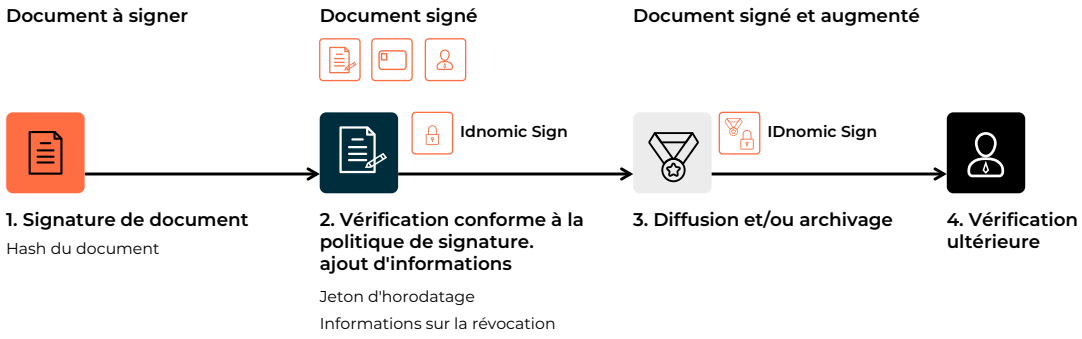
EVIDEN

IDnomic Sign

Création et vérification de signatures électroniques non répudiables

Dans le contexte de dématérialisation des échanges, il devient nécessaire de pouvoir signer électroniquement des documents pour en garantir l'intégrité et pour apporter la preuve du consentement par le signataire. La signature doit pouvoir ensuite être vérifiée rigoureusement pour détecter tous les cas d'invalidité, quelques puissent être les circonstances. Eviden, acteur européen de la sécurité, propose avec IDnomic Sign, une solution complète de génération et de vérification de signatures électroniques.



Garder le contrôle sur la sécurité

Les signatures électroniques permettent d'assurer l'intégrité des documents et d'identifier les signataires. Une fois qu'un signataire a produit une signature et que celle-ci a été validée, il ne peut plus la répudier. C'est la propriété essentielle d'un service de non-répudiation.

Chaque signataire utilise une paire de clés, publique et privée, ainsi qu'un certificat généré par une Autorité de Certification.

Avec IDnomic Sign, Eviden propose une plateforme de signature électronique d'un très haut niveau sécuritaire, performante et flexible qui s'intègre nativement avec les composants d'une infrastructure de confiance. Disponible sous forme logicielle ou en mode SaaS, IDnomic Sign facilite la dématérialisation des processus métier et ainsi la transformation digitale des organisations.

Le serveur IDnomic Sign offre aux entreprises le moyen de mettre en œuvre au sein de leur système d'information une stratégie sécurisée et centralisée de signature électronique :

- Gestion du cycle de vie des clés cryptographiques des signataires afin qu'ils puissent réaliser une signature électronique à distance.
- Définition par l'entreprise, selon le cas d'usage et sa criticité, de la politique de signature à appliquer (formats, algorithme de signature, longueur des clés, etc...).
- Création de signatures de personnes morales (mode cachet) ou des signatures de personnes physiques.
- Mise en œuvre de workflows de signature, pour orchestrer la signature d'un document entre les différents acteurs d'une procédure métier
- Gestion améliorée et personnalisée des visuels de signature pour les formats PAdES
- Un tableau de bord général présentant les principaux indicateurs de fonctionnement du serveur de signature,

EVIDEN

Le serveur IDnomic Sign

IDnomic Sign offre les principales fonctions suivantes :

- **Création de signature**: création au format attendu en utilisant la politique de signature et la ressource cryptographique configurée ;
- **Vérification immédiate et augmentation**: vérification cryptographique après sa création et ajout d'informations afin d'en maintenir la validité sur le long terme avec constitution d'un rapport détaillé.
- **Vérification ultérieure**: vérification a posteriori avec constitution d'un rapport détaillé.

