République Algérienne Démocratique et Populaire

Présidence de la République

Certification Electronique
&
Sécurité de l'Information

09 décembre 2009 - Alger

PLAN DE LA COMMUNICATION

Introduction

Vulnérabilités, attaques et Sécurité de l'Information

Cryptographie et certification

Aperçu sur la l'aspect législatif et règlementaire

Conclusion

INTRODUCTION

Message de S.E le Président de la République, M. Abdelaziz Bouteflika à la «Journée Internationale des Télécommunications», Alger le 17 mai 2001.

«L'Etat, en tant que facteur de modernité et fédérateur des potentialités nationales, a un rôle déterminant à jouer dans cette nouvelle dynamique».

Message de S.E le Président de la République, M. Abdelaziz Bouteflika au «Symposium International sur les Technologies de l'Information et de la Communication et la Société de l'Information », Alger, le 09 décembre 2002.

« Consciente de cet impératif et du rôle stratégique des technologies de l'information et de la communication (TIC) dans l'édification de la société de l'avenir, l'Algérie s'est attelée, conformément à nos orientations à la préparation de son entrée dans le monde de l'information avec toutes les mesures et les dispositions que cela suppose, et nous sommes sûrs de pouvoir relever le défi politique induit par cette démarche».

Les axes majeurs du plan multisectoriel de développement des TIC proposé par le MPTIC en concertation avec les institutions, les opérateurs publics et privés et la communauté scientifique et universitaire, sont :

- **Accélération de l'usage des TIC dans l'administration publique et au niveau des entreprises et des ménages;**
- **L'impulsion du développement de l'économie fondée sur le savoir;**
- **Renforcement de l'infrastructure de télécommunication à haut et très haut débit;**
- **Le développement des compétences humaines et le renforcement de la recherche et de l'innovation;**
- **Mise à niveau du cadre juridique national et élaboration d'un plan de Communication;**
- **Valorisation de la coopération internationale;**
- **Moyens financiers, mesures organisationnelles et mécanismes d'évaluation.**

SYSTEMES D’INFORMATION

- De nos jours, l'information est devenue une ressource importante, offrant un atout supplémentaire pour ceux qui la possède.

- Elle peut occuper un rang stratégique au niveau d'une nation, d'un organisme ou d'une entreprise.

- Elle concerne tous les domaines :

  - ✓ Militaire;
  - ✓ Diplomatique;
  - ✓ Economique;
  - ✓ Industriel;
  - ✓ Financier;
  - ✓ Commercial;
  - ✓ Scientifique;
  - ✓ Technologique;
  - ✓ …

- Les informations qui étaient dans le passé confinées, sont devenues accessibles de presque n'importe quel point du globe.

- Elles sont traitées, stockées et échangées à travers des systèmes d'information composés majoritairement de réseaux locaux communiquant avec l'extérieur.

- Les Systèmes d'Information sont composés de :

  - ✓ Logiciels;
  - ✓ Matériels;
  - ✓ Réseaux;
  - ✓ Sites;
  - ✓ Organisations;
  - ✓ Personnels.

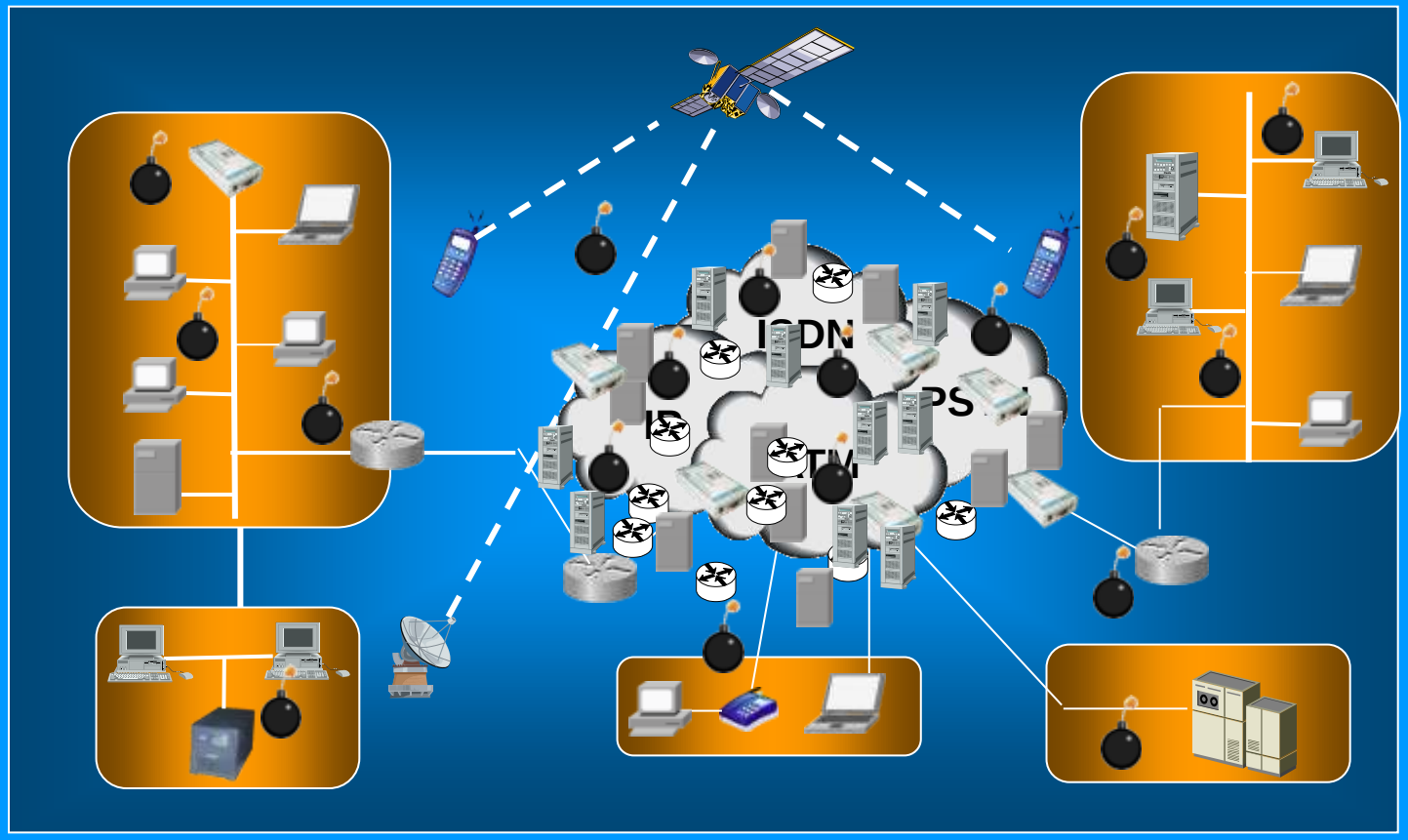
Ces entités porteuses de vulnérabilités exposent les Systèmes d'Information à des menaces permanentes et multiformes

