Certificate Revocation Checking Using OCSP and CRL in VMware® View™ 4.5/4.6

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Introduction 3
About VMware View 3
About Smart Card Certificate Authentication 3
Smart Card Authentication Infrastructure Requirements 3
Revocation Overview 4
Certificate Revocation List (CRL) 4
Online Certificate Status Protocol (OCSP) 5
Configuring VMware View for Certificate Authentication and Revocation Checking . 5
Configuring VMware View for Smart Card Authentication 5
Using/Configuring Certificate Revocation Checking in VMware View 5
Revocation Checking with CRL 6
Revocation Checking with OCSP 6
OCSP Update Intervals 7
Revocation Checking with both CRL and OCSP 7
OCSP/CRL Revocation Checking with Local Mode 9
Tips and Tricks 9
Cross-forest Certificate Enrollment with Windows Server 2008 9
Configuring VMware View to Use HTTP Proxy 10
Basic Troubleshooting 11
About the Authors 11

Introduction

About VMware View

VMware® View™ is a best-in-class enterprise desktop virtualization platform. VMware View solution separates the personal desktop environment from the physical system by moving desktops to a datacenter, and then accessing the desktops using a client-server computing model. VMware View satisfies a rich set of features required for any enterprise deployment by providing a robust platform for hosting virtual desktops from VMware vSphere™. Additional capabilities such as distributed infrastructure services and virtual desktop failover and recovery make it an ideal solution for desktop virtualization.

VMware View provides different authentication mechanisms such as username-password, smart card or RSA, along with further enhancements like single sign-on (SSO) and Triple SSO. With VMware View 4.5/4.6, smart card authentication has additional manageability with the introduction of OCSP and CRL features. This paper provides a technical overview of these features, in addition to the specific configurations required in common implementations. Overall, this paper covers:

- A brief discussion of smart card certificate authentication
- A brief discussion of OCSP and CRL features
- VMware View integration with OCSP and CRL
- Some tips and tricks
- Basic troubleshooting

About Smart Card Certificate Authentication

Smart card certificate authentication is used by many enterprises as a security measure. Smart card authentication is a widely used two-factor authentication (TFA) mechanism. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and 'something you have' as the other factor. A common example of TFA is a debit card, where the card itself is the physical item you have, and the personal identification number (PIN) is something you know that is associated with it.

Smart Card Authentication Infrastructure Requirements
The following prerequisites should be appropriately configured for successful smart card authentication:

- Certificate Authority – Managed within the enterprise (for example, Microsoft Certificate Authority) or by a trusted external Certificate Authority (for example, VeriSign).
  - Configure the Certificate Authority (CA) to issue the proper certificates.
  - Specify policy that dictates which users can enroll for those certificates.
- Enrollment Agent – This role should be configured in a CA or on a dedicated system. This role is required for registering user certificates to a smart card.
- Smart Card – Generally, a plastic card with embedded integrated circuits (for example, an employee ID card).
- Smart Card Reader – A communication medium between the smart card and the host.
- Cryptographic Service Provider (CSP) drivers – An interface to the smart card (for example, Microsoft CSP).

For further information on enrolling user certificates on to smart cards, refer to a Microsoft online resource: http://technet.microsoft.com/en-us/library/cc736901%28WS.10%29.aspx.

Revocation Overview

Generally, certificates are issued for a defined period and configured with validity parameters that include start time and an explicit expiration date. This effectively means the certificate can be issued with a validity of one day, one year or several years. Once issued, a certificate becomes valid from the beginning of its validity time, and it is considered valid until its expiration date is reached. Apart from this, there can be different scenarios which cause a certificate to become invalid prior to expiration. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

To enable revocation, RFC 5280 lists the following states that can be applied by a CA to any of its issued certificates.

