a Sopra Steria company

Une solution d'infrastructure de Gestion de clés **(IGC/PKI)** permettant de générer et gérer vos propres certificats, pour rester maître de vos clés et de vos choix.

TrustyKey® se distingue par l'ergonomie de son administration, la souplesse de déploiement et ses capacités fonctionnelles sans compromis.

S'adresse aux organisations qui souhaitent :
La sécurité sans la complexité

TRUSTY KEY

TrustyKey® est la solution la plus sûre et la plus aboutie pour l'utilisation de clés cryptographiques avec une gestion complète du cycle de vie des certificats.

Ces clés, maillons particulièrement sensibles du système, nécessitent la mise en place d'une IGC éprouvée et des mécanismes de sécurité renforcés. TrustyKey® inclut une autorité d'enregistrement (RA) pour la gestion des demandes de certificats.

Cas d'usage

- **Listes de confiance**
- **Identité électronique** (passeports et titres d'identité, cartes d'agent)
- **Identité numérique**
- **Certificats eIDAS** qualifiés ou non (de signature ou de cachet électronique...)
- **Dispositifs matériels** (cartes à puce, TPM, Secure Element)
- **Agents logiciels** (les navigateurs internet, les référentiels des systèmes d'exploitation ou les fichiers tels que les fichiers PKCS#12) généralement utilisés pour gérer les certificats X.509 et les clés privées correspondantes

*Et prochainement de **nouveaux usages** pour les registres vérifiables d'attestations électroniques (qualifiées) pour les **EUDIW**, EUropean Digital Identity Wallets.*

Performance

Une performance assurée pour les usages d'aujourd'hui et de demain, pour générer tout type de certificats X509, avec une architecture haute disponibilité pour prendre en compte les exigences SLA de votre service.

Simplicité de déploiement et d'exploitation

Le déploiement de TrustyKey® est **souple et capable de s'adapter** au dimensionnement et aux contraintes de sécurité de votre organisation. Deux modes de déploiement sont ainsi possibles

- **Connecté** : La connexion à une ou plusieurs Autorités de Certification (AC) permet une gestion centralisée et efficace.
- **Déconnecté** : Une configuration et une gestion, de une ou plusieurs AC, sans connexion réseau assure une sécurité maximale pour les clés des autorités de certification les plus sensibles.

L'administration des AC, y compris la définition des modèles de certificats, se fait uniquement par des outils graphiques simples. Un administrateur prend ainsi rapidement en main le produit et peut maîtriser l'infrastructure sans difficulté.

De plus, TrustyKey® supporte la gestion automatisée de certificats électroniques reposant sur les protocoles SCEP et ACME.

Les services de certification et de révocation sont accessibles via un protocole sécurisé normalisé.

L'intégration de TrustyKey® avec des solutions de gestion de cartes (Card Management System, CMS) est directe et fait uniquement appel à des protocoles et formats standard de la sécurité.

Haut niveau de sécurité

TrustyKey® est une IGC conçue nativement pour apporter le plus haut niveau de sécurité, que ce soit dans son utilisation, son administration ou son déploiement.

Les mécanismes de sécurité concernent par exemple :

- L'authentification multifactorielle forte des opérateurs
- La sécurisation de toutes les communications avec les clients et les opérateurs
- La signature des requêtes, programmatiques ou manuelles
- La journalisation de tous les événements
- La protection en intégrité des journaux
- L'exploitation de clés cryptographiques sur HSM, supports matériels certifiés
- Les autocontrôles et la génération d'alertes de sécurité

La sécurité apportée par TrustyKey® est démontrée par une certification selon les Critères Communs au niveau EAL3+.

TrustyKey® est conforme au RGS et est déployé dans des infrastructures gouvernementales de niveau RGS.

Nos expérimentations avancées réalisées sur HSM Soft avec les algorithmes PQC tels que Falcon, Crystals-Dilithium et GeMSS, permettent de préparer TrustyKey® à la migration vers la cryptographie post-quantique (PQC) de nouvelle génération en conformité avec les standards du NIST (FIPS 204 et FIPS 206) ou des exigences françaises régaliennes spécifiques.

Caractéristiques Techniques

Certificats	• X.509 v3 conformément à RFC 5280 et à toutes les extensions prévues • X.509 avec extensions propriétaires possibles pour représenter une identité numérique ou pour représenter des attributs d'identité • Requêtes CMP, PKCS#10
Liste des révocations	• CRL X.509 v2 • Service d'information OCSP
Annuaire	• LDAPv3
Environnement serveur	• Distribution Linux (Debian, Redhat, Ubuntu) • Windows Server
Base de données	• Oracle, PostgreSQL
HSM	• Thales HSM (PSE3 et Luna) • Entrust nShield (Connect, Edge) • Bull TrustWay Proteccio (qualifié renforcé ANSSI) • Soft HSM Post-Quantique et autres HSM au standard PKCS#11
Algorithmes	• RSA jusqu'à 8192 bits • Courbes elliptiques P-256, P-384 et P-521 • SHA-256 jusqu'à SHA-512
Certifications	• Critères Communs EAL3+ (version V6.0.14) • Conforme au RGS v2
Intégration de CMS	• Ilex CMS d'Inetum • Nexus CMS (IN Groupe)
Autorité d'enregistrement (RA)	• RA WEB, RA SCEP, RA ACME

Nous contacter :
Mail : contact.cyber@cs-soprasteria.
Découvrez notre offre trusty

a Sopra Steria company