

Certificat et Signature électroniques

Partenaire Certificat SSL et Signatures



La signature électronique est associée à un certificat électronique personnel.

Elle authentifie le signataire et scelle numériquement le contenu associé, ce qui permet de déceler toute altération ultérieure du document même minime.

Le certificat électronique personnel est une identité électronique.

Il associe le signataire, une clé secrète et le domaine d'application de cette identité. Il permet de signer électroniquement tous types de documents. L'utilisateur a la responsabilité de l'usage de cette identité.

- Le signataire doit être équipé d'un certificat accepté par l'organisme proposant la signature électronique.
- Les règles élémentaires de sécurité doivent être respectées (accès restreints, codes confidentiels,...)
- L'organisation des pouvoirs de signature doit respecter les exigences de sécurité propres à l'entreprise.

Un certificat peut être délivré selon deux modes

- Dans un support matériel : soit fixe, sur un disque dur, soit mobile sur une carte à puce ou clé USB.
- Sous une forme logicielle : acceptés dans toutes les téléprocédures des autorités administratives.

Le certificat est émis par une tierce partie de confiance pour une personne ou une entité réseau.

Du point de vue juridique, on distingue deux types de signature électronique :

- **La signature simple** : la charge de la preuve de la validité de la signature revient au signataire.
- **la signature sécurisée ou qualifiée (SEQ)** : certifiée par un organisme agréé, elle bénéficie d'une présomption de fiabilité en justice : la charge de la preuve revient à l'organisme qui conteste la signature.

Trois classes de certificat électronique pour trois niveaux de confiance.

En fonction de ses besoins, l'utilisateur peut acquérir une solution payante ou gratuite, correspondant à un niveau de sécurité variable :

- Classe I : ne garantit pas l'identité du titulaire mais seulement l'existence de son adresse e-mail.
- Classe II : garantit l'identité du titulaire, sur pièces justificatives transmises par voie postale.
- Classe III : garantit l'identité du titulaire, sur pièces justificatives présentées par le demandeur.
- Classe 3+ : certificat de classe III, sur support physique (carte à puce ou clé USB).

Nos solutions fonctionnent avec les matériels standards de numérisation et sont compatibles avec Windows à 100%
www.syged.com Agences Languedoc-Roussillon, PACA, Rhône-Alpes, Paris, Antilles

Les certificats électroniques personnels (personne morale ou physique) permettent différents usages de la signature électronique :

- **Gestion de la TVA et des impôts :** Déclaration, consultation des déclarations, paiement et suivi des paiements, des créances et des remboursements de crédits (Chambersign / Télétva ; Le compte fiscal)
- **Gestion des cotisations sociales :** Déclarations sociales par mail ou Internet et règlement de cotisations par e-mail Chambersign / Portail Net Entreprise ; Ducs-Edi)
- **Gestion du parc de véhicules :** Déclaration d'achat et de cession de véhicules, et délivrance de cartes grises sans se déplacer à la Préfecture (Chambersign / Téléc@rte Grise ; SVI)
- **Gestion des marchés publics :** Réponses à des appels d'offres en ligne (Chambersign / Marché publics)
- **Gestion des documents internes :** (Contrats, bons de commande, congés, factures (Chambersign / Signatures de documents ; Factures dématérialisées)
- **Gestion des correspondances :** Sécurisation de mails, lettre simple et courrier recommandé (Chambersign / Sécuriser les mails ; courrier dématérialisé)

La mise en œuvre de la signature électronique s'appuie sur des solutions logicielles et des services mutualisés de gestion en masse ou en mode embarqué, répondant aux différentes problématiques générées par la dématérialisation « légale » :

- **La signature de documents électroniques en ligne :** sans déploiement sur le poste client, et activable par tout moyen d'authentification existant (KEYNECTIS / Websign)
- **La signature de documents PDF, vérifiable par tout interlocuteur :** depuis n'importe quel poste, avec un certificat électronique personnel stocké sur clé USB, ou en masse sur l'intranet de l'organisation : (KEYNECTIS / K.Sign® for PDF ; K. Signer for PDF)
- **La gestion des PKI (clés publiques) :** permettant d'émettre, de valider et de contrôler les cycles de vie des certificats électroniques, des autorités de certification et/ou d'enregistrement d'une organisation, (Solutions logicielles ou services mutualisés : KEYNECTIS / Séquoia ; Keyseed ; Trust Center ; K Registration)
- **L'horodatage électronique :** permettant d'apposer un jeton d'horodatage sur les documents électroniques en gérant plusieurs sources de temps (KEYNECTIS /K.Stamp®)

La dématérialisation est implicite pour les informations ou documents publiés et circulant via Internet, et génère également des besoins de sécurisation vis-à-vis des sources de données, comme de leurs utilisateurs.

L'usage de certificats SSL permet d'authentifier les serveurs et les utilisateurs d'Internet et de sécuriser ainsi les transactions réalisées par accès distant (réseaux intranet et extranet, site web).