CRL REASON	REASON CODE
Unspecified	0
keyCompromise	1
cACompromise	2
affiliationChanged	3
Superseded	4
cessationOfOperation	5
certificateHold	6
Not Used	7
removeFromCRL	8
privilegeWithdrawn	9
aACompromise	10

There are two popular certificate validation mechanisms:

- CRL – Certificate Revocation List
- OCSP – Online Certificate Status Protocol

Certificate Revocation List (CRL)

A certificate revocation list (CRL) is a digitally signed list issued by a CA that contains certificates that have been revoked. The list includes the serial number of the certificate, the date certificate was revoked, and the reason for revocation. VMware View Connection Server can perform CRL checking to determine a presented certificate's revocation status. There are two variants of CRL:

- Base/Full CRL: A type of CRL that contains a list of certificates revoked and published automatically in specified intervals as defined by the administrator of CA.
- Delta CRL: A type of CRL that contains a list of certificates revoked since the last base/full CRL was published.

Online Certificate Status Protocol (OCSP)

The Online Certificate Status Protocol (OCSP) supplements CRL validation, and enables high-performance validation of certificate status. Further, an OCSP server can retrieve the CRLs from all CAs in an organization. Upon implementation, an organization can use an OCSP server as a single point of contact for revocation validation. This enables client applications to obtain timely information on the revocation status of a certificate.

An OCSP server works using a Responder-Repeater configuration. Typically, an enterprise would configure a single OCSP Responder and multiple OCSP Repeaters.

Configuring VMware View for Certificate Authentication and Revocation Checking

Configuring VMware View for Smart Card Authentication

The following steps are required for smart card authentication in VMware View:

- Obtain a root certificate from the CA
- Create a trust store using the keytool
- Create a `locked.properties` file with appropriate attributes

For further details regarding the configuration of smart card authentication with respect to VMware View, refer to VMware VMware View 4.5/4.6 Administrator's Guide.

Using/Configuring Certificate Revocation Checking in VMware View

VMware View supports revocation checking with CRLs as well as OCSP in environments with VMware Connection Server and VMware Security Server. Both CRL and OCSP features can be configured on a single server (standard, replica, security) instance. When both types of certificate revocation checking mechanism are configured, VMware View attempts to use OCSP first, and falls back to the CRL. However, please note that VMware View does not fall back to OCSP if the CRL fails.

For further details regarding the configuration of CRLs and OCSPs with respect to VMware View, refer to the VMware View 4.5/4.6 Administrator's Guide.

Revocation Checking with CRL

When VMware View is configured for revocation checking with the CRL, the revocation status of a certificate is determined by accessing the CRL published by the appropriate CA. If a certificate is found to be revoked, ther VMware View client throws an appropriate error: **Smart card authentication failed. Please contact your Administrator. (Revocation Checks failed)**.

When configuring CRL with VMware View, you will need to follow the steps mentioned under the section Configuring Smart Card Authentication. Once you have successfully completed these steps, you will need to update the `locked.properties` file with appropriate attribute values.

The following `locked.properties` attribute values are mandatory when configuring CRL revocation checking in VMware View:

```
trustKeyfile=longa.key

trustStoretype=JKS

useCertAuth=true

enableRevocationChecking=true

crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

Once the above attributes are configured, restart the VMware View Connection Server service for the changes to take effect.

Revocation Checking with OCSP

When VMware View is configured for revocation checking with OCSP, the revocation status of a certificate is determined by sending a verification request to an OCSP Responder. If a certificate is found to be revoked, VMware View client sends an appropriate error message.

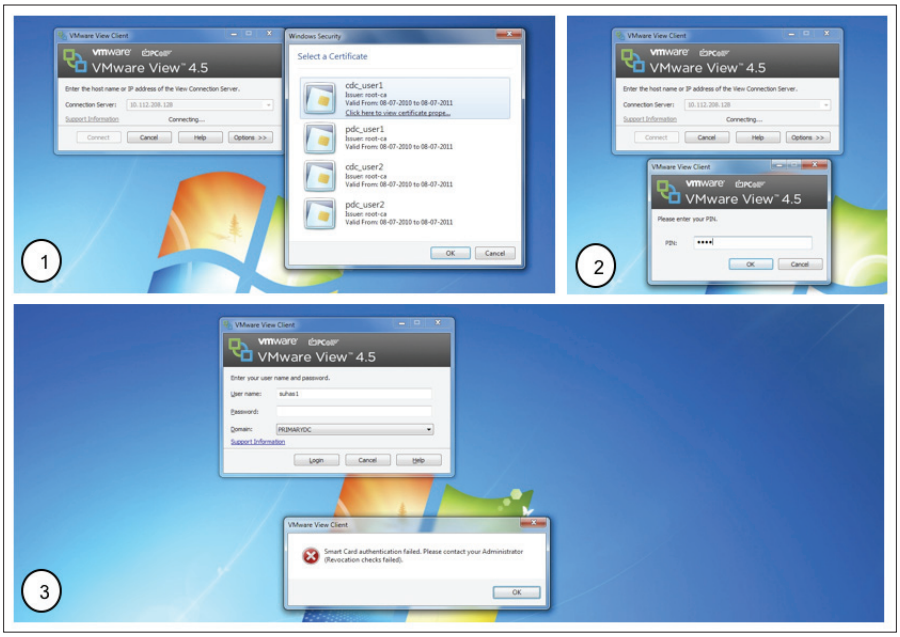

Figure 1: Clockwise from left: 1. VMware View Client prompts user to select a certificate from the list of available certificates; 2. User is prompted for PIN entry; 3. Error message stating certificate revocation

The following `locked.properties` attribute values are mandatory when configuring OCSP revocation checking in VMware View:

