



Étude technique

Cryptographie à clé publique et signature numérique  
Principes de fonctionnement

Étude technique réalisée par CGI  
Septembre 2002

## Introduction

L'un des principaux défis auxquels nous devons faire face en tant que conseiller consiste à maintenir un niveau de connaissance des technologies nouvelles et émergentes allant au-delà du superficiel ou de la jargonnerie. Nous devons atteindre un niveau de compréhension qui nous permette de communiquer efficacement tant avec les fournisseurs qu'avec les clients, de façon à pouvoir faire valoir :

- notre connaissance des enjeux commerciaux en cause;
- le rôle que peut jouer la technologie dans l'apport de solutions;
- les avantages commerciaux que le client en retirera;
- les contraintes qui demeureront et qu'il faudra pallier d'autres façons.

La cryptographie à clé publique existe depuis un certain temps déjà. Un grand nombre de travaux intéressants ont été menés par différents comités (tels IETF/PKIX et PKCS<sup>1</sup>) pour définir des normes et techniques en matière de cryptographie à clé publique. Mais savons-nous au juste de quoi il en retourne? En comprenons-nous le fonctionnement? Regardons donc sous le capot pour examiner le moteur et comprendre enfin le véritable fonctionnement de la cryptographie à clé publique et de la signature numérique.

Cet article constitue un point de départ pour se faire une idée du vaste domaine qu'est l'**ICP** ou infrastructure à clé publique. Ce domaine englobe les mécanismes décrits dans cet article, ainsi qu'un ensemble de logiciels, matériel et processus régis par des règles et normes convergeant vers le haut niveau de confiance exigé et attendu de l'industrie.

---

<sup>1</sup> IETF/PKIX correspond à Internet Engineering Task Force/Public-Key Infrastructure (X509). PKCS correspond à Public Key Cryptography Standards, normes qui ont été élaborées par RSA conjointement avec des fournisseurs tels que Microsoft, Apple, Sun, etc.

## 1. Qu'est-ce que la cryptographie à clé publique?

La cryptographie à clé publique désigne un mécanisme de chiffrement et de déchiffrement. Elle porte le nom de *clé publique* pour la différencier du mécanisme cryptographique classique et plus intuitif connu sous le nom de *cryptographie à clé secrète, à clé partagée, à clé symétrique*, ou encore, *à clé privée*.

La cryptographie à clé symétrique est un mécanisme selon lequel la même clé est utilisée pour le chiffrement et le déchiffrement; elle est plus intuitive à cause de sa similarité avec ce que l'on s'attend à utiliser pour verrouiller et déverrouiller une porte : la même clé. Cette caractéristique requiert des mécanismes sophistiqués pour distribuer en toute sûreté la clé symétrique aux deux parties<sup>2</sup>.

La cryptographie à clé publique, quant à elle, repose sur un autre concept faisant intervenir une paire de clés : l'une pour le chiffrement et l'autre pour le déchiffrement. Ce concept, comme vous le verrez ci-dessous, est ingénieux et fort attrayant, en plus d'offrir un grand nombre d'avantages par rapport à la cryptographie symétrique :

- distribution simplifiée des clés;
- signature numérique;
- chiffrement de longue durée.

Il est toutefois important de signaler que la cryptographie à clé symétrique joue encore un rôle prépondérant dans la mise en œuvre d'une infrastructure à clé publique ou *ICP*.

### 1.1 Définition

L'expression «cryptographie à clé publique» est couramment utilisée pour désigner une méthode cryptographique faisant intervenir une *paire de clés asymétriques*<sup>3</sup> : une *clé publique* et une *clé privée*<sup>4</sup>. La cryptographie à clé publique utilise cette *paire de clés* pour le chiffrement et le déchiffrement. La clé publique est rendue publique et distribuée librement. La clé privée n'est jamais distribuée et doit être gardée secrète.

Étant donnée une paire de clés, les données chiffrées à l'aide de la clé publique ne peuvent être déchiffrées qu'avec la clé privée correspondante; inversement, les données chiffrées à l'aide de la clé privée ne peuvent être déchiffrées qu'avec la clé publique correspondante. Cette caractéristique est utilisée pour mettre en œuvre les principes de la cryptographie et de la signature numérique, comme le montrent les figures 1 et 2.

### 1.2 Chiffrement et déchiffrement

Le chiffrement est un mécanisme selon lequel un message est transformé de sorte que seul l'expéditeur et le destinataire peuvent le voir. Supposons, par exemple, qu'Alice veut envoyer un message privé à Bob. Pour ce faire, elle doit d'abord connaître la clé publique de Bob; étant donné que tout le monde peut voir sa clé publique, Bob peut l'envoyer en clair sur le réseau sans s'inquiéter. Une fois qu'Alice possède la clé publique de Bob, elle chiffre le message à l'aide de la

