans leur rapport entre les reconstructions des données publiques d'utilisateurs et les clefs privées comme suit :

(a) Classe 1 : la clef privée d'un utilisateur est calculée comme une fonction de reconstruction de données et cette clef privée est calculée par l'autorité de confiance;

(b) Classe 2 : la donnée de reconstruction est calculée comme une fonction de la clef publique de l'utilisateur et la clef correspondante privée est calculée par la partie elle-même.

6. Dans les trois approches, à quelques étapes, le tiers en qui on a confiance à quelque niveau est exiger pour fournir une liaison transférant la confiance entre utilisateurs qui pourront ne jamais se rencontré et ne pourront partager rien de commun autre que le système des paramètres authentiques (et probablement la connaissance des identités d'autres utilisateurs).

Remarque : (la révocation des clefs dans les systèmes basés sur l'identité) la révocation des clefs publiques peut être adressée dans les arrangements basés sur l'identité et les systèmes employant des clefs publiques implicitement certifiées en fusionnant une information comme la validité de la période d'une clef ou le numéro de série dans la chaîne d'identification employée pour calculer la clef publique d'une entité. La question de révocation est alors analogue comme pour les certificats a clefs publiques.

VI / Les techniques pour le contrôle de l’usage des clefs :

Cette partie prend en compte les techniques pour la limitation de l’utilisations pré autorisées des clefs.

1 / La séparation des clefs et contraintes d'utilisation :

L'information qui peut être associée aux clefs cryptographiques inclut les deux attributs qui limitent leur utilisation et d'autres informations d'utilisation opérationnelle. Ceux-ci incluent :

1. Le propriétaire de la clef.
2. La validité de la période (cryptoperiodes).
3. l’identificateur de la clef.
4. L'utilisation destinée (**Table 2)**.
5. Algorithme spécifique.
6. Système ou environnement d'utilisation destiné, ou les utilisateurs autorisés des clefs.

2 /La séparation des clefs et la menace de leur usage impropre :

Dans les systèmes de gestion des clefs simples, les informations associées aux clefs, incluant les utilisations autorisées, sont déduites par le contexte. Pour plus de clarté ou de contrôle, l’information spécifiant les utilisations explicitement permises peut accompagner des clefs distribuées à être mise en application par la vérification, au moment de l’utilisation.

Le principe de ‘séparation des clefs’ est que les clefs pour des buts différents doivent être crypto graphiquement séparées. La menace d'usage impropre des clefs

peut être dressée par des techniques qui assurent que les clefs sont employées seulement pour ces buts pré autorisés au moment de la création des clefs.

Les restrictions sur l'utilisation des clefs peuvent être mises en application par des techniques procédurales (protection physique), ou des techniques cryptographiques.

Remarque : (des raisons cryptographiques pour la séparation des clefs) un principe d’une bonne conception cryptographique est qu’on doit éviter l'utilisation de la même clef cryptographique pour des buts multiples. Une clef de chiffrement de clef ne doit pas être employée de façon interchangeable (OTK) comme une cléf de chiffrement de données.

Le chiffrement asymétrique distinct et la signature des clefs sont généralement employés, en raison de leurs différentes exigences du cycle de vie et la prudence cryptographique. Les défauts surgissent potentiellement si :

Des clefs asymétriques sont employées pour la signatures et l'authentification d'entité de réponse; les clefs sont employées, et pour le chiffrement et pour l'authentification d'entité de réponse; des clefs symétriques sont employées, et pour le chiffrement et pour l’authentification de message.

3/ Les techniques pour le contrôle d'utilisation des clefs symétriques :

La technique principale discutée ci-dessous est l'utilisation des vecteurs de contrôle. L’étiquette des clefs / variantes des clefs et la certification des clefs sont aussi discutées.

(a) Étiquettes des clefs et variantes des clefs :

Les étiquettes des clefs fournissent une méthode simplifiée pour la spécification des utilisations permises des clefs.

Une étiquette de clef est un vecteur bit ou un champ structuré qui l’accompagne et reste associé à une clef sur toute sa durée de vie (de fonctionnement).