```
trustKeyfile=lonqa.key

trustStoretype=JKS

useCertAuth=true

enableRevocationChecking=true

enableOCSP=true

allowCertCRLs=true

ocspSigningCert=te-ca.signing.cer

ocspURL=http://te-ca.lonqa.int/ocsp
```

You need to place OCSP Responder signing certificates alongside the `locked.properties` file, and specify the name under the attribute `ocspSigningCert`.

Once you have configured these attributes, restart the VMware View Connection Server service for the changes to take effect.

OCSP Update Intervals

A CA publishes CRLs at regular intervals based on the configuration. However, you can configure the OCSP Responder to refresh its revocation lists based on either the validity period of the CRL being used, or at a manually configured interval.

Windows 2008 Server can be configured as an OCSP Responder. For detailed instructions on setting up and configuring OCSP, refer to the Microsoft TechNet article.

Revocation Checking With Both CRL and OCSP

You can configure VMware View to use both CRL and OCSP mechanisms together. The following `locked.properties` attribute values are mandatory when configuring both CRL and OCSP revocation checking in VMware View:

```
trustKeyfile=lonqa.key

trustStoretype=JKS

useCertAuth=true

enableRevocationChecking=true

enableOCSP=true

ocspCRLFailover=true

allowCertCRLs=true

ocspSigningCert=te-ca.signing.cer

ocspURL=http://te-ca.lonqa.int/ocsp

crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

When both CRL and OCSP are configured, OCSP will have higher priority over CRL revocation checking. In such a configuration, if OCSP validation fails then VMware View will fall back to CRL validation. This fall back mechanism is controlled by the attribute `ocspCRLFailover` in `locked.properties` file. Once you configure these attributes, restart the VMware View Connection Server service for the changes to take effect.

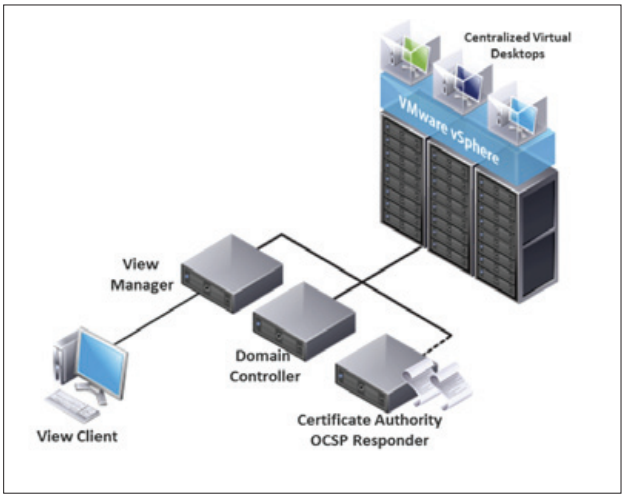

Figure 2: A pictorial representation of VMware View integration with OCSP Responder

The VMware View administration interface provides various options for smart card authentication. These are:

- Optional – If **smart card authentication** is set to **optional**, the user is allowed to login using username/password on smart card authentication failure.
- Required – If **smart card authentication** is set to **required**, the user is NOT allowed to login using username/password on smart card authentication failure.
- Not allowed – If **smart card authentication** is set to **not allowed**, the user is NOT allowed to login using a smart card.

