REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

AUTORITE DE REGULATION DE LA POSTE ET DES TELECOMMUNICATIONS

Certification Electronique en Algérie: Situation et Perspectives

Ahmed BERBAR, chef du projet C.E

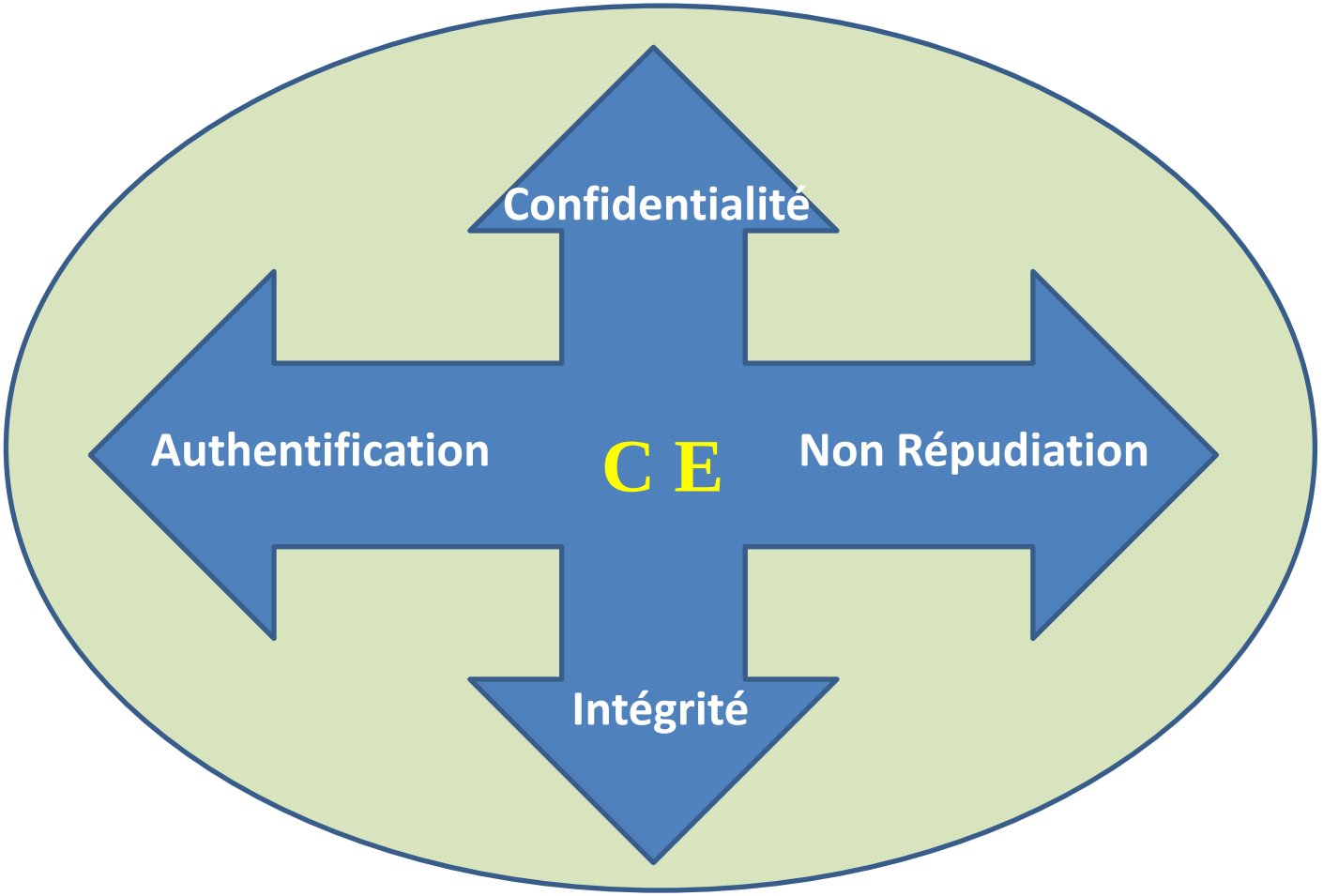
PLAN

- La Certification Electronique (C.E)
- Quelques Modèles d'Organisation de la C.E
- Organisation de la C.E dans certains pays
- Certification Electronique en Algérie
  - Etat des lieux
  - Modèle à mettre en œuvre
  - La mise en œuvre
- Conclusion

