



Certificate Validation Risk Mitigation

Distributed OCSP Risk Mitigation Overview

As a technology that relies on the availability of specific components within a TCP/IP network, any validation solution deployed must provide for the mitigation of specific component failure(s) across the fabric. The CoreStreet Validation Suite incorporates many feature sets that mitigate the risk of failure of any of these components or the supporting fabric.

The following diagram indicates the possible points of failure that are inherent in any validation infrastructure. The discussion that follows the diagram describes available mitigation techniques that are employed in the CoreStreet Validation suite, specifically as related to PIV card based network logon, since this is one of the most critical functions supported by the validation infrastructure.

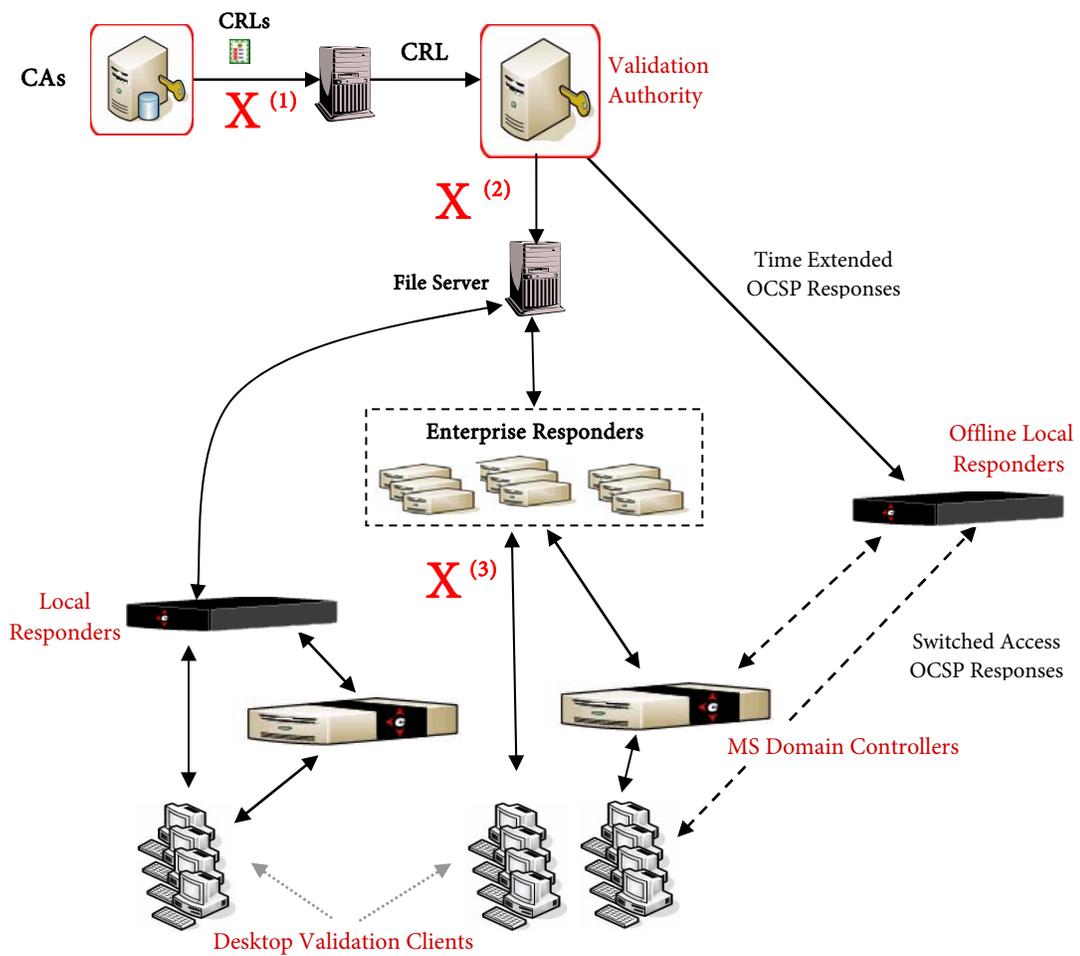


Figure 1. Mitigating Risks due to Network/Component Failures

As depicted above, there are several possible points of failure for any validation architecture, represented in the diagram as large red X's (and annotated numerically for ease of discussion). The following cases are indicated by these possible outage situations:

1. **X⁽¹⁾ CRL Outage:** A Certificate Authority (CA) does not publish an updated CRL within the expected publishing time frame or the LDAP repository cannot be reached for retrieval of the CRL data
2. **X⁽²⁾ Authority Outage:** The Enterprise Responders as well as any local responders do not receive the pre-signed proof sets from the CoreStreet Validation Authority (VA) within the scheduled update interval, and the proof set data on the responders is "stale"
3. **X⁽³⁾ Enterprise Responder Outage:** Relying Party software cannot reach the Enterprise Responders for validation
4. **Extended Site Isolation:** There is going to be a known outage for an extended period of time, in which communications outside of an enterprise location will not be possible.