Les bits d'étiquette sont chiffrés conjointement avec la clef et ainsi rattaché à elle, apparaissant en forme de texte claire seulement quand la clef est décryptée. Si la combinaison des bits d'étiquette et la clef est suffisamment courte pour permettre le chiffrement dans une opération de bloc simple (par exemple, une clef à 56 bits avec une étiquette à 8 bits pour un bloc à 64 bits), alors l'intégrité inhérente fournie par le chiffrement empêche la manipulation significative de l'étiquette.

Une méthode naïve fournissant la séparation des clefs est de dériver des clefs séparées d'une simple base de clef utilisant des paramètres complémentaires non-secrets et une fonction non-secrète. Les clefs résultantes sont appelées des variantes clefs ou des clefs dérivées.

Une technique pour les clefs variables est les clefs contrebalancées, par laquelle une clef de chiffrement de clef K est modifiée sur une base se lisant attentivement par un compteur N incrémenté après chaque utilisation. Cela peut empêcher la réutilisation des clefs chiffrées. La clef modifiée $K + N$ est employée pour chiffrer une autre clef. Le destinataire modifie de même K pour décrypter la clef de session.

Exemple : Supposons exactement trois classes de clefs. Construisez des clefs en employant des variations K_1 et K_2 d'une clef principale K, avec $K1 = K + v1$, et $K2 = K + v2$, et $v1$, $v2$ les valeurs non secrètes d'un masque. En employant K, $K1$ et $K2$ pour chiffrer d'autres clefs permettent alors la séparation des clefs dans les trois classes. Si le processus de dérivation est réversible, la clef de base peut être récupéré de la clef dérivée. Idéalement, la technique de dérivation est non-réversible (à sens unique), impliquant la compromission d'une clef dérivée ne compromettraient pas la clef de base ou d'autres clefs dérivées. Encore un autre exemple de dérivation des clefs a cette propriété :

calculer $Ki = E_K (ri)$, où ri est un nombre aléatoire, on remplace la fonction de chiffrement E par un MAC, ou simplement hacher K et ri en utilisant une fonction de hachage h avec des propriétés appropriées.

(b) La certification des clefs :

La certification de clef est une technique destinée à empêcher la substitution des clefs en exigeant des spécifications explicites des identités des parties impliquées dans la sécurité d'une communication. Une clef est authentifiée avec respect à ces identités (prévention de l'usurpation d'identité) en modifiant une clef de chiffrement de clef tel qu'une identité correcte doit être spécifiée pour récupérer proprement la clef protégée. On dit que la clef est scellée avec ces identités.

Prévenir la substitution de clef est une exigence dans tous les protocoles d'établissement des clefs. La certification exige l'information de contrôle appropriée pour le rétablissement précis des clefs chiffrées, fournissant la protection implicite et analogue aux clefs publiques implicitement certifiées.

La technique de base (la certification simple de clef) implique un serveur de confiance, ou l'une des partie partageant la clef, employant une clef de chiffrement de clef, *K* pour chiffrer une clef de session *S*, destiné pour une utilisation avec la partie émettrice *i* et le destinataire *j*, comme : $E_{K + (i//j)} (S)$. Ici *i* et *J* sont assumés pour identifier des entités uniques dans le système donné.

Exemple : **S**oient *E* un chiffrement en bloc fonctionnant sur des blocs de 64 bits avec une clef à 64 bits, et $K = K_L // K_R$ une clef à 128 bits chiffrant une clef, *N* un compteur à 64 bits, et $i = i_L // i_R$, $j = j_L // j_R$ identificateurs de la source et de la destination à 128 bits. Pour la certification des clefs, on calcule :

$K_1 = E_{KR} + i_L(j_R) + K_L+N$; $K_2 = E_{KL} + j_L (i_R) + K_R + N$. La clef certifiée résultante à 128 bits (*K1; K2*) sert alors comme une clef chiffrant une autre, le résultat en quantités et analogue alors à celui employés dans la certification de clef simple (c'est-à-dire, fonctions de *K, i, j*). Pour *K* une clef (de longueur simple) à 64 bits, le processus est modifiée comme suit : Utilisant *KL = KR = K*, on calcule le cachet f1 (*KR; je; j*), f2 (*KL; i; j*) comme ci-dessus, enchaîner les 32 bits a l'extrêmes gauches de f1 avec l'extrême droit de f2 pour obtenir f, calculent ensuite *f + K + N* comme la clef certifiée

.

