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. Atos, acteur européen de la sécurité, propose **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.

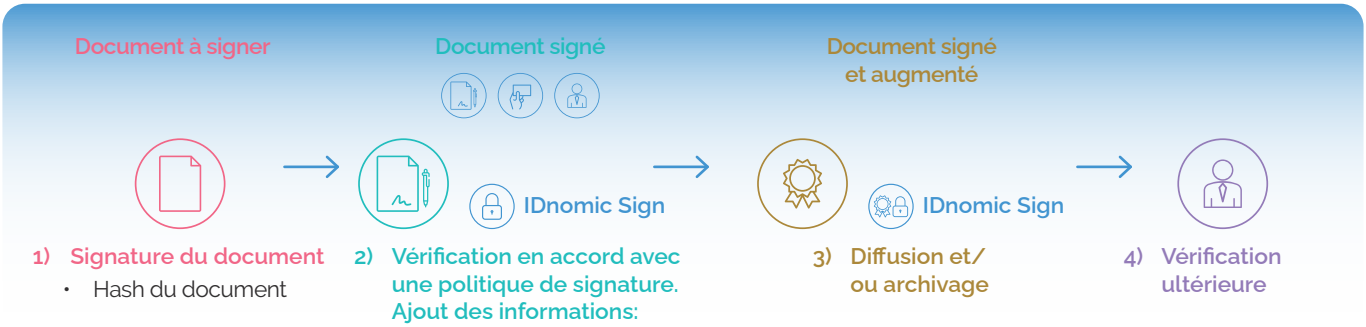
Chaque signataire utilise une paire de clés, publique et privée, ainsi qu'un certificat généré par une Autorité de Certification. Le serveur IDnomic Sign est en mesure d'utiliser des certificats fournis par la solution ID PKI d'Atos ou par tout autre solution IGC (ou PKI) du marché.

Le serveur IDnomic Sign gère les clés cryptographiques au nom des signataires. Il les stocke de manière sécurisée et n'en autorise l'accès qu'à son propriétaire. Il permet également dans une intégration web d'utiliser des clés stockées localement dans une carte à puce par exemple.

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 comme la solution TSP d'IDnomic ou des services d'horodatage tiers.

IDnomic Sign offre les fonctions suivantes :

- **Création de signature:** création au format attendu en utilisant la politique de signature et la ressource cryptographique configurée ; signature multiple et co- signature
- **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.



Atos

L'offre IDnomic Sign et ses fonctionnalités

Le serveur IDnomic Sign

Le serveur IDnomic Sign offre une mise en œuvre centralisée d'un service implémentant toutes les opérations de la signature électronique sécurisée et de la vérification de signatures.

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

Il dispose également d'une fonction portail de signature.

Le serveur permet de créer des signatures de personnes morales (mode cachet) ou des signatures de personnes physiques avec gestion sécurisée des bi-clés des signataires.

Les signataires peuvent utiliser des certificats de signatures stockés dans une carte à puce qu'ils détiennent, ou des certificats localisés en central au niveau du serveur IDnomic Sign.

Politiques de signature normalisées

IDnomic Sign permet de définir des politiques de signature évoluées. Ces politiques seront utilisées au moment de la construction de la signature afin de contrôler et d'autoriser pour une politique donnée, un algorithme de chiffrement, une taille de clés, une autorité de confiance, etc…

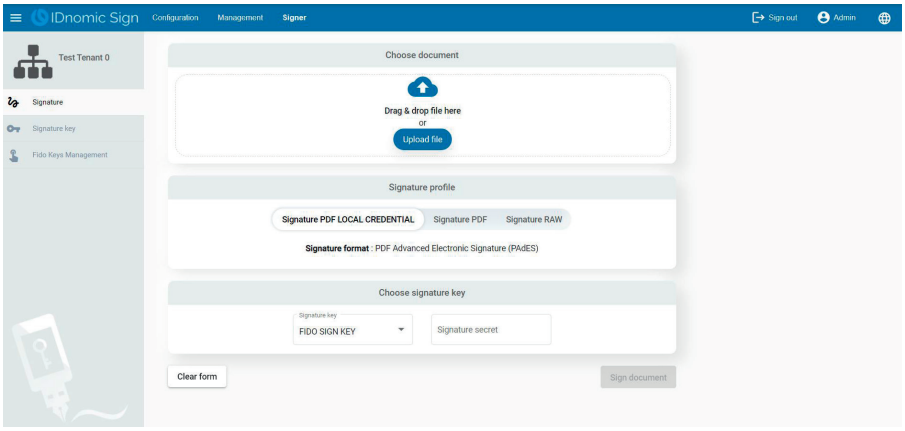
Vérification avancée des certificats

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.

Signature Qualifiée à distance

En option du serveur IDnomic Sign, Atos propose pour réaliser des signatures qualifiées à distance en conformité avec eIDAS, une appliance dédiée, « l'Explicit Consent Manager ». Ce matériel est utilisé pour gérer en complément du serveur IDnomic Sign, le consentement du signataire via un OTP ou une authentification FIDO. Cette appliance se comporte comme un « Signature Activation Module (SAM) » selon la terminologie de l'ETSI CEN 419 241-2.

Atos est engagé dans un processus de certification avec l'ANSSI pour cette appliance.



Normes et spécifications techniques

Normes et standards

- Format de certificat compatible avec ITU-T X.509v3, RFC 5280 et RFC 3739
- 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
- Authentification Open ID Connect pour l'API REST
- PKCS#11 pour les interfaces avec un module de sécurité matériels (Hardware Security Module – HSM)
- Local credentials

Conformité

Conforme à la directive européenne 1999/93/CE et au réglement eIDAS

Exigences techniques

IDnomic Sign est exécutable sur l'environnement d'exécution Java 11

La bonne implémentation des normes et standards par IDnomic Sign est validée lors de la participation fréquente aux Plugtests d'intéropérabilité de l'ETSI

Le serveur IDnomic Sign s'exécute sur Linux (Red Hat/ CentOS 7.5 ou supérieur). Le produit est complètement intégré et livré avec les composants Open Source Apache, PostgreSQL, Tomcat, Keycloak (fournisseur d'identité), Ansible (script d'installation).

Veuillez trouver plus d'information sur atos.net/fr/solutions/cybersecurite/identites-numeriques-de-confiance/idnomic-sign