For Scenario **X⁽¹⁾**, the CRL Outage situation is completely mitigated by the VA through its standard operating mode. The VA, on a scheduled interval for each publisher (i.e., CA), simply generates new signed status data (i.e., OCSP responses or proof set) from the last retrieved CRL data from the repository (i.e., best available data). If that data is expired, then the VA provides an error notification of this situation, but continues to process the data and generate signed OCSP responses with a configurable validity period from the date/time of the signing. For example, suppose the Enterprise CPS establishes a validity period of seven (7) days for its CRLs. If a particular CRL is not published again within that 7-day window, this will not stop the generation of OCSP responses. The VA will continue to generate proof sets based on the last good (but stale) CRL that was received. This is a configurable feature that allows the Administrator to codify the policy to be followed in the VA so that the user never knows that any CRL outage occurred, and thereby can continue to logon to their network and validate other user's certificates without interruption.

In Scenario **X⁽²⁾** which depicts an outage related to the VA (either server- or communications-based), the relying party software will continue to function properly for as long as the validity period for the OCSP responses has not expired. Once the proof set has expired, action needs to be taken within the relying party software for the user to continue to be unaffected by the outage. All of the CoreStreet desktop and server components allow for the configuration of an extension of the validity period of the proof set data, with a maximum skew of the expiration date of up to 60 days from the date presented in the proof set.

Additionally, each component can be configured to locally cache any OCSP response data for up to 60 days. The caching solution is good for short periods of time, but obviously, the cache will only contain the status of those certificates that were validated up until the point of the outage,

and only until the host desktop or server is re-booted (at which time the cache location would be flushed). Generally, caching is intended to simply provide a mechanism to reduce the number of repeated duplicate requests, primarily during email review, so this is not meant as a long-term outage mitigation technique, but is available as needed.

Both of these configurations can be updated via Group Policy and pushed to the user. As before, if this situation actually arises, a warning identifying the expiration condition will be made by each component in the audit data. The audit data is configurable for presentation in either (or both) the standard log file location and/or the Windows Event Viewer.

In the case of Scenario **X⁽³⁾**, the unavailability of the Enterprise Responders, the simplest resolution is to deploy Local Responders at each site. In fact, if Local Responders are instantiated, several benefits can be gained. First, the local device can be configured as the primary point of validation (with failover out to the other responder locations) and thereby effectively increase the speed and availability of the validation to the users due to their proximity to the device. Second, the site now has the ability to operate with only intermittent connection to the Enterprise network for periodic updates of the proof sets.

In the unlikely case where updates of the proof set data are required during a prolonged and unplanned outage condition, the proof sets can be copied onto permanent media, delivered out of band, and then directly imported to the Responder.

The last scenario, **Extended Site Isolation**, is applicable when a site needs to physically disconnect from the local network for an extended period of time (that is, a period of time longer than the standard validity period for the proof set data and/or the proof set validity period extension, as configured in the desktop and server software). This situation is handled with the establishment of Offline Local Responders and the execution of an Alternate proof set generation task by the VA. The Offline Local Responders would be configured to use the exact same IP addressing definition as the primary responder set(s), but would be physically disconnected from the local network until such time as they were to be used. At that time, the Offline Local Responders would be connected to the local network, and the primary responders disconnected. The Alternate proof sets, generated at the same time as the standard proof sets, would simply be defined with an extended validity period to cover the time anticipated for the outage. That is, if the outage was anticipated to last 45 days, then the Alternate proof sets could be generated with a validity period of 45 days. Again, there is no impact to the end user, and validation data is available throughout the period of isolation.

Note: This technique could also be used to mitigate “unplanned” outages such as described in Scenarios **X⁽²⁾** and **X⁽³⁾**.

In all of these scenarios, the techniques applied as part of one mitigation strategy may apply across multiple situations. Note that the configuration of the desktop and server components to sequentially rollover from one responder to another if a time-out condition ensues is a very

simple configuration that greatly enhances the availability of the validation service that is critical to the accessibility of network resources by the end user. As all responders are addressable via a single URL and all of the Signing Authorities use the same key, no specific modifications to the relying party components is required. This provides an extremely robust failover capability. Once again, the end user continues to be able to perform a validated logon to the system as well as other certificate validations, with no indication of the outage or subsequent failover. This responder definition and sequencing can be done by the Administrator at the initial configuration of the software and pushed to the user, or the Administrator can apply a Group Policy update to the configuration, as needed, after the initial push.

CoreStreet will work with your implementation team to determine the most robust and cost effective configuration for your validation solution.



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