IDnomic Sign génère et vérifie des signatures électroniques avancées dans les formats CAdES, XAdES et PAdES en conformité avec des politiques de signature normalisées. IDnomic Sign s'appuie sur un service d'horodatage externe comme la solution TSP d'IDnomic ou des services d'horodatage tiers respectant la RFC 3161.

Ce serveur est accessible en mode « Web services » (API REST) permettant l'intégration de la signature électronique au sein des applications métiers de l'entreprise.

Le serveur de signature offre également un portail de signature qui peut être utilisé directement par les utilisateurs authentifiés sur le serveur, pour signer et vérifier des documents, gérer ses clés de signature et ses préférences.

Pour réaliser la signature, les signataires peuvent utiliser des certificats de signatures stockés dans une carte à puce, soit des certificats préalablement enrôlés et sécurisés en central au niveau du serveur IDnomic Sign ou encore des certificats de courte durée générés à la volée au moment de la signature. L'interface avec la PKI peut être réalisée avec le protocole propriétaire pour la PKI ID PKI ou avec les protocoles normalisés SCEP ou EST pour n'importe quelle PKI respectant ce protocole.

IDnomic Sign permet de définir des politiques de signature évoluées, utilisées au moment de la construction de la signature et de la vérification afin de contrôler et d'autoriser cette dernière.

La signature électronique au format PAdES (fichier pdf) autorise l'insertion d'une représentation visuelle de la signature dans le document signé. Chaque utilisateur peut gérer ses propres visuels, sur la base de modèles mis à disposition par l'administrateur de la solution.

IDnomic Sign dispose également de la fonction parapheur.

Pour des entreprises importantes ou pour des opérateurs (tiers de confiance), IDnomic Sign permet avec une installation unique de servir plusieurs "tenants" en totale isolation. Ainsi, il sera possible de servir des projets ou des clients différents sans aucune perméabilité entre les données utilisées dans chacun des tenants.

Vérification avancée des certificats

Vericert est un composant serveur, optionnel de IDnomic Sign. Il permet de construire et de vérifier les chemins de certification vis à vis des politiques de validation configurées dans son administration. Les services de vérification sont disponibles en mode web service. La vérification peut se faire par rapport à l'instant présent ou par rapport à une date passée. Les Autorités de Certification de confiance peuvent être extraites automatiquement des « Trusted List » (TSL) européennes.

Standards et spécifications techniques

Normes et standards

» Format de certificat compatible avec ITU-T X.509v3, RFC 5280 et RFC 3739t
» XAdES : XML Advanced Electronic Signature ETSI TS 101 903
» CAdES : CMS Advanced Electronic Signature ETSI TS 101 733
» PAdES : PDF Advanced Electronic Signature ETSI TS 102 778 incluant le format LTV (part 4) et le visuel de signature (part6)
» Format des politiques de signature XML ETSI TR 102 038
» RFC 3161 : Protocole d'obtention des contremarques de temps (jetons d'horodatage)
» Authentification OpenID Connect et OAuth2
» PKCS#11 pour les interfaces avec un module de sécurité matériels (Hardware Security Module – HSM)
» Algorithmes de signature ECDSA et/ou RSA disponibles dans le HSM utilisé

Conformité

» Conforme à la directive européenne 1999/93/CE et au réglement eIDAS
» La bonne implémentation des normes et standards est validée par la participation fréquente aux Plugtests d'interopérabilité de l'ETSI.

Configuration requise

» Exécutable sur l'environnement d'exécution Java 11
» Linux (Red Hat/ CentOS 7.5 ou supérieur).
» Intégré et livré avec les composants Open Source Apache, PostgreSQL, Tomcat, Ansible (script d'installation).
» L'authentification sur le serveur de signature IDnomic Sign doit être déléguée à un fournisseur d'identité (Identity Provider) utilisant les mécanismes d'authentification OpenID Connect et OAuth2.

En savoir plus sur nous: www.idnomic.com

Connectez-vous avec

eviden.com