a Sopra Steria company

Un serveur distant qui permet de récupérer en ligne, les informations sur le statut de révocation d'un certificat en évitant la complexité de la récupération et de la consultation des listes de révocation de certificats (CRLs).

S'adresse aux organisations qui souhaitent **un protocole en ligne de vérification de certificats** en alternative aux listes de révocations.

TRUSTY OCSP

TrustyOCSP® comprend deux composants logiciels majeurs :

- Le service de réponse OCSP : Un service web traitant les requêtes de demande de statut de révocation d'un ou plusieurs certificats envoyés par les clients,
- Le service d'administration : Une application web traitant les requêtes d'administration (configuration, exploitation, audit) en provenance des administrateurs.

L'accès à l'administration est distinct de l'accès au service métier pour renforcer la sécurité.

TrustyOCSP® s'appuie sur deux ressources clés :

- La base de données qui contient la configuration et le journal d'audit de l'application ;
- Une ressource cryptographique de type HSM qui, génère, protège et utilise les clés privées de signature des réponses OCSP. Cet HSM est exploité aussi bien par le service métier que le service administration.
- Lorsque plusieurs serveurs d'application sont installés, chacun peut exploiter le même HSM ou un HSM propre.

Performance

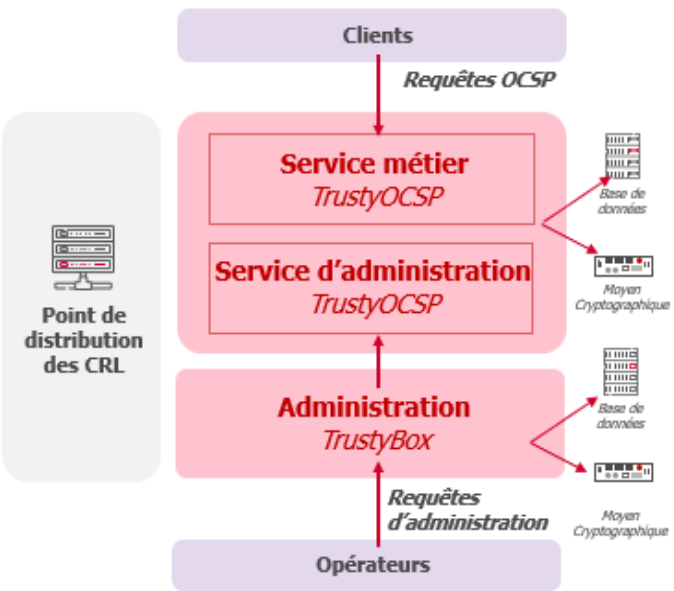
TrustyOCSP® Aide à prévenir la surcharge du service OCSP intégré à l'Infrastructure de Gestion de Clés (IGC/PKI), assurant ainsi la continuité opérationnelle même en cas d'afflux important de requêtes.

La distinction de TrustyOCSP® en deux services distincts répond aussi aux problématiques de charge et de disponibilité. Le service métier peut être instancié sur de multiples serveurs en actif-actif.

L'augmentation du nombre de HSMs augmente la disponibilité globale et la charge admissible.

Il est possible de bénéficier des fonctions dynamiques de répartition de charge et de haute disponibilité du fournisseur du HSM.

L'architecture est capable de répondre à un besoin de service jusqu'à 600 requêtes par seconde.



Conformité règlementaire

TrustyOCSP® est un service de demande de statut de révocation de certificats, conforme à la norme RFC 6960.

Administration

TrustyOCSP® bénéficie de l'interface d'administration graphique en client léger de TrustyBox® qui en assure l'administration du service.

TrustyBox® permets des configurations distinctes pour chaque Autorité de Certification (AC) avec un mode alternatif de vérification via une liste CRL (liste de révocation de certificats).

TrustyBox® s'appuie aussi sur une base de données et un HSM pour ses besoins propres.

Une sécurité native

•En tant que **relais OCSP**, TrustyOCSP® permet de renforcer la sécurité d'une IGC (PKI) en évitant l'exposition directe de la base de données de cette dernière.

•**L'accès à l'administration** est distinct de l'accès au service métier.

•TrustyOCSP® permet un mode d'**authentification mutuelle** pour lequel le service affichera le nom du client référencé et le DN (Distinguished Name) du certificat SSL client présenté lors de la requête OCSP.

L'audit participe à cette sécurité native.

L'audit fourni par TrustyOCSP® permet à la fois de **contrôler les opération**s qui ont été réalisées et de **comprendre la suite d'actions** qui a abouti à une situation finale. L'audit du service OCSP se fait par différents moyens complémentaires :

- **La supervision et la consultation de la configuration du système** (serveur, ressources cryptographiques et bases de données) permet de s'assuser de l'état global du service et détaillé de chacune des ses composantes.
- **Le journal d'audit** est constitué par le relevé de toutes les opérations réalisées (dont les logs d'accès et identification des clients OCSP). Tout évènement métier ou administration est enregistré dans la base de données et scellé cryptographiquement, avec une clé secrète du HSM, afin que toute modification d'une propriété de l'évènement soit détectable.
- **les tests automatisés** sont des outils efficaces pour vérifier tant la disponibilité que la performance du service.

Caractéristiques Techniques

Certificats	Certificats X509 V3 conformément à RFC 5280 et à toutes les extensions prévues Listes de révocation : CRL X.509 v2
Algorithmes cryptographiques	Algorithme d'empreinte utilisé lors du processus de signature des réponses OCSP : SHA-256, SHA-384, SHA-512 Taille des clés cryptographiques : 3072 bits, 4096 bits
Conformité au standard OCSP	RFC6960
Base de données	PostgreSQL
Environnement serveur	Distribution Linux (Debian, Redhat, Ubuntu) Windows Server
Ressources cryptographiques	HSM Bull TrustWay Proteccio 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
a Sopra Steria company