CoreStreet
An ActivIdentity Company

CoreStreet Validation Authority™

The CoreStreet Validation Authority is a complete software solution that enables digital certificate validation in a scalable, secure, and cost effective manner.

Overview

A digital certificate provides a secure way to authenticate the identity of a person or computer. Unfortunately, authentication does not determine whether the certificate itself is still valid, or whether its associated roles and privileges are still current. A relying party must check for status changes and revocation to implement a truly secure Public Key Infrastructure (PKI) This validation check must be both fast and secure to support a medium to large PKI environment.

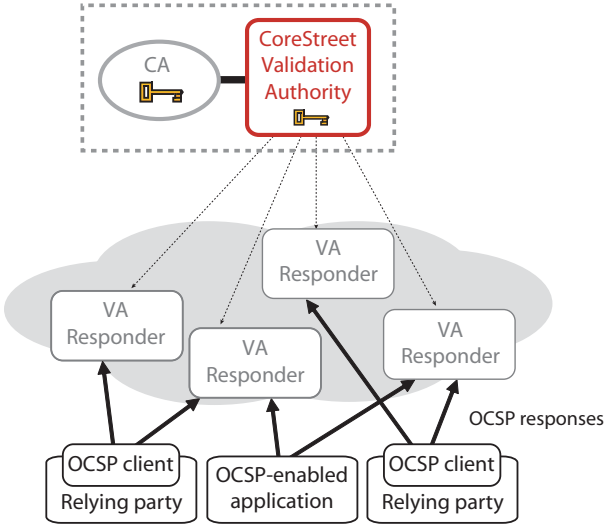
Classically, there have been two approaches to certificate validation. In the first solution, a trusted authority periodically publishes a signed master list of all valid or revoked certificates. This Certificate Revocation List (CRL) rapidly grows to an unusable size for environments with more than a few thousand certificates.

The second approach requires direct communications to a secured, trusted authority that can verify the validation status of each certificate. This approach, known as Traditional OCSP, requires each validation server to be protected against both physical and network attacks, since any successful compromise can allow an intrusion by revoked or stolen certificates. The security risks and associated costs make this approach unacceptable for most medium and large PKI environments with more than one validation authority.

The CoreStreet Validation Authority (VA) provides a revolutionary third approach for digital certificate validation called Distributed OCSP. This is based on the centralized (potentially offline) generation of signed validation proofs that can be published through an extremely scalable network of lightweight, unsecured Responders. The VA serves as a fully compatible drop-in replacement for a Traditional OCSP infrastructure offering radically improved security at a fraction of the total cost.

Components

The CoreStreet VA is composed of two software components that together build a secure certificate validation infrastructure, as shown in the following diagram.



Typically, a PKI environment will deploy one Validation Authority in a single, secured location, which may be the same location as the Certificate Authority (CA). The Validation Authority publishes Distributed OCSP validation proofs to any number of VA Responders, which provide standard OCSP service to relying parties using an OCSP toolkit, application, or plug-in.

Key features

The CoreStreet VA introduces a distributed infrastructure for certificate validation that is fundamentally superior to any CRL or Traditional OCSP scheme in the following areas:

- **Security** CoreStreet VA Responders have no private keys, thus requiring little physical or network protection. VA Responders cannot provide false responses even if compromised. Additionally, the CoreStreet VA is FIPS 140-2 certified.

CoreStreet Validation Authority

- **Scalability** CoreStreet VA Responders can be rapidly deployed in any number of locations, allowing for scalability to hundreds of remote sites.
- **Availability** Since the VA Responders can be easily replicated in many locations, overall service availability is extremely high with excellent survivability under attack when compared to centralized, trusted topologies.
- **Performance** CoreStreet VA Responders can be placed close to relying parties allowing extremely low latency for OCSP responses.
- **Cost effective** Validation Authority pricing allows for unlimited Responder deployment without software fees. In addition, there are no per-transaction costs.
- **Ease of management** Since the Responders represent stateless, appliance-grade functionality, only the central Validation Authority requires management. To ease management, the VA is configurable through a full-featured web interface.
- **Fully licensed** The VA represents the only authorized OCSP implementation covered by CoreStreet's intellectual property, such as US patents 5,666,416 and 5,717,758. For more information on CoreStreet patents, go to www.corestreet.com/library.
- **Standards compliant** While the VA represents a revolutionary approach to certificate validation, it integrates seamlessly with existing PKI products from CoreStreet, and other vendors, through standards such as X.509, OCSP, and LDAP. The CoreStreet Validation Authority is FIPS 201 approved.

Smart Data Bridge™ (optional)

The Smart Data Bridge is an optional component, which constantly monitors data sources for certificate status updates, and pushes these changes to the CoreStreet Validation Authority whenever they occur.

Requirements

Supported platforms
- Sun® Solaris™ 8
- Sun Solaris 10
- Red Hat® Enterprise Linux v.4
- Microsoft® Windows® 2000 operating system
- Microsoft Windows XP Professional operating system
- Microsoft Windows Server® 2000 operating system
- Microsoft Windows Server 2003 operating system

Supported databases
- PostgreSQL 7.4
- Oracle® 9i
- Oracle 10g
- Microsoft SQL Server™ 2000 database software
- Microsoft SQL Server Desktop Engine (bundled with product)
- McKoi (bundled with product for evaluation)

Supported certificate authorities
- Supports all industry standards-compliant certificate authorities

Supported security modules
- SafeNet® Luna® SA
- nCipher® nShield™
- Sun® JCE software-only provider
- AEP™ Keyper Professional firmware version 2.3
- AEP Keyper Enterprise firmware version 1.4

Complementary CoreStreet products

- Desktop Validation Client™
- Responder Appliance 2400™
- Server Validation Extension™ for Microsoft IIS
- Server Validation Extension™ for Microsoft Domain Controller
- Server Validation Extension™ for Microsoft Exchange Outlook® Web Access

Licensing

Whether used for information security such as secure email, or for physical security such as an electronic access control system, a secure PKI needs a strong validation infrastructure to provide secure authorization using digital certificates.

The CoreStreet VA is currently available for purchase and deployment. Contact CoreStreet to receive more information or to discuss professional services to assist in the deployment of a secure and scalable validation infrastructure.

Common Criteria ®

www.corestreet.com
+1 617 661 3554
info@corestreet.com

Additional whitepapers and datasheets available at:
www.corestreet.com/library