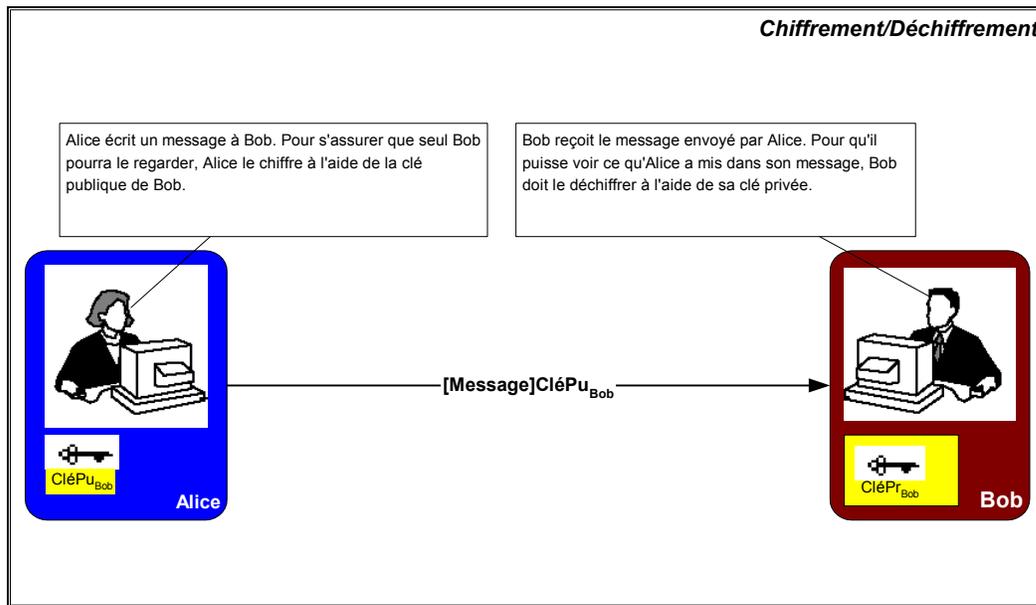
---

<sup>2</sup> Des infrastructures comme Kerberos assurent la distribution et la gestion des clés symétriques.

<sup>3</sup> L'expression «cryptographie asymétrique» par rapport à «cryptographie symétrique» constitue une autre façon de différencier les deux mécanismes.

<sup>4</sup> Prenez garde de ne pas confondre le mécanisme à clé privée et la clé privée. Pour éviter toute confusion, l'expression «cryptographie à clé symétrique» sera utilisée dans cet article chaque fois qu'il est question du mécanisme.

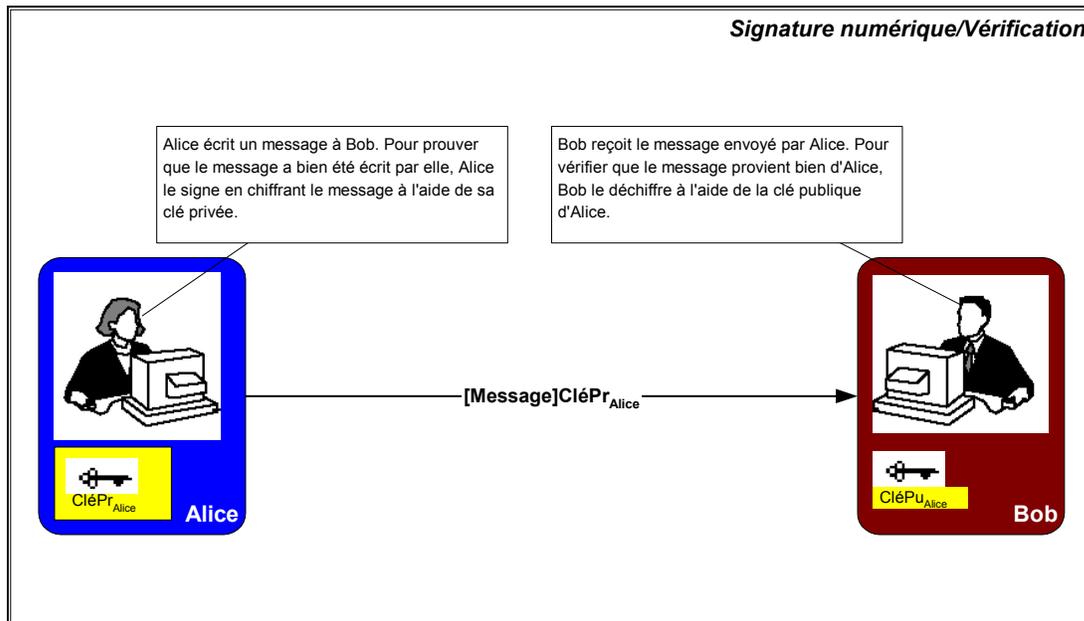
clé publique de Bob et l'envoie à Bob. Bob reçoit le message d'Alice et, à l'aide de sa clé privée, le déchiffre.



**Figure 1 : Principes de chiffrement et de déchiffrement**

### 1.3 Signature numérique et vérification

La signature numérique est un mécanisme qui permet d'authentifier un message, autrement dit de prouver qu'un message provient bien d'un expéditeur donné, à l'instar d'une signature sur un document papier. Supposons, par exemple, qu'Alice veut signer numériquement un message destiné à Bob. Pour ce faire, elle utilise sa clé privée pour chiffrer le message, puis elle envoie le message accompagné de sa clé publique (habituellement, la clé publique est jointe au message signé). Étant donné que la clé publique d'Alice est la seule clé qui puisse déchiffrer ce message, le déchiffrement constitue une vérification de signature numérique, ce qui signifie qu'il n'y a aucun doute que le message ait été chiffré à l'aide de la clé privée d'Alice.



