IDnomic metasign

Création de signatures non répudiables et vérification dans le temps

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 **metasign**, une solution complète de génération et de vérification de signatures électroniques.

Garder le contrôle de 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 - une personne ou une application - utilise une paire de clés, publique et privée, ainsi qu'un certificat généré par une Autorité de Certification.

Metasign est en mesure d'utiliser des certificats fournis par la solution metapki de Atos ou par tout autre solution IGC (ou PKI) du marché.

Pour les personnes, metasign utilise des certificats et des clés privées qui peuvent être stockés dans une carte à puce, dans une clé USB, ou encore dans un fichier supportant le format PKCS#12. Les clés privées et les certificats sont accessibles via l'interface PKCS#11 ou MSCAPI.

Pour les applications, metasign interface des modules de sécurité matériels (HSM - Hardware Security Modules).

Metasign génère et vérifie des signatures électroniques avancées dans les formats CAdES, XAdES et PAdES en conformité avec les politiques de signature. metasign s'appuie sur un service d'horodatage comme la solution Digital ID de Atos ou des services d'horodatage tiers.

Metasign 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 à posteriori avec constitution d'un rapport détaillé.

Trusted partner for your **Digital Journey**

Atos

L'offre metasign et ses fonctionnalités

Metasign-server

Metasign-server délivre ses services de signature et de vérification de signature dans le mode « web service » (SOAP et REST). L'administration graphique du serveur permet de configurer les usages des applications ainsi que les politiques de signatures. Le serveur permet de créer des signatures de personnes morales (mode cachet) ou des signatures de personnes physiques avec gestion sécurisée, en central, des bi-clés des signataires.

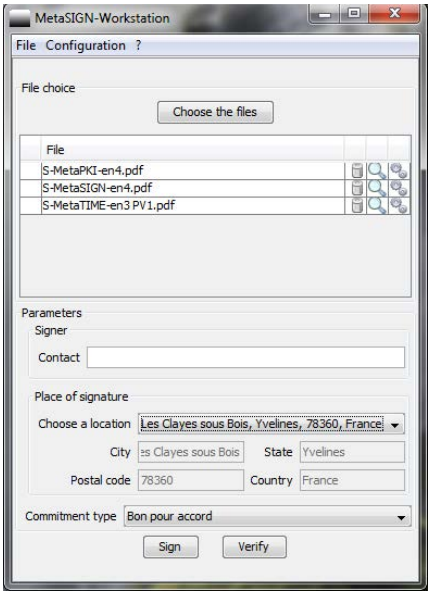
Metasign-api

Metasign-api constitue un ensemble d'interfaces programmables en Java permettant de construire les natures d'applications suivantes :

- Applets Java pour les navigateurs web
- Des applications autonomes pour les ordinateurs personnels
- Des applications supportées par un serveur.

Metasign-workstation

Metasign-workstation est une application graphique destinée aux postes de travail, elle permet de signer plusieurs documents en une seule étape. La simplicité d'utilisation et du déploiement de la signature électronique est l'objectif recherché par cette application.

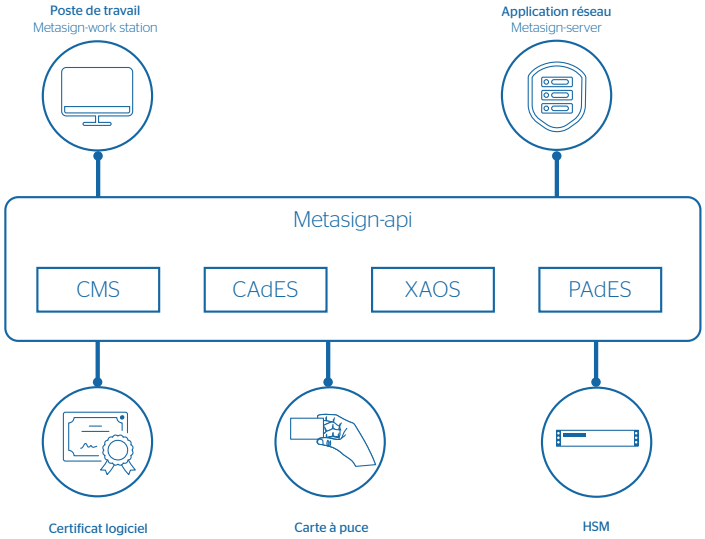


Vericert

Vericert est un composant serveur, optionnel de metasign. Il permet de construire et/ou 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 des « Trusted List » (TSL) européennes.

Formats de signatures

Metasign génère et vérifie des signatures électroniques avancées conformes aux standards CMS, CAdES (CMS Advanced Electronic Signature), XAdES (XML Advanced Electronic Signature) et PAdES (PDF Advanced Electronic Signature) définis par les spécifications techniques de l'ETSI (European Telecommunication Standardisation Institute).



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 • PKCS#11 et MSCAPI pour les interfaces avec les supports cryptographiques. Support des cartes IAS et lecteurs PINPAD • PKCS#11 pour les interfaces avec un module de sécurité matériels (Hardware Security Module – HSM) • PKCS#12 pour le stockage (dans le cas fichier) des clés privées de signature et des certificats

Conformité
Conforme à la directive européenne 1999/93/CE et au réglement eIDAS
✓ VISA DE SÉCURITÉ Atos a reçu le 25/03/2016 de l'ANSSI le Visa de sécurité pour la certification Critères Communs au niveau EAL 3 augmenté de ses produits MetaSIGN-API et MetaSIGN-Applet version 3.3.5.

Exigences techniques
Metasign est exécutable sur l'environnement d'exécution Java 8
La bonne implémentation des normes et standards par metasign est validée lors de la participation fréquente aux Plugtests d'intéropérabilité de l'ETSI
Les solutions serveur Vericert s'exécutent sur des plateformes Linux (c-à-d Red Hat or SUSE). Ces solutions sont complètement intégrées et livrées avec les composants Open Source Apache, PostgreSQL, PHP et Tomcat

Veuillez trouver plus d'information sur
atos.net/fr/products/cyber-security/digital-identities/metasign