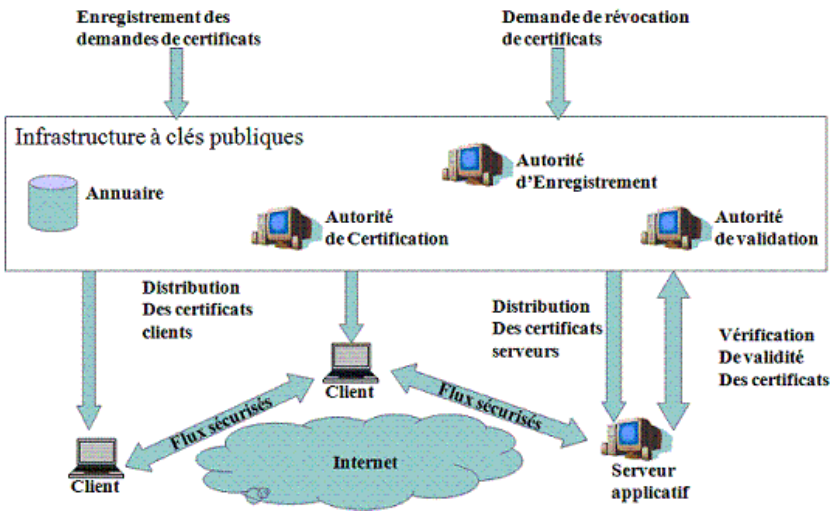
ierie des Protocoles et Logiciels Sécurisés

Infrastructures à Clés Publiques

Version 1



YACINE CHALLAL

14/01/2015

Table des matières

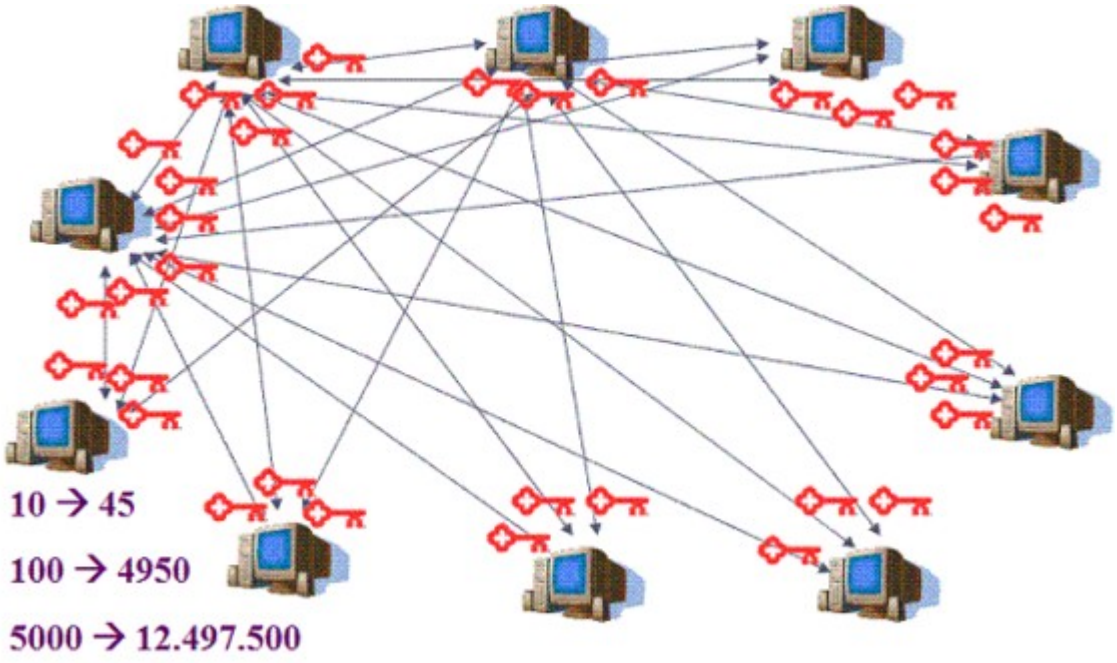
I

PKI : Infrastructures à clés publiques

A. Systèmes asymétriques : atouts et limites

La gestion des clés est plus facile avec les systèmes asymétriques

Dans ce scénario, si le réseau est composé de n noeud alors il faudra gérer n.(n-1)/2 clé, ce qui ne s'adapte pas au facteur d'échelle. Avec 500 noeud, on arrive déjà à plus de 12 millions de clés à gérer.



Limites de la gestion de clés symétriques

Par contre, avec un système asymétrique chaque utilisateur aura besoin d'une paire de clés. Donc on aura à gérer seulement 2.n clés au lieu des n.(n-1)/2 clés dans le cas symétrique.

Utilité d'un système asymétrique dans l'authentification

Nous avions déjà vus que l'usage d'un système asymétrique est indispensable pour

garantir la non-répudiation de l'origine.

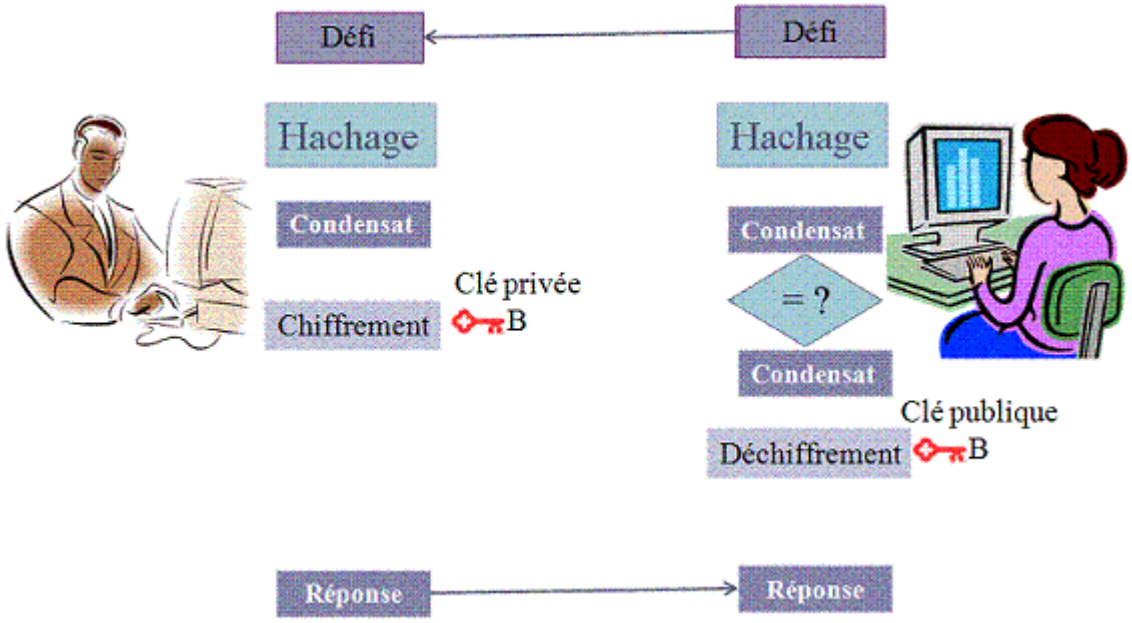
L'usage d'un système asymétrique est également utile pour l'identification comme expliqué plus bas.

Dans ce scénrio, Alice veut s'assurer de l'identité de Bob. Elle ne connaît de Bob que sa clé publique.

Pour s'assurer de l'identité de Bob, Alice lui envoie un défi (un nombre aléatoire).

Pour prouver son identité à Alice, Bob signe le défi avec sa clé privée et envoie sa signature sur le défi à Alice.

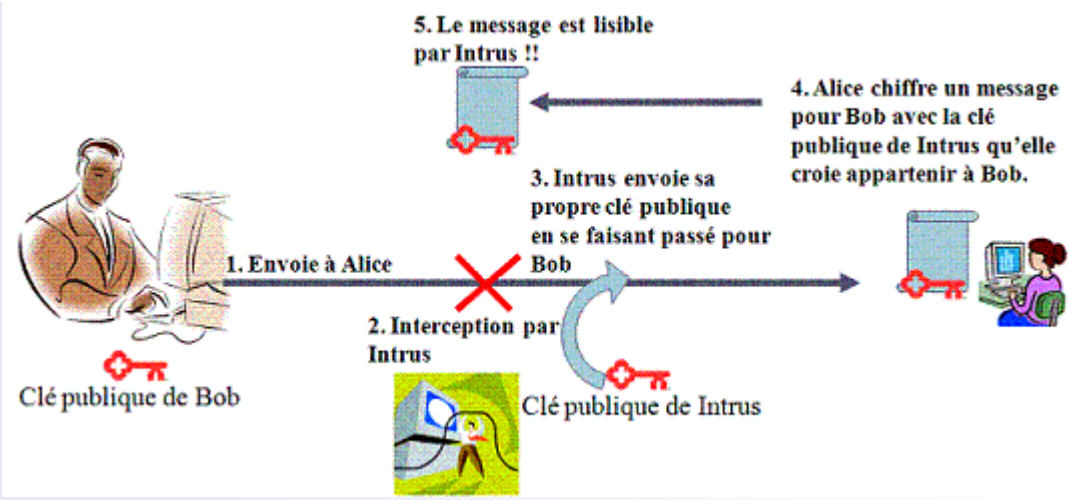
Pour vérifier l'identité de Bob, il suffit que Alice vérifie la signature de Bob avec sa clé publique comme illustré sur la figure ci-contre.



Identification avec un système asymétrique

Attention : Comment garantir qu'une clé publique correspond bien à l'entité avec qui on communique ?

Jusque là, nous avions toujours supposé que la clé publique est distribuée d'une manière sécurisée. Si cette hypothèse n'est pas vérifiée, un schéma asymétrique peut subir une attaque de type "Man in the Middle". Une telle attaque est illustrée dans le scénario ci-après.



Man in the middle

Méthode : Certification numérique

La solution au problème dit "man in the middle" est l'usage d'un certificat numérique qui assure la liaison entre l'identité et la clé publique correspondante dans un document numérique signé par une tierce partie de confiance dite autorité de certification.