**Figure 2 : Principes de signature numérique et de vérification**

#### 1.4 Au-delà des principes

Les deux paragraphes qui précèdent illustrent les principes de chiffrement/déchiffrement et de signature/vérification. Il est possible de combiner chiffrement et signature numérique et, par conséquent, d'assurer confidentialité et authentification.

Comme nous l'avons mentionné plus tôt, la cryptographie à clé symétrique joue un rôle important dans la mise en œuvre des systèmes à clé publique. Cela est dû au fait que les algorithmes de chiffrement à clé asymétrique<sup>5</sup> sont plus lents que ceux à clé symétrique<sup>6</sup>.

Pour la signature numérique, une autre technique utilisée est le *hachage*. Cette technique permet de produire un *condensé de message* qui est une représentation réduite et unique<sup>7</sup> (qui s'apparente à une somme de contrôle sophistiquée) du message complet. Les algorithmes de hachage<sup>8</sup> sont des algorithmes de chiffrement unidirectionnels; il est donc impossible de retrouver le message d'origine à partir du condensé.

Les raisons principales pour lesquelles on produit un condensé de message sont :

1. l'intégrité du message envoyé est préservée; toute altération du message sera aussitôt détectée;
2. la signature numérique sera appliquée au condensé dont la taille est habituellement beaucoup plus petite que le message lui-même;

<sup>5</sup> Exemples d'algorithme à clé asymétrique : RSA, DSA et ECDSA.

<sup>6</sup> Exemples d'algorithme à clé symétrique : RC2, RC4, DES et triple DES.

<sup>7</sup> En fait, le condensé de message est fort probablement unique dans le sens où il est presque impossible de trouver deux messages significatifs qui produiraient simultanément le même condensé. Par conséquent, la probabilité qu'un message trafiqué produise le même condensé que l'original est quasiment nulle.

<sup>8</sup> Exemples d'algorithme de hachage : SHA-1 et MD5.

- les algorithmes de hachage sont bien plus rapides que n'importe quel algorithme de chiffrement (que ce soit à clé publique ou à clé symétrique).

Les sections suivantes expliquent ce qui se produit réellement au chiffrement et à la signature d'un message d'une part, et au déchiffrement d'un message et à la vérification de sa signature d'autre part.

#### 1.4.1 Étapes de signature et de chiffrement d'un message

La Figure 3 ci-dessous montre la série d'opérations qu'Alice doit exécuter pour envoyer un message signé et chiffré à Bob.

