



a Sopra Steria company

TrustyServerSeal® est une solution de confiance offrant les services de cachet électronique et validation de cachet électronique.

S'adresse aux organisations qui souhaitent :

Une solution serveur unifiée et performante de **gestion des cachets électroniques**.

TRUSTY ServerSeal

TrustyServerSeal® est une plateforme centralisée :

- Qui autorise la réalisation de cachet électronique, de **tout type de document** et de leur validation,
- Qui est rendue **accessible au réseau d'entreprise** via des protocoles standards,
- Qui peut **s'interfacer avec différents services** de confiance pouvant être requis pour la gestion, l'administration (horodatage, validation de certificats, enrichissement du cachet électronique...).

Performance

TrustyServerSeal® a été conçu avec une architecture haute disponibilité pour offrir des performances élevées.

A titre d'exemple, TrustyServerSeal® permet à des administrations publiques de générer et valider des cachets électroniques en volume (une dizaine de millions de signatures cachet serveur par an) sur tout type de document, dont des procédures pénales pour en garantir l'intégrité et l'authenticité de leur origine.

Simplicité de déploiement et d'exploitation

Le rapprochement de différents services au sein d'une plateforme centralisée apporte une grande simplicité de déploiement, et permet la mutualisation de matériels et ressources d'exploitation.

TrustyServerSeal® est capable de s'adapter à de nombreux contextes de déploiement (on premise ou cloud) grâce aux possibilités étendues de configuration de chacun des services.

Conformité et sécurité

- TrustyServerSeal® s'appuie sur des services cryptographiques matériels certifiés pour proposer des mécanismes cryptographiques **à l'état de l'art**.
- TrustyServerSeal® est conforme au **Référentiel Général de Sécurité (RGS)** de l'administration française.
- TrustyServerSeal® sera prêt à la migration vers la **cryptographie post-quantique (PQC)** en conformité avec les nouveaux standards du NIST (FIPS 204 et FIPS 206) ou des exigences françaises régaliennes spécifiques. Les formats de cachet électronique CAdES, XAdES et PAdES ont déjà fait l'objet d'expérimentation avec les algorithmes PQC suivants : Falcon, Crystals-Dilithium Crystals-Dilithium et GeMSS.

Exploitation personnalisée

L'administrateur de TrustyServerSeal® peut configurer finement les règles à appliquer lors :

- De la création du cachet électronique et de leur vérification,
- De la validation de certificats.

Ces politiques sont déclarées par l'administrateur de sécurité.

TrustyServerSeal® permet, en plus, de configurer les droits d'accès et d'usage par application cliente et par politique de cachet ou de chiffrement.

Les fonctionnalités additionnelles offertes par TrustyServerSeal® :

- Sur demande du client, horodater les cachets via TrustyTime® à l'issue du processus de cachet et de validation de cachet.
- Ré-horodater, via TrustyTime®, pour la préservation de l'intégrité des données et la maintenance de leur caractère « non répudiable » sur le long terme.
- Enrichir avec les chaînes de certification et les listes de révocation actualisées, en vue d'une conservation du document signé sur le long terme.

Caractéristiques Techniques

Plateforme

- Serveurs physiques
- Machines virtuelles

Signature

- Formats XAdES, PAdES, CAdES
- Niveaux B, T et LTA
- Signatures RSA 3072, 4096 bits

Horodatage (option)

- Compatible avec les serveurs d'horodatage RFC3161

Validation de certificat et service

- OCSP (RFC 2560) pour fournir le statut de révocation du certificat (en mode proxy et/ou autonome)
- Support de plusieurs hiérarchies d'Autorités de Certification (AC)
- Cache de CRL

Ressources cryptographiques

- HSM Bull TrustWay Proteccio (qualifié renforcé ANSSI)
- Thales HSM (PSE3 et Luna)
- Entrust nShield (Connect)
- Autres HSMs au standard PKCS#11



Nous contacter :

Mail : contact.cyber@cs-soprasteria.

← Découvrez notre offre trusty