B. La certification numérique

Définition : Certificat numérique

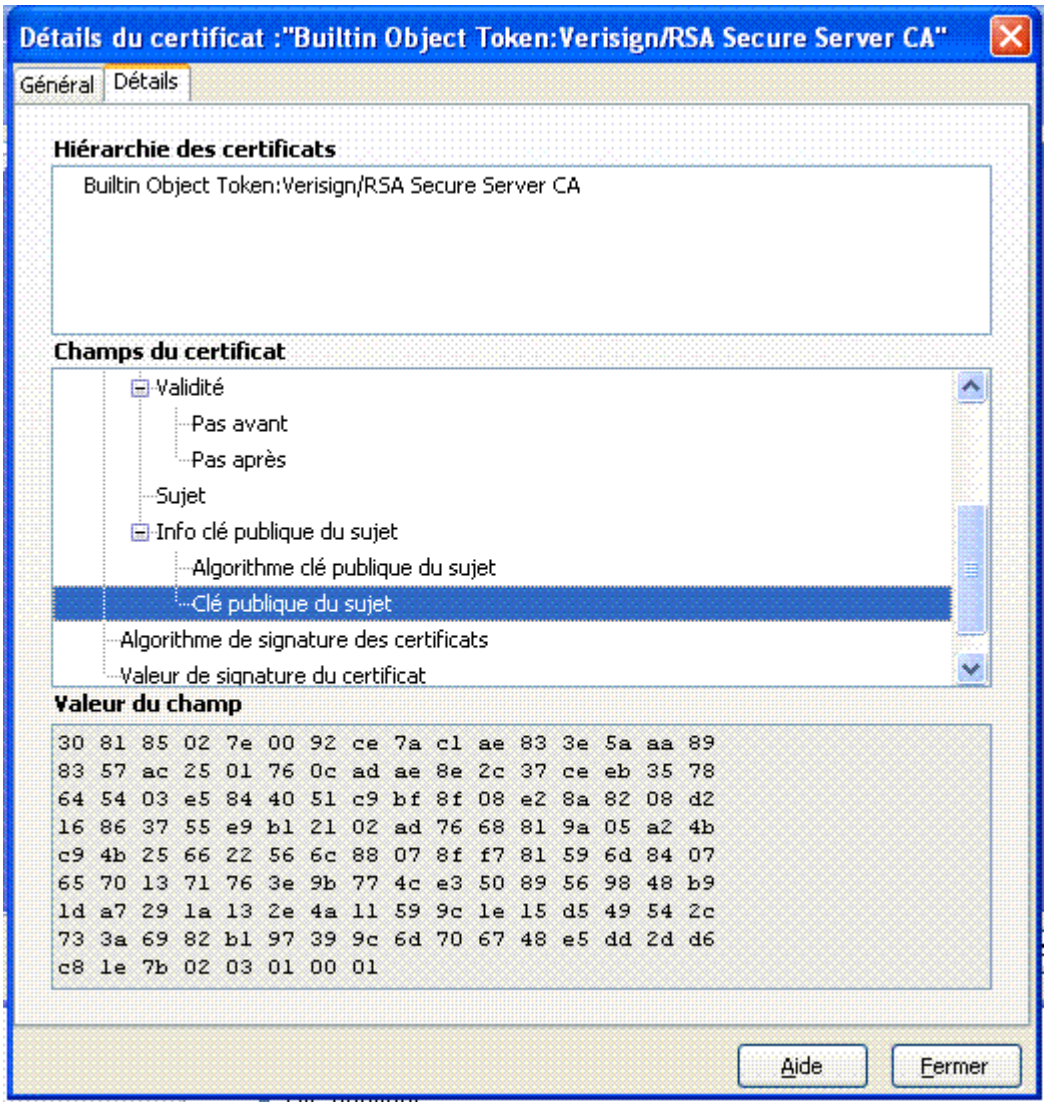
- Un certificat à clé publique est un certificat numérique qui lie l'identité d'un système à une clé publique, et éventuellement à d'autres informations;
- C'est une structure de donnée signée numériquement qui atteste sur l'identité du possesseur de la clé privée correspondante à une clé publique.
- Un certificat est signé numériquement par une autorité de certification à qui font confiance tous les usagers et dont la clé publique est connue par tous d'une manière sécurisée. Ainsi, afin de publier sa clé publique, son possesseur doit fournir un certificat de sa clé publique signé par l'autorité de certification. Après vérification de la signature apposée sur le certificat en utilisant la clé publique de l'autorité de certification, le récepteur peut déchiffrer et vérifier les signatures de son interlocuteur dont l'identité et la clé publique sont inclus dans le certificat.

Exemple : Structure d'un certificat X.509

- Version
- Numéro de série
- Algorithme de signature du certificat
- Signataire du certificat
- Validité (dates limite)
  - Pas avant
  - Pas après
- Détenteur du certificat
- Informations sur la clé publique
  - Algorithme de la clé publique

  - Clé publique
- Identifiant unique du signataire (Facultatif)
- Identifiant unique du détenteur du certificat (Facultatif)
- Extensions (Facultatif)
  - Liste des extensions...

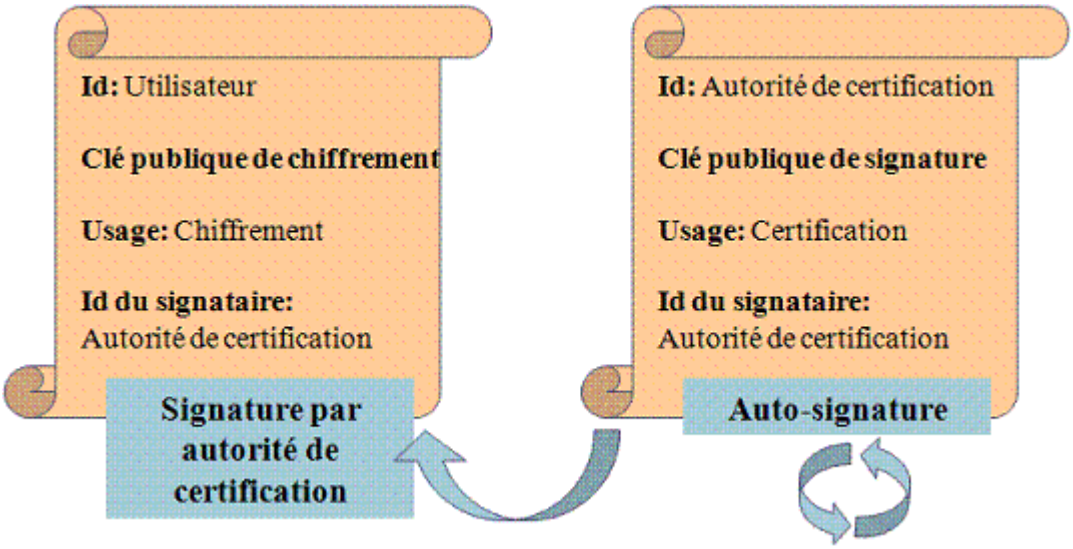
La figure suivante illustre un tel certificat inclus dans un navigateur web



Certificat Numérique

Définition : Autorité de certification

Une autorité de certification est toute entité qui délivre des certificats de clé publique



Autorité de certification

Remarque : Auto signature

Une autorité de certification auto-signe son certificat numérique. ceci ne posant pas de problème puisque la clé publique d'une autorité de certification est censée connue d'une manière sécurisée (remise en main propre pas exemple).

Autorité de certification et confiance

L'autorité de certification certifie la correspondance Clé publique – Identité pour l'ensemble d'une population. Ceci mène à faire régner la confiance par transitivité :

- A fait confiance à l'Autorité de Certification
- L'Autorité de Certification délivre un certificat à B
- A est assuré de l'identité de B

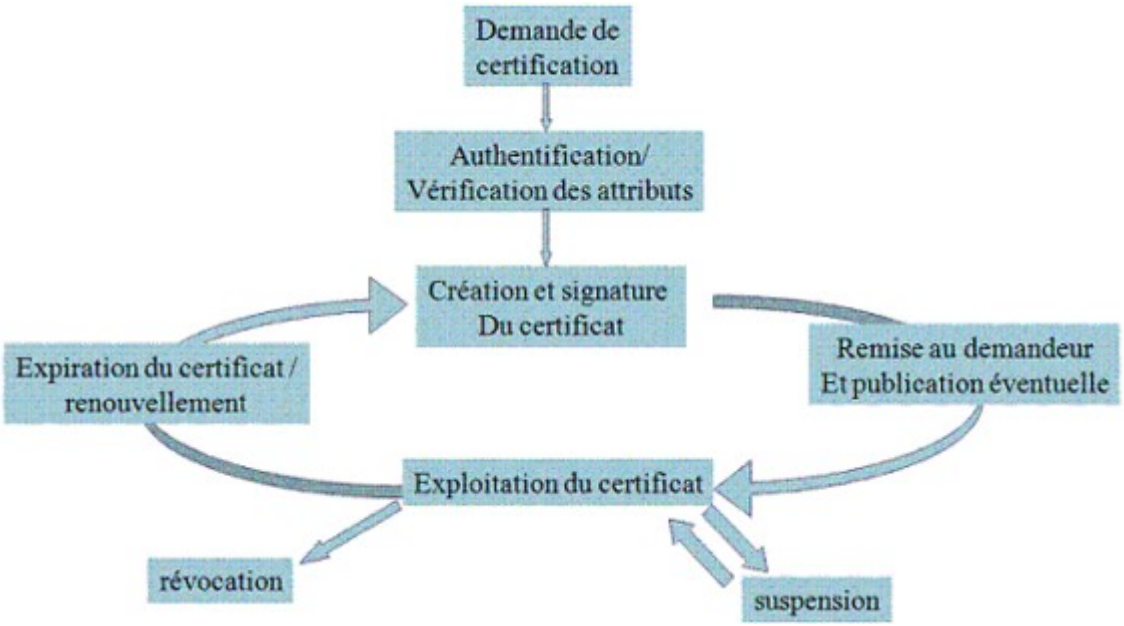
C. PKI : Infrastructure à clés publiques

Définition : Infrastructure à clés publiques

« Ensemble de composants, fonctions et procédures dédié à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique ». [Politique de certification type: Ministère de l'Economie, des Finances et de l'Industrie, Fr]

Méthode : Cycle de vie d'un certificat

La figure suivante illustre le cycle de vie d'un certificat de sa délivrance et à sa destruction



Cycle de vie d'un certificat numérique

Fonctions d'une PKI

Enregistrer et vérifier les demandes de certificats

- Autorité d'enregistrement

Créer et distribuer des certificats

- Autorité de certification

Vérification de validité de certificats

- Autorité de validation

Gérer à tout moment l'état des certificats et prendre en compte leur révocation

- Dépôt de listes de certificats révoqués – CRL (Certificate Revocation List)

Publier les certificats dans un dépôt

- Dépôt de certificats (Annuaire)

Modèles de confiance dans les PKI

Modèle monopoliste

- Une CA pour tout le monde

Modèle monopoliste avec Autorités d'enregistrement

- Une CA avec plusieurs RAs pour la vérification des identités, ...