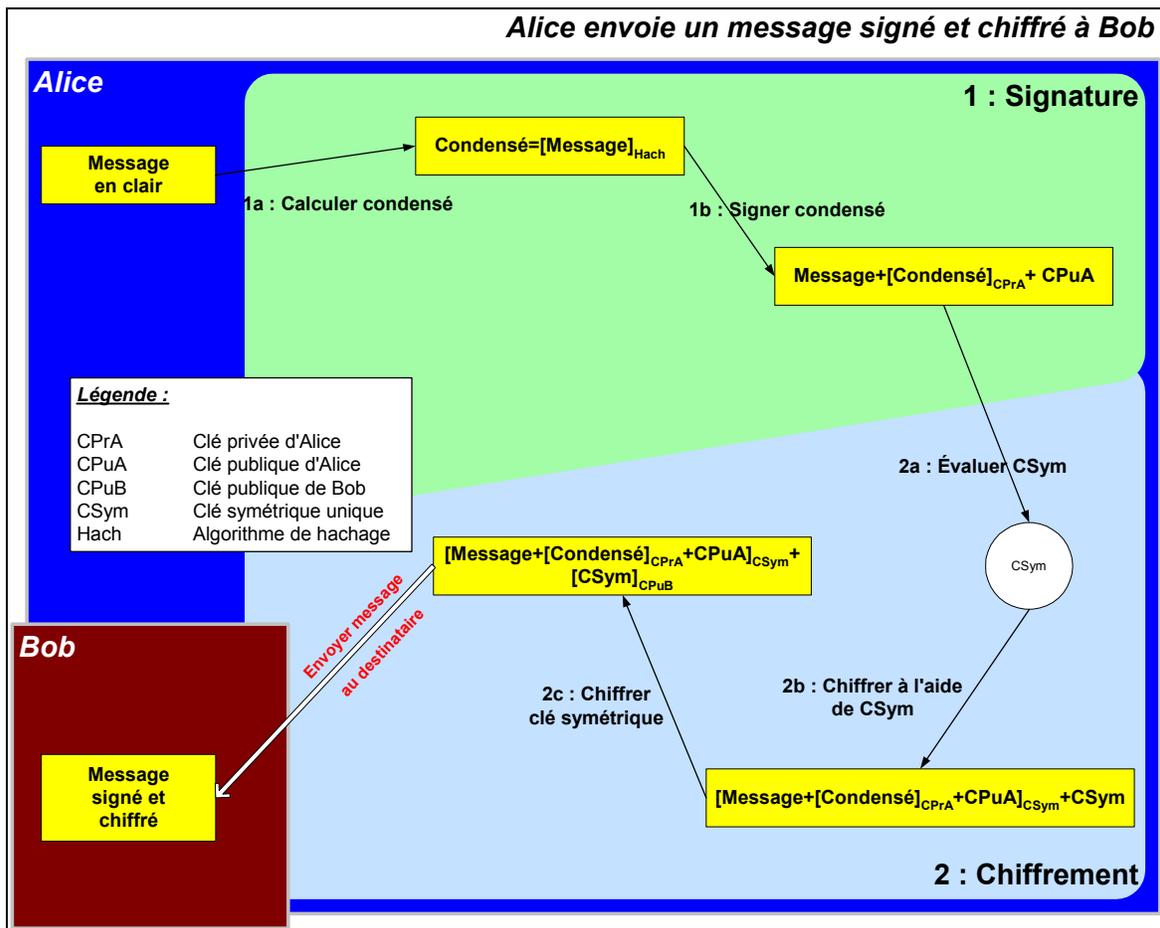


Figure 3 : Processus détaillé de signature et de chiffrement à l'aide de clés

- Signature du message. La signature numérique comprend deux étapes :
  - Évaluation du condensé de message. Le but principal de l'évaluation d'un condensé est de s'assurer que le message ne sera pas altéré; c'est ce qu'on entend par intégrité du message.
  - Signature du condensé. Une signature est en fait un chiffrement à l'aide de la clé privée de l'émetteur (Alice dans le cas présent). On retrouve également dans cette

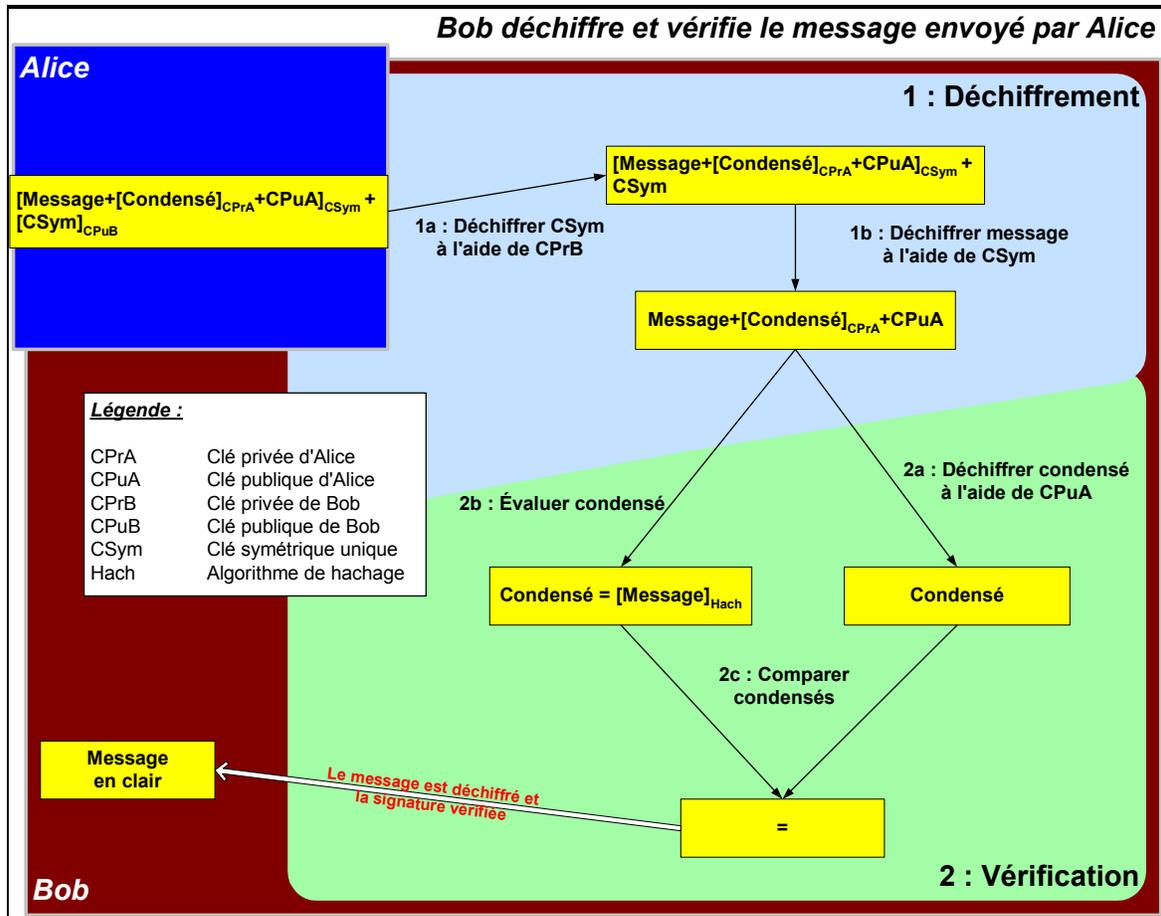
signature le nom de l'algorithme de hachage utilisé par l'émetteur. La clé publique de l'émetteur est aussi annexée à la signature. Grâce à ces informations, n'importe qui peut déchiffrer et vérifier la signature à l'aide de la clé publique et de l'algorithme de hachage de l'émetteur. Étant donné les propriétés du chiffrement à clé publique et des algorithmes de hachage, le destinataire a la preuve que :

