vCenter 6.5
Smart Card Authentication Configuration Guide

Prepared by

Lincoln Porter
Staff Program Manager

Ryan Lakey
Consulting Architect

Version History

Date	Ver.	Author	Description	Reviewers
07 FEB 2019	1.2	Lincoln Porter	Minor tweaks for inclusion into the vSphere 6.5 STIG Removed reverse proxy config	Ryan Lakey Ron Albrecht
05 FEB 2019	1.1	Lincoln Porter	Updated OCSP override settings	Ryan Lakey Ron Albrecht
20 MAR 2017	1.0	Lincoln Porter	Initial release forking from 6.0 version	Ryan Lakey

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

1. Overview

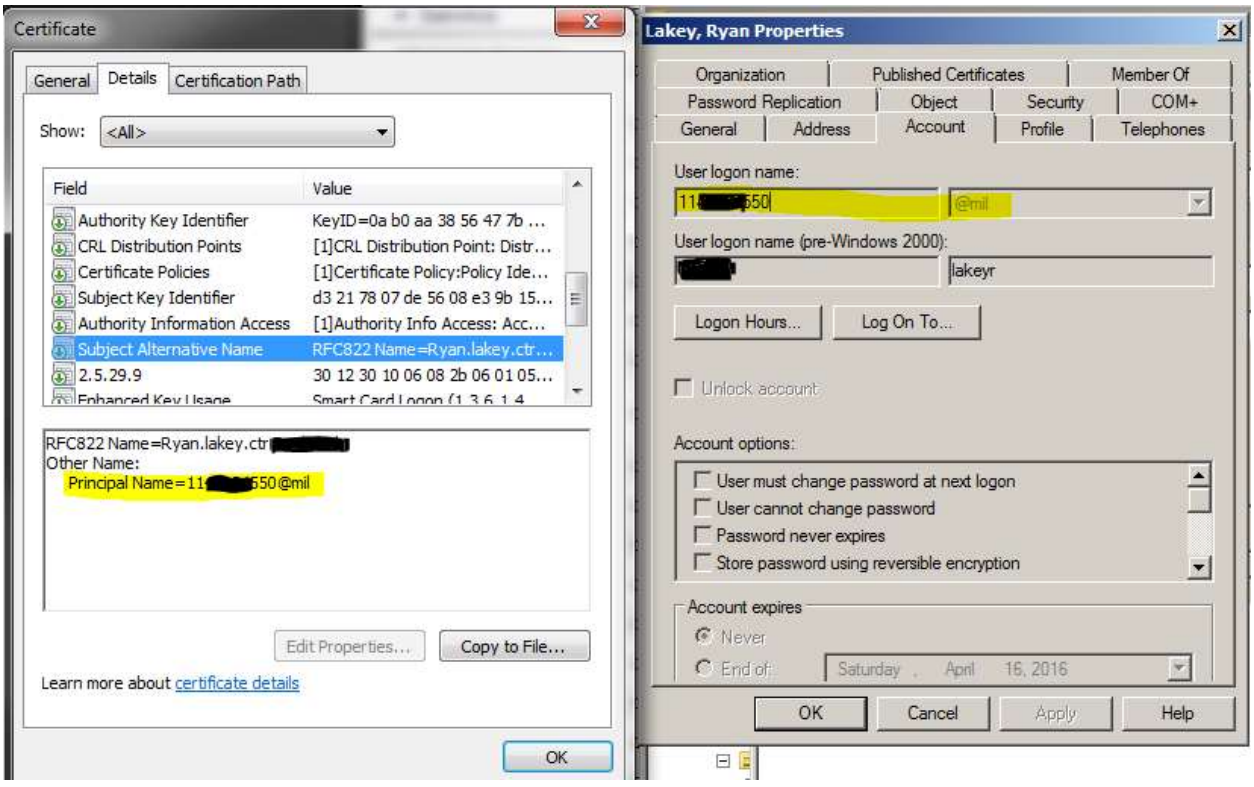
1.1 Summary

The Platform Services Controller (PSC) that was released as part of Single Sign-On (SSO) in vSphere 6.0GA only supported username/password for authentication. 6.0 Update 2 and later allows the configuration of a PSC to support multiple new forms of authentication. The focus of this document is the configuration of certificate-based authentication in vSphere 6.5 as the configuration is distinctly different from the 6.0 branch, there is a separate document for that version. This feature is biased towards Department of Defense Common Access Card (CAC) implementations but may fit other environments as well. This document will not tell you how to implement PKI, only how to integrate vSphere SSO into an existing PKI.

