

Les recommandations du séminaire sur la certification électronique

Suite aux différentes interventions des experts ayant participé à notre séminaire, un ensemble de points importants a été abordé, conditionnant le succès de l'instauration d'un climat de confiance au sein d'un pays en matière de certification électronique. L'étude de ces points a permis de formuler un certain nombre de recommandations.

Celles-ci concernent cinq plans principaux à savoir : le plan stratégique, le plan organisationnel, le plan juridique, le plan sécuritaire et le plan technique et formation.

1) Sur le plan stratégique,

- Il faut envisager une stratégie nationale de cyber-sécurité afin de prévoir une vision globale de la cyber-sécurité à court et long termes dans l'ère de la numérisation.
- la certification électronique ne doit pas être une fin en soi mais plutôt un socle technologique dans une perspective d'édification d'une économie numérique et une société de l'information
- La mise en œuvre graduelle du processus de dématérialisation selon les objectifs de l'Etat et les besoins économiques du marché
- Prévoir une fédération des différents systèmes d'identification au profit du citoyen

2) Sur le plan organisationnel,

- Le choix d'un modèle de confiance repose essentiellement sur la situation spécifique à chaque pays, à savoir ses orientations politiques, ses conditions économiques propres et enfin le cadre juridique relatif à cette activité.

3) Sur le plan juridique,

- Il est important de réfléchir à la mise en place d'un cadre global lié à cette activité afin de créer un environnement ou un écosystème propice à l'édification du climat de confiance.
- La mise en place d'une veille juridique s'avère indispensable pour l'accompagnement de l'évolution de cette activité.
- La possibilité de l'option entre signature électronique sécurisée et signature électronique simple sans présomption de fiabilité a pour vertu d'élargir le champ des activités liées à la certification électronique.
- Dans le cadre de la reconnaissance mutuelle entre les différents pays, il est indispensable d'homogénéiser les règles générales de la certification électronique.
- Cependant la mise en place d'un cadre réglementaire est insuffisante à elle seule car ce dernier permet seulement la prévention et la répression des comportements délictueux. Aussi faut-il approcher la sécurité sous tous ses autres aspects : technique, juridique, politique et organisationnel.
- Il est souhaitable de prévoir avant le lancement de l'activité une réglementation qui régit l'archivage et la conservation de la valeur probante des preuves électroniques.

4) Sur le plan de la sécurité,

- La nécessité de l'élaboration d'une politique et d'une méthodologie, respectant les normes et standards internationaux d'audit et de contrôle.
- La mise en place d'une infrastructure d'accueil de la PKI adaptée aux normes en vigueur et sécurisée.

5) Sur le plan technique et formation,

- La mobilisation des ressources humaines et matérielles indispensables au lancement des PSC avant le démarrage de l'activité
- La disponibilité d'une infrastructure de télécommunications assurant une bonne qualité et une sécurité appréciable.
- La sensibilisation et la formation continue de la composante humaine.
- La sensibilisation des citoyens et la diffusion de la culture numérique

Pour finir, l'IUT s'est engagé à assister et à aider l'ensemble des pays arabes dans l'édification de la stratégie et de l'infrastructure relative au domaine des télécommunications.