(c) Vecteurs de contrôle : Tandis que la certification des clefs peut être vue comme un mécanisme pour l'établissement des clefs authentifiées, Les vecteurs de contrôle fournissent une méthode pour contrôler l'utilisation des clefs, en combinant l'idée d'étiquette des

clefs avec le mécanisme de certification de clef simple. Associé à chaque clef *S*, un vecteur de contrôle *C*, qui est un champ de données (semblable à une étiquette de clef) définissant les utilisations autorisées de la clef.

Le décryptement des clefs exige ainsi que le vecteur de contrôle soit correctement spécifié, aussi bien que la clef de chiffrement de clef; si la quantité combinée $K + C$ est incorrecte, une clef fausse d'aucun avantage pour un adversaire n'est récupérée. Liant crypto graphiquement le vecteur de contrôle *C* à *S* au moment de la génération de clef empêche la manipulation non autorisée de *C*, assumant seulement les parties autorisées qui ont l'accès à la clef de chiffrement de clef *K*.

Les vecteurs de contrôle peuvent englober la certification des clefs en employant un ou plus d'un champs dans *C*. Par rapport aux modèles standard pour le contrôle d'accès, le vecteur de contrôle peut être employé pour spécifier l'identité d'un sujet (*Si*) et les privilèges ($A_{i;j}$) quant à l'utilisation d'une clef (K_j).

Note : (modèles pour le contrôle d'accès) Plusieurs méthodes sont disponibles pour contrôler l'accès aux ressources. Le modèle de matrice d'accès emploi une matrice bidimensionnelle A_{ixj} avec une rangée pour chaque sujet (*Si*) et une colonne pour chaque objet (*Oj*) et dépend sur l'identification appropriée des sujets *Si*. Chaque rapport d'accès *Ai,j* spécifie les privilèges qu'a l'entité *Si* sur l'objet *Oj* (par exemple, une application devrait lire, écrire, modifie, ou exécute des privilèges sur un fichier). La colonne *J* peut alternativement servir comme une liste d'accès pour l'objet *Oj*, ayant des entrées (*Si; Pij*) où *Pij = Ai,j*.

Exemple : (les utilisations types des vecteurs de contrôle) les vecteurs de contrôle peuvent être employés pour fournir une clef publique comme fonctionnalité comme suit. Deux copies d'une clef symétrique sont distribuées, une cataloguée pour permettre le chiffrement seulement (ou la génération de MAC) et une deuxième permettant le décryptement seulement (ou la vérification MAC).

Remarque : (la vérification de clef et la prévention de la réutilisation) Réutiliser des clefs distribuées par les protocoles de transport de clef peut être reprise par les mêmes techniques utilisées pour fournir unicité et empêche la réutilisation de message.

4/ La distribution des certificats et révocation :

Une liste d'adresses de certificat est une base de données qui exécute un modèle (pull) de traction, de ce modèle les utilisateurs extraient des certificats de la base de données au besoin. Un modèle différent de la distribution de certificat, le modèle push, implique des certificats étant émise à tous les utilisateurs sur création de certificat ou périodiquement; cela peut être approprié pour des systèmes fermés.

Alternativement, des utilisateurs individuels peuvent fournir leurs certificats à d'autres quand c'est nécessaire, par exemple, pour la vérification de signature.

Dans les systèmes basés sur certificat avec listes de révocation de certificat (CRL - Voir ci-dessous), une méthode pour la distribution de CRL aussi bien que pour certificats sont exigées.

La liste d'adresses de certificat est d'habitude vue comme un tiers sans garantie. Tandis que le contrôle d'accès à la liste d'adresses en forme d'écriture et de suppression, la protection est nécessaire pour permettre la maintenance et la mise à

jour sans démenti de service, les certificats elles-mêmes sont individuellement garanties par les signatures, sur-ce, et n'ont pas besoin d'être transférées sur des canaux sures. Une exception est les certificats On line, qui sont créés par une autorité de certification en temps réel a la demande et n'ayant aucune durée de vie (de fonctionnement), ou sont distribuées par une partie de confiance qui garantit qu’elles n'ont pas été révoquées.

