



الوكالة الوطنية للمصادقة الإلكترونية
Agence Nationale de Certification Electronique
National Digital Certification Agency

La Certification Electronique

en toute **Simplicité**

Pour la Sécurité de vos échanges sur Internet



La Certification Electronique

en toute **Simplicité**

- Le certificat électronique : votre pièce d'identité sur Internet • **P.01**
 - Signez électroniquement vos documents. • **P.03**
- La technologie ICP (Infrastructure à clé Publique) • **P.05**
 - La réglementation en vigueur. • **P.06**
 - L'Agence Nationale de Certification Electronique • **P.07**
 - Comment obtenir votre certificat ANCE ? • **P.08**
 - L'installation de votre certificat personnel ANCE (MS Windows) • **P.09**
- Comment utiliser votre certificat personnel ANCE ? (messagerie sécurisée sur Microsoft Outlook) • **P.11**
 - Les applications de la certification en Tunisie. • **P.13**

Le certificat Electronique

vosre **pièce d'identité** sur Internet

Sur Internet, les interactions se font à travers un réseau ouvert, dans lequel il n'y a pas de présence physique. Nous ne connaissons donc pas l'identité des personnes avec lesquelles nous communiquons et nous échangeons. Le virtuel nous confronte à un certain nombre de risques tels que l'interception de nos messages par des tiers ou encore la réputation d'un acte de vente, de paiement ou d'échange. Dans ce cadre, la mise en place de services de sécurité tels que le certificat électronique et la signature électronique s'avère être une nécessité.

Un certificat électronique fait office de pièce d'identité électronique sur Internet et permet d'établir un environnement de confiance entre deux entités distantes (personnes physiques, serveurs web, routeurs) qui ont besoin de s'identifier pour communiquer entre elles, et d'échanger des informations confidentielles.

Un certificat spécifie le nom d'une personne, société ou entité et certifie qu'une clé publique, incluse dans le certificat, lui appartient.





Tout certificat électronique est émis par un tiers de confiance ou autorité de certification. Il s'agit d'une entité responsable de l'émission, de la délivrance et de la gestion des certificats électroniques. L'identité du propriétaire d'un certificat est garantie par l'autorité de certification.

Il existe trois types de certificats électroniques :

- **certificat personnel** : Il permet d'associer l'identité d'une personne à une clé publique. Il peut être utilisé pour signer et crypter des messages électroniques ainsi que pour s'authentifier lors d'une session sécurisée par exemple pour consulter son compte bancaire.
- **certificat serveur** : Il associe l'identité d'un serveur web à une clé publique. Il permet la sécurisation des échanges entre le serveur et ses clients lors de l'établissement d'une session sécurisée par exemple pour un achat ou paiement en ligne sur un site marchand.
- **certificats VPN** : Il permet d'associer des informations relatives à certains noeuds du réseau (routeurs, firewalls, concentrateurs, ...) à une clé publique. Ce certificat est utilisé pour garantir la sécurité des échanges effectués entre une organisation et ses filiales à travers des tunnels sécurisés dans le réseau de communication.

Signez électroniquement

VOS documents

La cryptographie à clé publique

La cryptographie à clé publique est une méthode utilisée pour transmettre et échanger des messages de manière sécurisée (authentification de l'émetteur, garantie d'intégrité et de confidentialité).

Cette technique repose sur le principe de "paire de clés asymétriques", ou "bi-clé", qui sont des clés de chiffrement. Dans ce cas, ce qui est chiffré par une clé ne peut être déchiffré que par la clé qui lui est associée et vice versa.

Chaque individu engagé dans une transaction est muni d'une "clé privée" et d'une "clé publique". Sa clé privée ne doit être communiquée à personne, tandis que sa clé publique est transmise à tous ses interlocuteurs, sans aucune restriction.

Si un individu A veut envoyer un message crypté et veut être sûr que seul B pourra le lire, il devra crypter le message avec la clé publique de B. Celui-ci ne pourra déchiffrer le message qu'avec sa clé privée (secrète).





La Signature électronique

Au même titre que la signature manuscrite, la signature électronique est un procédé qui permet, l'authentification d'un signataire ainsi que la manifestation de son consentement par rapport au contenu d'un acte signé.