Délégation de pouvoir de certification

- Une CA délègue le pouvoir de certification à d'autres entités qui deviennent CA à leur tour, en leur fournissant un certificat qui certifie leur capacité d'être CA.

Modèle oligarchique

- Déploiement des produits (comme les navigateur web) avec plusieurs entités de confiance qui sont des CA. Le navigateur fera confiance à tout certificat signé par l'une de ces CA dans sa liste

Modèle anarchique

- Chaque utilisateur établit la liste des entités à qui il fait confiance

Validation de certificat

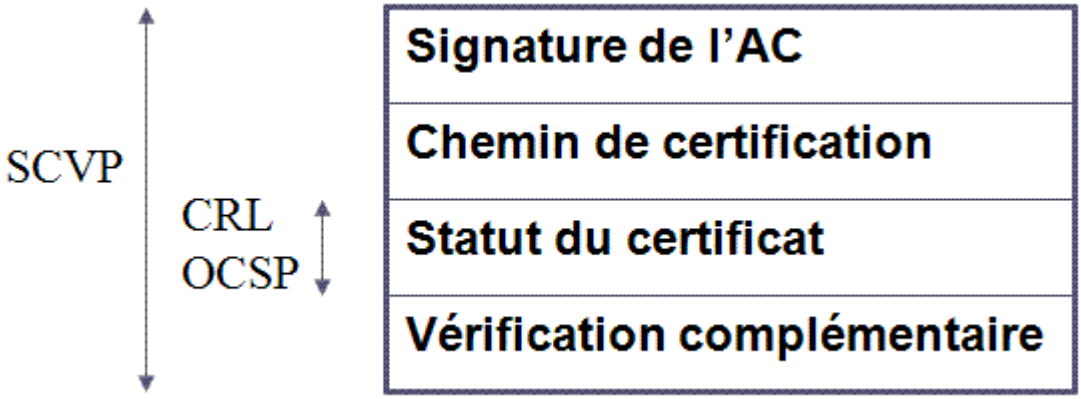
Pour pouvoir se fier au contenu d'un certificat, il est nécessaire de réaliser les vérifications suivantes:

Vérification	Commentaire
Signature de l'AC	L'application doit vérifier que le certificat est intègre et authentique
Chemin de certification	L'application doit vérifier qu'il existe une chaîne de certificats valide permettant de remonter à une AC de confiance
Période de validité	L'application doit vérifier que le certificat présenté n'est pas expiré
Statut du certificat	L'application doit vérifier que le certificat n'est pas révoqué (ni suspendu)

Validation d'un certificat numérique

Il existe par ailleurs différents moyens et techniques standards pour offrir ce service

- Vérification du statut du certificat par récupération régulière de CRL
- Vérification du statut du certificat en ligne : OCSP (On-line Certificate Status Protocol)
- Vérification complète du certificat en ligne : SCVP (Simple Certificate Validation Protocol)



Protocoles de vérification de certificats

Attention : Révocation de certificats

Un certificat peut être révoqué. La révocation intervient quand la fin de validité réelle précède la fin de validité prévue. La révocation peut avoir plusieurs motifs :

- Compromission réelle ou suspectée de la clé privée
- Modification d'un au moins de attributs certifiés
- Perte de la clé privée (effacement d'un disque dur, perte ou détérioration d'une carte à puce, oubli du code PIN, ...)

- Évolution de l'état de l'art cryptographique (la cryptanalyse de la clé privée entre dans le domaine du possible)
- Perte de confiance vis-à-vis d'un acteur ou d'un composant de la PKI

Le demandeur doit être habilité et authentifié

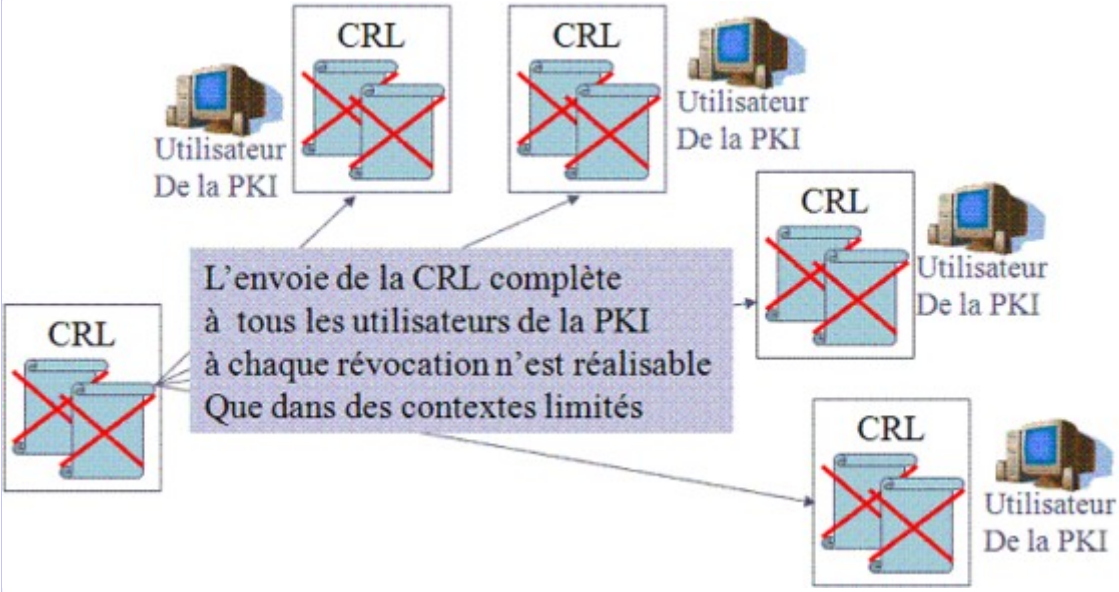
- Le propriétaire du certificat
- Son supérieur hiérarchique
- Le service de gestion du personnel ...

La méthode de révocation dépend de la méthode de validation

- Utilisation d'annuaire « positif » ==> La révocation consiste à enlever le certificat révoqué de l'annuaire
- Utilisation d'un annuaire « négatif » ou CRL ==> La révocation consiste à inscrire le certificat dans une liste de révocation de certificat

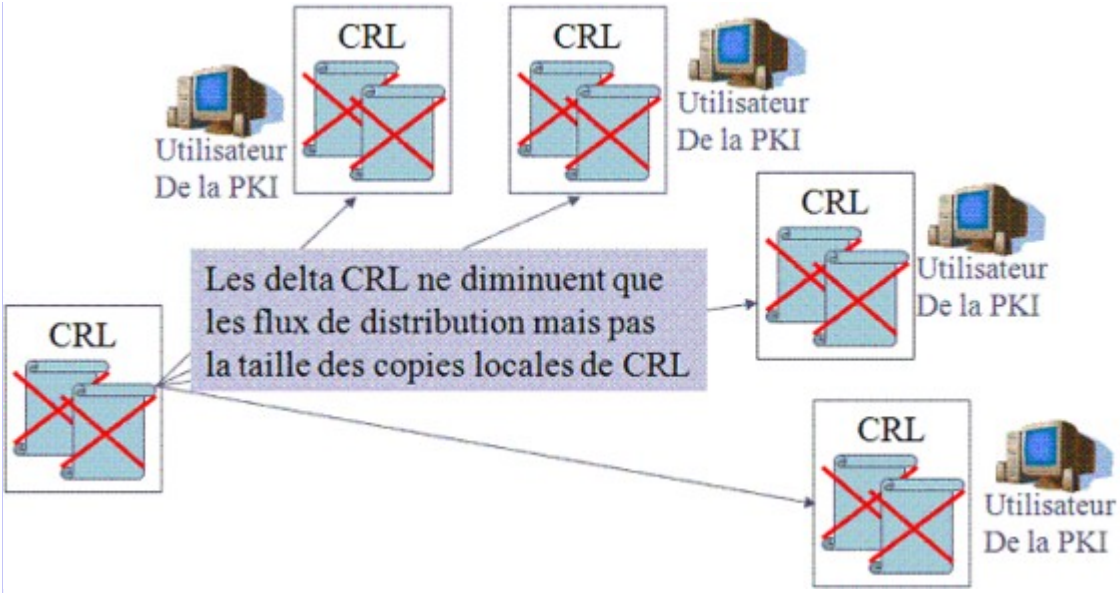
Remarque : La gestion des CRL

La gestion des CRL peut devenir complexe et lourde :



Gestion des CRL

Les delta CRL ne contiennent que les changements depuis la dernière diffusion :



Gestion des delta CRL

Fondamental : Schéma fonctionnel simplifié d'une PKI

En résumé, voici les différents composants d'une PKI :