- i) Le condensé a été chiffré à l'aide de la clé privée de l'émetteur;
  - ii) Le message est protégé contre toute altération.
- 2) *Chiffrement* du message. Le chiffrement comprend les trois étapes suivantes :
- a) *Création d'une clé de chiffrement/déchiffrement unique*. Rappelons que les algorithmes de chiffrement et de déchiffrement qui utilisent des clés asymétriques sont trop lents pour être utilisés pour de longs messages; les algorithmes à clé symétrique sont très efficaces et sont donc utilisés.
  - b) *Chiffrement du message*. La totalité du message (le message proprement dit et la signature) est chiffrée à l'aide de CSym, la clé symétrique évaluée ci-dessus.
  - c) *Chiffrement de la clé symétrique*. CSym est également utilisée par le destinataire pour déchiffrer le message. Elle ne doit donc être accessible qu'au destinataire (Bob). Pour dissimuler CSym à tous sauf au destinataire, il suffit de la chiffrer à l'aide de la clé publique du destinataire. Étant donné que CSym représente un très petit élément d'information comparé au message (qui pourrait être très long), l'inefficacité relative des algorithmes à clé asymétrique devient acceptable.

Il est intéressant de souligner que si Alice voulait envoyer le même message à plusieurs destinataires, Bob et John par exemple, la seule opération supplémentaire qu'elle aurait à exécuter serait de répéter l'étape 2) c) pour John. Par conséquent, le message que Bob et John recevraient prendrait la forme suivante : **[Message+[Condensé]<sub>CPuA</sub>+CPuA]<sub>CSym</sub>+ [CSym]<sub>CPuB</sub>+ [CSym]<sub>CPuJ</sub>** . Notez que Bob et John utiliseront exactement la même CSym pour déchiffrer le message.

### 1.4.2 Étapes de déchiffrement et de vérification de la signature d'un message

La Figure 4 ci-dessous montre la série d'opérations que Bob doit exécuter pour déchiffrer et vérifier le message envoyé par Alice.



**Figure 4 : Processus détaillé de déchiffrement et de vérification à l'aide de clés**

- 1) *Déchiffrement du message.* Le déchiffrement comprend les étapes suivantes :
  - a) *Déchiffrement de la clé symétrique.* La clé symétrique unique a été utilisée pour chiffrer le message. Cette clé (CSym) a été chiffrée à l'aide de la clé publique du destinataire (Bob). Seul Bob peut déchiffrer CSym et l'utiliser pour déchiffrer le message<sup>9</sup>.
  - b) *Déchiffrement du message.* Le message (qui comprend le message proprement dit et la signature) est déchiffré à l'aide de CSym.
- 2) *Vérification de la signature.* La vérification de signature comprend les trois étapes suivantes :

<sup>9</sup> En fait, tous les destinataires seraient en mesure de déchiffrer leur propre copie de CSym. Les opérations qui suivent peuvent donc être exécutées par chaque destinataire.

- a) *Déchiffrement du condensé de message.* Le condensé a été chiffré à l'aide de la clé privée de l'émetteur (Alice). Le condensé est maintenant déchiffré à l'aide de la clé publique de l'émetteur incluse dans le message.
- b) *Évaluation du condensé.* Étant donné que le hachage est un processus unidirectionnel, autrement dit qu'il est impossible de retrouver le message d'origine à partir du condensé, le destinataire doit réévaluer le condensé en utilisant exactement le même algorithme de hachage que l'émetteur.
- c) *Comparaison des condensés.* Le condensé déchiffré en a) et le condensé évalué en b) sont comparés. S'ils concordent, la signature est de ce fait vérifiée et le destinataire peut alors avoir la certitude que le message a été envoyé par l'émetteur et n'a pas été altéré. S'ils ne concordent pas, il est possible que :
  - (i) le message n'ait pas été signé par l'émetteur ou que
  - (ii) le message ait été altéré.Dans les deux cas, le message doit être rejeté.

### **1.5 Identité et clés**

Jusqu'à présent, nous avons pris pour acquis que les clés utilisées pour le chiffrement et le déchiffrement ainsi que pour la signature numérique et la vérification appartiennent à Bob et Alice. Comment pouvons-nous être certains qu'Alice est bien Alice? Et comment Alice peut-elle s'assurer que seul Bob verra ce qu'elle a chiffré? La seule certitude que nous avons est que l'utilisateur d'une paire de clés donnée a signé et chiffré le message. Mais s'agit-il réellement de son propriétaire? George, par exemple, a pu envoyer un message à Bob en se faisant passer pour Alice; Bob ne peut dire si c'est Alice ou George qui lui a envoyé le message. Les mêmes incertitudes s'appliquent à la clé publique de Bob. L'utilisation de certificats permet de résoudre ce problème.

## 2. Qu'est-ce qu'un certificat?

Un certificat est un élément d'information qui prouve l'identité du propriétaire d'une clé publique. À l'instar d'un passeport, un certificat est une preuve reconnue de l'identité d'une personne. Les certificats sont signés et transmis de façon sécuritaire par un tiers de confiance appelé autorité de certification (AC). Tant que Bob et Alice ont confiance en ce tiers, ils peuvent être assurés que les utilisateurs de ces clés en sont bel et bien les propriétaires.

Un certificat contient notamment :

- 1) l'identité de l'AC;
- 2) L'identité du propriétaire;
- 3) la clé publique du propriétaire;
- 4) la date d'expiration du certificat;
- 5) la signature de l'AC qui a délivré le certificat;
- 6) d'autres informations qui n'entrent pas dans la portée de cet article.