LA CERTIFICATION ÉLECTRONIQUE

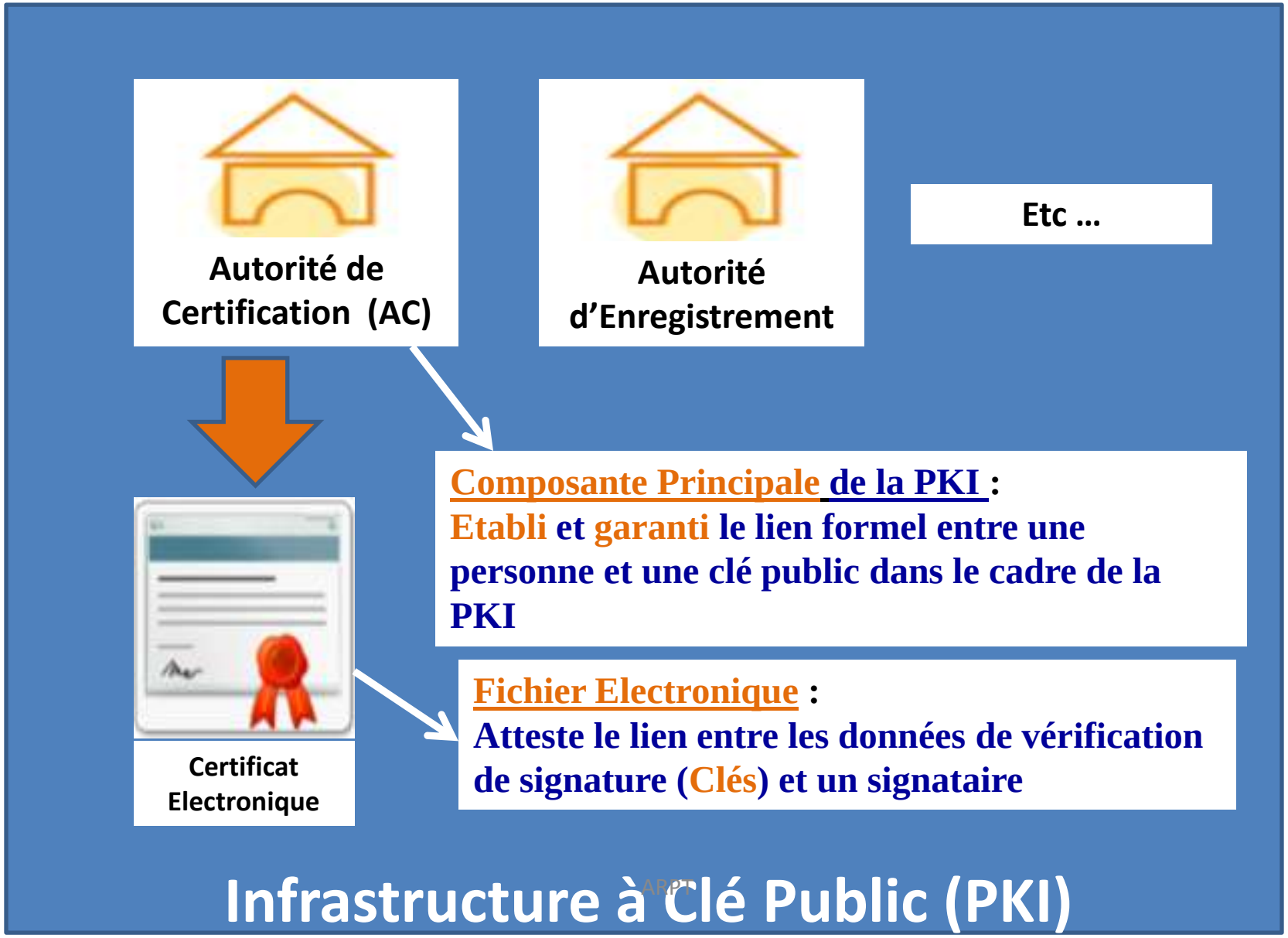
Les objectifs

Permet de garantir 4 aspects de Sécurité des échanges électroniques:



