TRUSTYSERVER®

Serveur de confiance multiservices

TrustyServer® est une solution centralisée de confiance offrant les services de :

> Signature et validation de signature électronique
> Chiffrement et déchiffrement
> Validation de certificats

TrustyServer® apporte une solution unifiée et performante à ces besoins, accessibles par le réseau d'entreprise via des protocoles standards.
Le rapprochement de ces différents services apporte une grande simplicité de déploiement, et permet la mutualisation de matériels et ressources d'exploitation.

Les atouts

> Solution centralisée multi-services
- Signature et vérification de la signature électronique
- Chiffrement et déchiffrement
- Validation de certificats

> Enrichissement de la signature
> Cache auto-synchrone de validation
> Haute disponibilité et performances élevées
> Respect des normes et des standards
> Basé sur le SDK TrustySign évalué EAL3+
> Intégré dans la solution TrustyBox de CS

Services de confiance

Pour répondre aux besoins de sécurité dans le cadre de la dématérialisation des informations, CS propose tout une gamme de services pour répondre aux attentes en matière de :

> Authentification
> Confidentialité
> Signature et horodatage
> Archivage long terme
> Card Management System et Infrastructure de clés publiques

SIMPLICITÉ DE DÉPLOIEMENT ET D'EXPLOITATION

TrustyServer® est capable de s'adapter à de nombreux contextes de déploiement grâce aux possibilités étendues de configuration de chacun des services. L'administrateur peut configurer finement les règles à appliquer lors de la signature et la vérification de signature, le chiffrement et déchiffrement, la validation de certificats. Ces politiques sont signées par l'administrateur de sécurité.
TrustyServer® permet de plus de configurer les droits d'accès et d'usage par applications clientes et par politiques de signature ou de chiffrement.
TrustyServer® se déploie aisément dans le SI de votre entreprise grâce à son intégration dans la solution **TrustyBox®** de CS.
TrustyServer® dispose ainsi d'une interface graphique d'administration en client léger, puissante et ergonomique. L'administrateur dispose d'une vision globale et précise du système et peut entièrement configurer les paramètres techniques et métiers de la solution. L'interface d'administration permet de piloter la génération, la mise en production et la destruction des clés cryptographiques. Elle gère automatiquement la réplication des configurations métier et des clés lors de l'ajout de serveurs supplémentaires pour augmenter les capacités du système.
Le journal d'audit sécurisé présente toutes les opérations réalisées par les utilisateurs et opérateurs. **TrustyServer®** s'intègre nativement aux infrastructures standards de supervision via les protocoles SNMP et Syslog.

SIGNATURE ET ENRICHISSEMENT DE SIGNATURES

Les politiques de signature gérées par **TrustyServer®** sont des ensembles de règles liées à la création et la validation de la signature électronique. Cet ensemble de règles définit par exemple :
- règles de création comprenant les algorithmes et le format de signature à créer,
- règles d'utilisation et d'accès aux magasins de certificats de confiance et de listes de révocation
- règles de validation de la signature comprenant les champs à vérifier ou enrichir.

TrustyServer® supporte la signature et la vérification de tout type de document :
- Signatures XML-DSIG et XAdES
- Signature PDF et PAdES de documents PDF
- Signature CMS et CAdES

Au-delà des simples signatures et vérification de signature, **TrustyServer®** peut, sur demande du client, horodater les signatures présentes via **TrustyTime®** à l'issue du processus de signature et de validation de signature.
TrustyServer® propose également des fonctions de ré-horodatage via **TrustyTime®** dans le cadre de la préservation de l'intégrité des données et la maintenance de leur caractère « non répudiable » sur le long terme.
La signature peut être enrichie avec les chaînes de certification et les listes de révocation actuelles, en vue d'une conservation du document sur le long terme.

VALIDATION DE CERTIFICATS

TrustyServer® propose deux protocoles distincts de validation de certificats :

- OCSP (RFC 2560) pour fournir uniquement le statut de révocation du certificat
- XKMS pour contrôler le statut du certificat et sa chaîne de certification.

TrustyServer® a été conçu pour offrir des performances élevées afin de répondre aux pics de charge souvent constatés sur les services de validation. La gestion d'un cache auto-synchrone de sécurité permet de fournir des réponses XKMS et OCSP en un temps très court. Ce système permet aussi de supporter des coupures temporaires du réseau vers un serveur central et d'installer efficacement des sites distants partiellement autonomes.

SÉCURITÉ

L'application **TrustyServer®** est basée sur le cœur de l'application de création de signature **TrustySign®** qui est certifiée selon les Critères Communs au niveau EAL3+. La sécurité du logiciel est ainsi garantie pour ses utilisateurs et administrateurs.

TrustyServer® supporte les algorithmes cryptographiques à l'état de l'art. Il s'appuie sur des matériels cryptographiques HSM certifiés et qualifiés de dernière génération pour les signatures, chiffrement et déchiffrement de données. Pour les services les plus critiques, **TrustyServer®** peut être embarqué directement dans une appliance cryptographique matérielle, comme le Bull TrustWay Proteccio OEM ou le Safenet Luna SP.

INTEROPÉRABILITÉ ET ÉVOLUTIVITÉ

TrustyServer® respecte les normes et les standards de l'IETF (XAdES, PAdES, OCSP, XKMS, x509, LDAP, ...). Il dispose ainsi d'une grande capacité d'interopérabilité et d'évolutivité dans les différents contextes de déploiement.

CARACTERISTIQUES TECHNIQUES DE TRUSTYSERVER®

> PLATEFORME	• Appliance cryptographique : > HSM Bull TrustWay Proteccio OEM > HSM SafeNet Luna SP • Serveurs physiques • Machines virtuelles
> SIGNATURE (AVEC OU SANS HORODATAGE) VÉRIFICATION SIGNATURE ÉLECTRONIQUE	• Gestion par politiques de Signature • Format XML DSIG et XAdES, PDF et PAdES, CMS • Signatures RSA 1024, 2048, 4096 bits • Empreintes SHA-1, SHA-2 • Compatible avec les serveurs d'horodatage RFC3161, OCSP
> CHIFFREMENT DÉCHIFFREMENT	• Compression avant chiffrement • Gestion par politiques de Chiffrement • Algorithme 3DES, AES 128, AES 256 bits
> VALIDATION DE CERTIFICAT ET SERVICE OCSP	• Validation de certificat via le protocole XKMS • Validation OCSP (mode proxy et/ou mode autonome) • Support de plusieurs hiérarchies d'Autorités de Certification • Cache auto-synchrone de sécurité pour une haute disponibilité et performance
> CERTIFICATION	• Basé sur le TrustySign certifié Critères Communs EAL3+
> RESSOURCES CRYPTOGRAPHIQUES	• HSM Bull TrustWay Proteccio NetHSM • HSM Bull TrustWay Box RSA • HSM SafeNet Luna SA • HSM Thales nShield Connect

CONTACT : trusty@c-s.fr
www.c-s.fr

À PROPOS DE CS

Concepteur et intégrateur de systèmes clés en main performants et innovants, CS intervient sur l'ensemble de la chaîne de valeur de ses clients. Avec 170 M€ de chiffre d'affaires et 1 700 collaborateurs, CS s'impose aujourd'hui comme un fournisseur de confiance, reconnu par ses grands clients en raison de l'expertise, de l'engagement et du sens du service de ses collaborateurs.

La force de l'innovation

CS Communication & Systèmes
22, avenue Galilée - 92350 Le Plessis Robinson
tél : +33 (0)1 41 28 40 00 - fax +33 (0)1 41 28 40 40