En disposant d'un certificat au lieu d'une clé publique, le destinataire peut maintenant vérifier un certain nombre d'aspects au sujet de l'émetteur pour s'assurer que le certificat est valide et qu'il appartient bien à la personne à qui il est censé appartenir. Il peut notamment :

- 1) comparer l'identité du propriétaire;
- 2) vérifier que le certificat est toujours valide;
- 3) vérifier que le certificat a été signé par un AC de confiance;
- 4) vérifier la signature du certificat de l'émetteur pour s'assurer que ce dernier n'a pas été altéré.

Bob peut maintenant vérifier le certificat d'Alice et avoir la certitude que c'est bien la clé privée d'Alice qui a servi à signer le message. Alice doit prendre des précautions avec sa clé privée et ne pas révéler comment y accéder; ce faisant, elle met en pratique une partie de la non-répudiation, une caractéristique associée à la signature numérique. Comme nous le verrons à la section 3.2, d'autres conditions sont essentielles au maintien de la non-répudiation.

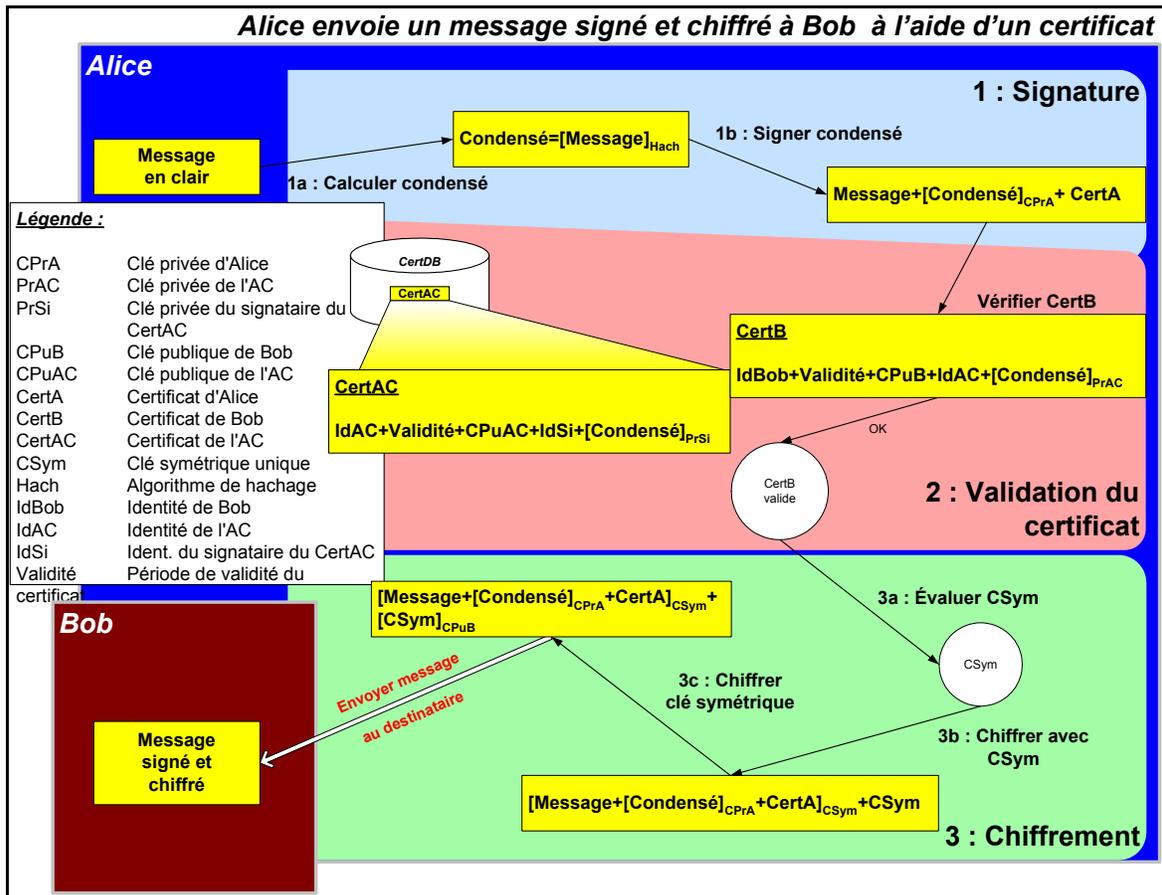
Notez que les certificats sont signés par une AC, ce qui signifie qu'ils ne peuvent être altérés. La signature de l'AC peut, à son tour, être vérifiée à l'aide du certificat de cette AC.

### 2.1 Validation de certificat ajoutée au processus

Quand Alice chiffre un message destiné à Bob, elle utilise le certificat de Bob. Avant d'utiliser la clé publique incluse dans le certificat de Bob, des étapes supplémentaires sont nécessaires pour valider le certificat de Bob. Il faut vérifier :

- 1) la période de validité du certificat de Bob;
- 2) que le certificat appartient bien à Bob;
- 3) que le certificat n'a pas été altéré;
- 4) que le certificat de Bob a été signé par une AC de confiance.

De plus, si Alice doute de l'authenticité de l'AC de Bob, d'autres étapes seraient nécessaires pour valider le certificat de cette AC. Ces étapes sont identiques à celles requises pour valider le certificat de Bob. Dans l'exemple ci-dessous, il est présumé que Bob et Alice ont tous deux confiance en l'AC.