Climat de Confiance

Infrastructure à Clé Public (PKI)

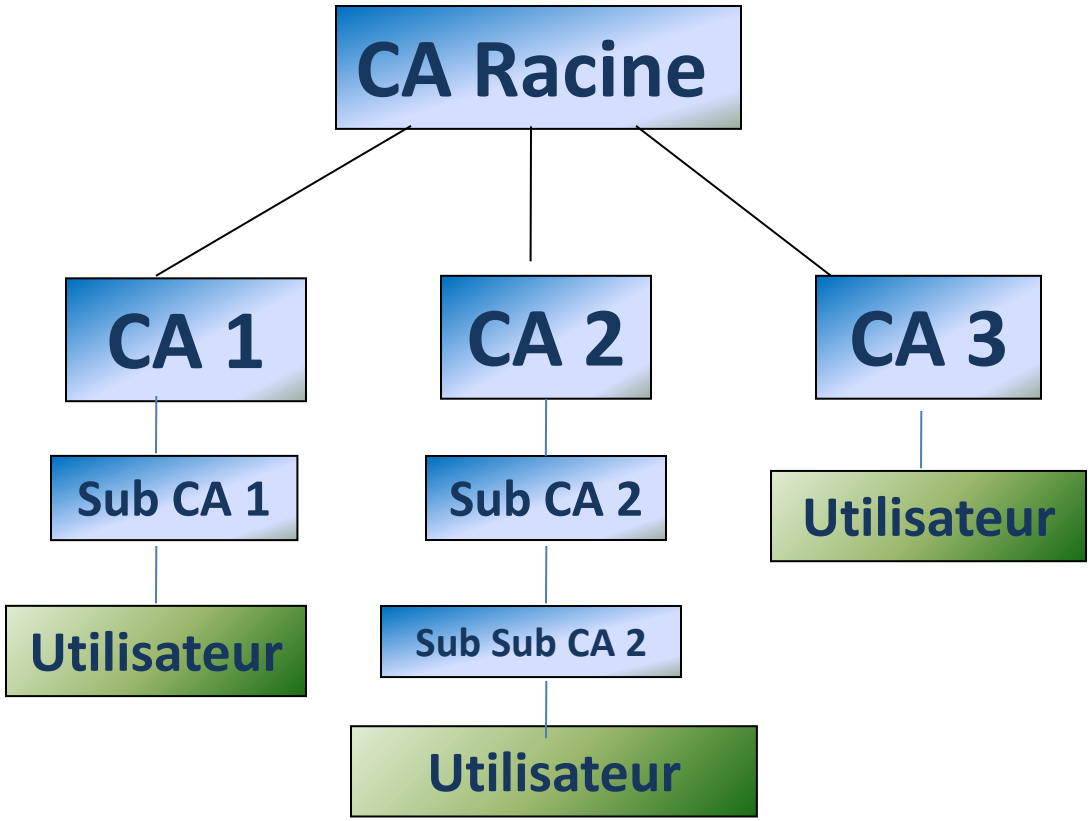


QUELQUES MODÈLES D'ORGANISATION DE LA C.E

Modèle Hiérarchique (CA Racine)

•**C'est un modèle :**
- Evolutif
- Sécurisé
- Assurant l'Interopérabilité
- Offrant un contrôle total
- Offre un chemin de certification unique et simple.

