Certificate Validation Use Cases

Distributed OCSP Use Case Overview

Validation Components

The figure below represents CoreStreet's recommended approach for implementing validation components at local facilities in support of local relying parties. The figure also depicts scheduled synchronization(s) to the Enterprise Responders and to Local Responder Appliances to provide improved availability and failover in the event network connectivity to the Enterprise Responders is lost. The workstation icons presented in this picture represent relying party software, without regard to the specific platform on which the software is to be deployed. Specific relying party software requirements are best discussed in terms of the use case(s) being supported. A pictorial representation of the components required for each use case is presented in Figure 1.

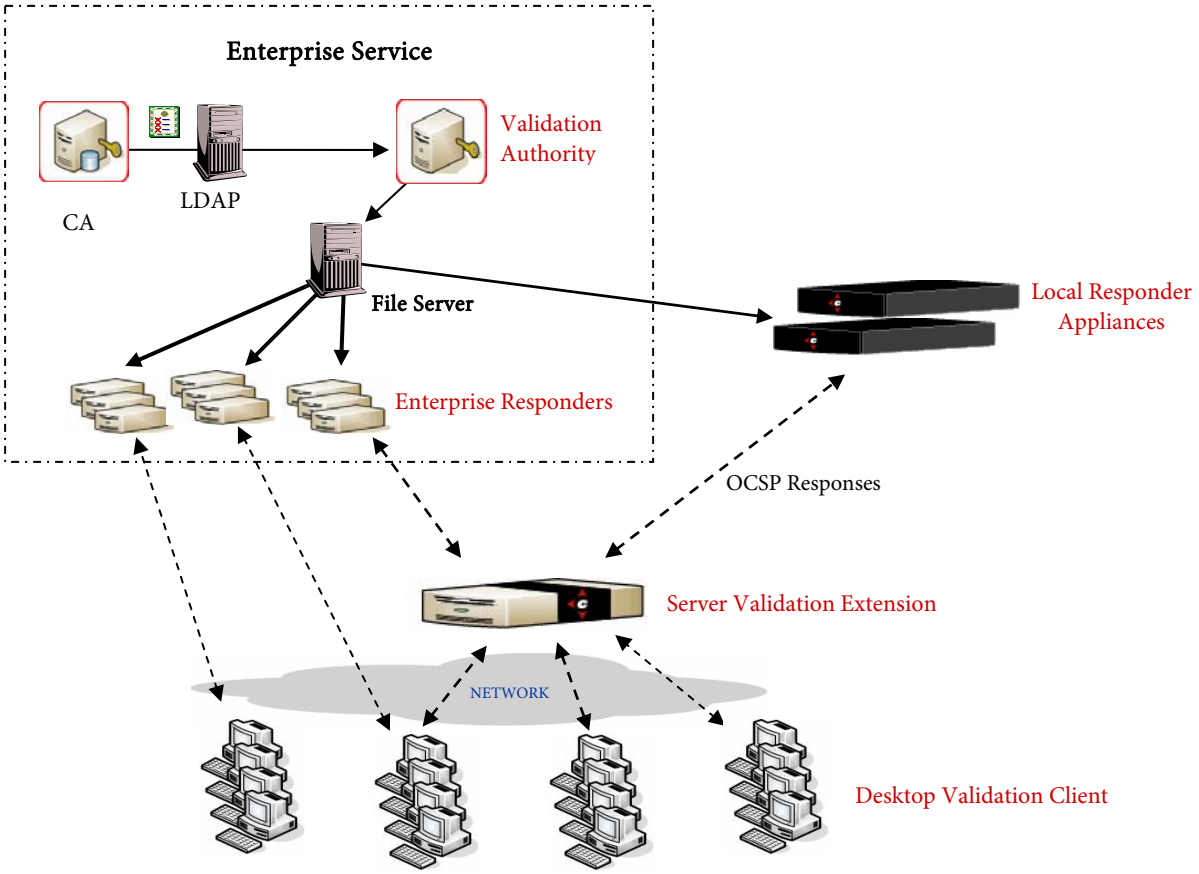

Figure 1. Certificate Validation Components.

Since each certificate validation component within the CoreStreet solution set provides different support capabilities, each of the use cases supported by these components is described in the following sections.

Use Case – Validation of Digitally Signed E-Mail

Microsoft Outlook

The support for validation of digitally signed electronic mail, reviewed in Microsoft Outlook, is accomplished through the implementation of CoreStreet's Desktop Validation Client (DVC). The DVC can be pre-configured by the local administrator or an installation package with configuration information (or separate packages with different configurations) can be created and pushed to each user with an automated tool (i.e., .msi via SMS), thereby installing the product without user intervention. For users that cannot receive software and configuration updates automatically via the network, a pre-configured CD can be created for out-of-band installs.

In addition to the validation of digitally signed email, the DVC provides a complete set of PKI validation functionality which includes:

- support for standard Online Certificate Status Protocol (OCSP) requests with and without a nonce
- support for specific capabilities in low-bandwidth and communication-constrained environments
- the ability to cache responses locally for a configurable period of time
- the ability to extend the validity period of "stale" revocation data so that the user is able to continue to perform validations
- support for access to responders via a proxy server
- the ability for the Administrator to pre-configure the desktop functionality and presentation components (to prevent alteration of security-related configuration data by the end user) and to create an installation package based on this configuration right from the client GUI and push this configuration as an .msi package
- the ability to sign OCSP requests with a user's FIPS 201 signing certificate
- the ability to manage client configurations using enterprise tools such as Microsoft Group Policy
- the ability to configure multiple fallback responder URLs on a per-CA basis to handle server downtime.