The figure below illustrates these options:

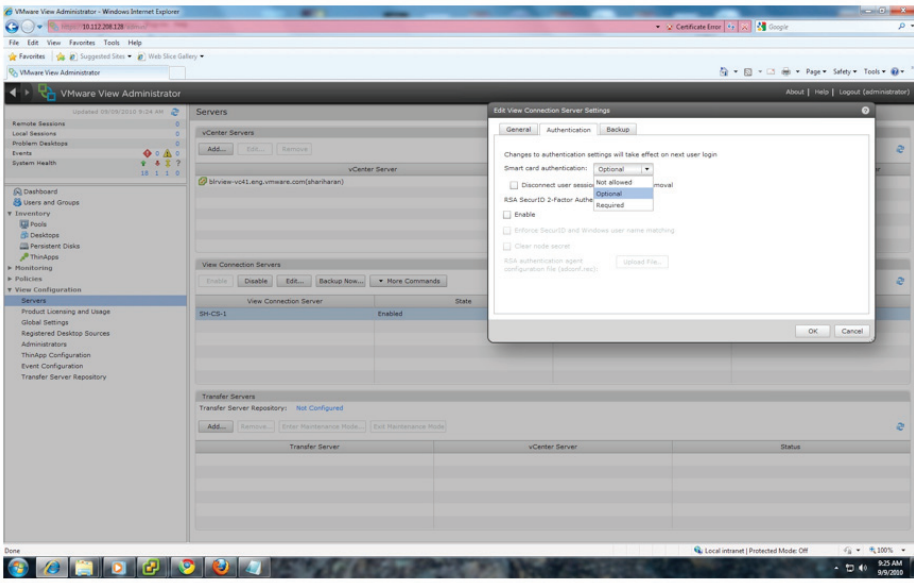

Figure 3: VMware View administration interface options for smart card authentication.

OCSP/CRL Revocation Checking with Local Mode

In Local Mode, Revocation checking is performed only if VMware View Client can communicate with VMware View Connection Server

Certificate revocation checking is performed as in a normal remote session.

- User Certificate is unrevoked. If the user certificate is not revoked, the authentication succeeds.
- User Certificate is revoked. If the user certificate is revoked, the authentication fails.

Tips and Tricks

Cross-forest Certificate Enrollment With Windows Server 2008

Traditionally, an enterprise CA is limited to issuing certificates only to the clients that belong to the same Active Directory (AD) forest. This means that user and client computers would only attempt to enroll certificates from a CA in the local forest, especially in auto-enrollment scenarios. Further, this drawback forces administrators to have at least one CA per forest.

Starting with Windows Server 2008 R2, this barrier is removed by supporting cross-forest certificate enrollment. This feature enables clients to enroll a certificate from a CA of a different AD forest, further reducing the number of CAs in a multiforest environment.

For further details regarding the cross-forest certificate enrollment, refer to the Microsoft white paper Cross-forest Certificate Enrollment with Windows Server 2008 R2.