VULNERABILITES DES SYSTEMES D'INFORMATION

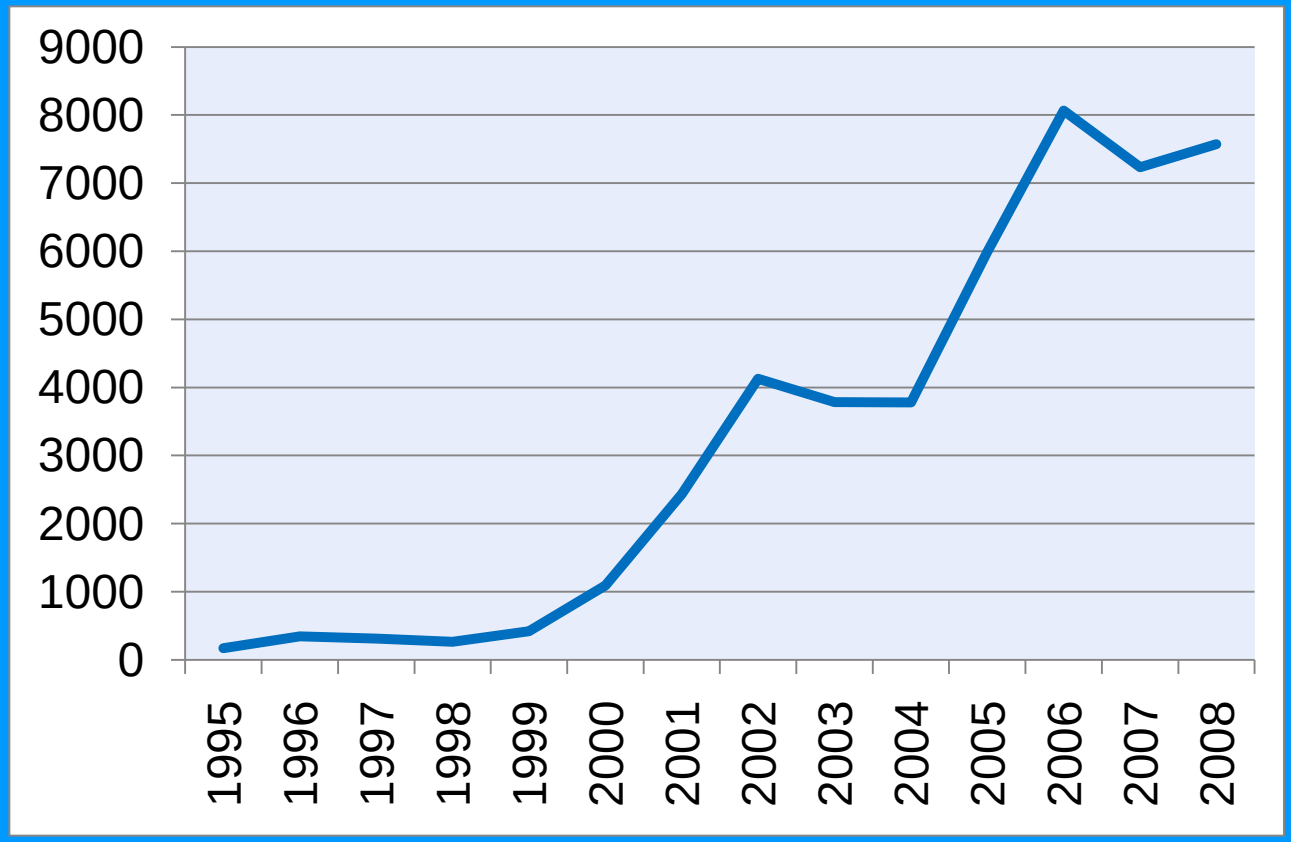
2. VULNERABILITES DES SYSTEMES D'INFORMATION

Expansions des systèmes d'information + Concentration et disponibilité des données sur les réseaux + Failles liées aux systèmes d'information

