

Les caractéristiques techniques du dispositif de création de la signature électronique

Arrêté du Ministre des Technologies de la Communication du 19 juillet 2001

fixant les caractéristiques techniques du dispositif de création de la signature électronique

(J.O.R.T n°60 du 27 juillet 2001)

Article 1 : Le présent arrêté fixe les caractéristiques techniques du dispositif de création de la signature électronique.

Article 2 : Toute personne désirant créer une signature électronique doit utiliser un dispositif comprenant :

- une paire de clés propre à lui, composée d'une clé privée utilisée pour la création de la signature et d'une clé publique utilisée pour la vérification de la signature,
- un mot de passe.

Article 3 : Les paires de clés sont créées par un dispositif et des procédés fiables, et ce, en tenant compte du progrès technique dans le domaine et de l'unicité et de la puissance des paires créées et du niveau d'assurance de la confidentialité de la clé privée.

Article 4 : Le dispositif de création des paires de clés doit garantir notamment :

- La création des paires de clés sous une forme conforme aux normes internationales en vigueur,
- La conformité des paires de clés aux conditions des algorithmes de création et de vérification de la signature,
- L'unicité des paires de clés.

Article 5 : Les paires de clés doivent être uniques et personnelles et elles ne peuvent être ni cédées ni transférées aux tiers à quelque titre que ce soit.

Article 6 : Le titulaire de la clé privée doit garantir les conditions de sécurité et de protection de la clé des risques de son utilisation par les tiers, et ce, par l'encodage de la clé en utilisant un mot de passe placé dans un support électronique sécurisé.

Article 7 : Le fournisseur de services de certification doit contrôler l'accès au dispositif de création déposé chez lui, identifier chaque utilisateur de ce dispositif et enregistrer toutes les opérations réalisées par l'utilisation de ce dispositif dans un registre particulier.

Article 8 : Les paires de clés sont conservées obligatoirement auprès du fournisseur de services au moyen d'un mot de passe. Elles sont divisées en plusieurs parties dont chacune est conservée auprès d'une entité différente des services du fournisseur.

Article 9 : Le fournisseur de services de certification doit vérifier la conformité du dispositif de création des clés aux conditions de sécurité prévues dans le présent arrêté et aux caractéristiques et normes internationales de sécurisation des technologies de l'information.

Article 10 : Le titulaire de la clé et le fournisseur doivent utiliser un dispositif de signature qui permet :

- De conserver et d'utiliser la clé privée au moyen d'un mot de passe,
- De cacher la clé privée après chaque utilisation.

Article 11 : En cas de perte de la clé privée, le titulaire de la clé doit demander au fournisseur de services la suspension ou l'annulation du certificat.

Article 12 : Les paires de clés utilisées par le fournisseur de services de certification électronique sont classées selon leurs fonctions en trois catégories :

- Les paires utilisées pour la création et la vérification de la signature électronique,
- Les paires utilisées pour la création et la vérification de la signature inscrite sur le certificat électronique et les registres y afférents,
- Les paires utilisées pour l'inscription de la date et de l'horaire.

Les clés ci-dessus mentionnées ne peuvent être utilisées que dans les fonctions qui leur sont réservées.

Article 13 : Le présent arrêté sera publié au Journal Officiel de la République Tunisienne.

Le ministre des technologies de la communication

AhmedFriâa

Tunis le, 19 juillet 2001