5/ Révocation de certificat et CRL (Certificate Révocation List) :

Sur la compromission d'une clef secrète, les dégâts peuvent être réduits au minimum en empêchant suivants l’utilisation ou la confiance au matériel associé. (Notez que les implications diffèrent entre la signature et les clefs de chiffrement.). Ici la compromission inclut n'importe quelle situation par laquelle un adversaire bénéficie de la connaissance des données secrètes. Si des clefs publiques doivent être obtenues en temps réel par un serveur de confiance On line, les clefs en question peuvent être immédiatement retirées ou remplacées. La situation impliquant des certificats est plus difficile, comme toutes les copies distribuées doivent être efficacement rétractées. Tandis que la clef compromise peut être rare, il peut y avoir d'autres raisons qu’une CA dissoudra prématurément son lien d'une clef publique à un nom d'utilisateur (c'est-à-dire, révoquer le certificat).

1. Avis manuel. Tous les utilisateurs de système sont informés de la clef révoquée par des moyens ou canaux spéciaux. Cela peut être faisable dans de petits systèmes ou des systèmes fermés.

2. Fichier publique des clefs révoquées. Un fichier publique est établi, identifiant les clefs révoquées, à être vérifiez par tous les utilisateurs avant l'utilisation des clefs.

3. Listes de révocation de certificat (CRL). Une CRL est une méthode pour gérer un fichier public de clefs révoquées.

Une CRL est une liste signée d'entrées correspondantes aux clefs publiques révoquées, avec chaque entrée indiquant le numéro de série du certificat associé, la révocation était d'abord faite, et probablement d'autres informations comme la raison de révocation. La signature de la liste, garantissant son authenticité, est produite par le CA qui a à l'origine publié les certificats. L'inclusion d'une date sur une CRL fournit une indication de sa fraîcheur. Si les CRL sont distribuées en employant un modèle de traction (pull) (par exemple, via une base de données publique), elles doivent être publiées à intervalles réguliers même s'il n'y a aucun changement, pour empêcher que de nouvelles CRL soient avec malveillance remplacées par de vielles CRL.

Les certificats mutuels Révoqués peuvent être spécifiés dans des listes de révocation d'autorité séparées (ARL), analogue au CRL (qui est alors limité aux certificats d'utilisateur final révoqués).

VII/ Le cycle de vie des clefs :

La gestion des clefs est la plus simple quand toutes les clefs cryptographiques sont fixées pour toujours. Les cryptoperiodes nécessitent la mise à jour des clefs. Cela impose des exigences complémentaires, par exemple, sur les autorités de certification qui maintiennent et mettent à jour des clefs d'utilisateurs. Le jeu d'étapes par lequel la clef progresse pendant son existence, mentionnée comme le cycle de vie des clefs, est discutée dans cette Section.

1 / Les exigences de la protection de durée de vie des clefs :

Les contrôles sont nécessaires pour protéger les clefs pendant l'usage et le stockage. Quant au stockage des clefs de longs termes, la durée de protection exigée dépend de la fonction cryptographique (par exemple ; chiffrement, signature, authentification / intégrité d'origine des données).

2 / Les exigences de stockage de durée de vie pour les types divers des clefs :

Les clefs secrètes stockées doivent être sécurisées afin de fournir, confidentialité et authenticité.

Les clefs publiques stockées doivent être sécurisées tel que leur authenticité est vérifiable. Confidentialité et authenticité garantissent, respectivement résistance aux menaces de révélation et modification, Peuvent être fourni par des techniques cryptographiques, des techniques procédurales (basées sur confiance), ou Protection physique (matériel résistant).

La vérification des signatures des clefs publiques peut exiger la vérification des signatures aux points futurs du temps, incluant probablement après que les

clefs privées cessent d'êtres employées. Certaines applications peuvent exiger que la signature des clefs privées ne soient ni sauvegardées, ni archivées : telles les clefs révélées à n'importe quelle partie autre que le propriétaire infirment potentiellement la propriété de non répudiation. Il faut notez ici que la perte (sans compromission) d'une signature de clef privée peut être adressée par la création d'une nouvelle clef, et est non-critique comme une clef privée n'est pas nécessaire pour avoir accès aux transactions passées; de la même façon, des clefs publiques de chiffrement n'ont pas besoin d'être archivées.

