

# CoreStreet Validation Authority

Le logiciel Real Time Credentials Validation Authority (RTC VA) est une solution logiciel complète qui permet de valider des certificats numériques de façon flexible, sécurisé et rentable.

## Vue d'ensemble

Un certificat numérique permet d'authentifier l'identité d'une personne ou d'un ordinateur de façon sécuritaire. Malheureusement, l'authentification ne permet pas de déterminer si le certificat lui-même est encore valide ou si les fonctions et privilèges rattachés à ce certificat sont encore en vigueur. Une partie utilisatrice doit vérifier les changements d'état et les révocations de façon à implanter une infrastructure à clé publique (ICP ou Public Key Infrastructure). La vérification de la validité doit être à la fois rapide et sécuritaire pour fonctionner avec un environnement d'infrastructure ICP moyen ou grand.

Il y a deux approches classiques à la problématique de la validation des certificats.

Dans la première approche, un tiers de confiance (trusted authority) publie périodiquement une liste maîtresse signée de tous les certificats valides et révoqués. La liste des certificats révoqués s'allonge rapidement et devient d'une taille inutilisable pour les environnements qui ont plus de quelques milliers de certificats.

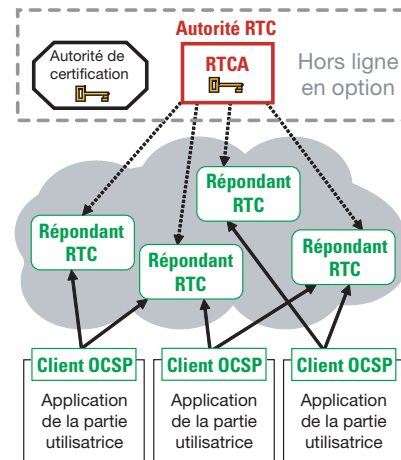
La deuxième approche classique nécessite une communication directe et sécuritaire à un tiers de confiance qui peut vérifier la validité de l'état de chaque certificat. Cette approche a été mise en place avec les serveurs traditionnels OCSP (Online Certificate Status Protocol : Protocole de vérification de statut de certificat en ligne). Elle nécessite que chaque serveur de validation soit protégé contre les attaques physiques et celles du réseau, puisque toute compromission réussie peut donner lieu à une intrusion par un certificat révoqué ou volé. Les risques concernant la sécurité et les frais qui s'y rattachent font de cette approche une solution inacceptable pour les environnements d'infrastructure ICP moyens ou grands avec plus d'une autorité de validation.

Le RTC VA de CoreStreet propose une troisième approche révolutionnaire pour les certificats numériques de validation : le OCSP réparti. Cette approche est basée sur une pré-génération centralisée (avec possibilité d'être hors ligne) de preuves de validation signées, qui peuvent être publiées à travers un réseau

très flexible de répondants non sécuritaire et de tâche légère. Le RTC VA peut être utilisé comme un remplacement complètement compatible d'une infrastructure traditionnelle OCSP, offrant une sécurité fondamentalement améliorée pour seulement une partie des coûts totaux.

## Composantes

Le RTC VA de CoreStreet inclut trois composantes logicielles qui servent à construire une infrastructure sécuritaire de validation des certificats, comme l'indique le schéma suivant:



L'environnement ICP déploiera une autorité RTC (RTCA) à un seul endroit sécurisé, qui peut être le même que celui de l'autorité de certification (CA). Ce RTCA publie des preuves de validation OCSP répartie à un nombre illimité de répondants RTC, ce qui fournit un service standard OCSP aux parties utilisatrices, qu'ils fonctionnent avec les outils RTC OCSP Client inclus ou avec tout autre outils OCSP, applications ou modules d'extension de tierce partie.

## Caractéristiques-clés

Le RTC VA de CoreStreet présente une infrastructure répartie pour la validation des certificats qui est fondamentalement supérieure à tout modèle CRL ou OCSP traditionnel dans les aspects suivants.

- **Sécurité** Les répondants RTC n'ont pas de clés privées, alors ils n'ont besoin que de peu de protection physique ou du réseau. Les répondants RTC ne peuvent pas fournir de fausses réponses même s'il y a eu compromission.