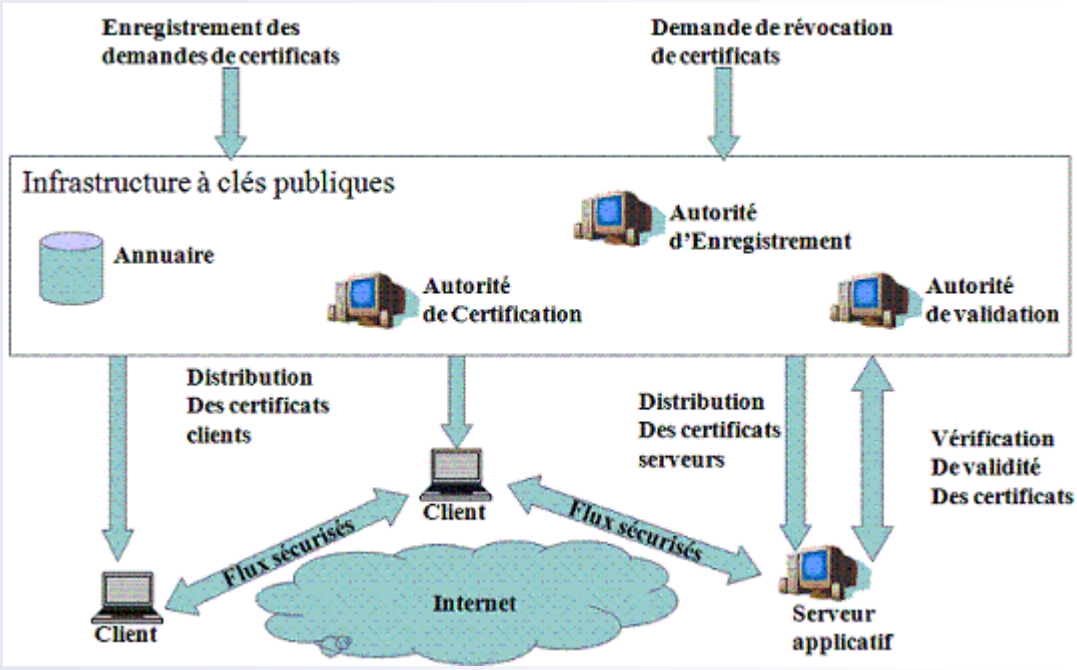


Schéma fonctionnel d'une PKI

D. Secure Socket Layer : SSL

Aperçus générale

SSL/TLS est un protocole de sécurisation des échanges développé par Netscape. Il assure les transactions Client / Serveur sur Internet. Il a été intégré dans les navigateurs web depuis 1994. La vesrion 3.1 est baptisée Transport Layer Security TLS. Cette version a été standardisée à l'IETF: RFC 2246. Le protocole fonctionne au dessus de la couche TCP

Services de sécurité assurés par SSL

Confidentialité

- Obtenue par chiffrement symétrique

Intégrité

- En utilisant des MAC : MD5(128 bits), SHA1(160 bits)

Authentification

- Identification des deux entités (client optionnel) basée sur les certificats X. 509
- Authentification de l'origine des données basée sur des MAC

Sous protocoles de SSL

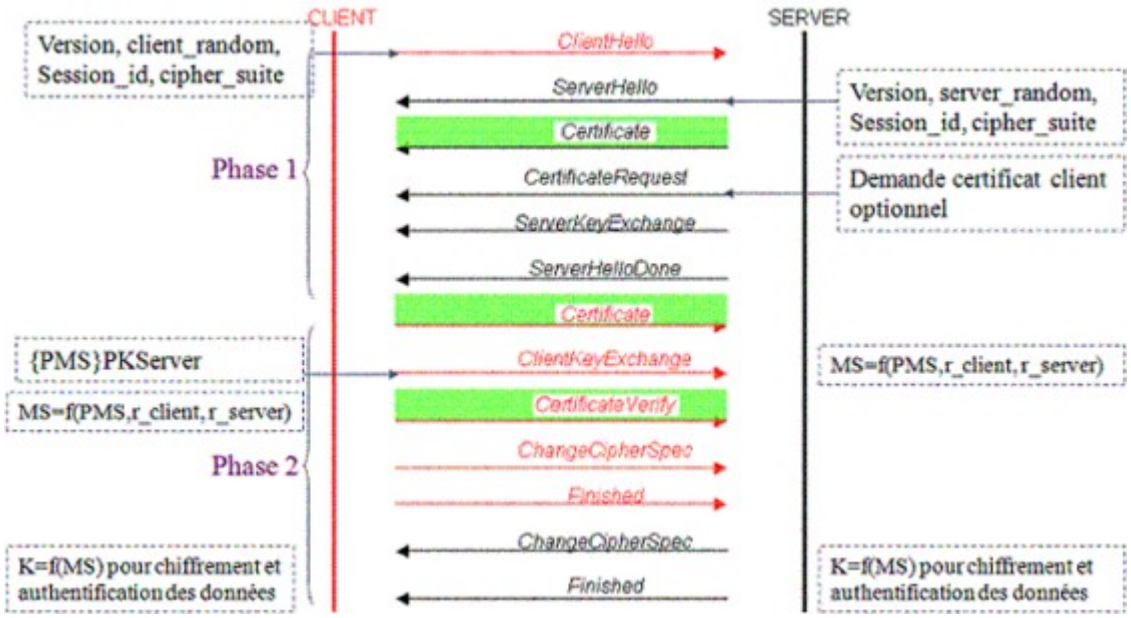
SSL se déroule selon quatre sous protocoles

1. Handshake
   - Authentification mutuelle
   - Négociation des algorithmes de chiffrement et de hachage
   - Échange des clés symétriques
2. Change Cipher Spec
   - Indiques la mise en place des algorithmes de chiffrement négocié
3. Record
   - Garantir la confidentialité à l'aide du chiffrement, et L'authentification à l'aide de condensât
4. Alert
   - Émission de messages d'alertes suites aux erreurs que peuvent s'envoyer le client et le serveur

Déroulement du protocole SSL

SSL se déroule en deux phases

1. Phase 1: authentification du serveur
   - Requête client
   - Le serveur envoie son certificat et une liste d'algo de crypto à négocier
   - Le client vérifie le certificat du serveur à l'aide de la clé publique du CA contenu dans le navigateur
   - Le client génère un pré-master secret (PMS)(48 octets) qui sera utilisé pour générer le master-key (48 octets).
   - PMS est chiffré avec la clé publique du serveur
   - Les données échangées entre le client et le serveur seront chiffrées et authentifiées avec des clés dérivées du master-secret
2. Phase 2: authentification du client
   - Le serveur peut demander au client de s'authentifier en lui demandant son certificat
   - Le client répond en envoyant son certificat puis en signant un message avec sa clé privé (contient des info sur la session et le contenu des messages précédents)



Le protocole SSL/TLS

Testez vos connaissances

II

A. Man in the Middle

Soit le protocole cryptographique suivant
M1 : B ==> A : B.PKb
M2 : A ==> B : {m}PKb
Ce protocole est vulnérable à une attaque de type « man in the middle ». Un intrus "I" peut attaquer ce protocole comme suit :

- ☐ I intercepte M1
I bloque M1
I remplace M1 par : M1 : I ==> B : A.PKi
I intercepte M2
I bloque M2
I remplace M2 par : M2 : I ==> A : {m}PKa
- ☐ I intercepte M1
I bloque M1
I remplace M1 par : M1 : I ==> A : B.PKi
I intercepte M2
I bloque M2
I remplace M2 par : M2 : I ==> B : {m}PKb
- ☐ I intercepte M1
I bloque M1
I remplace M1 par : M1 : I ==> A : B.SKb
I intercepte M2
I bloque M2
I remplace M2 par : M2 : I ==> B : {m}PKb

B. Certificat numérique

L'objectif d'un certificat numérique est d'assurer

☐	La confidentialité de la signature numérique du porteur du certificat
☐	L'authenticité de la clé publique correspondante à la clé privée du porteur du certificat
☐	La correspondance entre l'identité et la clé publique correspondante à la clé privée du porteur du certificat
☐	L'authenticité de la signature numérique de l'autorité de certification

C. SSL

Le protocole SSL/TLS permet d'assurer

☐	Le contrôle d'intégrité
☐	La confidentialité des échanges entre le client et le serveur
☐	L'authentification de l'origine de données
☐	L'authentification du serveur optionnellement
☐	L'authentification du client optionnellement

Série d'exercices II: Infrastructures à clés publiques

III

A. Télé-déclaration des revenus

Le ministère des finances décide d'automatiser la déclaration des revenus annuels imposables. Il existe une recette des impôts au niveau de chaque mairie, mais vu l'absence d'un réseau privé reliant ces structures administratives, le ministère décide de réaliser l'opération à travers le web. Ainsi, chaque personne physique ou morale concernée (commerçant, agriculteur, entreprise, ...) devrait pouvoir faire sa déclaration de revenus en utilisant un navigateur web. Le ministère met à disposition des citoyens un site web qui collectera les revenus déclarés en vu de les stocker dans une base de données. Le ministère fait appel à votre expertise et vous remet un cahier de charge, dans lequel on peut souligner les points suivants :

1. Le système de télé-déclaration fiscale doit être conforme à la loi 15-04 sur la certification électronique. Le texte de loi est joint à ce cahier de charge (cf Loi1504 certification Electronique).
2. Les déclarations doivent rester confidentielles ;
3. Chaque déclarant doit être authentifié avant de procéder à la déclaration ;
4. Afin de donner une valeur légale aux déclarations, les déclarants doivent signer numériquement leur déclaration ;
5. Les structures du ministère ne seront pas disposées à recevoir les déclarants. Tout rapprochement nécessaire de l'administration fiscale devrait se faire au niveau des recettes des impôts des mairies.

Question 1

Proposez une architecture, à base d'une PKI, pour sécuriser le système de télé déclaration tout en répondant au cahier de charge du ministère des finances.

Question 2

Citez puis expliquez succinctement comment les protocoles et mécanismes cryptographiques, que vous introduisez, réalisent les impératifs du cahier de charge.

Question 3

Expliquez comment déployer votre système à l'échelle nationale.