Elle procure, en plus, l'intégrité des documents et la non-répudiation. La signature électronique permet donc de reproduire sur Internet l'environnement de confiance des échanges physiques (courriers traditionnels en particulier), puisqu'il devient impossible de répudier un document électronique (un bon de commande, un ordre de paiement...).

La signature électronique utilise le principe de cryptage à clé publique, le chiffrement est réalisé avec la clé privée, et le déchiffrement avec la clé publique. Un document à signer est tout d'abord traité par une fonction (hachage) qui permet d'obtenir son empreinte digitale. Celle-ci est ensuite cryptée avec la clé privée du signataire. Le résultat obtenu constitue la signature électronique du document.

Un individu A peut signer un document avec sa clé privée et l'envoyer à B. Ce dernier ne peut décrypter le document de A qu'avec la clé publique de A. Dans ce cas B aura la possibilité de vérifier que A lui a envoyé le document et que ce dernier n'a pas été altéré en cours de route.

« Infrastructure à Clé Publique »



L'infrastructure à clé publique (ICP) ou Public Key Infrastructure (PKI) est un ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

L'ICP permet de répondre aux besoins d'authentification, de confidentialité, de contrôle d'accès, de non répudiation et d'intégrité.

Une ICP est constituée de l'autorité de Certification (AC), de l'autorité d'Enregistrement (AE), d'un annuaire LDAP des certificats valides et révoqués (Liste des Certificats Révoqués LCR), d'un système d'archivage des certificats, des utilisateurs finaux et administrateurs et de la Politique de Certification qui décrit les relations entre les différents composants.

Les services offerts dans le cadre d'une ICP sont

- L'enregistrement des utilisateurs finaux
- La création des certificats
- La publication (annuaire LDAP) des certificats ou d'une LCR
- Le renouvellement des certificats
- La révocation des certificats
- L'archivage des clés de chiffrement
- La validation des certificats
- L'horodatage



L'Agence Nationale de Certification Electronique



الوكالة الوطنية للمصادقة الإلكترونية
Agence Nationale de Certification Electronique
National Digital Certification Agency

L'Agence nationale de Certification électronique (ANCE) est l'autorité de certification racine en Tunisie. Elle représente le plus haut niveau de confiance dans le domaine de la certification électronique et de la sécurité des transactions électroniques. A travers les services qu'elle propose, l'ANCE a pour but de favoriser un environnement de confiance et de sécurité des échanges sur Internet tels que les services de e-commerce, e-gouvernement, e-finance et e-banking. Pour ce faire, l'ANCE dispose de solutions de cryptage à base d'Infrastructure à Clé Publique (ICP) tels que le certificat électronique et la signature électronique.

Les services de l'ANCE

- Sécurisation des transactions et des échanges électroniques dans les domaines de e-commerce, e-gouvernement, e-banking, e-finance ...
- Etablissement des accords de confiance mutuelle avec les Autorités de Certification étrangères.
- Gestion des certificats électroniques (génération, révocation, publication et conservation de certificats)
- Octroi d'autorisations d'activité de fournisseur de service de certification électronique
- Solutions de signature électronique
- Homologation des systèmes de cryptage
- Solutions de sécurité dans le cadre de la certification électronique pour vos réseaux et services Internet et Intranet
- Formation en signature électronique et ICP

Nous faisons de votre sécurité, notre priorité

Comment obtenir

voire **certificat ANCE ?**

Certificat personnel

- Un formulaire dûment rempli.
- Copie de CIN du demandeur de certificat

Certificat personnel autorisé par l'entreprise

- Un formulaire dûment rempli.
- Extrait de registre de commerce datant d'au plus d'un mois.
- Copie de CIN du demandeur de certificat.
- Copie de la décision de la nomination du premier responsable.
- Un bon de commande ou accusé de paiement de redevances fixes selon les tarifs en vigueur.