Les clefs employées pour l'authentification d'entité n'ont pas besoin d'être sauvegardées ou archivées. Toutes les clefs secrètes employées pour le chiffrement ou l'authentification d'origine des données doivent rester secrètes aussi longtemps que possible que les données sécurisées exigent en dessous la protection continue, la sauvegarde est exigée pour empêcher la perte de ces données.

3/ Cycle de vie de la gestion des clefs :

Sauf dans les systèmes simples où des clefs secrètes restent fixées pour toujours, les cryptoperiodes associées avec des clefs exigent que les clefs soient mises à jour périodiquement. La mise à jour des clefs nécessite des procédures et protocoles complémentaires, incluant souvent des communications avec les tiers dans les systèmes a clefs publiques. L'ordre des états que la sécurité du matériel progresse par sa durée de vie est appelé le cycle de vie de la gestion des clefs.

4/ Initialisation des systèmes et installation des clefs :

Les systèmes de gestion des clefs exigent un rapport de verrouillage initial

pour fournir un canal sûr et soutient facultativement l'établissement des clefs opérationnelles (long terme et court terme) par des techniques automatisées. Le processus d'initialisation implique typiquement des procédures non-cryptographiques.

La sécurité d'un système correctement conçu est réduite à la sécurité du matériel de sécurité, et en fin de compte à la sécurité d'installation de la clef initiale.

5/ Non répudiation et certification de signatures digitales :

L'aspect de non répudiation des signatures digitales est un avantage primaire de la cryptographie a clef publique. Par cette propriété, un signataire est empêché de signer un document et par la suite devenir capable avec succès nier faire ainsi. Un service de non répudiation exige la spécification des détails précis incluant un processus de jugement et un juge, qu'elle preuve serait soumise au juge, et quel processus précis le juge doit suivre pour rendre le jugement sur des litiges. Le rôle d'un juge est distinct de celui d'un agent **d'horodatage** ou le **notaire** qui produit la preuve.

Remarque : (authentification d'origine / signature non-repudiable) Une distinction fondamentale existe entre une partie A étant capable de se convaincre de la validité d'une signature digitale *S* à un point dans le temps t_0 et cette partie étant capable de le convaincre d'autres à quelque temps, $t_1 >= t_0$ que *S* était valable au temps t_0. Le premier ressemble à l'authentification d'origine de données comme typiquement fourni par le mécanismes d'authentification de l'origine de la clef symétrique et

peut être accepté par un vérificateur comme une forme d'autorisation dans un environnement de confiance mutuelle. Cela diffère de la signature digitale qui est non-repudiable dans l'avenir. L'authentification de l'origine de données fournie par une signature digitale est valable seulement tandis que le secret de la clef privée du signataire est maintenu. Une menace qui doit être relevée est que le signataire révèle intentionnellement sa clef privée et revendique ensuite qu'une signature précédemment valable a été forgée. (Un problème semblable existe avec les cartes de crédit et d'autres méthodes d'autorisation).

Pour des messages signés ayant des durées de vie courtes (c'est-à-dire, dont la signification ne s'étend pas loin dans l'avenir), la non répudiation est moins importante et la certification peut être inutile.

Pour d'autres messages, l'exigence pour une partie pour être capable de vérifier les signatures à un point plus loin dans le temps (incluant pendant ou après que des signatures des clefs ont étés mises à jour ou révoquées), comme le processus de jugement lié à la non répudiation de signatures, places des demandes complémentaires sur les systèmes pratiques de gestion des clefs. Ceux-ci peuvent inclure le stockage (par exemple, clefs, certificats, CRL) probablement exigé comme preuve à un point futur du temps.