B. Travail Pratique : Sécuriser l'échange entre un client et un serveur web Apache avec SSL

Objectifs

Se familiariser avec les concepts d'une infrastructure à clés publiques :

- Déploiement de PKI
- Création d'une autorité de certification
- Création de certificats numériques
- Signature de certificats numériques

Configuration de la sécurité d'un serveur web Apache avec le protocole SSL

Configuration d'un navigateur Web pour l'authentification d'un client et d'un serveur web avec SSL.

Installation et environnement logiciel

Pour avoir plus de détails sur les commandes de OpenSSL et leurs options, vous pouvez vous référer au manuel suivants :

Pour réaliser ces ateliers vous devez disposer de OpenSSL, Apache et TinyCA, qui sont déjà installés sur la machine virtuelle.

Attention

- Il faut remplacer partout dans les commandes ci-dessous /opt/lampp par le chemin exacte vers votre installation de Apache
- Penser toujours à sauvegarder la dernière version d'un fichier de configuration avant une nouvelle modification.

1. Créer un espace de Publication Web Apache

Syntaxe

1. Création d'un répertoire pour le test "delta" sous le DocumentRoot de apache: "htdocs"
2. Modifier le fichier lampp/etc/httpd.conf en conséquence :
   - #DocumentRoot "/opt/lampp/htdocs"
   - DocumentRoot "/opt/lampp/htdocs/delta"
   - #<Directory "/opt/lampp/htdocs">
   - <Directory "/opt/lampp/htdocs/delta">
3. Mettre une page web dans ce répertoire "delta": "index.html"
4. Relancer apache : sudo ./lampp restart
5. Tester avec le navigateur: http://localhost

Ceci va constituer la zone libre accès du serveur

2. Créer un répertoire pour la zone sécurisée

Syntaxe

1. Sous "htdocs/delta" créer un répertoire "secure"
2. Modifier le fichier config "httpd-ssl.conf" en conséquence. Ce fichier se trouve sous "/opt/lampp/etc/extra".
   - #DocumentRoot "/opt/lampp/htdocs"
   - DocumentRoot "/opt/lampp/htdocs/delta/secure"

3. Mettre une page web dans ce répertoire "delta/secure": "index.html"

3. Créer les certificats et les clés pour la CA et le Serveur Web

Syntaxe

1. Création du certificat du CA
   Utiliser TinyCA pour générer la clé privée et certificat du CA (commande tinyca2)
2. Sous le répertoire "lampp/etc" créer un répertoire "delta" et deux sous-répertoires "delta/certifs" et "delta/cles". Ces deux répertoires serviront à stocker les certificats et les clés de CA et de notre serveur.
3. Création du certificat du serveur
   Utiliser TinyCA pour générer une clé privée du serveur Web dans le fichier /opt/lampp/etc/delta/cles/serveurkey.pem et un certificat signé par la CA dans /opt/lampp/etc/delta/certifs/serveurcert.pem
   Lors de la création du certificat du serveur web, il faut donner le nom du serveur qui est indiqué dans /opt/lamp/etc/extra/httpd-ssl.conf, par exemple : localhost, et laisser le champ email vide.
   Quand vous exportez la clé privée du serveur, choisissez (Sans mot de passe PKCS12) pour éviter que Apache ne se bloque en l'attente de saisie du mot de passe.
4. Modifier le fichier config "httpd-ssl.conf" en conséquence. Ce fichier se trouve sous "lampp/etc/extra".
   - #SSLCertificateFile /opt/lampp/etc/ssl.crt/server.crt
   - SSLCertificateFile /opt/lampp/etc/delta/certifs/serveurcert.pem
   - #SSLCertificateKeyFile /opt/lampp/etc/ssl.key/server.key
   - SSLCertificateKeyFile /opt/lampp/etc/delta/cles/serveurkey.pem

4. Les tests

Syntaxe

1. Relancer apache
2. On teste "https://localhost"
   Ca nous demande si on accepte le certificat du serveur: On regarde les détails du certificat et on accepte temporairement (pour la session)
   Redémarrer le navigateur pour voir que de nouveau le certificat n'est pas accepté automatiquement.
3. Exporter le certificat du CA en utilisant tinyca2
   Inclure ce certificat du CA dans le navigateur et on se connecte de nouveau, si le certificat respecte certaines règles il sera accepté automatiquement car signé par un CA reconnu par le navigateur

5. Analyse et comparaison des échanges

Analyser et comparer les échanges entre le client (navigateur) et le serveur (serveur web) dans les deux configurations : HTTP simple, HTTPS.

Pour cela, utilisez WireShark (un sniffer)

6. Ajouter un certificat Client

Syntaxe

1. Création du certificat du client
   En utilisant TinyCA générer la clé du Client dans /opt/lampp/etc/delta/cles/clientkey.pem et un certificat Client dans /opt/lampp/etc/delta/certifs/clientcert.pem
2. Modification de apache en conséquence pour que le serveur exige un certificat pour le client:
   #SSLCACertificatePath /opt/lampp/etc/ssl.crt
   #SSLCACertificateFile /opt/lampp/etc/ssl.crt/ca-bundle.crt
   SSLCACertificatePath /opt/lampp/etc/delta/certifs/
   SSLCACertificateFile /opt/lampp/etc/delta/certifs/cacert.pem
   #SSLVerifyClient require
   #SSLVerifyDepth 10
   SSLVerifyClient require
   SSLVerifyDepth 2
3. On relance apache et on teste
4. On ajoute le certificat client dans le navigateur
   Pour mozilla/firefox un certificat en format PKCS12 est demandé
   En utilisant TinyCA on peut générer le certificat dans ce format conf\delta\certifs\clientcert.p12
   Dans le navigateur on ajoute "clientcert.p12" dans "your certificates"
5. On relance apache et on teste

Art. 18. — Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 100.000 DA à 500.000 DA, tout titulaire d'un certificat électronique qui continue à l'utiliser tout en sachant que ledit certificat est arrivé à échéance ou révoqué.

Art. 19. — La présente loi sera publiée au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le 11 Rabie Ethani 1436 correspondant au 1er février 2015.

Abdelaziz BOUTEFLIKA.

———★———

Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques.

———

Le Président de la République,

Vu la Constitution notamment, ses articles 119, 120, 122, 125 et 126 ;

Vu l'ordonnance n° 66-155 du 8 juin 1966, modifiée et complétée, portant code de procédure pénale ;

Vu l'ordonnance n° 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal ;

Vu l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil ;

Vu l'ordonnance n° 75-59 du 26 septembre 1975, modifiée et complétée, portant code de commerce ;

Vu la loi n° 84-17 du 7 juillet 1984, modifiée et complétée, relative aux lois de finances ;

Vu la loi n° 88-01 du 12 janvier 1988 portant loi d'orientation sur les entreprises publiques économiques ;

Vu la loi n° 90-21 du 15 août 1990, modifiée et complétée, relative à la comptabilité publique ;

Vu la loi n° 2000-03 du 5 Joumada El Oula 1421 correspondant au 5 août 2000, modifiée, fixant les règles générales relatives à la poste et aux télécommunications ;

Vu l'ordonnance n° 03-03 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003, modifiée et complétée, relative à la concurrence ;

Vu la loi n° 04-02 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004, modifiée et complétée, fixant les règles applicables aux pratiques commerciales ;

Vu la loi n° 04-04 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004 relative à la normalisation ;

Vu la loi n° 04-08 du 27 Joumada Ethania 1425 correspondant au 14 août 2004, modifiée et complétée, relative aux conditions d'exercice des activités commerciales ;

Vu la loi n° 08-09 du 18 Safar 1429 correspondant au 25 février 2008 portant code de procédure civile et administrative ;

Vu la loi n° 09-03 du 29 Safar 1430 correspondant au 25 février 2009 relative à la protection du consommateur et à la répression des fraudes ;

Vu la loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication ;

Après avis du Conseil d'Etat ;

Après adoption par le Parlement ;

Promulgue la loi dont la teneur suit :

TITRE I

DISPOSITIONS GENERALES

Chapitre 1er

Objet

Article 1er. — La présente loi a pour objet de fixer les règles générales relatives à la signature et à la certification électroniques.

Chapitre 2

Définitions

Art. 2. — Il est entendu par :

1- Signature électronique : données sous forme électronique, jointes ou liées logiquement à d'autres données électroniques, servant de méthode d'authentification.

2- Signataire : personne physique qui détient des données de création de signature électronique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente.

3- Données de création de signature électronique : données uniques, telles que des codes ou des clés cryptographiques privés, que le signataire utilise pour créer une signature électronique.

4- Dispositif de création de signature électronique : matériel ou logiciel destiné à mettre en application les données de création de signature électronique.

5- Données de vérification de signature électronique : des codes, des clés cryptographiques publiques ou d'autres types de données, qui sont utilisées pour vérifier une signature électronique.

6- Dispositif de vérification de signature électronique : matériel ou logiciel destiné à mettre en application les données de vérification de signature électronique.

7- Certificat électronique : document sous forme électronique attestant du lien entre les données de vérification de signature électronique et le signataire.

8- Clé cryptographique privée : chaîne de chiffres détenue exclusivement par le signataire et utilisée pour créer une signature électronique, cette clé est liée à une clé cryptographique publique.

9- Clé cryptographique publique : chaîne de chiffres mise à la disposition du public afin de lui permettre de vérifier la signature électronique, elle est insérée dans le certificat électronique.

10- Autorisation : désigne le régime d'exploitation de services de certification électronique et se matérialise par le document officiel délivré au prestataire de manière personnelle lui permettant de commencer la fourniture effective de ses services.

11- Tiers de confiance : personne morale qui délivre des certificats électroniques qualifiés ou éventuellement fournit d'autres services en matière de certification électronique au profit des intervenants dans la branche gouvernementale.

12- Prestataire de services de certification électronique : personne physique ou morale qui délivre des certificats électroniques qualifiés et fournissant éventuellement d'autres services en matière de certification électronique.

13- Intervenants dans la branche gouvernementale : institutions et administrations publiques, établissements publics tels que définis par la législation en vigueur, institutions nationales autonomes, autorités de régulation, intervenants dans les échanges interbancaires, ainsi que toute personne ou entité qui de par sa nature ou mission fait partie de la branche gouvernementale.

