IDnomic Appliance
AC Déléguée Technique

Sécurisez vos équipements grâce aux certificats

La garantie des échanges numériques de manière sécurisée et transparente entre des tiers, comme des sites internet ou des serveurs web s'appuie sur le déploiement de certificats numériques émis par des autorités de confiance. Il est ainsi possible de protéger et de garantir la fiabilité de millions d'échanges au quotidien.

L'identité de vos équipements

Les certificats sont au cœur de la sécurisation des connexions et des échanges numériques. Ils garantissent l'identité numérique des tiers qui peuvent échanger en toute confiance. Ils vont permettre également le chiffrement des données échangées. Ils garantissent les 3 principes fondamentaux en sécurité informatique : intégrité, confidentialité et authenticité.
Les certificats sont émis par des autorités de confiance (AC) qui sont déployées de manière pyramidale : une AC racine au sommet de la pyramide et des AC déléguées qui lui sont rattachées.

L'appliance AC Déléguée Technique complète l'AC racine qui a pour fonction d'émettre les certificats des autorités déléguées et d'assurer le cycle de vie des ACs qui lui sont rattachées. Les AC déléguées techniques émettent des certificats pour les équipements. Ces certificats peuvent avoir différentes fonctions (authentification, signature, chiffrement...).

Protégez vos infrastructures avec une appliance

L'appliance AC Déléguée Technique permet le déploiement d'une ou plusieurs autorités de confiance (AC) déléguées afin d'émettre en toute sécurité, des certificats pour des équipements ou des personnes de manière rapide et économique. Le certificat de l'AC déléguée peut-être émis par une AC Racine (Appliance IDnomic AC Racine par exemple) ou par l'AC de l'appliance elle-même (certificat auto-signé). La clé privée est conservée dans le module matériel de sécurité (HSM) Trustway Proteccio, à la pointe de la technologie, où l'appliance AC Déléguée Technique est exécutée. Elle est utilisée pour créer des certificats pour les équipements.

L'appliance AC Déléguée Technique est configurée pour émettre des certificats feuilles pour des équipements (AC Déléguée Technique). Les profils de certificats sont créés à partir de modèles définis et peuvent être associés à des clés RSA ou ECDSA.

La production de certificats est conforme à la politique de certification définie par le client et aux exigences des organismes de surveillance. Les utilisations typiques incluent le déploiement de certificats d'authentification pour garantir l'identité des équipements via un processus d'enrôlement automatique (SCEP ou CMP) facilitant la gestion du cycle vie des certificats comme l'auto-enrôlement.

L'appliance AC Déléguée Technique aide les organisations à réaliser leur projet rapidement et à moindre coût :

- Une configuration prédéfinie est mise en place : l'appliance est livrée avec une configuration standard qui peut être utilisée dans la plupart des cas d'usage, minimisant les délais des phases de spécifications ou d'intégration,
- Le produit est livré dans une solution matérielle unique avec des fonctions et une base de données préconfigurées,
- Une configuration minimale est effectuée lors de la première exécution pour que l'appliance soit prête à être utilisée.

La maintenance et le support du système sont simplifiés car l'appliance est une solution tout-en-un facilitant les tâches complexes d'une implémentation classique pour des configurations spécifiques de VMs, serveurs, intégration avec le HSM...

Renforcez le contrôle de la sécurité de votre système d'information et son indépendance avec des solutions "as-a-service" basées sur une solution matérielle certifiée, ainsi qu'une mise en œuvre simple et rapide.

Un modèle adapté à vos besoins

Atos propose une large gamme d'appliances d'infrastructure de confiance (PKI, signature électronique, consentement explicite de l'utilisateur, horodatage, blockchain) et propose différents modèles d'appliances en fonction des besoins de l'infrastructure :

- Un **modèle de base** avec un seul service intégré dans le HSM. Ce modèle simple est autonome et ne nécessite pas de gestion de gros volumes de données. Il peut être déployé rapidement car il ne dépend pas de l'infrastructure. À titre d'exemple, ce modèle est entièrement adapté à l'appliance AC Racine.
- Un **modèle haute disponibilité** qui permet de déployer plusieurs appliances pour garantir un haut niveau de disponibilité en assurant une continuité de service avec une base de données centralisée.
- Un **modèle multi-services** avec plusieurs services intégrés dans le HSM. De cette façon, il est possible de combiner de nombreux services tels que la signature électronique ou l'horodatage avec une infrastructure à clé publique.

L'appliance AC Déléguée Technique prend en charge les modules fonctionnels suivants :

- Génération de la CSR pour rattachement à une autorité de certification racine ou génération d'un certificat auto-signé,
- Génération des certificats initiaux avec un processus d'enrôlement automatique (SCEP, CMP...),
- Gestion du cycle de vie des certificats (révocation, renouvellement, suspension...),
- Génération de la liste de révocation de certificats (LCR).

L'appliance AC Déléguée Technique propose différents profils de certificats :

- Rattachement à une autorité racine : la paire de clés est générée par l'infrastructure de l'AC déléguée. Une demande de signature de certificat (CSR) est produite et transmise à l'opérateur de l'autorité de certification racine afin de produire le certificat correspondant signé par l'autorité de certification racine.
- Production des certificats pour des équipements : une CSR est envoyée à l'AC Déléguée (soit par l'équipement, soit par le gestionnaire de l'infrastructure). Si l'équipement supporte les protocoles d'enregistrement automatique (SCEP, CMP), un déploiement automatique du certificat peut être mis en place facilitant ainsi la gestion du cycle de vie des certificats.

L'appliance AC Déléguée Technique intègre des mécanismes de sécurité de haut niveau :

- L'accès à tous les modules fonctionnels est contrôlé. Les opérateurs et les administrateurs doivent être authentifiés à l'aide d'une authentification forte (avec une carte à puce ou un jeton USB).
- Toutes les actions liées à la gestion des certificats sont enregistrées dans une base de données accessible uniquement aux opérateurs autorisés. Tous les événements sont enregistrés.
- Les communications entre les modules fonctionnels et les informations stockées dans la base de données sont toutes protégées. Les informations sensibles sont chiffrées.
- Les clés privées sont protégées à l'aide de modules matériels de sécurité (HSM).

Standards et spécifications techniques

HSM Certifications

- Critères Communs EAL4+ conformes au CWA 14167-2-PP
- NATO SECRET
- Conformité eIDAS
- Qualification Renforcée (ANSSI)
- FIPS 140-2 niveau 3 (en cours)

Administration

- Définition de profils cryptographiques
- Mises à jour sécurisées des logiciels intégrés
- Répartition de charge

Interfaces Physiques

- 2 ports Ethernet 10/100/1000BASE-T
- 4 ports USB2
- 1 port VGA
- Clavier et lecteur de carte à puce intégrés
- Alimentation électrique redondante
- Bouton de réinitialisation en façade
- Lien RPC sécurisé par SSL vers serveurs Windows, Linux et AIX 32/64

Appliance AC Déléguée Technique

- Conformité des certificats à UIT-T X.509v3, RFC 5280 et RFC 3739
- Conformité des informations de révocation avec la liste de révocation de certificats UIT-T X.509v2
- Format de demande de certification : PKCS # 10
- Algorithmes : Courbes nommées RSA 4096 et ECDSA secp224r1, secp384r1, frp256v1
- Support des protocoles d'enrôlement automatique SCEP et CMP (V1.1, V1.2)

For more information:
https://atos.net/fr/solutions/cybersecurite-produits/digital-identities/appliances-d-infrastructures-de-confiance