Once the DVC has been installed, a request to validate ***any*** certificate can be made, regardless of the issuer. For example, certificates attached to documents (such as Adobe PDF files) or certificates used to sign software applications or ActiveX controls can be validated and their certificate status presented to the end user. For software packages that rely on the Microsoft Cryptographic Application Programming Interface (CAPI) for certificate processing (such as the *Silanis Approve-It* digital signature software), validation is automatic.

Subsequent configuration updates of the DVC can be pre-configured by the administrator for automated distribution to the end user. While the administrator will normally configure the appropriate settings for client behavior, such as logging activities, certificate issuer/responder mappings and failover responder sets, validation authority trust anchors, response caching and validity buffering intervals, use of a proxy server and/or MiniCRLs, and user notification behavior, they can also limit the user's ability to change these settings. Typically, the only items that the administrator might want to allow the user to adjust are the notification settings.

Microsoft Outlook Web Access

The support for validation of digitally signed electronic mail, reviewed via a web browser using Microsoft Outlook Web Access (OWA), is accomplished through the implementation of CoreStreet's Server Validation Extension for Microsoft Exchange OWA (SerVE-OWA). SerVE-OWA enables Exchange Server to use CAPI to validate the revocation status of digital certificates contained in digitally-signed email messages using OCSP or MiniCRL responses. In the event of a network outage, a local cache of Certificate Revocation Lists (CRLs) can also be created.

Administrative tools supplied with SerVE-OWA allow an administrator to deploy the software on servers easily and rapidly and in a wide variety of network configurations. Site administrators can create a pre-configured installer customization using all appropriate options and security information, and deploy the installer customization to servers without technical support for each installation.

Use Case – Validated Access to Web Servers

The support for validated access to web servers can be enabled through one of two CoreStreet products. For web servers running Microsoft Internet Information Services (IIS) that require the presentation of a digital certificate from a user prior to access, the CoreStreet Server Validation Extension for IIS (SerVE-IIS) is used. SerVE-IIS enables IIS to use CAPI to validate the revocation status of digital certificates using OCSP or MiniCRL responses. In the event of a network outage, a local cache of CRLs can also be created.

Administrative tools supplied with SerVE-IIS allow an administrator to deploy the software on servers easily and rapidly and in a wide variety of network configurations. Site administrators can create a pre-configured installer customization using all appropriate options and security information, and deploy the installer customization to servers without technical support for each installation.

CoreStreet's Path Builder SSL Gateway allows secure, standards-compliant validation of a client's digital certificate to determine whether or not to allow access to secure web resources. The SSL Gateway can use Server-based Certificate Validation Protocol (SCVP), OCSP, CRLs and MiniCRLs to aid in this validation. The SSL Gateway acts as a reverse HTTP proxy for the web

server that manages these resources, and can be deployed in front of web servers running IIS, Apache HTTP Server, Netscape Enterprise Server, etc.

Use Case – Cryptographic (PIV CARD-based) Logon

The support for validation of a certificate-based (e.g., FIPS 201 PIV card) logon to the network is enabled through the deployment of the CoreStreet Server Validation Extension for Microsoft Domain Controllers (SerVE-MDC) to each Microsoft Domain Controller (MDC) instantiated within the enterprise. SerVE-MDC enables MDC to use CAPI to validate the revocation status of digital certificates using OCSP or MiniCRL responses. In the event of a network outage, a local cache of CRLs can also be created.

As with the other SerVEs, tools are supplied that allow an administrator to deploy the software on servers easily and rapidly and in a wide variety of network configurations. Site administrators can create a pre-configured installer customization using all appropriate options and security information, and deploy the installer customization to servers without technical support for each installation.

Use Case – Local Responder Implementation

The instantiation of a local responder capability in support of any of the validation use cases presented above is enabled through the deployment of the CoreStreet Responder Appliance 2400 (RA2400). The RA2400 is a cost-effective, turnkey implementation of a device containing a pre-defined hardware/operating system package. The RA2400 is rated as having the processing capacity to handle in excess of 2,400 responses per second through a single appliance. Certainly, multiple appliances can be deployed to a location for additional capacity or redundancy. Depending on the transaction volume and transaction types, a single RA2400 can handle approximately 50,000 users.

Generally, CoreStreet recommends the deployment of the RA2400s in pairs, thereby facilitating a local failover capability. The RA2400 is a one unit (1U), rack-mount appliance that runs on a hardened version of Debian Linux, with all non-essential administrative commands removed. It can be easily installed within an installation and then synchronized on a scheduled basis with the Validation Authority file server housing the pre-computed, D-OCSP and MiniCRL proof sets. The appliance can also be updated via an out-of-band import of proof sets from a CD or via a remote administrative SSH update to the box.

The appliance has been configured to only recognize, and reply to, OCSP requests. Additionally, the system has been hardened against external hacking threats and known operating system vulnerabilities. All software routines that are not required to support the CoreStreet responder application have been eliminated from the device.

The RA2400 can be considered a true turnkey solution as it is a plug-and-play OCSP responder that requires very little technical knowledge to install and maintain. The appliance therefore greatly reduces the drain on IT resources normally associated with prolonged installation, education and maintenance costs of software solutions. Furthermore, the RA2400 provides for remote troubleshooting and can be easily swapped out should a unit fail. A Responder Appliance eliminates the need for IT resource expertise in different operating systems and databases.

About CoreStreet

Every day, the world's most demanding government and commercial enterprises rely on CoreStreet software and expertise to power their smart credential and convergence programs.

For more information, including detailed product and solution information, technical briefs, and case studies, see **www.corestreet.com**

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

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

w06-05v2