14- Titulaire de certificat électronique : personne physique ou morale à laquelle un prestataire de services de certification ou un tiers de confiance a délivré un certificat électronique.

15- Politique de certification électronique : ensemble des règles et procédures organisationnelles et techniques liées à la signature et à la certification électroniques.

16- Audit : vérification de la conformité par rapport à un référentiel.

Chapitre 3

Principes généraux

Art. 3. — Sans préjudice de la législation en vigueur, nul ne peut être contraint d'accomplir un acte juridique signé électroniquement.

Art. 4. — Le document signé électroniquement est conservé dans sa forme d'origine. Les modalités de conservation du document signé électroniquement sont définies par voie réglementaire.

Art. 5. — Toutes les données et informations à caractère personnel recueillies par les prestataires de service de certification électronique, les tiers de confiance et les autorités de certification électronique ainsi que les bases de données qui les contiennent doivent être hébergées sur le territoire national et ne peuvent être transférées en dehors de celui–ci que dans les cas prévus par la législation en vigueur.

TITRE II

DE LA SIGNATURE ELECTRONIQUE

Chapitre 1er

Principes d'assimilation et de non-discrimination de la signature électronique

Art. 6. — Une signature électronique a pour fonction d'authentifier l'identité du signataire et de manifester l'adhésion de ce dernier au contenu de l'écrit sous forme électronique.

Art. 7. — La signature électronique qualifiée est une signature électronique qui satisfait aux exigences suivantes :

1- être réalisée sur la base d'un certificat électronique qualifiée,

2- être liée uniquement au signataire,

3- permettre l'identification du signataire,

4- être conçue au moyen d'un dispositif sécurisé de création de signature électronique,

5- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif,

6- être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée.

Art. 8. — Seule la signature électronique qualifiée est assimilée à une signature manuscrite, qu'elle soit le fait d'une personne physique ou morale.

Art. 9. — Nonobstant les dispositions de l'article 8 suscité, une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif qu'elle :

1. se présente sous forme électronique, ou

2. ne repose pas sur un certificat électronique qualifié, ou

3. n'est pas créée par un dispositif sécurisé de création de signature électronique.

Chapitre 2

Des dispositifs de création et de vérification de la signature électronique qualifiée

Art. 10. — Le dispositif de création de la signature électronique qualifiée doit être sécurisé.

Art. 11. — Le dispositif sécurisé de création de signature électronique est un dispositif de création de signature électronique qui satisfait aux exigences suivantes :

1- il doit, au moins, garantir, par les moyens techniques et les procédures appropriées, que :

a. les données utilisées pour la création de la signature électronique ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit assurée par tous les moyens techniques disponibles au moment de l'homologation ;

b. les données utilisées pour la création de la signature électronique ne puissent être trouvées par déduction et que la signature électronique soit protégée contre toute falsification par les moyens techniques disponibles au moment de l'homologation ;

c. les données utilisées pour la création de la signature électronique puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2- il ne doit pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

Art. 12. — Le dispositif de vérification de la signature électronique qualifiée doit être fiable.

Art. 13. — Le dispositif fiable de vérification de la signature électronique est un dispositif de vérification de la signature électronique qui satisfait aux exigences suivantes :

1. les données utilisées pour vérifier la signature électronique correspondent aux données affichées lors de la vérification de la signature électronique ;

2. la signature électronique soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché ;

3. le contenu des données signées puisse être, si nécessaire, déterminé de manière sûre lors de la vérification de la signature électronique ;

4. l'authenticité et la validité du certificat électronique requis lors de la vérification de la signature électronique soient vérifiées de manière sûre ;

5. le résultat de la vérification ainsi que l'identité du signataire soient clairement et correctement affichés.

Art. 14. — La conformité du dispositif sécurisé de création de signature électronique qualifiée et du dispositif fiable de vérification de signature électronique qualifiée aux exigences édictées aux articles 11 et 13 ci-dessus est attestée par l'entité nationale en charge de l'homologation des dispositifs de création et de vérification de la signature électronique.

TITRE III

DE LA CERTIFICATION ELECTRONIQUE

Chapitre 1er

Du certificat électronique qualifié

Art. 15. — Le certificat électronique qualifié est un certificat électronique qui satisfait aux exigences suivantes :

1. être délivré par un tiers de confiance ou un prestataire de services de certification électronique conformément à la politique de certification électronique approuvée ;

2. ne peut être délivré qu'au signataire ;

3. doit comporter notamment :

a. une mention indiquant que le certificat électronique est délivré à titre de certificat électronique qualifié,

b. l'identification du tiers de confiance ou du prestataire de services de certification électronique autorisé émetteur du certificat électronique ainsi que le pays dans lequel il est établi,

c. le nom du signataire ou un pseudonyme permettant d'identifier ledit signataire,

d. la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat électronique est destiné,

e. des données de vérification de signature qui correspondent aux données de création de signature électronique,

f. l'indication du début et de la fin de la période de validité du certificat électronique,

g. le code d'identité du certificat électronique,

h. la signature électronique qualifiée du prestataire de services de certification électronique ou du tiers de confiance, qui délivre le certificat électronique,

i. les limites à l'utilisation du certificat électronique, le cas échéant,

j. les limites à la valeur des transactions pour lesquelles le certificat électronique peut être utilisé, le cas échéant et,

k. une référence au document certifiant la représentation d'une autre personne physique ou morale, le cas échéant.

Chapitre 2

Des autorités de certification électronique

Section 1

De l'autorité nationale de certification électronique

Art. 16. — Il est créé, auprès du Premier ministre, une autorité administrative indépendante jouissant de la personnalité morale et de l'autonomie financière, dénommée autorité nationale de certification électronique ci-après désignée « autorité ».

Les crédits nécessaires au fonctionnement de l'autorité sont inscrits au budget de l'Etat.

Art. 17. — Le siège de l'autorité est fixé par voie réglementaire.

Art. 18. — L'autorité est chargée de promouvoir l'utilisation et le développement de la signature et la certification électroniques et de garantir la fiabilité de leurs usages.

Dans ce cadre, elle a pour missions :

1. d'élaborer sa politique de certification électronique et veiller à son application, après avis favorable de l'entité en charge de l'approbation ;

2. d'approuver les politiques de certification électronique émises par les Autorités gouvernementale et économique de certification électronique ;

3. de conclure les conventions de reconnaissance mutuelle à l'international ;

4. de proposer au Premier ministre des avant-projets de textes législatifs ou réglementaires portant sur la signature électronique ou la certification électronique ;

5. d'auditer les Autorités gouvernementale et économique de certification électronique à travers l'entité gouvernementale en charge de l'audit.

L'Autorité est consultée pour la préparation de tout projet de texte législatif ou réglementaire en relation avec la signature ou la certification électroniques.

Art. 19. — L'Autorité est composée d'un conseil et de services techniques et administratifs.

Le conseil de l'Autorité se compose de cinq (5) membres, dont le président, nommés par le Président de la République en raison de leurs compétences, notamment, en matière des sciences techniques relatives aux technologies de l'information et de la communication (TIC), du droit des (TIC) et de l'économie des (TIC).

Le conseil dispose de toutes les prérogatives pour l'accomplissement des missions de l'Autorité, à ce titre il peut faire appel à toute compétence susceptible de l'aider dans ses travaux.

Le mandat des membres du conseil de l'Autorité est fixé à quatre (4) ans renouvelable une seule fois.

Art. 20. — Les services techniques et administratifs de l'Autorité sont gérés par un directeur général nommé par le Président de la République, sur proposition du Premier ministre.

L'organisation, le fonctionnement et les missions de ces services sont précisés par voie réglementaire.

Art. 21. — La fonction de membre du conseil de l'Autorité et du directeur général est incompatible avec tout autre emploi public, emploi dans le secteur privé, profession libérale, tout mandat électif, toute publicité ou subvention ainsi que la détention directe ou indirecte de tout intérêt dans les sociétés intervenant dans le secteur des technologies de l'information et de la communication (TIC).

Art. 22. — Le président du conseil de l'Autorité est ordonnateur de paiement, il peut déléguer cette prérogative au directeur général.

Art. 23. — Les décisions du conseil de l'Autorité sont prises à la majorité, en cas d'égalité des voix, celle du président est prépondérante.

Art. 24. — Le système de rémunération du président et des membres du conseil de l'Autorité et du directeur général est fixé par voie réglementaire.

Art. 25. — Le conseil de l'Autorité adopte son règlement intérieur qui sera publié au *Journal officiel*.

Section 2

De l'Autorité gouvernementale de certification électronique

Art. 26. — Il est créé auprès du ministre chargé de la poste et des technologies de l'information et de la communication, une autorité gouvernementale de certification électronique jouissant de l'autonomie financière et de la personnalité morale.

Art. 27. — La nature, la composition, l'organisation et le fonctionnement de cette Autorité gouvernementale de certification électronique sont fixés par voie réglementaire.

Art. 28. — L'Autorité gouvernementale de certification électronique est chargée du suivi et du contrôle de l'activité de certification électronique des tiers de confiance ainsi que la fourniture de services de certification électronique au profit des intervenants dans la branche gouvernementale.

Dans ce cadre, elle a pour missions :

1. d'élaborer et soumettre pour approbation, à l'Autorité, sa politique de certification électronique et veiller à son application ;

2. d'approuver les politiques de certification émises par les tiers de confiance et veiller à leurs applications ;

3. de conserver les certificats électroniques expirés et les données liées à leurs délivrances par les tiers de confiance afin de les remettre aux Autorités judiciaires compétentes, le cas échéant, conformément aux dispositions législatives et réglementaires en vigueur ;

4. de publier le certificat électronique de clé publique de l'Autorité ;

5. de transmettre à l'Autorité, périodiquement ou sur sa demande, l'ensemble des informations relatives à l'activité de certification électronique ;

6. de procéder à l'audit des tiers de confiance à travers l'entité gouvernementale chargée de l'audit, conformément à la politique de certification.

Section 3

De l'Autorité économique de certification électronique

Art. 29. — L'Autorité en charge de la régulation de la poste et des télécommunications est désignée, au sens de la présente loi, autorité économique de certification électronique.