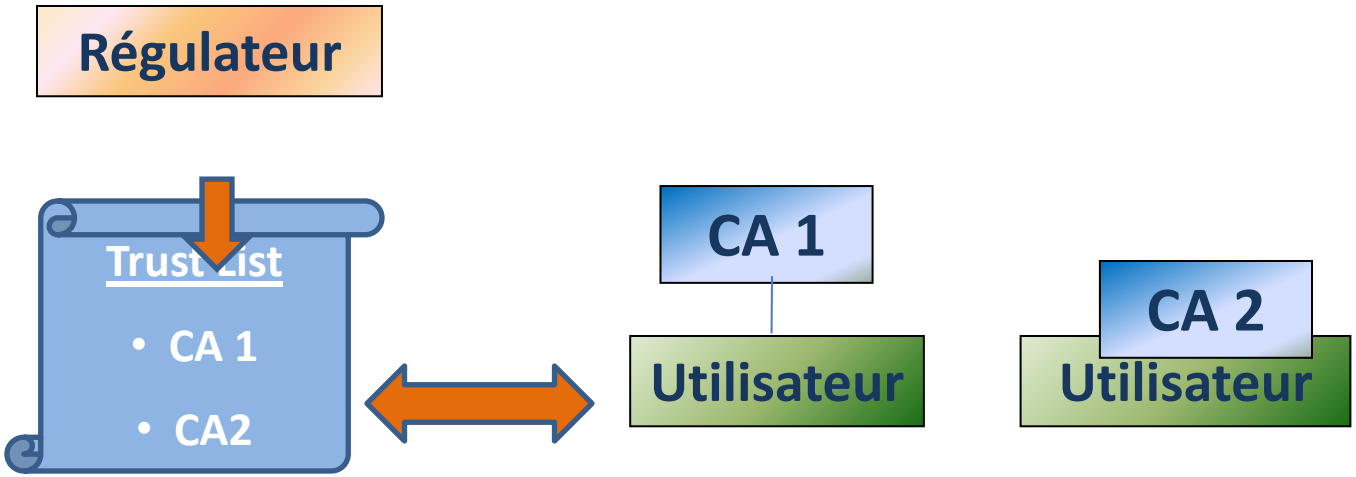
•**Mais** très rigide nécessitant un contrôle très intensif.



La CA racine pays :

•Est l'ancre de confiance.
• Certifie toutes les autres CA
•Signe les conventions de reconnaissance mutuelles avec les instances internationales.

Modèle Trust List



Une ***Trust List*** est un document publié par une entité indépendante (généralement le régulateur de l'activité de certification)

Modèle plus ouvert, plus flexible que le modèle hiérarchique

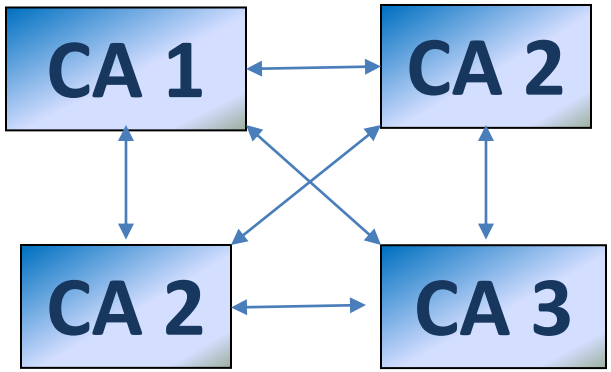
Absence de :

• Contrôle

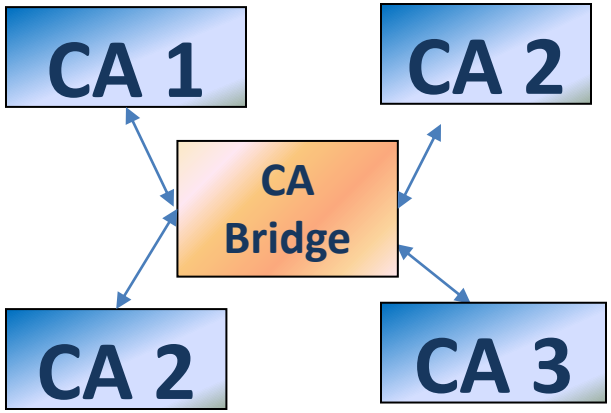
• Processus de normalisation et de validation ⟹ interopérabilité

• Une entité nationale qui signe les conventions de reconnaissance mutuelles avec les instances internationales.

Modèle Maillé / Bridge



Maillé



Bridge

Modèle maillé

- Absence de hiérarchisation.
- Absence de contrôle.
- Reconnaissance mutuelle entre **toutes** les CA

Modèle bridge

- Diminue le nombre de reconnaissances mutuelles (CA Bridge).
- Dédié généralement à un modèle d'organisation **fédéral**.