Vulnérabilités des systèmes d'information

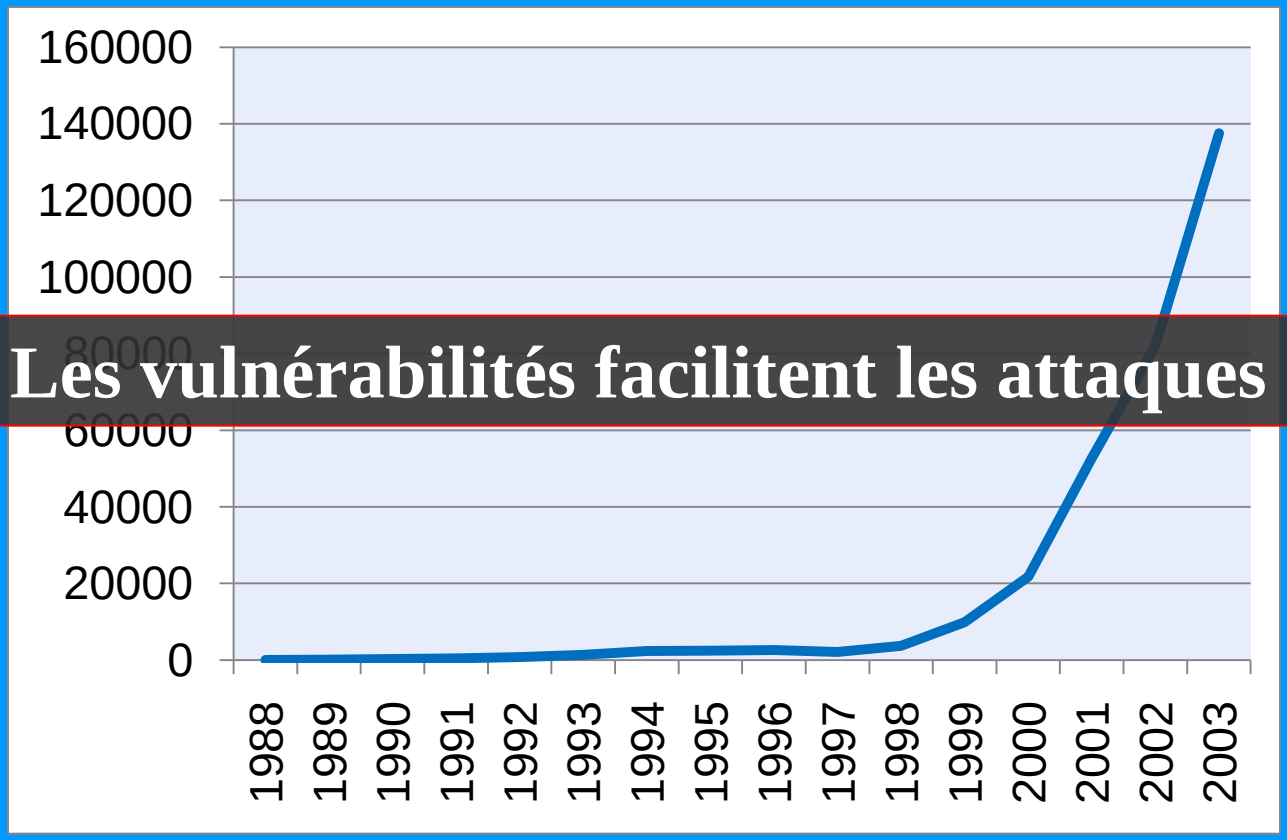


- Les vulnérabilités sont découvertes et exploitées à très grande vitesse.



CERT(C) Evolutions des vulnérabilités déclarées

Nouvelles vulnérabilités ➡ Augmentation du nombre d'agresseurs



Les vulnérabilités facilitent les attaques

CERT(C) Evolutions des incidents

ATTAQUES DES SYSTEMES D’INFORMATION

3. ATTAQUES DES SYSTEMES D'INFORMATION

- **Définition:**

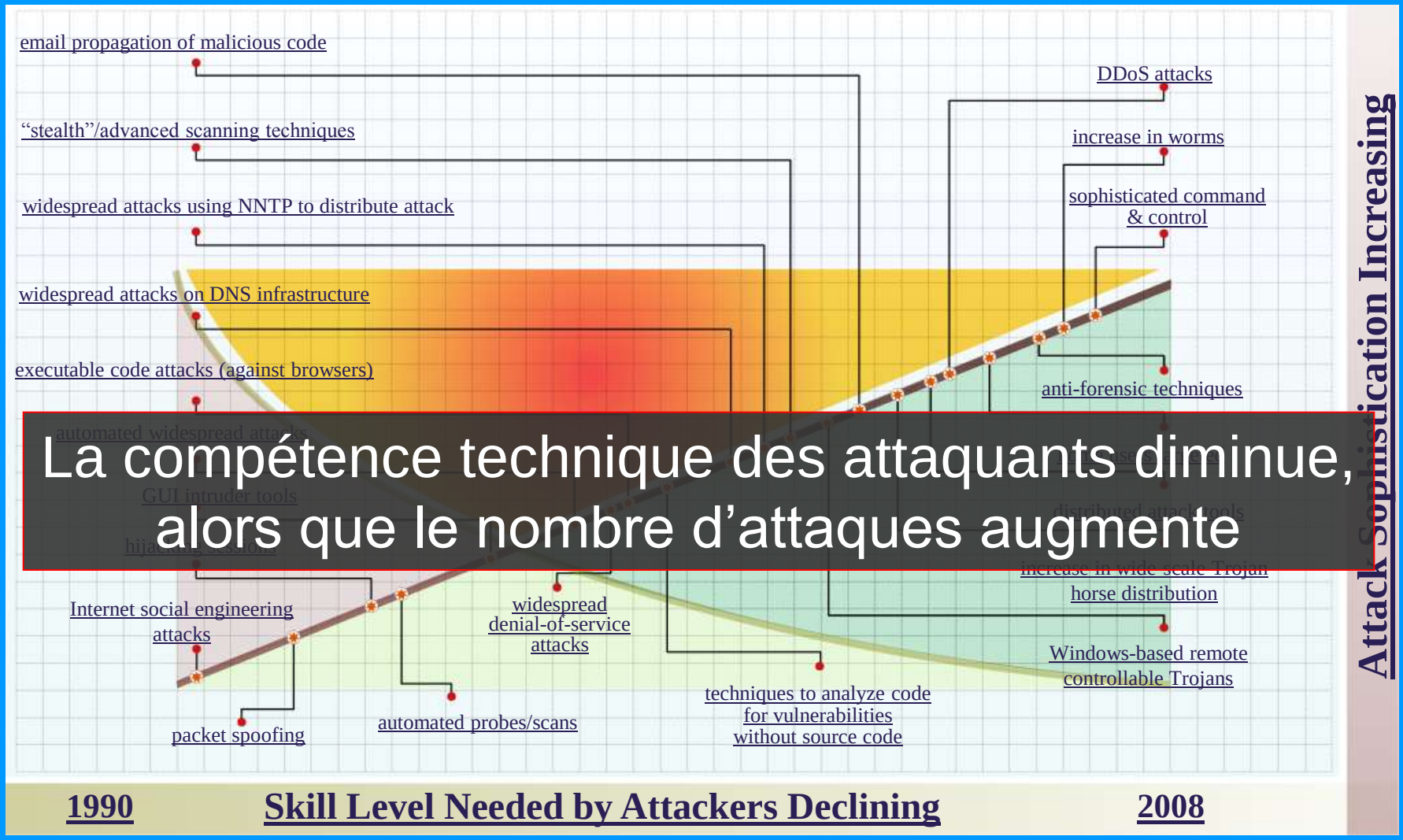
  Action de malveillance pour tenter de contourner les fonctions de sécurité.

