a Sopra Steria company

Logiciel certifié EAL3+ (V2.1.5), permettant de **générer des jetons d'horodatage** de confiance dans un environnement de Confiance et Souverain.

S'adresse aux organisations et fournisseurs de services qui souhaitent :
- **Associer** une date fiable à une donnée (document ou transaction)
- En **garantissant** une valeur probante.

TRUSTY TIME

Conformité règlementaire

Trustytime® permet de satisfaire
- **Les exigences de la règlementation européenne** eIDAS et peut donc être intégré pour délivrer un service eIDAS qualifié d'horodatage par un Prestataire de Service de Confiance Qualifié.
- **Le cahier des charges de l'ANSSI** pour une qualification en France d'un service d'horodatage eIDAS, en particulier grâce à sa certification certification Critères Communs EAL3+ (V2.1.5), et sa conformité aux exigences régaliennes françaises spécifiques (RGS et décret N° 2011-434 du 20 avril 2011 pour un horodatage qualifié).

Performance

100 jetons générés par seconde par serveur, signés par une clé RSA.

Le déploiement peut aussi être basé sur plusieurs HSM et serveurs travaillant en répartition de charge. Les performances et la disponibilité du service sont ainsi largement augmentées.

Cas d'usage

Protection de tout bien immatériel en conférant une valeur probante à une date et heure de génération et/ou d'enregistrement. *Par exemple pour prouver une antériorité devant un juge.*

Traçabilité de transactions tout en offrant une piste d'audit fiable et de recevabilité juridique.

Renforcer la sécurité juridique d'un cachet électronique par un horodatage fiable afin de fournir une preuve fiable de l'heure du scellement.

Horodatage avec valeur probante de la date et l'heure d'envoi et de réception d'un recommandé électronique qualifié ou de toutes modifications des données du recommandé, tel que défini par la règlementation eIDAS.

Etendre et conserver la validité des documents archivés sur le long terme et peut agir en complément de TrustyArchive®.

Une sécurité certifiée

Certifié selon les Critères Communs au niveau EAL3+ pour attester de la sécurité des services et de l'exploitation du produit.

TrustyTime® s'appuie sur des services cryptographiques matériels certifiés pour proposer des mécanismes cryptographiques à l'état de l'art : **clés RSA jusqu'à 8192 bits** et calculs d'empreinte à l'état de l'art.

Le déploiement dans une appliance renforce la sécurité du système en contrôlant de manière plus forte l'accès à la plateforme d'exécution des services.

Simplicité de déploiement et d'exploitation

- **Disponible potentiellement sous la forme d'une appliance autonome**, c.à.d un matériel cryptographique HSM, qui intègre le serveur d'application et les clés de signature.
- **Mise en oeuvre d'une ou plusieurs politiques d'horodatage** que l'administrateur peut configurer finement pour répondre aux besoins des différentes applications.
- **Capable de contrôler la dérive de son horloge interne** par rapport à plusieurs sources de temps sûres externes.
- **Garantit la fiabilité et la précision** des dates fournies dans ses réponses.
- Solution interfaçable avec **différents HSMs.**

INTEROPÉRABILITÉ ET ÉVOLUTIVITÉ

- ✓ **TrustyTime® est d'ores et déjà conforme à eIDAS1** et évoluera pour se conformer aux exigences des nouveaux standards ou spécifications des actes d'implémentation eIDAS2.
- ✓ **TrustyTime® respecte déjà les normes et les standards de l'IETF** (RFC 3161, certificats X.509,…) et dispose ainsi d'une grande capacité d'interopérabilité et d'évolutivité dans les différents contextes de déploiement.
- ✓ **TrustyTime® est immédiatement compatible avec des applications de création de signature tierces** ou des outils standards tels que Syslog-ng.
- ✓ **TrustyTime®** peut permettre de générer des jetons avec des **algorithmes PQC** (Falcon, Crystals-Dilithium et GeMSS), **pour anticiper la migration vers la cryptographie post-quantique (PQC)** en conformité avec les standards du NIST (FIPS 204 et FIPS 206) ou des exigences françaises régaliennes spécifiques.

Caractéristiques Techniques

Plateforme	• Appliance réseau : HSM Bull TrustWay Proteccio OEM • Serveurs physiques • Machines virtuelles
Ressources cryptographiques	• HSM Bull TrustWay Proteccio (qualifié renforcé par l'ANSSI) • HSM Thales (PSE3 et Luna) • HSM Entrust nShield (Connect) • Soft HSM Post-Quantique
Certification du logiciel	• Certifié Critères Communs EAL 3+ (version V2.1.5) • Conforme au RGS et au décret d'horodatage qualifié
Conformité aux standards	• RFC 3161 • Certificats X.509 v3
Serveur de temps	• Exploitation de multiples sources de temps (DCF, GPS, NTP…)
Cryptographie	• Signature des jetons par clés RSA jusqu'à 8192 bits

Nous contacter :
Mail : contact.cyber@cs-soprasteria.
Découvrez notre offre trusty
a Sopra Steria company