Un certificat SLL permet de contrôler l'accès aux informations sensibles d'une plate-forme Internet et d'identifier les utilisateurs, avec une efficacité supérieure à l'usage du login et mot de passe.

Nos solutions fonctionnent avec les matériels standards de numérisation et sont compatibles avec Windows à 100%
www.syged.com Agences Languedoc-Roussillon, PACA, Rhône-Alpes, Paris, Antilles

Délivrance et reconnaissance des certificats SSL :

Les certificats Internet sont des identités électroniques délivrées par des autorités de certification (CA), tierces parties de confiance servant de caution morale, dont le crédit confèrera un champ d'exploitation variable aux certificats délivrés.

Ces CA peuvent être reconnus par le navigateur d'un utilisateur, si le certificat de l'autorité de certification a été installé sur le navigateur. La procédure d'authentification d'un certificat serveur ou utilisateur fait appel à une connexion sécurisée par SSL (Secure Socket Layer).

Sécurité et sauvegarde des certificats SSL :

Les certificats sont protégés par des clés privées (codes) associées, et restent sous la responsabilité de leurs propriétaires.

Les propriétaires se doivent de garantir leur sécurité et leur confidentialité par tous les moyens disponibles :

- Certificats stockés dans une base de certificats : l'accès à la base doit être protégée par un mot de passe local.
- Certificats stockés dans une base non sécurisée : le poste contenant la base de certificats non protégée doit être protégé par un mot de passe.

La copie des certificats et clés privées sur un support de stockage externe permet d'assurer leur sauvegarde et autorise leur exploitation à partir de divers point d'accès Internet (mode embarqué).

L'authentification des serveurs et des internautes s'effectue grâce à deux types distincts de Certificats SSL.

✓ Les certificats serveurs

Le certificat serveur permet de prouver à l'internaute utilisateur l'identité du serveur émetteur d'informations selon deux modes possibles :

- Avec installation du certificat de l'autorité de certification : l'utilisateur s'assure alors de la signature du certificat serveur par le CA reconnue par son navigateur.
- Sans installation du certificat de l'autorité de certification : Le certificat du serveur est présenté à l'utilisateur qui lui accordera ou non sa confiance, via validation d'une fenêtre d'information. Le niveau de sécurité de cette option est plus faible que celui de la précédente.

✓ Les certificats utilisateurs

Les certificats utilisateurs sont des certificats personnels qui permettent aux utilisateurs de s'authentifier auprès d'un serveur.

✓ Les certificats temporaires

Les certificats temporaires sont exploitables lorsqu'un certificat permanent est indisponible. Doté d'un n° de série et émis sur autorisation de l'administrateur du certificat permanent, le certificat temporaire est automatiquement invalidé au bout de 24 heures mais sa demande peut être renouvelée.

Nos solutions fonctionnent avec les matériels standards de numérisation et sont compatibles avec Windows à 100%
www.syged.com Agences Languedoc-Roussillon, PACA, Rhône-Alpes, Paris, Antilles

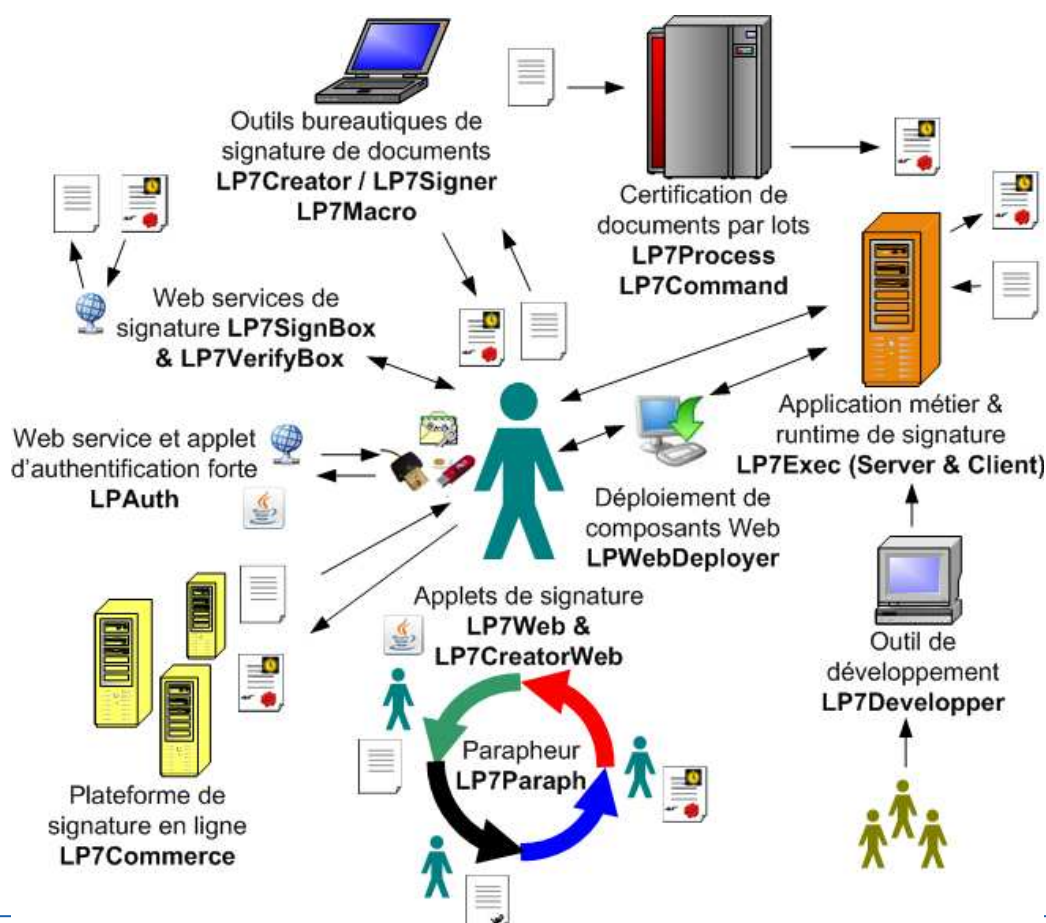
Des services associés à la délivrance des Certificats SSL permettent d'en faciliter l'accès et la gestion :

