



Certificats Electroniques

Datasheet

Fiche produit



Autorité Gouvernementale de Certification Electronique



Le Certificat Électronique Qualifié

Le Certificat Électronique désigne un document sous forme électronique attestant du lien entre les données de vérification d'une signature électronique qualifiée et le signataire.

Tel que défini par l'Article 15 de la Loi n°15-04, le certificat électronique qualifié est un certificat électronique qui satisfait aux exigences suivantes :

1. Etre délivré par un tiers de confiance ou un prestataire de services de certification électronique conformément à la politique de certification électronique approuvée ;
2. Ne peut être délivré qu'au signataire ;
3. Doit comporter notamment :
 - Une mention indiquant que le certificat électronique est délivré à titre de certificat électronique qualifié,
 - L'identification du tiers de confiance ou du prestataire de services de certification électronique autorisé émetteur du certificat électronique ainsi que le pays dans lequel il est établi,
 - Le nom du signataire ou un pseudonyme permettant d'identifier ledit signataire,
 - La possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat électronique est destiné,
 - Des données de vérification de signature qui correspondent aux données de création de signature électronique,
 - L'indication du début et de la fin de la période de validité du certificat électronique,
 - Le code d'identité du certificat électronique,
 - La signature électronique qualifiée du prestataire de services de certification électronique ou du tiers de confiance, qui délivre le certificat électronique,
 - Les limites à l'utilisation du certificat électronique, le cas Echant,
 - Les limites à la valeur des transactions pour lesquelles le certificat électronique peut être utilisé, le cas échéant et,
 - Une référence au document certifiant la représentation d'une autre personne physique ou morale, le cas échéant.





Le Certificat Électronique Qualifié

Avantages des Certificats Electroniques de l'AGCE

Apporte la preuve de l'identité en ligne :

- L'AGCE propose des certificats électroniques qui permettent d'identifier et d'authentifier les individus, les entreprises et les appareils.
- Les certificats électroniques de l'AGCE sont légaux et hautement sécurisés pour répondre aux besoins spécifiques des entités.
- Un Tiers de Confiance reconnu : Les certificats électroniques produits par l'AGCE, sont conformes aux Référentiels internationaux WebTrust for CA, Webtrust BR SSL et WebTrust for Code Signing, ainsi qu'au règlement européen eIDAS et à la réglementation algérienne en vigueur.

Sécurise les échanges entre les utilisateurs et l'entité :

- Renforce la protection contre l'usurpation d'identité : Les certificats électroniques de l'AGCE sont délivrés selon des procédures strictes de contrôle et de vérification des pièces justificatives, pour garantir l'identité de leur propriétaire.
- Maintient les communications confidentielles grâce au chiffrement : Les certificats électroniques délivrés par l'AGCE s'appuient sur la cryptographie asymétrique pour assurer la confidentialité des échanges entre les utilisateurs et l'entité.
- Les certificats électroniques fournissent un haut niveau de sécurité à leurs utilisateurs pour s'authentifier et accéder à distance aux services et applications en ligne.





Le Certificat Électronique Qualifié

Les Certificats de Personnes Physiques

Certificat de signature qualifiée

Utilisé pour produire des signatures électroniques qualifiées (haute assurance) sur les documents et les transactions électroniques.

La différence entre la signature qualifiée et les signatures simples et avancées est forte. Ce niveau de signature électronique a des contraintes réglementaires concrètement définies en matière de vérification de l'identité du signataire. Par ailleurs, son effet juridique est équivalent à celui d'une signature manuscrite, contrairement aux autres niveaux de signature électronique. La signature électronique qualifiée est ainsi réglementairement reconnue au niveau international.

Certificat de signature avancée

Utilisé pour produire des signatures électroniques avancées (assurance modérée) sur les documents et les transactions électroniques.

La signature électronique avancée doit répondre à des critères de vérification d'identité moins strictes que la signature électronique qualifiée, disposant ainsi d'un niveau de sécurité inférieur mais probant en interne pour les entités qui souhaitent l'utiliser

Certificat d'authentification :

Utilisé pour l'authentification des utilisateurs aux services en ligne.

Les méthodes d'authentification par mots de passe ne sont plus suffisante tel qu'auparavant. L'utilisation de certificats électroniques comme facteur d'authentification permet aux systèmes d'informations de restreindre l'accès aux seuls utilisateurs autorisés.

Certificat de chiffrement (Encryption)

Utilisé pour le chiffrement des données/documents. Les certificats de chiffrement AGCE vous permettent de signer et de crypter numériquement des documents, en protégeant les individus et les organisations contre les attaques et les violations de données, et en maintenant le respect de la réglementation en matière de confidentialité et de sécurité.





Le Certificat Électronique Qualifié

Les Certificats de Personnes Morales - High Trust

TLS/SSL : Certificats pour l'authentification des serveurs et le chiffrement des données de session

TLS (Transport Layer Security) est le successeur du protocole SSL (Secure Sockets Layer).

Les certificats électroniques utilisent le protocole TLS pour garantir et assurer une connexion sécurisée entre le serveur web et le navigateur.

Le protocole TLS permet de confirmer l'authenticité du serveur avec lequel nous communiquons. Ceci est vérifiable dans la plupart des navigateurs, soit en cliquant sur le cadenas dans la barre d'adresse, soit par la couleur verte de l'adresse et le nom de l'entreprise lorsque la page web est bien sécurisée par un certificat TLS/SSL.

VPN : Certificats pour l'identification, l'authentification ou le chiffrement des données de session

Les réseaux locaux d'entreprise sont des réseaux internes des entités, c'est-à-dire que les liaisons entre machines appartiennent à celles-ci.

Les entités ressentent aujourd'hui le besoin de communiquer avec des filiales, ou même du personnel géographiquement éloignées via internet mais de façon sécurisé.

Le certificat VPN est un certificat installé dans les équipements réseaux, permettant de chiffrer les flux de communication entre deux points (par exemple deux sites d'une entreprise).





Le Certificat Électronique Qualifié

Les Certificats de Personnes Morales - High Trust

Code Signing : Utilisé pour signer un code source/logiciel développé par une entité

Des programmes non signés peuvent subir des modifications, par exemple par l'insertion de logiciels espion ou code nuisible, puis être redistribués.

Une signature de code permet de prouver qu'un programme est légitime, provient d'une entité connue et que le code n'a pas été modifié depuis sa publication. Ceci ajoute un niveau de confiance supplémentaire à l'application.

eSeal (cachet électronique)

Utilisé pour ajouter un cachet électronique sur un document délivré par une entité.

Le cachet électronique eSeal est un moyen de sceller les documents des entités. Il s'agit d'une version électronique du cachet d'entreprise et est donc dédié aux personnes morales.

Grâce au cachet électronique, l'origine de tous les documents électroniques est garantie. L'horodatage qualifié inclus dans le service de cachet électronique, permet également aux documents de bénéficier d'une garantie supplémentaire en matière d'intégrité.

De par sa valeur juridique, le cachet électronique eSeal de l'AGCE renforce la valeur des documents professionnels dématérialisés et aide à prévenir toute contestation sur leur intégrité ou leur origine.

Le cachet électronique eSeal est également un moyen efficace de lutter contre la fraude documentaire.

