# IDnomic Appliance AC Racine

# Gérez le point d'ancrage de la chaîne de confiance de vos PKI

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.

## À la Racine de votre confiance

Les certificats racines sont au cœur de la sécurisation des connexions et des échanges numériques, permettant de valider les opérations de chiffrement. Les autorités de certification racine (AC) s'assurent que seuls les certificats racine officiels et de confiance sont émis pour maintenir des échanges sécurisés. En vérifiant les informations d'identification des utilisateurs, des périphériques ou des services en ligne, les autorités de certification approuvées lient leur identité à des clés de chiffrement.

Cela aide à éliminer le risque d'interceptions malveillantes ou d'usurpations d'identité, telles que les attaques d'interception (Man in the middle).

Une autorité de certification racine doit être digne de confiance, car les certificats signés avec la clé privée du certificat racine seront automatiquement approuvés par les navigateurs tant qu'ils sont valides. Cela signifie que si cette autorité racine est compromise, toute la hiérarchie de confiance sera affectée.

Il est donc primordial que l'autorité de certification racine soit hautement sécurisée, maintenue hors ligne et utilisée uniquement pour signer des autorités de certification déléguées. Dans une chaîne de certificats de confiance, les autorités de certification déléguées agissent comme une couche de sécurité supplémentaire, car l'autorité de certification racine n'a pas pour rôle d'émettre des certificats directement aux utilisateurs finaux ou aux périphériques.

## Protégez vos échanges avec une appliance

L'appliance AC Racine permet le déploiement d'une hiérarchie approuvée d'autorités de certification et l'émission, en toute sécurité, des certificats d'autorités de certification déléguées, de manière rapide et économique. Son certificat est 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 Racine est exécutée. Elle permet la création des certificats d'AC déléguées et peut être utilisée par un opérateur de PKI.

L'appliance AC Racine est configurée pour émettre des certificats d'autorités de certification déléguées afin de créer une hiérarchie d'autorités de certification. 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 d'AC est conforme à la politique de certification définie par le client et aux exigences des organismes de surveillance. Les cas d'usage caractéristiques incluent la création de nouvelles autorités de certification déléguées et la production de listes de révocation de certificats (LCR).

L'appliance AC Racine 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 ....

## 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 IDnomic Root CA.
- 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.

Un modèle haute disponibilité est également disponible pour les autres appliances d'infrastructure de confiance.

# 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.

### L'appliance AC Racine prend en charge les modules fonctionnels suivants

- Génération de l'autorité de certification racine et gestion de son cycle de vie lors de la cérémonie des clés,
- Génération des certificats initiaux de l'autorité de certification déléguée,
- Renouvellement des certificats d'AC déléguée (ACD),
- Génération de la liste de révocation de certificats (LCR).

### L'appliance AC Racine propose différents profils de certificats

- Production du certificat de l'autorité de certification racine : la paire de clés est générée lors d'une cérémonie de clé dans l'appliance HSM.
- Production des différentes autorités de certification déléguées : la paire de clés est générée par l'infrastructure PKI hébergeant l'autorité de certification déléguée (ACD). Une demande de signature de certificat (CSR) est produite par l'infrastructure à clé publique (ACD) et transmise à l'opérateur de l'autorité de certification racine Atos afin de produire le certificat correspondant signé par l'autorité de certification racine via l'interface graphique Atos.

### L'appliance AC Racine 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

### 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 Racine

- 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


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