- **Motivations:**

  - ✓ Espionnage;
  - ✓ Piratage;
  - ✓ Apport du gain;
  - ✓ Fraude;
  - ✓ Vol;
  - ✓ Défi intellectuel;
  - ✓ Vengeance;
  - ✓ Chantage;
  - ✓ Extorsion de fonds;
  - ✓ …

- **Origines :**

  - ✓ cause accidentelle ou délibérée;
  - ✓ nature interne ou externe.



La compétence technique des attaquants diminue, alors que le nombre d'attaques augmente

Data source: SEI/CERT CC

SECURITE DE L’INFORMATION

La sécurité de l'information n'est pas un ensemble de produits finis, c'est un processus dynamique nécessitant:

- ✓ Veille technologique permanente;
- ✓ Analyse des risques et des menaces;
- ✓ Sensibilisation continue;
- ✓ Sécurité physique;
- ✓ Sécurité organisationnelle;
- ✓ Disponibilité des équipements;
- ✓ Qualification et intégrité du personnel.

La négligence d'un seul aspect de sécurité peut la rendre caduque.

La Sécurité de l'Information a besoin

D'un cadre technique:

- ✓ Cryptographie;
- ✓ Signatures électroniques;
- ✓ Certificats.

D'un cadre organisationnel:

- ✓ Tiers de confiance assurant les relations entre différentes entités.

D'un cadre juridique:

- ✓ Règlementation nationale;
- ✓ Reconnaissance mutuelle;
- ✓ Normes internationales.

4. SECURITE DE L'INFORMATION

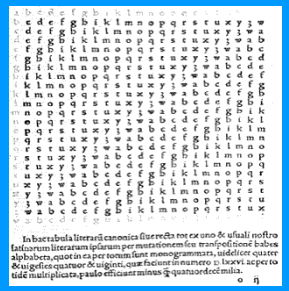
	Risques	Solutions
Confidentialité	Risque d'écoute	Chiffrement des échanges et des données
Authentification	Usurpation d'identité	Signature numérique Vérification de la validité du certificat
Intégrité	Modification des données	Signature numérique des données
Non répudiation	Nier un échange ou une transaction	Vérification de la signature électronique

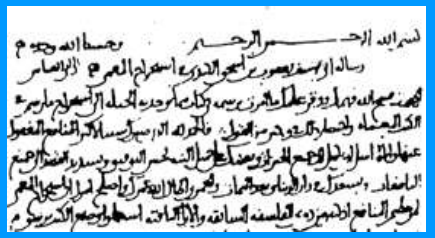
Services de la S.I

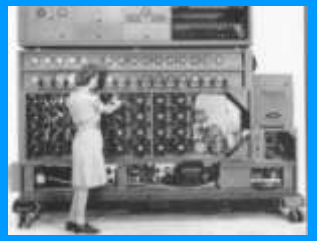
La Cryptographie est devenue l'outil indispensable qui garantie la sécurité de l'information et renforce la fiabilité de la signature électronique.

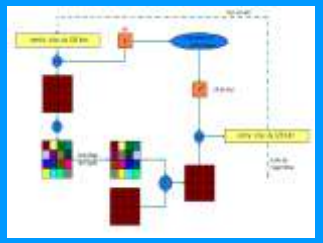
CRYPTOGRAPHIE

La Cryptographie, science qui a pour but de protéger le caractère confidentiel d'une information donnée, existe depuis des milliers d'années.