- **Extensibilité** Les répondeurs RTC peuvent être déployés rapidement en n'importe quel lieu, permettant de s'étendre à des centaines de locations.
- **Disponibilité** Puisque les répondeurs RTC peuvent facilement être répliqués en plusieurs endroits, la disponibilité générale du service est extrêmement élevée avec une excellente capacité de survie lors d'une attaque, en comparaison avec des topologies centralisées et sécuritaires.
- **Performance** Les répondeurs RTC peuvent être placés près des parties utilisatrices, ce qui réduit le temps d'attente pour les réponses OCSP.
- **Rentabilité** La tarification du RTC VA permet un déploiement de répondeurs illimité, sans coût relatif au logiciel. De plus, il n'y a aucun frais par transaction.
- **Gestion simplifiée** Puisque les répondeurs RTC représentent une fonctionnalité sans état et de serveur à fonction unique, il n'y a que l'autorité centrale RTC qui a besoin d'être géré. L'autorité RTC peut être configurée avec une interface Web complète, des outils de ligne de commande ou à travers un API.
- **Complètement sous licence** Le RTC VA est la seule implantation OCSP autorisée par la propriété intellectuelle RTC de CoreStreet, tel que stipulé dans les brevets 5,666,416 et 5,717,758 (États-Unis).
- **Conforme aux normes** Bien qu'il représente une approche révolutionnaire dans la validation des certificats, le RTC VA s'intègre parfaitement aux composants ICP existantes avec des normes comme X.509, OCSP et LDAP.

## Compatibilité

L'autorité RTC et le répondeur RTC fonctionnent avec les plateformes suivantes :

Plate-formes RTCA/RTCR

- Sun Solaris 8
- Redhat Linux 9
- Windows 2000
- Windows 2000 Server
- Windows Server 2003
- Windows XP Professional

Conditions minimales du système pour l'autorité RTC

- Processeur SPARC 1 GHz x86 ou 500 MHz
- 512 MB de mémoire vive
- 100 MB de mémoire

Conditions minimales du système pour le répondeur RTC

- Processeur SPARC 500 MHz x86 ou 300 MHz
- 256 MB de mémoire vive
- 100 MB de mémoire

Bases de données Autorité RTC

- PostgreSQL 7.3
- Oracle 9i
- MS SQL Server 2000
- MS SQL Server Desktop Engine (empaqueté avec le produit)
- McKoi (empaqueté avec le produit pour évaluation)

Autorités de certification compatibles

- Toutes les autorités de certification conformes aux normes de l'industrie.

Modules de sécurité compatibles

- Chrysalis<sup>MD</sup> Luna SA
- nCipher<sup>MD</sup> nShield
- Sun JCE fournisseur de logiciel seulement

Outils de la partie utilisatrice OCSP compatibles

- CoreStreet RTC client toolkit (inclus)
- Alacris<sup>MD</sup> OCSP client toolkit, plug-in
- AssuredBytes<sup>MD</sup> OCSP plug-in
- Valicert<sup>MD</sup> OCSP client toolkit, plug-in
- OpenSSL OCSP toolkit (code source libre)

Certification

- Critère commun EAL3 augmenté ALC\_FLR.1
- Certifié US Department of Defense JITC
- Conforme Identrus
- FIPS 140-2

## Concession de licence

Quelle soit utilisée pour la sécurité de l'information, comme dans les courriels sécuritaires, ou pour la sécurité physique, comme dans un système électronique de contrôle d'accès, une infrastructure à clé publique sécuritaire a besoin d'un système de validation solide pour gérer les autorisations sécuritaires à partir de certificats numériques. Le RTC Validation Authority de CoreStreet offre l'infrastructure de validation la plus flexible et sécuritaire possible, pour une partie des coûts que représentent les solutions OCSP traditionnelles.

Le RTC VA est présentement disponible pour achat et déploiement. Contactez CoreStreet pour recevoir plus d'information ou discuter des services professionnels offerts pour vous aider à déployer une infrastructure de validation sécuritaire et flexible.