1.2 System requirements

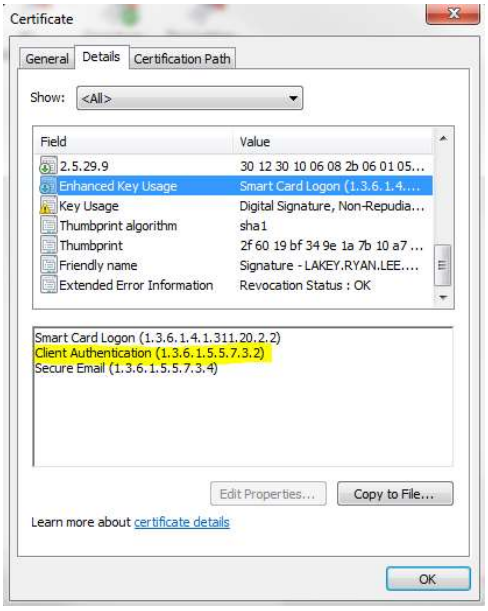
1. This deployment assumes that an enterprise PKI has been deployed. The end user is responsible for having the necessary tokens/cards and middleware so their certificate can be presented to the browser. The certificate selected by the user for authentication must meet the following requirements:
    a. The certificate will need to have a User Principal Name (UPN) in the Subject Alternative Name (SAN) extension. The UPN needs to correspond to an active directory account.

Figure 1. Example SAN corresponding to AD account



    b. The certificate will need to have “Client Authentication” as one of the “Application Policy” or “Enhanced Key Usage” purposes. If the certificate does not have this usage then it will not be selected by the browser for authentication.

Figure 2. Example Key Usage in Certificate



2. Smart card authentication must be backed by Active Directory and as such an AD identity source must be configured in SSO. Both native and AD over LDAP are supported, neither is better than the other. This must be done manually by the SSO administrator.
3. The enterprise PKI is configured so that the PSC is able to contact the OCSP and/or CRL servers specified in the certificate or optionally overridden by the SSO administrator.
4. All PSCs and vCenters are assumed to be on the same build of 6.5. This guide is not intended for a mixed environment of 6.0 and 6.5 PSCs and vCenters.

1.3 Browser support

- Internet Explorer and Chrome are supported.
- Firefox does not work with smart card authentication.
- Safari is untested.

1.4 Browser plugins

The Enhanced Authentication Plugin (EAP) is not required for smart card authentication. This feature is enabled by the browser's native certificate capabilities and the SSO reverse proxy. The EAP enables logging in to vCenter with your Windows session credentials.

2. Enabling smart card authentication

The following steps configure the smart card feature inside of SSO. This change replicates across the PSCs and therefore only needs to be done in one place. Option 1, the GUI method, is applicable to both appliance and Windows deployment models. Option 2, the CLI method, is applicable to both models but with different paths and script locations.

If you are on still on a Windows vCenter, please consider moving to the appliance in your next version upgrade. Windows vCenter deprecation has been announced and all new features are being implemented in the vCenter Server Appliance.

2.1 Option 1 : Configure smart card authentication from the PSC web interface

This second step configures the smart card feature inside of SSO using the PSC GUI. The GUI does not let you specify an OCSP signing cert or configure responders on a per-site basis, this must be done through the command line in section 2.2.

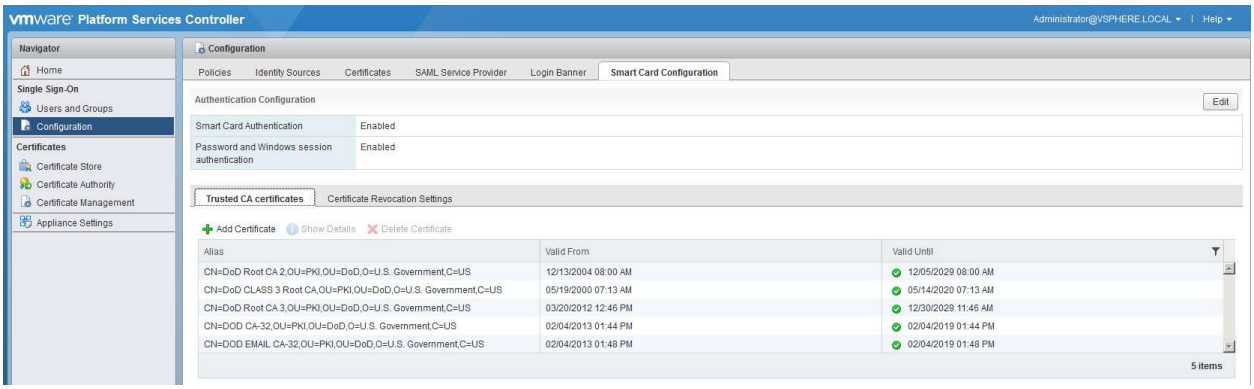
1. Login to the PSC web interface with administrator@vsphere.local from