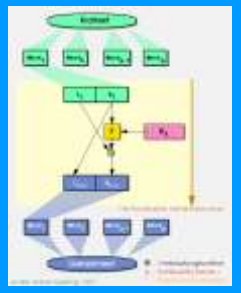








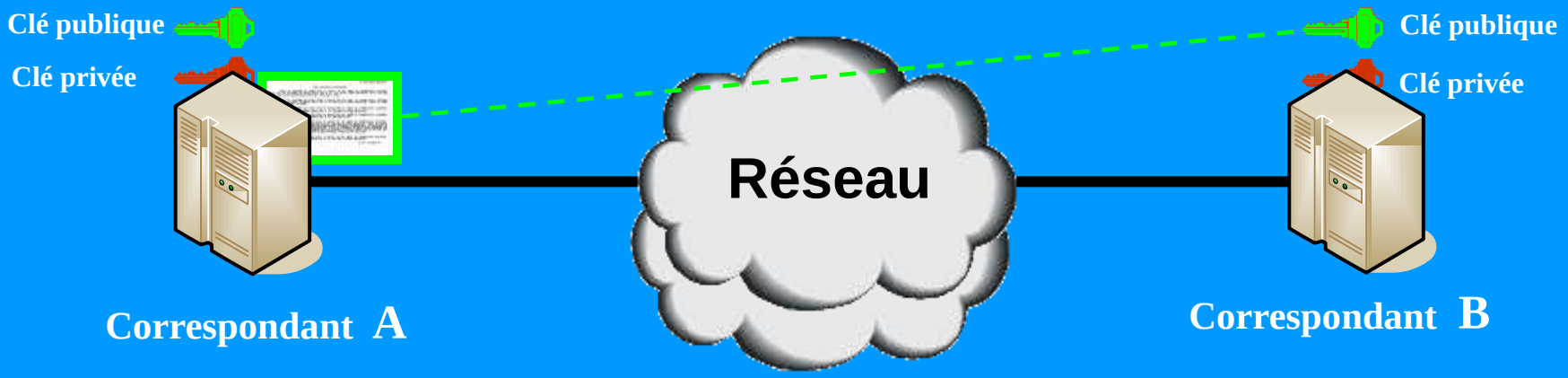
La Cryptographie se trouvant au confluent de plusieurs disciplines, va crescendo avec la technique. Inséparables, elles deviennent de nos jours inévitables.



Cryptographie Symétrique

Cryptographie Asymétrique

Confidentialité



Cryptographie Asymétrique

Intégrité , Authentification, Non Répudiation

- La cryptographie est considérée comme une arme de guerre. Son usage est soumis à une législation très stricte et son exportation à autorisation préalable.

Cipher	Version	Key exchange	Authentication	Encryption	Mac	Export
EDH-RSA-DES-CBC3-SHA	TLSv1/SSLv3	DH	RSA	3DES(168)	SHA1	No
EDH-DSS-DES-CBC3-SHA	TLSv1/SSLv3	DH	DSS	3DES(168)	SHA1	No
DES-CBC3-SHA	TLSv1/SSLv3	RSA	RSA	3DES(168)	SHA1	No
DHE-DSS-RC4-SHA	TLSv1/SSLv3	DH	DSS	RC4(128)	SHA1	No
IDEA-CBC-SHA	TLSv1/SSLv3	RSA	RSA	IDEA(128)	SHA1	No
RC4-SHA	TLSv1/SSLv3	RSA	RSA	RC4(128)	SHA1	No
RC4-MD5	TLSv1/SSLv3	RSA	RSA	RC4(128)	MD5	No
EDH-RSA-DES-CBC-SHA	TLSv1/SSLv3	DH	RSA	DES(56)	SHA1	No
EDH-DSS-DES-CBC-SHA	TLSv1/SSLv3	DH	DSS	DES(56)	SHA1	No
DES-CBC-SHA	TLSv1/SSLv3	RSA	RSA	DES(56)	SHA1	No
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES(168)	MD5	No
IDEA-CBC-MD5	SSLv2	RSA	RSA	IDEA(128)	MD5	No
RC2-CBC-MD5	SSLv2	RSA	RSA	RC2(128)	MD5	No
RC4-64-MD5	SSLv2	RSA	RSA	RC4(64)	MD5	No
DES-CBC-MD5	SSLv2	RSA	RSA	DES(56)	MD5	No
EXP1024-DHE-DSS-RC4-SHA	TLSv1/SSLv3	DH(1024)	DSS	RC4(56)	SHA1	Yes
EXP1024-RC4-SHA	TLSv1/SSLv3	RSA(1024)	RSA	RC4(56)	SHA1	Yes
EXP1024-DHE-DSS-DES-CBC-	TLSv1/SSLv3	DH(1024)	DSS	DES(56)	SHA1	Yes
EXP1024-RC4-MD5	TLSv1/SSLv3	RSA(1024)	RSA	RC4(56)	MD5	Yes
EXP-EDH-RSA-DES-CBC-SHA	TLSv1/SSLv3	DH(512)	RSA	DES(40)	SHA1	Yes
EXP-EDH-DSS-DES-CBC-SHA	TLSv1/SSLv3	DH(512)	DSS	DES(40)	SHA1	Yes
EXP-DES-CBC-SHA	TLSv1/SSLv3	RSA(512)	RSA	DES(40)	SHA1	Yes
EXP-RC2-CBC-MD5	TLSv1/SSLv3	RSA(512)	RSA	RC2(40)	MD5	Yes
EXP-RC4-MD5	TLSv1/SSLv3	RSA(512)	RSA	RC4(40)	MD5	Yes
EXP-RC2-CBC-MD5	SSLv2	RSA(512)	RSA	RC2(40)	MD5	Yes
EXP-RC4-MD5	SSLv2	RSA(512)	RSA	RC4(40)	MD5	Yes

SIGNATURE ELECTRONIQUE

- La signature électronique est un procédé qui permet l'authentification d'un signataire et procure l'intégrité des documents et la non répudiation.
- La signature électronique est reconnue juridiquement équivalente à la signature manuscrite.
- La signature électronique est fabriquée grâce à des algorithmes de chiffrement à clés publiques :
  - ✓ Le chiffrement est réalisé avec la clé privée de l'émetteur;
  - ✓ Le déchiffrement avec la clé publique de l'émetteur.

