Arrêté du ministre des technologies de la communication du 19 juillet 2001, fixant les données techniques relatives aux certificats électroniques et leur fiabilité.

Le ministre des technologies de la communication,

Vu la loi n° 2000-83 du 9 août 2000, relative aux échanges et au commerce électroniques et notamment son article 17,

Vu le décret n° 2000-2331 du 10 octobre 2000, fixant l'organisation administrative et financière et les modalités de fonctionnement de l'agence nationale de certification électronique,

Vu le décret n° 2001-1667 du 17 juillet 2001, portant approbation du cahier des charges relatif à l'exercice d'activité de fournisseur de services de certification électronique.

Arrête :

Article premier. – Le présent arrêté fixe les données techniques relatives aux certificats électroniques et les conditions de leur fiabilité.

Art. 2. – Le fournisseur de services de certification électronique est tenu d'émettre les certificats électroniques conformément à la norme internationale X509, émise par l'union internationale des télécommunications, mise à la disposition de ceux qui désirent exercer l'activité de fournisseur de services de certification électronique auprès de l'agence nationale de certification électronique.

Art. 3. – Le certificat électronique comprend les informations obligatoires suivantes :

- le niveau du certificat,

- le code unique identifiant le certificat,

- l'identité et l'adresse du fournisseur qui émet le certificat,

- l'identifiant unique du fournisseur de service,

- l'identité de la personne physique ou le nom social de la personne morale titulaire du certificat ou le nom du domaine et l'identité du gestionnaire des serveurs et le nom du domaine et l'identité du gestionnaire des réseaux,

- l'identifiant unique du titulaire du certificat,

- la date du commencement et de péremption du certificat en jour, heure, minute, seconde et dixième selon l'horaire de Greenwich (GMT),

- le dispositif de vérification de la signature du titulaire du certificat et les algorithmes y rattachés,

- la signature électronique du fournisseur de service et les algorithmes y rattachés.

Le certificat électronique peut comprendre, également, les informations optionnelles prévues par la norme X509.

Art. 4. – Les certificats sont utilisés pour la réalisation des opérations suivantes :

- l'identification de son titulaire,

- l'attestation de la réalisation d'une transaction ainsi que la fixation de sa date et son horaire,

- la réalisation des opérations de commerce électronique.

Art. 5. – Le fournisseur de services de certification électronique est chargé d'octroyer un code unique particulier à chaque certificat pour le distinguer des certificats qu'il émet, ceux valables ou annulés ou suspendus, et ce, conformément aux normes adoptées par l'agence nationale de certification électronique qui est chargée de fournir au fournisseur de services les champs de ces codes.

Art. 6. – Les fournisseurs de services de certification électronique doivent, lors de la signature d'un certificat, utiliser les algorithmes suivants :

- "RSA" conformément aux normes internationales PKCS1,

- "DSS" conformément aux normes internationales FIPS 186,

- "ECDSA" conformément aux normes internationales X9.62.

Art. 7. – Le présent arrêté sera publié au Journal Officiel de la République Tunisienne.

Tunis, le 19 juillet 2001.

Le Ministre des Technologies de la Communication

Ahmed Friâa

Vu

Le Premier Ministre

Mohamed Ghannouchi

MINISTERE DE L'INDUSTRIE