- Délivrance de certificat SSL à l'unité ou en masse
- Possibilité de centraliser ses demandes
- possibilité d'émettre ses propres certificats grâce à des droits d'émissions délivrés pour une période donnée avec validation en ligne par l'autorité de certification
- Outils de contrôle centralisé de tous les certificats SSL de l'organisation...

Partenaire Logiciels de signature



Syged met à votre disposition un ensemble d'outils pour authentifier vos



Nos solutions fonctionnent avec les matériels standards de numérisation et sont compatibles avec Windows à 100%
www.syged.com Agences Languedoc-Roussillon, PACA, Rhône-Alpes, Paris, Antilles

Environnement Bureautique → pour dématérialiser les actes de commerce ou les processus réglementaires : factures, commandes, devis, appels d'offre...

- **LP7Creator**, outil bureautique de création et de vérification de signature, validé Banque de France ; supporte les formats PDF signé, XAdES & CAdES ;
- **LP7Signer**, permet à son utilisateur de signer ou de contresigner des preuves électroniques en nombre illimité, de les vérifier et d'en extraire le contenu signé, etc.
- **LP7Macro**, macros pour signer électroniquement les documents depuis Microsoft Word, Excel et PowerPoint ; intégré à Microsoft Office
- **LP7Command**, logiciel qui peut être appelé depuis n'importe quelle application en «mode shell» pour certifier, signer et horodater tous types de documents

Environnement Web → pour les applications de type Intranet, Extranet, B2B ou Internet B2C

- **LP7Web et LP7CreatorWeb** : solution complète de signature électronique sécurisée, facile à intégrer dans toute application métier disponible en mode Web
- **LP7Commerce** : une plateforme de signature en ligne qui permet de dématérialiser les transactions commerciales, quel que soit le contexte de la relation client, distante via Internet, ou en face à face sur le point de vente
- **LP7Paraph** : un parapheur électronique communicant pour faire viser et signer en mode Web tous types de documents électroniques à valeur probatoire
- **LPWebDeployer** : outil pour faciliter le déploiement de logiciels et composants Web
- **LPAuth** : permet à l'utilisateur de s'authentifier d'une manière forte à un site web

Environnement Serveur → pour les applications lourdes qui touchent le cœur de l'entreprise

- **LP7Process** : logiciel qui permet de certifier et de vérifier les documents ou flux électroniques de toute nature, de manière industrielle, au fil de l'eau, ou par lot, de manière totalement automatisée
- **LP7Signbox** : un Web Service de signature pour signer et horodater, à la volée, tout type de document électronique, et garantir sa valeur probatoire
- **LP7Verifybox** : un Web Service de validation de signature pour vérifier tout type de preuve électronique et garantir son intégrité, son authenticité et sa validité

Environnement Développement → pour intégrer la gestion des preuves électroniques aux applications d'entreprises existantes : applications spécifiques, intégration base de données, GED, ERP, CRM...

- **LP7Developer** : destiné au SSII, aux Editeurs et aux Intégrateurs désireux de développer des applications de signature électronique pour leurs clients ou bien afin d'intégrer des fonctions de signature électronique dans leurs applications ou progiciels existants.
- **LP7Exec** : permet aux développeurs d'intégrer la signature électronique dans les applications métiers

Nos solutions fonctionnent avec les matériels standards de numérisation et sont compatibles avec Windows à 100%
www.syged.com Agences Languedoc-Roussillon, PACA, Rhône-Alpes, Paris, Antilles