Signature électronique opposable

⬇

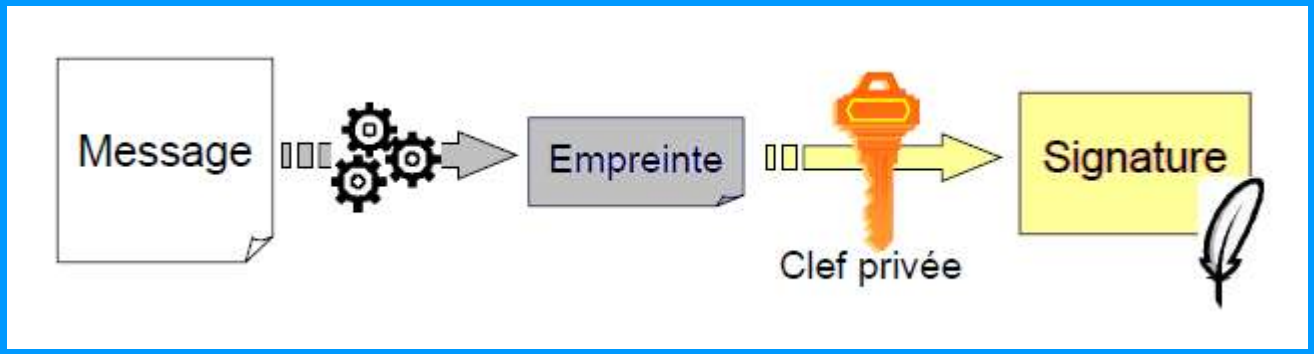
il faut qu'elle soit vérifiable

Signature électronique admissible

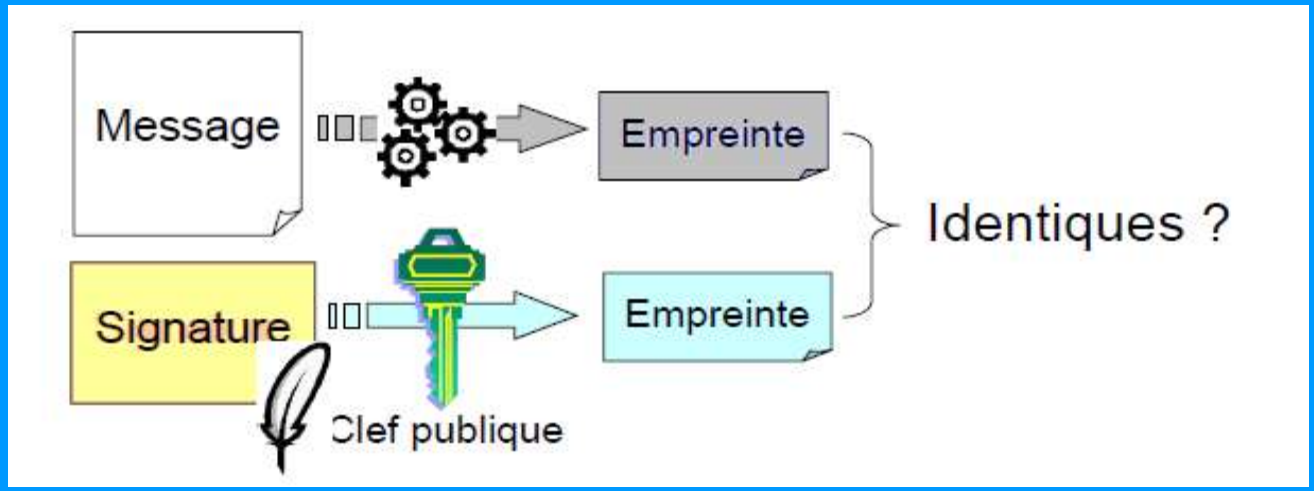
⬇

elle ne doit pas avoir de failles

Signature

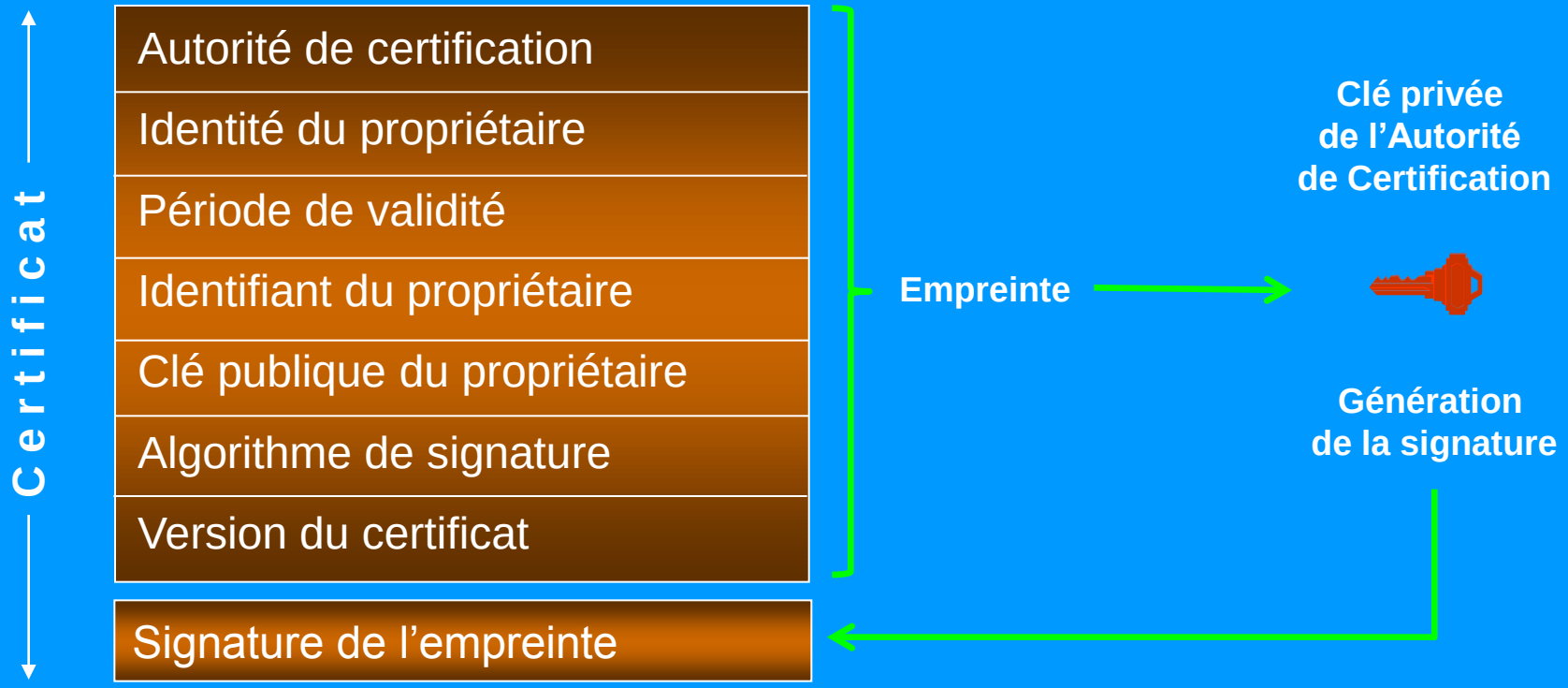


Vérification

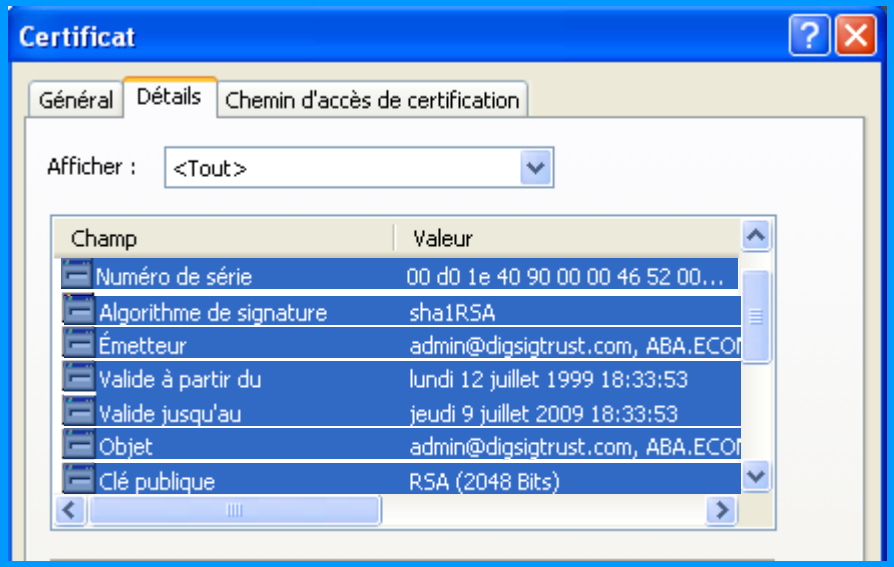


CERTIFICATION ELECTRONIQUE

Le certificat électronique est une structure de données liant différents éléments au moyen de la signature d'une autorité de confiance.



Eléments de base d'un certificat :



- [illegible] certificat

```
30 82 01 0a 02 82 01 01 00 b1 d3 11 e0 79
55 43 07 08 4c cb 05 42 00 e2 0d 83 46 3d
e4 93 ba b6 06 d3 0d 59 bd 3e c1 ce 43 67
01 8a 21 a8 ef bc cc d0 a2 cc b0 55 96 53
84 66 05 00 da 44 49 80 d8 54 0a a5 25 86
94 ed 63 56 ff 70 6c a3 a1 19 d2 78 be 68
2a 44 5e 2f cf cc 18 5e 47 bc 3a b1 46 3d
1e f0 b9 2c 34 5f 8c 7c 4c 08 29 9d 40 55
eb 3c 7d 83 de b5 f0 f7 8a 83 0e a1 4c b4
```

Les certificats sont utilisés pour :

- Authentification de l'utilisateur :
  - ✓ e-gouvernement;
  - ✓ e-banking;
  - ✓ e-learning;
  - ✓ services en ligne;
  - ✓ …
- Authentification des serveurs :
  - ✓ sites Web de e-commerce;
  - ✓ échanges électroniques;
  - ✓ …
- Vérification des signatures électroniques.

Gestion et responsabilité des certificats

+

Relation fiable entre entités

⇓

P.K.I

P.K.I

Une PKI, est un ensemble de :

- **Composants physiques**

✓Ordinateurs;
✓Equipements cryptographiques;
✓Cartes à puces.