Certificat électronique serveur web

- Un formulaire dûment rempli.
- Déclaration sur l'honneur de non-faillite pour les entreprises.
- Copie du nom de domaine.
- Extrait du registre de commerce datant d'au plus d'un mois.
- Copies des CINs (du premier responsable et du WEBMASTER).
- Copie de la décision de la nomination du premier responsable.
- Un Bon de Commande ou accusé de paiement de redevances fixes selon les tarifs en vigueur.

certificat personnel ANCE

Installation du certificat racine de l'ANCE

Avant d'installer le certificat personnel ANCE, il faut s'assurer que le certificat de l'autorité est correctement installé. Sinon il est nécessaire de procéder ainsi :

1. Téléchargez le certificat racine à partir du site Web de l'ANCE : www.certification.tn/Telechargement/cacert_mail.crt
2. Allez dans le répertoire contenant le certificat valide de l'autorité (magasin de certificats).
3. Ouvrez le certificat et vérifiez que son émetteur est bien l'ANCE ; appuyez ensuite sur le bouton « Installer le certificat ».
4. Un assistant vous guidera pour l'installation.
5. Activez la détection automatique du type du certificat
6. Confirmez l'ajout de l'autorité de confiance.
7. Pour vérifier que le certificat racine a été correctement importé, procédez comme suit :
 - a. Allez dans le panneau de configuration de Windows
 - b. Cliquez sur «Connexion réseau et Internet»
 - c. Cliquez sur «Options Internet».
 - d. Dans l'onglet «Contenu», appuyez sur le bouton «Certificats» pour ouvrir le gestionnaire des certificats.
 - e. Dans la rubrique «Autorités principales de confiance», vérifiez que le certificat racine de l'ANCE figure parmi les autorités de confiance.

Installation de votre certificat personnel ANCE

Une fois l'autorité installée, passez à l'installation du certificat de l'utilisateur :

1. Insérez la disquette délivrée par l'ANCE dans le lecteur.
2. Appuyez sur le bouton « Importer ».
3. Un assistant vous guidera durant l'installation.
4. Cliquez sur « Parcourir » pour sélectionner le certificat.
5. Saisissez le mot de passe de cryptage de la clé privée (différencier lettres minuscules et majuscules) et cochez les options d'activation de protection de la clé et l'option de clé exportable. Validez jusqu'à avoir la boîte de dialogue suivante.
6. Vous devez protéger votre clé privée en choisissant le niveau de sécurité haut et en définissant un mot de passe.

Le certificat est maintenant installé et prêt à être utilisé.

Comment utiliser votre

certificat personnel ANCE?

Le certificat électronique personnel ANCE est le garant de la sécurité de vos échanges sur Internet. Il vous permet d'envoyer des messages (e-mails) et des documents sécurisés et signés en toute confiance. Pour ce faire, il suffit de configurer votre logiciel client de messagerie de la manière suivante (Configuration de Microsoft Outlook) :

1. Lancez votre logiciel de messagerie (Outlook)
2. Sélectionnez la rubrique Outils puis choisissez Comptes
3. Dans l'onglet, Courrier sélectionnez votre compte e-mail puis cliquez sur Propriétés.



4. Dans l'onglet Sécurité, sélectionnez le certificat à utiliser pour la signature.
5. Choisissez votre certificat électronique puis cliquez sur OK
6. La démarche est identique pour le cryptage des messages. Dans l'onglet Sécurité, sélectionnez le certificat à utiliser pour le cryptage.
7. Choisissez votre certificat électronique puis cliquez sur OK

Les applications de la certification électronique en Tunisie

e-commerce

Le certificat serveur ANCE assure la sécurité de votre site marchand et vous permet d'établir une relation de confiance avec vos clients.



- Sécurité des sites marchands
- e-dinar
- Plateforme de paiement sécurisé



e-gouvernement

Grâce à la certification électronique, vous pouvez désormais faire votre déclaration fiscale sur Internet sans vous déplacer.



- Télédéclaration fiscale en ligne
- Constitution juridique des sociétés en ligne
- Déclaration des charges sociales en ligne



الوكالة الوطنية للمصادقة الإلكترونية
Agence Nationale de Certification Electronique
National Digital Certification Agency

Parc Technologique El Ghazala,
Route de Raoued, Km 3,5 – 2083 Ariana
Tel : +216 70 834 600
Fax : +216 70 834 555
e-mail : ance@certification.tn
Site Web : www.certification.tn