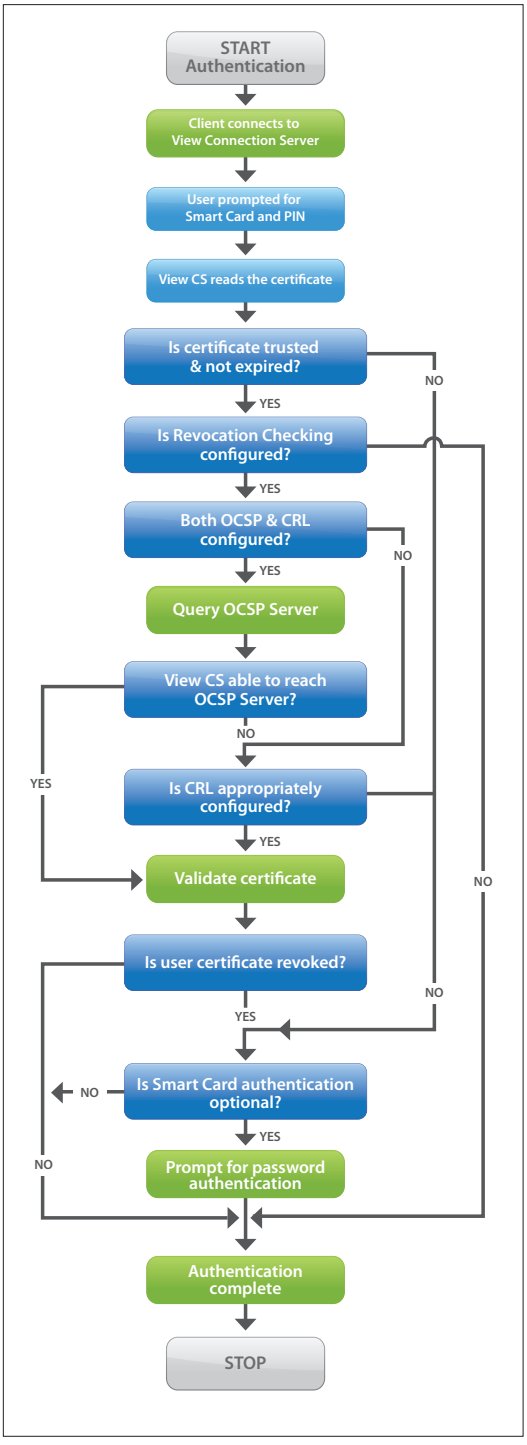

Figure 4: Authentication flow using OCSP/CRL revocation-checking mechanism.

Configuring VMware View to Use HTTP Proxy

If a proxy server is not configured in a company's environment, this step can be safely skipped.

There are instances where enterprises would have revocation-checking mechanisms placed outside a company's internal network. In such cases, the VMware View Connection Server needs to contact an entity outside the internal network. If the company has a policy to direct Internet traffic through a proxy, then VMware View Connection Server requires additional configuration to contact the OCSP Responder. This is because the VMware View Server uses a Java socket that doesn't depend on Internet Explorer proxy settings.

You can use the following steps to configure the VMware View Java socket layer to use a proxy for HTTPS requests. This enables the VMware View Server to contact the OCSP Responder.

- Open the Registry Hive

```
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\
VMware VDM\plugins\wsnm\TunnelService\Params
```

- Configure `Dhttp.proxyHost` and `Dhttp.proxyPort` keys.

  For example:

  ```
  Dhttp.proxyHost=<proxy123>
  ```

  ```
  Dhttp.proxyPort=<proxyport>
  ```

  Note: These values need to be appended and should not overwrite the previous values.

- Restart the VMware Connection Server Service for the changes to take effect.

Basic Troubleshooting

- Ensure that proper drivers are in place for smart card readers and smart cards on both client and agent machines.
- Ensure all entries in the `locked.properties` file are syntactically correct. Refer to the VMware View 4.5 /4.6 Administrator's Guide for correct syntax.
- Ensure the creation of `truststore` files with a valid and appropriate root CA certificate.
- Ensure the VMware View Server can contact the OCSP Responder by accessing the URL specified in `locked.properties.`
- Ensure the OCSP Responder signing certificate is valid.
- Ensure the OCSP Responder can communicate to the CA infrastructure.

About the Authors

Raghavendra Babu is a QE Manager at VMware. Currently he leads View–Mgmt QE efforts from Bangalore. He has a BE in Computer Science. His previous experience includes companies like Dell India R&D, Quark, and others.

Noble Peter is a Software QE Engineer at VMware. Currently, he is part of the View-Mgmt QE team in Bangalore. He has an MSc in DDES from Manipal University.

Suhas Hariharan is a Software QE Engineer at VMware. Currently, he is part of the View-Mgmt QE team in Bangalore. He has an MTech in Computer Science from Manipal University.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com