6/ Dépôt des clefs de chiffrement

L'objectif d'un système de dépôt des clefs de chiffrement est de fournir le chiffrement de trafic d'utilisateur (par exemple, la voix ou les données) tel que les clefs de session employées pour le chiffrement de trafic sont disponibles aux

tierces parties correctement autorisées dans des circonstances spéciales ("le cas d'accès d'urgence"). Cela accorde aux tierces parties qui ont contrôlées le trafic d'utilisateur la capacité de décrypter un tel trafic. L'intérêt publique à de tels systèmes a surgi quand les agences d'exécution de la loi ont promu leur utilisation pour faciliter la mise sur écoute légale d'une ligne téléphonique pour combattre les activités criminelles.

Cependant, d'autres utilisations dans l'industrie incluent le rétablissement de données chiffrées après la perte des clefs du matériel par une partie légitime, ou destruction des clefs en raison de l'échec d'équipement ou des activités malveillantes. On donne un exemple d'un système de dépôt de clé de chiffrement ci-dessous.

Exemple : (Le système de dépôt des clefs de chiffrement « Clipper ») :

Le système de dépôt des clefs de chiffrement « Clipper » implique l'utilisation du chip Clipper (ou un dispositif semblable) en conjonction avec certaines procédures et commandes administratives. L'idée de base est de déposer deux composantes clefs, qui déterminent conjointement une clef de chiffrement, avec deux tiers de confiance (des agents de dépôt), qui permettent par la suite (sur une autorisation appropriée) le rétablissement des données d'utilisateur chiffrées.

Plus spécifiquement, le chiffrement des télécommunications entre deux utilisateurs procède comme suit :

Chaque partie fait combiner un téléphone avec un chip de dépôt des clefs de chiffrement. Les utilisateurs négocient ou établissent autrement une clef de session

K_S, qui est l'entrée au chip de dépôt de la partie de chiffrement de données.

Comme fonction de K_S et vecteur d'initialisation (V), le chip crée par une méthode non révélée un bloc de données appelé *Law Enforcement Access Field (LEAF)*.

Le (LEAF) et le (V) sont transmis pendant la mise en place d'une session de communications.

Le chip chiffre alors les données d'utilisateur *D* sous K_S produisant $E_{K_S}(D)$, le chip déchiffre le trafic seulement si le (LEAF) transmit valide correctement. Une telle vérification exige que le chip a l'accès à une clef de famille commune K_F.

Le LEAF contient une copie de la clef de session chiffrée sous une clef spécifique du dispositif K_U. K_U est produite et chargée dans le chip au moment de la fabrication du chip, mais avant que le chip ne soit incorporé dans un produit de sécurité. Le système rencontre son objectif en fournissant au tiers l'accès sous l'autorisation appropriée (comme défini par le Système de Dépôt des clefs de chiffrement) à la clef du dispositif K_U d'individus visés.

Pour dériver la clef K_U incorporé dans un chip de dépôt avec identificateur *UID*, deux composantes clefs (K_{C1} , K_{C2}) sont créés dont le XOR est K_U. Chaque composante est chiffrée sous une clef ($K_{CK} = K_{N1}$ XOR K_{N2}), où K_{Ni} est l'entrée au chip. (Employées pour programmer quelques chips, K_{Ni} est stockée par l'agent de dépôt pour le rétablissement ultérieur de K_{CK}.) Une composante clef chiffrée est donnée alors à chaque agent de dépôt, qui la stocke avec l'UID pour entretenir des demandes postérieures. Les données Stockées des deux agents doivent être

obtenues par la suite par un fonctionnaire autorisé pour permettre le rétablissement de K_U (en récupérant d'abord $K_{CK,}$ et ensuite K_{C1} , K_{C2} et $K_U = K_{C1}$ *XOR* K_{C2}).

Chaque chip de dépôt contient un dispositif identificateur unique (UID) à 32 bits, un dispositif a clef unique (K_U) à 80 bits et un dispositif a clef familiale (*KF*) à 80 bits communs à une plus grande collection de dispositifs. Le *LEAF* contient une copie de la Clef de session à 80 bits K_S chiffrée sous K_U, L'UID, et un authentificateur de chiffrement a 16 bits (EA) créé par une méthode non révélée; ceux-ci sont alors chiffrées sous K_F. Le rétablissement de *Ks* du LEAF exige ainsi K_F et K_U. L'authentificateur de chiffrement est un contrôleur conçu pour permettre la détection de falsification du LEAF (par exemple, par une tentative adverse d'empêcher le rétablissement autorisé de K_S et ainsi *D*).