[m1]

**Figure 5 : Processus détaillé de signature et de chiffrement à l'aide de certificats**

Dans la figure 5 ci-dessus, une étape de validation de certificat a été ajoutée par rapport aux étapes illustrées à la figure 3. Seuls les champs requis pour la validation d'un certificat sont affichés.

Alice veut s'assurer que la CPuB incluse dans le CertB appartient bien à Bob et qu'elle est toujours valide.

- Elle vérifie le champ Id et trouve IdBob, qui représente l'identité de Bob. En fait, la seule chose qu'elle sait réellement est que ce certificat semble appartenir à Bob.
- Elle vérifie ensuite les champs de validité et constate que la date et l'heure actuelles entrent dans la période de validité. Jusque-là, le certificat semble bien appartenir à Bob et être valide.
- La dernière vérification consiste à vérifier la signature du CertB à l'aide de la clé publique de l'AC (CPuAC incluse dans le CertA)<sup>10</sup>. Si la signature du CertB est valide, cela signifie que :

<sup>10</sup> Rappelons qu'une signature est le condensé d'un message (dans le cas présent, le message est CertB) chiffré à l'aide de la clé privée de l'émetteur (il s'agit ici de la clé privée de l'AC). Le processus de vérification de la signature de l'AC est identique à celui illustré à la figure 4 où Bob vérifie la signature d'Alice.

- a) Le certificat de Bob a été signé par l'AC en laquelle Alice et Bob ont pleinement confiance.
- b) L'intégrité du certificat de Bob est prouvée et il n'y a donc eu aucune altération.
- c) L'identité de Bob est assurée et la clé publique incluse dans le certificat est toujours valide et appartient bien à Bob. Par conséquent, Alice peut chiffrer le message et avoir la certitude que seul Bob pourra le lire.

Bob exécutera les mêmes étapes pour le certificat d'Alice avant de vérifier la signature d'Alice.

## 2.2 Au-delà de la mécanique

Jusqu'à présent, nous avons examiné principalement les mécanismes de clé publique associés au chiffrement et à la signature numérique. Dans la section 2, la notion d'autorité de certification est apparue. L'AC constitue le noyau de l'infrastructure à clé publique (ICP).

## 3. Qu'est-ce qu'une ICP?

Une ICP est une combinaison de logiciels et de méthodes offrant un moyen de gérer les clés et les certificats et de les utiliser efficacement. Il suffit de songer à la complexité des opérations décrites plus tôt dans cet article pour comprendre l'absolue nécessité de fournir aux utilisateurs un soutien logiciel approprié en matière de cryptographie et de signature numérique. Mais rien n'a été dit encore au sujet de la gestion.

### 3.1 Gestion des clés et des certificats

La gestion des clés et des certificats englobe la série d'opérations requises pour créer et maintenir les clés et les certificats. La liste qui suit décrit les principaux aspects pris en charge par une solution de gestion ICP :

1. *Création des clés et des certificats* : Comment générer des paires de clés? Comment délivrer des certificats aux utilisateurs?  
Une ICP doit offrir un soutien logiciel pour la génération des paires de clés et les demandes de certificat. De plus, des méthodes doivent être mises en place pour vérifier l'identité de l'utilisateur avant de l'autoriser à demander un certificat.
2. *Protection des clés privées* : Comment l'utilisateur protégera-t-il sa clé privée pour empêcher d'autres utilisateurs de s'en servir à mauvais escient?  
Les certificats sont librement accessibles parce qu'ils sont utilisés pour le chiffrement ou la vérification de signature. Les clés privées requièrent un niveau de protection raisonnable car elles sont utilisées pour le déchiffrement ou la signature numérique. Un solide mécanisme de mot de passe doit faire partie des caractéristiques d'une ICP efficace.
3. *Révocation de certificat* : Comment gérer la situation quand la clé privée d'un utilisateur est compromise? Ou encore, comment gérer la situation quand un employé quitte la compagnie? Comment savoir si un certificat a été révoqué?  
Une ICP doit offrir un moyen de révoquer un certificat. Une fois révoqué, le certificat doit être inclus dans une liste de révocation accessible à tous les utilisateurs. Un mécanisme doit être fourni pour vérifier cette liste de révocation et interdire l'utilisation d'un certificat révoqué.
4. *Sauvegarde et récupération des clés* : Qu'arrive-t-il aux fichiers chiffrés quand un utilisateur perd sa clé privée?  
Si la sauvegarde des clés n'est pas assurée, tous les messages et fichiers qui ont été chiffrés à l'aide de sa clé publique ne peuvent plus être déchiffrés et sont donc perdus à