Art. 30. — L'Autorité économique de certification électronique est chargée du suivi et du contrôle des prestataires de services de certification électronique qui fournissent les services de signature et de certification électroniques au profit du public.

Dans ce cadre, elle a pour missions :

1. d'élaborer et soumettre pour approbation, à l'Autorité, sa politique de certification électronique et veiller à son application ;

2. de délivrer des autorisations aux prestataires de service de certification électronique, après avis favorable de l'Autorité ;

3. d'approuver les politiques de certification émises par les prestataires de services de certification électronique et veiller à leurs applications ;

4. de conserver les certificats électroniques expirés et les données liées à leurs délivrances par les prestataires de services de certification électronique afin de les remettre aux autorités judiciaires compétentes, le cas échéant, conformément aux dispositions législatives et réglementaires en vigueur ;

5. de publier le certificat électronique de clé publique de l'Autorité ;

6. de prendre les mesures nécessaires pour assurer la continuité de services en cas d'incapacité du préstataire de services de certification électronique de fournir ses services ;

7. de transmettre à l'Autorité, périodiquement ou sur sa demande, l'ensemble des informations relatives à l'activité de certification électronique ;

8. d'auditer les demandeurs d'autorisation elle-même ou à travers les cabinets d'audit accrédités, conformément à la politique de certification ;

9. de veiller à l'existence d'une concurrence effective et loyale en prenant toutes les mesures nécessaires afin de promouvoir ou de rétablir la concurrence entre les prestataires de services de certification électronique ;

10. d'arbitrer les litiges qui opposent les prestataires de services de certification électronique entre eux ou avec les utilisateurs conformément à la législation en vigueur ;

11. de requérir des prestataires de services de certification électronique et de toute personne concernée, tout document ou information utile pour l'accomplissement des missions qui lui sont dévolues par la présente loi ;

12. d'élaborer le cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique et le soumettre à l'Autorité pour approbation ;

13. d'éffectuer tout contrôle conformément à la politique de certification électronique et au cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique ;

14. de produire les rapports et statistiques publiques ainsi qu'un rapport annuel comportant la description de ses activités, sous réserve de la protection de la confidentialité.

L'autorité économique de certification électronique signale tout fait à caractère pénal au ministère public relevé à l'occasion de l'exercice de ses missions.

Section 4

Des voies de recours

Art. 31. — Les décisions prises par l'Autorité économique de certification électronique peuvent faire l'objet de recours auprès de l'Autorité dans un délai d'un (1) mois à compter de leur notification. Ce recours n'est pas suspensif.

Art. 32. — Les décisions prises par l'Autorité peuvent faire l'objet de recours auprès du Conseil d'Etat dans un délai d'un (1) mois à compter de leur notification. Ce recours n'est pas suspensif.

Chapitre 3

Du régime juridique de la prestation de service de certification électronique

Section 1

Du prestataire de services de certification électronique

Sous-section 1

De l'attestation d'éligibilité et de l'autorisation

Art. 33. — La prestation de service de certification électronique est soumise à une autorisation délivrée par l'autorité économique de certification électronique.

Art. 34. — Tout demandeur d'une autorisation pour la prestation de service de certification électronique doit réunir les conditions suivantes :

— être de droit algérien pour la personne morale ou de nationalité algérienne pour la personne physique ;

— disposer de capacités financières suffisantes ;

— avoir des qualifications et une expérience avérée dans le domaine des technologies de l'information et de la communication pour la personne physique ou le gérant de la personne morale ;

— ne pas avoir fait l'objet de condamnation pour crime ou délit incompatible avec l'activité de prestation de services de certification électronique.

Art. 35. — Préalablement à l'octroi de l'autorisation, une attestation d'éligibilité est délivrée pour une durée d'une (1) année, renouvelable une seule fois, elle est délivrée à toute personne physique ou morale pour la mise en place de tous les moyens nécessaires à l'activité de certification électronique.

Dans ce cas, l'attestation est notifiée dans un délai maximum de soixante (60) jours à compter de la date de réception de la demande attestée par un accusé de réception.

Le détenteur de cette attestation ne peut fournir les services de certification électronique qu'après l'obtention de l'autorisation.

Art. 36. — L'autorisation est délivrée au détenteur de l'attestation d'éligibilité et notifiée dans un délai maximum de soixante (60) jours à compter de la date de réception de la demande de l'autorisation attestée par un accusé de réception.

Art. 37. — Le refus de délivrance de l'attestation d'éligibilité et de l'autorisation doit être motivé, il est notifié contre un accusé de réception.

Art. 38. — L'autorisation est assortie d'un cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique ainsi que la signature du certificat électronique du prestataire par l'autorité économique de certification électronique.

Art. 39. — L'attestation d'éligibilité et l'autorisation sont personnelles et ne peuvent être cédées à des tiers.

Art. 40. — L'autorisation est délivrée pour une durée de cinq (5) ans. Arrivée à terme, elle est renouvelée conformément aux conditions définies dans le cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique.

L'autorisation est soumise au paiement d'une contrepartie financière dont le montant est fixé par voie réglementaire.

Sous-section 2

De la prestation de service de certification électronique

Art. 41. — Le prestataire de services de certification électronique est chargé de l'enregistrement, de l'émission, de la délivrance, de la révocation, de la publication et de la conservation des certificats électroniques, conformément à sa politique de certification approuvée par l'autorité économique de certification électronique.

Art. 42. — Le prestataire de services de certification électronique doit préserver la confidentialité des données et des informations liées aux certificats électroniques délivrés.

Art. 43. — Le prestataire de services de certification électronique ne peut recueillir des données personnelles qu'après consentement explicite de l'intéressé.

Le prestataire ne doit recueillir que les données personnelles nécessaires à la délivrance et à la conservation du certificat électronique. Ces données ne peuvent être traitées à d'autres fins.

Art. 44. — Préalablement à la délivrance du certificat électronique, le prestataire de services de certification électronique doit vérifier la complémentarité des données de création et vérification de signature.

Après avoir vérifié son identité et, le cas échéant, ses qualités spécifiques, le prestataire de services de certification électronique délivre un ou plusieurs certificats électroniques à toute personne qui en fait la demande.

En ce qui concerne les personnes morales, le prestataire de services de certification électronique tient un registre contenant l'identité et la qualité du représentant légal de la personne morale qui fait usage de la signature liée au certificat électronique qualifié, de manière à pouvoir établir l'identité de la personne physique à chaque utilisation de cette signature électronique.

Art. 45. — A la demande du titulaire du certificat électronique qualifié, préalablement identifié, le prestataire de services de certification électronique révoque le certificat électronique dans les délais fixés dans la politique de certification.

Le prestataire de services de certification électronique révoque également un certificat électronique qualifié lorsque :

1. il a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat électronique ne sont plus conformes à la réalité ou que la confidentialité des données de création de signature a été violée ;

2. il n'est plus conforme à la politique de certification ;

3. le prestataire de services de certification est informé du décès de la personne physique ou de la dissolution de la personne morale titulaire du certificat électronique.

Le prestataire de services de certification électronique est tenu d'informer le titulaire du certificat électronique qualifié de la révocation et sa motivation.

Le prestataire de services de certification électronique est tenu de notifier au titulaire, dans les délais prescrits dans la politique de certification, l'expiration de son certificat électronique qualifié.

La révocation d'un certificat électronique qualifié est définitive.

Art. 46. — Conformément à sa politique de certification approuvée par l'autorité économique de certification électronique, le prestataire de services de certification électronique, prend les mesures nécessaires afin de répondre à une demande de révocation.

La révocation est opposable aux tiers à partir de sa publication, conformément à la politique de certification électronique du prestataire de services de certification électronique.

Art. 47. — Le prestataire de services de certification électronique est tenu de transférer à l'autorité économique de certification électronique les informations concernant les certificats électroniques qualifiés après leur expiration en vue de leur conservation.

Art. 48. — Le prestataire de services de certification électronique ne peut ni conserver, ni copier les données de création de signature de la personne à laquelle il a fourni un certificat électronique qualifié.

Art. 49. — Les prestataires de services de certification électronique ont l'obligation d'appliquer des tarifs pour les services fournis en adéquation avec les principes de tarification définis par l'autorité économique de certification électronique et fixés par voie réglementaire.

Art. 50. — Le prestataire de services de certification électronique fournit ses services dans le cadre des principes de transparence et de non-discrimination.

Le prestataire de services de certification électronique ne peut refuser de fournir ses services sans motif valable.

Sous-section 3

Du contrôle et de l'audit

Art. 51. — Un audit d'évaluation est réalisé, sur requête du détenteur de l'attestation d'éligibilité, préalablement à l'octroi de l'autorisation de prestation de services de certification électronique, par l'autorité économique de certification électronique ou par un cabinet d'audit accrédité, conformément à la politique de certification électronique de l'autorité économique et au cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique.

Art. 52. — Le contrôle des prestataires de services de certification électronique par l'autorité économique s'effectue, notamment, à travers des audits périodiques et des contrôles inopinés, conformément à la politique de certification de l'autorité économique et au cahier des charges fixant les conditions et les modalités de la prestation des services de certification électronique.

Section 2

De la responsabilité du prestataire de services de certification et du titulaire de certificat électronique

Sous-section 1

Des obligations et de la responsabilité du prestataire de services de certification électronique

Art. 53. — Un prestataire de services de certification électronique qui délivre un certificat électronique qualifié est responsable du préjudice causé à tout organisme ou personne physique ou morale qui se fie à ce certificat électronique, pour ce qui est de :

1. l'exactitude de toutes les informations contenues dans le certificat électronique qualifié à la date où il a été délivré et la présence, dans ce certificat électronique, de toutes les données prescrites pour un certificat électronique qualifié ;

2. l'assurance que, au moment de la délivrance du certificat électronique, le signataire identifié dans le certificat électronique qualifié détenait les données de création de signature correspondant aux données de vérification de signature fournies ou identifiées dans le certificat électronique ;

3. l'assurance que les données de création et de vérification de signature puissent être utilisées de façon complémentaire ;

Sauf si le prestataire de services de certification électronique apporte la preuve qu'il n'a commis aucune négligence.