VIII/ L’échange des clefs :

Diffie-Hellman :

Principe de l'algorithme

Soient 2 personnes **A** et **B** désirant communiquer sans utiliser une clef secrète.

Ils se mettent d'accord sur un canal qui n'est pas forcément sécurisé, sur deux grands entiers premiers entre eux, *n* et *g*, tels que $n>g>1$.

Pour que l'échange de clefs soit sécurisé, il faut que *n* ait une taille de l'ordre de 512 ou 1024 bits.

A choisit un grand nombre entier aléatoire *x*.

A calcule $X=g^x \ mod[\ n]$ et l'envoie à **B**.

B choisit un grand nombre entier aléatoire *y*.

B calcule $Y=g^y \ mod\ [n]$ et l'envoie à **A**.

Ensuite, chacun de leur coté :

- **A** calcule $k=Y^x \ mod\ n$
- **B** calcule $k'=X^y \ mod\ n$

On constate alors que $k = k' = g^{xy} \ mod\ [n]$ et donc que **A** et **B** sont parvenus à établir une clef secrète commune qui sera ensuite utilisée par un algorithme symétrique.

La clef publique correspond aux valeurs *X* et *Y* échangées par les deux protagonistes.

La clef privée correspond aux valeurs *x* et *y* conservées par les deux protagonistes.

Remarque

L'attaque possible de cet algorithme repose sur l'espionnage des nombres échangés entre **A** et **B**, soient *n*, *g*, *X* et *Y*.

Cette attaque est particulièrement évidente puisque l'échange de ces valeurs peut se faire en clair. Mais, pour retrouver *x* et *y* indispensables pour recomposer la clef secrète, il faut effectuer le calcul d'un logarithme discret modulo n, ce qui est très coûteux actuellement. C'est sur ce principe que repose la sécurité de l'algorithme de Diffie-Hellman.

Diffie-Hellman peut-être vulnérable à «l'attaque de l'homme au milieu» : un attaquant se place entre les deux protagonistes et substitue systématiquement toutes les valeurs échangées par de nouvelles valeurs qu'il a lui-même générées.

Les protagonistes croiraient ainsi avoir échangé une clé secrète alors qu'ils l'auraient en fait échangée avec l'attaquant. Ce dernier est alors en mesure de déchiffrer les communications qui l'utiliseraient.

La parade est de signer toutes les transactions à l'aide de clés asymétriques certifiées par une autorité reconnue par les protagonistes.

Conclusion :

La clef (la solution) de la bonne tenue d'un état, d'une institution, d'une entreprise est une bonne gestion de ses dernières, alors quand il s'agit de sécuriser nos communications une certaine gestion celle des clefs est plus que nécessaire.

On peut dire qu'on ne peut pas conclure un sujet pareil, car, la il s'agit de traiter ou d'étudier un thème qui est assez personnel et secret pour une institution par rapport a une autre pour se rabattre sur une seule solution, mais néanmoins on peut dire que pour faire une gestion adéquate des clefs de chiffrement il est nécessaire de faire une synthèse des applications auxquelles ses clefs seront destinées, aussi il faut être sure de l'origine des clefs, et de toutes les étapes qui suivent (citées dans ce mémoire).

Comprehensive treatment of key management, Davies and Price.

Special key management techniques (transaction keys reduce the implications of terminal key compromise). Davies, Davies and Price. Meyer and Matyas

Compare symmetric and public-key techniques; the formalization proposed by Rueppel.

KDCs et KTCs ont etes publiés par l'ANSI. Needham and Schroeder.

Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S.Vanstone.

General symmetric-key techniques, EFT applications.

Overview of key management concepts and life cycles aspects, Fumy and Landrock.

Regarding key management principles, Abadi and Needham, and Anderson and Needham.

Key management for security (authentication and encryption) in North American digital cellular systems.

Specifies key management techniques and life cycle principles for use in banking systems,

The Kerberos authentication service.