ORGANISATION DE LA C.E DANS CERTAINS PAYS

Organisation de la C.E dans certains pays

Afin d'encadrer et de réguler l'activité liés aux Tics, chaque pays a adopté sa propre approche organisationnelle en mettant en place des organismes activant dans le domaine de la **certification électronique**.

Le modèle hiérarchique
- Allemagne (BNetzA)
- Tunisie (ANCE)
- Egypte (ITIDA)

Le modèle hybride
- France

Le modèle Trust List
- Espagne (*Ministére de l'Industrie, du Tourisme et du Commerce)*
- Suisse (OFIT)

Le modèle bridge
- U.S.A (NIST)

Le choix du modèle organisationnel repose sur plusieurs facteurs néanmoins dans la plupart des cas il reste imposé par la stratégie adoptée par le pays.

La Certification électronique en Algérie

Etat des lieux

Cadre réglementaire en vigueur

- L'article 39 de la **loi 2000-03** du 05 Août 2000 fixant les règles générales relatives à la poste et aux télécommunications confère à l'ARPT le pouvoir de délivrer des **autorisations** aux prestataires de services.

- La **loi n° 05-10** du 20 juin 2005 modifiant et complétant l'ordonnance n° 75-58 relative au code civile reconnait **l'écrit électronique** comme étant un **moyen de preuve**.

- Le **décret exécutif n° 07-162** du 30 mai 2007 a expressément soumis l'activité de **certification électronique** au **régime** de **l'autorisation.**

Constat des insuffisances du cadre juridique

L'analyse du cadre juridique a dégagé un certain nombre d'insuffisances dues notamment à :

- L'insuffisance de textes réglementaires spécifiques liés à la protection des données électroniques à caractère personnel (lois 04-14 / 04-15);
- Le code civil reconnait l'écrit électronique, mais le principe de l'équivalence entre la signature manuscrite et la signature électronique n'est pas expressément consacré par ce dernier ;
- L'insuffisance de définitions spécifiques liées à la certification électronique, telles que les définitions de l'horodatage, de l'archivage électronique, l'authentification, clé de chiffrement…
- Etc…

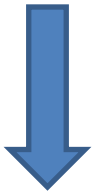
Certification électronique en Algérie

Modèle à mettre en œuvre en Algérie

Interprétation du cadre juridique en vigueur

•Les services de certification électronique au sens du décret 07-162 dans son article 3 sont **soumis à une autorisation délivrée par l'ARPT**.

•l'article **3ter du même décret** confère à l'ARPT le pouvoir de **conclure des conventions de reconnaissance mutuelle sur le plan international**.



•l'ARPT serait **le seul représentant légal de l'Etat sur le plan international** et dont les conventions seraient opposables à tous les prestataires de service de certifications algériens.

Contrôle du flux

La régulation de la circulation de l'information électronique consiste à définir le cheminement de l'information et la durée de conservation des documents électroniques.

Les expériences étrangères ont démontré la nécessité de l'existence d'une autorité de régulation des flux électroniques

(flux échangés entre l'état, l'administration, les entreprises et le citoyen).

Exemple: E-commerce

La dématérialisation des transactions commerciales implique une obligation d'archivage de ces transactions de la part des opérateurs commerciaux. D'où la nécessité d'un organisme qui contrôlera le respect de cette exigence. Cette tâche incombera au régulateur de flux qui aura toute la latitude de sanctionner les contrevenants.

Avantages du modèle (AC racine + Contrôle du flux)

Le choix d'une solution basée uniquement sur l'établissement d'une autorité de certification en l'absence d'une vision globale des flux d'information a conduit plusieurs pays à revoir toute leur approche organisationnelle suite aux différents problèmes rencontrés tel que:

- l'identification du cheminement de l'information,
- la définition des droits et obligations des différents intervenants en termes d'archivage et de stockage de l'information.