Art. 54. — Le prestataire de services de certification électronique qui a délivré un certificat électronique qualifié est responsable du préjudice résultant de la non révocation de ce certificat, causé à un organisme ou à une personne physique ou morale qui se prévaut du certificat électronique, sauf si le prestataire de services de certification électronique apporte la preuve qu'il n'a commis aucune négligence.

Art. 55. — Le prestataire de services de certification électronique peut indiquer, dans un certificat électronique qualifié, les limites fixées à son utilisation, à condition que cette indication soit visible et compréhensible par des tiers. Dans ce cas, le prestataire de services de certification électronique ne peut être tenu responsable du préjudice résultant de l'usage d'un certificat électronique qualifié qui dépasse les limites fixées à son utilisation.

Art. 56. — Le prestataire de services de certification électronique peut indiquer, dans un certificat électronique qualifié, la valeur maximale des transactions pour lesquelles le certificat électronique peut être utilisé, à condition que cette indication soit visible et compréhensible par des tiers. Dans ce cas, le prestataire de services de certification électronique n'est pas responsable des dommages qui résultent du dépassement de cette valeur maximale.

Art. 57. — Le prestataire de services de certification électronique n'est pas responsable du préjudice résultant du non-respect des conditions d'utilisation des données de création de la signature électronique par le titulaire du certificat électronique qualifié.

Art. 58. — Le prestataire de services de certification électronique informe l'autorité économique de certification électronique dans un délai défini dans la politique de certification de cette autorité, de son intention de cesser ses activités de prestataire de services de certification électronique ainsi que de toute action qui pourrait conduire à la cessation de ses activités.

Dans ce cas, le prestataire de services de certification électronique se conforme aux dispositions de la politique de certification de l'autorité économique de certification électronique relatives à la continuité de service.

La cessation d'activité engendre le retrait de l'autorisation.

Art. 59. — Le prestataire de services de certification électronique qui cesse ses activités pour des raisons indépendantes de sa volonté, doit informer immédiatement l'autorité économique de certification électronique qui procède à la révocation de son certificat électronique qualifié après appréciation des raisons évoquées.

Dans ce cas, le prestataire prend les mesures nécessaires, prévues dans la politique de certification électronique de l'autorité économique, pour la conservation des informations liées aux certificats électroniques qualifiés délivrés.

Art. 60. — Le prestataire de services de certification électronique est tenu de souscrire aux assurances prévues dans la politique de certification électronique de l'autorité économique.

Sous-section 2

De la responsabilité du titulaire de certificat électronique

Art. 61. — Dès la signature de son certificat électronique, le titulaire est seul responsable de la confidentialité des données de création de sa signature.

En cas de doute quant au maintien de la confidentialité des données de création de la signature ou de la perte de conformité à la réalité des informations contenues dans le certificat électronique, le titulaire est tenu de le faire révoquer par le prestataire de services de certification électronique.

Lorsqu'un certificat électronique est arrivé à échéance ou a été révoqué, le titulaire de celui-ci ne peut utiliser les données de création de signature correspondantes pour signer ou faire certifier ces données par un autre prestataire de services de certification électronique.

Art. 62. — Le titulaire ne peut utiliser son certificat électronique qualifié à des fins autres que celles pour lesquelles il a été délivré.

Chapitre 4

De la reconnaissance mutuelle

Art. 63. — Les certificats électroniques délivrés par un prestataire de services de certification électronique établi dans un pays étranger ont la même valeur que ceux délivrés par un prestataire de services de certification électronique établi en Algérie, à condition que ce prestataire étranger agisse dans le cadre d'une convention de reconnaissance mutuelle conclue par l'autorité.

TITRE IV

DES SANCTIONS

Chapitre 1er

Des sanctions pécuniaires et administratives

Art. 64. — Lorsque le prestataire de services de certification électronique ne respecte pas les dispositions de son cahier des charges ou de sa politique de certification électronique approuvée par l'Autorité économique de certification électronique, cette dernière prononce a son encontre une sanction pécuniaire dont le montant varie de deux cent mille dinars (200.000 DA) à cinq millions de dinars (5.000.000 DA), selon la classification des manquements, prévue dans le cahier des charges du prestataire et le met en demeure de se conformer auxdites dispositions dans un délai allant de huit (8) jours à trente (30) jours, selon le cas. Les griefs retenus contre le prestataire lui sont notifiés afin de lui permettre de présenter, dans les délais précités, ses justifications écrites.

Si le prestataire de services ne se conforme pas à la mise en demeure, l'autorité économique prononce à son encontre le retrait de son autorisation et la révocation de son certificat, selon le cas, après avis favorable de l'autorité.

Les modalités de recouvrement des sommes correspondantes à la sanction pécuniaire mentionnée au premier paragraphe du présent article sont fixées par voie réglementaire.

Art. 65. — Dans le cas d'une atteinte à des impératifs exigés par la défense nationale et la sécurité publique par un prestataire de services de certification électronique, l'autorité économique de certification électronique procède, après avis favorable de l'Autorité, au retrait, sans délais, de l'autorisation.

Ses équipements font l'objet de mesures conservatoires conformément à la législation en vigueur et ce, sans préjudice des poursuites pénales.

Chapitre 2

Des dispositions pénales

Art. 66. — Est punie d'une peine d'emprisonnement de trois (3) mois à trois (3) ans et d'une amende de 20.000 DA à 200.000 DA ou de l'une de ces deux peines seulement, toute personne qui use de fausses déclarations pour l'obtention d'un certificat électronique qualifié.

Art. 67. — Est puni d'une peine d'emprisonnement de deux (2) mois à une (1) année et d'une amende de 200.000 DA à 1.000.000 DA ou de l'une de ces deux peines seulement, tout prestataire de services de certification électronique ayant failli à l'obligation d'informer l'autorité économique de certification électronique de sa cessation d'activité, dans les délais prévus aux article 58 et 59 de la présente loi.

Art. 68. — Est punie d'une peine d'emprisonnement de trois (3) mois à trois (3) ans et d'une amende de 1.000.000 DA à 5.000.000 DA ou de l'une de ces deux peines seulement, toute personne qui détient, divulgue ou utilise les données de création de signature électronique qualifiée d'autrui.

Art. 69. — Est punie d'une peine d'emprisonnement de deux (2) mois à trois (3) ans et d'une amende de 20.000 DA à 200.000 DA ou de l'une de ces deux peines seulement, toute personne qui manque sciemment à l'obligation d'identifier le demandeur de certificat électronique qualifié.

Art. 70. — Est puni d'une peine d'emprisonnement de trois (3) mois à deux (2) ans et d'une amende de 200.000 DA à 1.000.000 DA ou de l'une de ces deux peines seulement, tout prestataire de services de certification électronique qui ne se conforme pas aux dispositions de l'article 42 de la présente loi.

Art. 71. — Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et d'une amende de 200.000 DA à 1.000.000 DA ou de l'une de ces deux peines seulement, tout prestataire de services de certification électronique qui ne se conforme pas aux dispositions de l'article 43 de la présente loi.

Art. 72. — Est punie d'une peine d'emprisonnement d'un (1) an à trois (3) ans et d'une amende de 200.000 DA à 2.000.000 DA ou de l'une de ces deux peines seulement, toute personne qui fournit au public des services de certification électronique sans autorisation ou tout prestataire de services de certification électronique qui reprend ou poursuit son activité après retrait de l'autorisation.

Les équipements ayant servi à commettre l'infraction font l'objet de confiscation conformément à la législation en vigueur.

Art. 73. — Est punie d'une peine d'emprisonnement de trois (3) mois à deux (2) ans et d'une amende de 20.000 DA à 200.000 DA ou de l'une de ces deux peines seulement, toute personne chargée de l'audit qui révèle des informations confidentielles dont elle a eu connaissance lors de l'audit.

Art. 74. — Est punie d'une amende de 2.000 DA à 200.000 DA, toute personne qui utilise son certificat électronique qualifié à d'autres fins que celles pour lesquelles il a été délivré.

Art. 75. — La personne morale qui a commis l'une des infractions prévues par le présent chapitre est punie d'une amende équivalente à cinq (5) fois le maximum de l'amende prévue pour la personne physique.

TITRE V

DISPOSITIONS TRANSITOIRES ET FINALES

Art. 76. — Les entités utilisant la signature et la certification électroniques à la date de la promulgation de la présente loi, sont tenues de s'y conformer suivant les modalités définies par l'autorité et ses orientations.

Art. 77. — Les certificats électroniques émis par les entités utilisant la signature et la certification électroniques avant la promulgation de la présente loi restent valables jusqu'à leur expiration dans la limite des délais maximaux fixés par l'autorité.

Art. 78. — Les missions d'homologation de l'entité prévue dans l'article 14 de la présente loi sont assurées par les services compétents en la matière pour une période transitoire jusqu'à la création de l'entité en charge de cette mission, à condition que cette période ne dépasse pas cinq (5) ans à partir de la date de publication de cette loi au *Journal officiel*.

Art. 79. — Les missions d'audit de l'autorité, des autorités économique et gouvernementale, des tiers de confiances ainsi que des prestataires de services de certification électronique sont assurées par les services compétents en la matière, déterminés par voie réglementaire pour une période transitoire jusqu'à la création de l'entité en charge de cette mission à condition que cette période ne dépasse pas cinq (5) ans à partir de la date de publication de cette loi au *Journal officiel*.

Art. 80. — La mission d'approbation de l'entité prévue au point premier de l'article 18 de la présente loi est assurée par le conseil de l'autorité pour une période transitoire jusqu'à la création de l'entité en charge de cette mission, à condition que cette période ne dépasse pas cinq (5) ans à partir de la date de publication de cette loi au *Journal officiel*.

Art. 81. — Toutes dispositions contraires à la présente loi sont abrogées.

Art. 82. — La présente loi sera publiée au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le 11 Rabie Ethani 1436 correspondant au 1er février 2015.

Abdelaziz BOUTEFLIKA.