- **Logiciels**

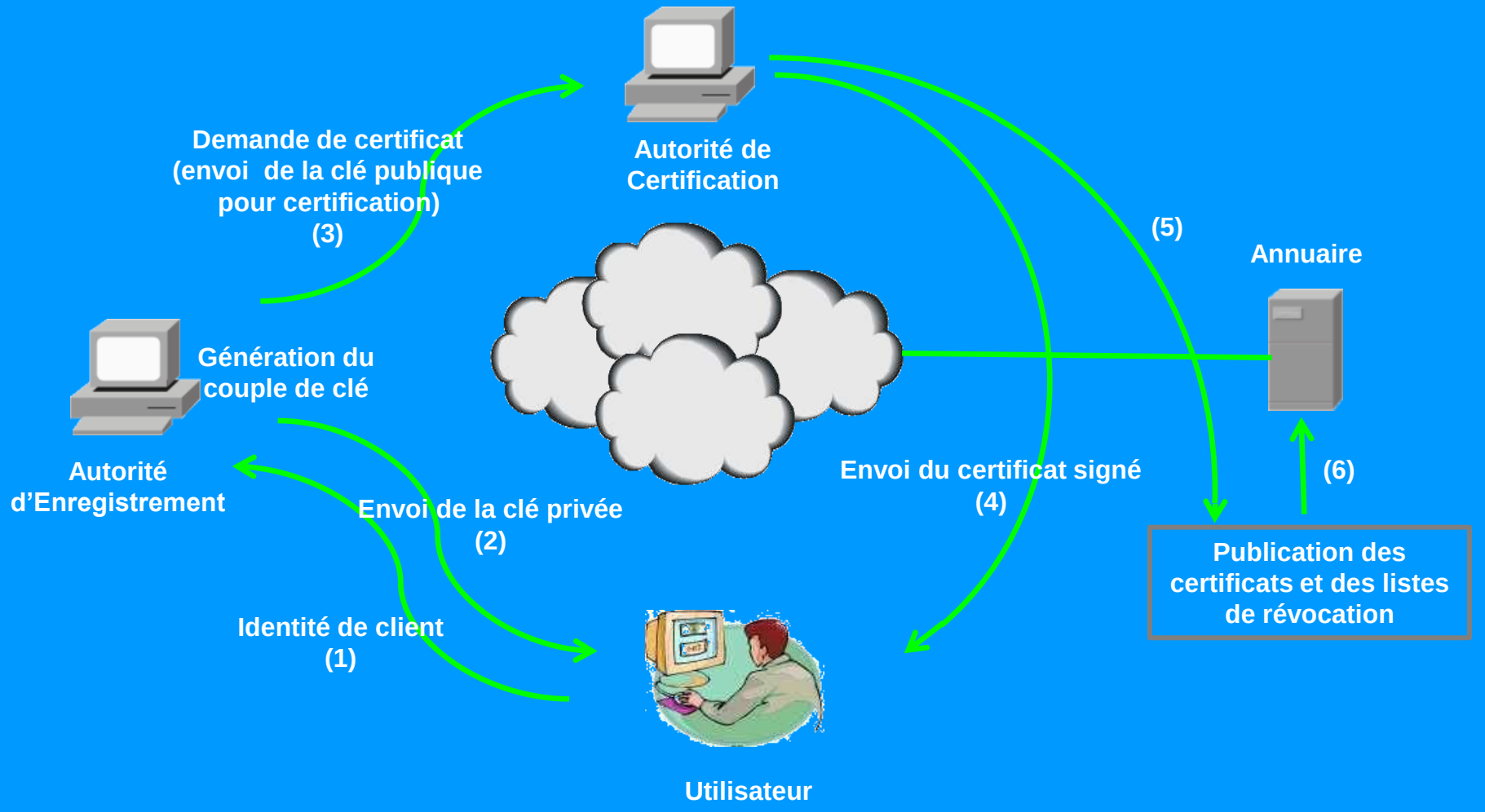
✓Système;
✓Application.

- **Procédures**

✓Vérification;
✓Validation.

- **Une politique de gestion des clés doit assurer les services suivants:**

  - ✓ Enregistrement, identification et authentification des utilisateurs;
  - ✓ Génération des certificats;
  - ✓ Renouvellement ou révocation des certificats;
  - ✓ Publication des certificats et des listes de révocation;
  - ✓ Archivage des certificats.


Autorité de Certification
Demande de certificat (envoi de la clé publique pour certification) (3)
(5)
Annuaire
Génération du couple de clé
Autorité d'Enregistrement
Envoi de la clé privée (2)
Envoi du certificat signé (4)
(6)
Publication des certificats et des listes de révocation
Identité de client (1)
Utilisateur

LEGISLATION ALGERIENNE EN MATIERE DE

CERTIFICATION ELECTRONIQUE
&
SECURITE DE L'INFORMATION

9. LEGISLATION ALGERIENNE EN MATIERE DE C.E & S.I

Les services de la Présidence de la République s'assurent de la sécurité et de la protection permanente des systèmes de communications et de télécommunications gouvernementaux.

Décret exécutif fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles, adopté en Conseil des Ministres le 19 octobre 2009

Exigence réglementaire de l'homologation des équipements et des logiciels de chiffrement.

Loi n° 05-10 du 20 juin 2005

Loi n° 05-10 du 13 Joumada El Oula 1426 correspondant au 20 juin 2005 modifiant et complétant l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil.

Art. 44. — L'ordonnance n° 75-58 du 26 septembre 1975 susvisée, est complétée par les *articles 323 bis et 323 ter,* rédigés comme suit :

"Art. 323 bis. — La preuve par écrit résulte d'une suite de lettres ou de caractères ou de chiffres ou de tout autre signe ou symbole doté d'une signification intelligible, quels que soient leurs supports et leurs modalités de transmission".

"Art. 323 ter. — L'écrit sous forme électronique est admis en tant que preuve au même titre que l'écrit sur support papier, à la condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité".

Décret exécutif n° 07-162 du 30 mai 2007

Décret exécutif n° 07-162 du 13 Joumada El Oula 1428 correspondant au 30 mai 2007 modifiant et complétant le décret exécutif n° 01-123 du 15 Safar 1422 correspondant au 9 mai 2001 relatif au régime d'exploitation applicable à chaque type de réseaux, y compris radio-électriques et aux différents services de télécommunications.

"Art. 3. — Sont subordonnés à l'octroi d'une autorisation délivrée par l'autorité de régulation de la poste et des télécommunications, l'établissement et l'exploitation :

— des services de certification électronique.

CONCLUSION

- **Compte tenu de l'importance qu'accorde l'Etat au développement de l'économie basée sur le savoir, il s'est pleinement engagé à lancer, booster et accompagner le processus de mise en œuvre de la certification électronique.**

- **L'Etat concilie entre les impératifs de la société de l'information et les exigences de la sécurité nationale. Il encourage le développement des procédures et des modalités pratiques ainsi que l'épanouissement des activités et des métiers liés à ce secteur, tout en définissant les lignes directrices et en garantissant l'instauration d'un climat de confiance.**

- **L'Etat s'assure, dans le domaine de la certification électronique, de l'édification d'un service universel basé sur les normes internationales et les conventions de reconnaissances mutuelles.**

Merci de votre attention