La prise en compte des expériences étrangères dans le domaine permettra à l'Algérie :

- Non seulement un gain de temps considérable en évitant d'adopter des solutions jugées déficientes et incomplètes par d'autres pays;
- La généralisation du climat de confiance;
- Au développement des Tic.

Autorité racine pays et Contrôle du Flux

De ce qui précède, on a déduit que le modèle racine est préconisé pour l'Algérie et l'ARPT aura le rôle de l'autorité de certification racine et du contrôleur de flux d'information électronique.

Ce modèle a été soumis à l'approbation des pouvoirs publics qui l'ont entériné.

Rôle de l'ARPT dans la C.E

Initialement, le rôle de l'ARPT consistera principalement à :

- Octroyer des autorisations d'exercice aux éventuels prestataires de services.
- Contrôler et auditer les prestataires ;
- Délivrer des certificats numériques aux prestataires publiques et privés.
- Mettre en place les accords de reconnaissance mutuelle avec les autorités de certification électronique étrangères.
- Réguler la circulation de l'information électronique.

Certification électronique en Algérie

La mise en œuvre

Plan de travail suivi

- ***Phase 1 :*** Etude de faisabilité faite en collaboration avec un bureau d'études espagnol.

- ***Phase 2 :*** Appel d'offre relatif à la mise en œuvre de la Certification électronique en Algérie.

- ***Phase 3 :*** Lancement du projet

Etude de faisabilité

A mis en évidence certaines carences sur les plans :

- Législatif;
- Réglementaire;
- Organisationnel.

Appel d'offres

- L'appel d'offre à été lancé le 06 Septembre 2009
- Le dernier délais de retrait des cahiers des charges était fixé au : 04 octobre 2009
- Le derniers délais de dépôt des offres : 29 octobre 2009
- Délais prorogé jusqu'au : 15 Novembre 2009

Prestations demandées

•**Tâche 1 :** Elaboration et mise en place d'un planning de mise en œuvre de l'activité de certification électronique en Algérie : les différentes étapes, les procédures à mettre en place, les équipements à acquérir ainsi que le personnel nécessaire.

•**Tâche 2 :** Proposition d'un ou de plusieurs modèles de confiance appropriés pour l'Algérie ;

•**Tâche 3 :** Proposition d'un complément du cadre juridique encadrant toute l'activité au regard de l'existant ;

•**Tâche 4:** Proposition des outils techniques et réglementaires applicables à la cryptographie ;

•**Tâche 5 :** L'élaboration du cahier des charges réglementant les droits et devoirs du Prestataire de services de certification (PSC) et de l'utilisateur ;

Prestations demandées

•**Tâche 6 :** Proposition d'une organisation interne au niveau de l'ARPT avec les profils des éléments en charge de l'activité de certification électronique.

•**Tâche 7:** Conception des procédures de délivrance des autorisations pour la prestation des services de certification ;

•**Tâche 8:** Conception des outils nécessaires pour le suivi et le contrôle des PSC ;

•**Tâche 9:** Etablissement d'une stratégie et d'un plan de communication afin de sensibiliser la société des bénéfices de l'utilisation des certificats et des signatures électroniques.

•**Tâche 10:** Elaboration d'un référentiel documentaire relatif aux accords de cross certification avec d'autres organismes internationaux. Homologation de l'autorité racine afin qu'elle soit reconnue par les instances internationales.

•**Tâche 11:** Mise en œuvre de la solution proposée : l'offre technique doit contenir une description détaillée des différentes variantes de la solution proposée.

Quelques résultats

- Vingt et un (21) prestataires ont retiré le cahier des charges
- Huit (08) prestataires ont déposé des offres
- Ouverture publique des plis a eu lieu le : Dimanche 15 Novembre 2009
- L'évaluation des offres est en cours

Conclusion

- Le modèle organisationnel pour la mise en œuvre de la certification électronique, qui offre le plus de sécurité est le modèle d'autorité racine. Ce modèle contribuera à assurer un meilleur contrôle des transactions tant au niveau national qu'international.
- L'autorité racine se verra confier la mission du contrôle de flux des données électroniques, indispensable pour la traçabilité des documents et des transactions électroniques.
- L'activité de certification sera lancé à la fin du processus de mise en place.

Merci