- jamais. Une ICP doit offrir un mécanisme de sauvegarde et de récupération des clés privées afin que l'utilisateur puisse récupérer sa clé privée et accéder à ses fichiers<sup>11</sup>.
5. *Mise à jour des clés et des certificats* : Qu'arrive-t-il quand un certificat atteint ou est sur le point d'atteindre sa date d'expiration?  
Les clés et certificats ont une durée limitée. Une ICP doit offrir un mécanisme permettant au moins de mettre à jour la date d'expiration des certificats. Il est de bonne pratique, toutefois, d'assurer la mise à jour des clés et des certificats. Cette mise à jour peut se faire automatiquement, auquel cas l'utilisateur final reçoit un avis l'informant que la mise à jour a été effectuée, ou elle peut nécessiter une intervention de l'utilisateur au moment ou avant le moment où ses clés et certificats arrivent à expiration; dans ce cas, l'ICP doit informer au préalable l'utilisateur qu'une intervention de sa part est nécessaire.
6. *Gestion de l'historique des clés* : Après plusieurs mises à jour des clés, comment l'utilisateur saura-t-il quelle clé privée utiliser pour déchiffrer les fichiers?  
Chaque fois qu'une clé est mise à jour, une nouvelle paire de clés est générée. Les fichiers qui ont été chiffrés à l'aide d'une ancienne clé publique ne peuvent être déchiffrés qu'avec la clé privée correspondante. Si la gestion de l'historique des clés n'est pas assurée, l'utilisateur devra lui-même déterminer quelle clé il doit utiliser pour déchiffrer un fichier donné<sup>12</sup>.
7. *Accès aux certificats* : Comment un utilisateur qui veut envoyer un message à plusieurs destinataires pourra-t-il obtenir leurs certificats?  
Une ICP doit offrir un moyen facile et commode d'accéder à ces certificats. Un répertoire LDAP est couramment utilisé à cette fin.

### 3.2 Renforcement de la protection contre la répudiation de signature numérique

Un point important qui doit être clarifié est la non-répudiation de signature numérique. Cette notion renvoie au fait qu'un utilisateur ne peut nier avoir signé un message donné. Cela implique que l'utilisateur qui a signé le message est le seul à avoir accès à la clé privée utilisée pour la signature. Toutefois, comme nous l'avons vu précédemment, dans un environnement de gestion ICP, les clés privées sont conservées par l'AC aux fins de récupération des clés. Par conséquent, l'utilisateur et l'AC connaissent tous deux la clé privée, ce qui signifie qu'ils sont deux à pouvoir (en théorie) l'utiliser pour signer un message. Un utilisateur peut ainsi nier avoir signé le message en question.

Pour éviter cette situation et mieux se prémunir contre la répudiation de signature numérique, une seconde paire de clés doit être utilisée à seules fins de signature et de vérification. Aucune sauvegarde n'est faite des clés privées de signature et seul l'utilisateur y a accès. Si l'utilisateur perd son mot de passe, il perd également sa clé de signature. Lors du processus de récupération, il retrouve sa paire de clés de chiffrement/déchiffrement, mais une nouvelle paire de clés de signature/vérification est générée. Cela ne pose aucun problème étant donné que chaque fois qu'un utilisateur signe un document, le certificat de vérification correspondant y est annexé, de sorte que la signature du document peut être vérifiée à n'importe quel moment.

---

<sup>11</sup> La sauvegarde des clés privées est également utilisée pour la garde en fiducie des clés; en d'autres termes, comme moyen pour l'entreprise ou un tiers habilité d'accéder aux fichiers utilisateurs pouvant contenir des renseignements irremplaçables qui, autrement, seraient perdus à jamais.

<sup>12</sup> Supposons, par exemple, qu'à la dernière mise à jour de ses clés, Alice a reçu la paire CPuAn/CPrAn et qu'elle a gardé un message qui avait été chiffré à l'aide de CPuA1, sa première clé publique. Elle doit alors utiliser CPrA1 pour déchiffrer le message.

**En conclusion**

La cryptographie à clé publique est extrêmement attrayante et riche en perspectives, intégrant à la fois le chiffrement et la signature numérique. Elle constitue une véritable percée par rapport aux systèmes cryptographiques à clé symétrique.

Au-delà de l'aspect technique, il faut voir la nécessité de mettre en place une architecture, soit une ICP, qui comprend les outils nécessaires pour gérer et utiliser efficacement les clés et certificats. La section 3.1 donne un aperçu de la façon dont une ICP bien gérée répond aux principales préoccupations en matière d'utilisation et de gestion des clés et certificats. Nous en traiterons plus en détail dans un autre article.

Pour terminer, au-delà de l'infrastructure même, il y a lieu de préparer, d'étayer et de maintenir cette infrastructure. D'un point de vue technique, la mise en œuvre d'une ICP est une question de jours. D'un point de vue affaires, la mise en œuvre d'une ICP est une toute autre histoire... qui fera l'objet d'un autre article.

## Références

- [1] Curry, Ian, Entrust Technologies, «Getting Acquainted With Entrust/Solo and Public-key Cryptography», version 1.0, juillet 1997
- [2] Netscape, «Introduction to Public-Key Cryptography»,  
<http://developer.netscape.com/docs/manuals/security/pkin/contents.htm>
- [3] Curry, Ian, Entrust Technologies, «Version 3 X.509 Certificates», version 1.0, juillet 1996
- [4] Branchaud, Marc, «A Survey of Public-key Infrastructures», Département d'informatique, Université McGill, Montréal, 1997
- [5] Curry, Ian, Entrust Technologies, «Key Update and the Complete story on the Need for Two Key Pairs», version 1.2, août 2000
- [6] RSA, «Intro to PKCS Standards»,  
<http://www.rsasecurity.com/solutions/developers/whitepapers/IntroToPKCSstandards.pdf>
- [7] Site Web de l'IETF/PKIX, <http://www.ietf.org/html.charters/pkix-charter.html>

[m1]J'ai modifié légèrement la figure