   https://<FQDN or IP of PSC>/psc

   In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

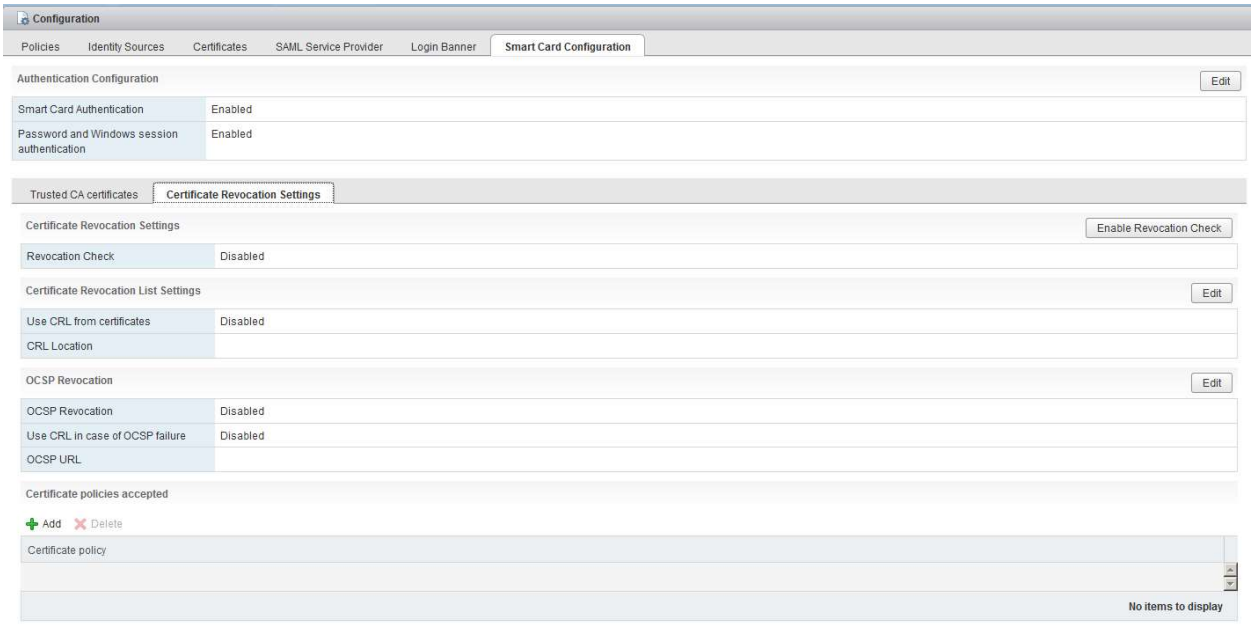
   If you specified a different SSO domain during installation, log in as administrator@mydomain.
2. Browse to Single Sign-On > Configuration.
3. Click Smart Card Configuration, select “Edit” next to “Authentication Configuration”, check the box next to “Smart Card Authentication”.
4. In this same window if you uncheck “Password and Windows session authentication” then smart card login will be mandated and no user/pass logins will be allowed including vsphere.local. This can be rolled back via CLI in section 2.3 if access to vCenter via smart card is somehow lost.
5. On the same page, select the Trusted CA certificates tab.
6. To add one or more trusted certificates, click “Add Certificate”, click “Browse” and select a certificate, and click “OK”.

Figure 3. PSC Admin Console Smart Card Configuration



7. To change certificate revocation settings click on the “Certificate Revocation Settings” tab and enable/disable revocation checking and CRL/OCSP settings per your environment.
8. By default CRL checking using the certificates distribution point is enabled and OCSP is disabled. We recommend turning on OCSP and using CRL as fallback. We further recommend, optionally, configuring alternate, local OCSP responders and CRL repos to further limit WAN traffic. Per-site OCSP responders can only be configured through the command line as detailed in section 2.2.

Figure 4. PSC Admin Console Smart Card Certificate Revocation Settings



9. Configure the login banner according to your requirements.

Figure 5. Logon banner configuration

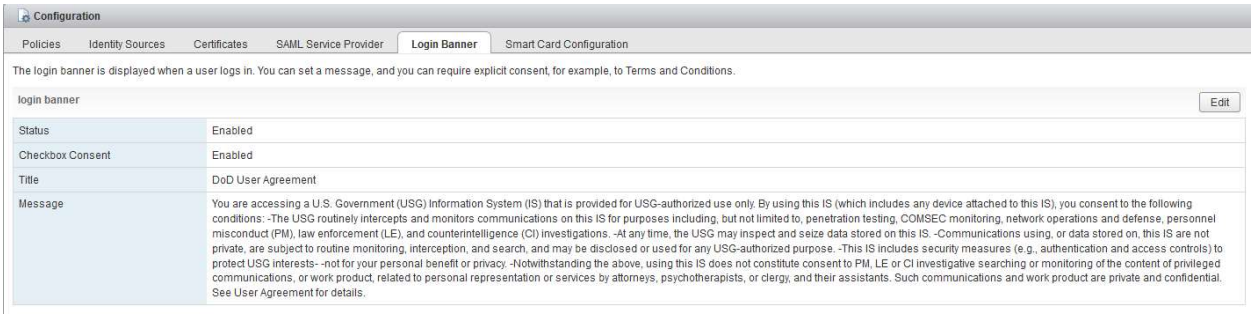
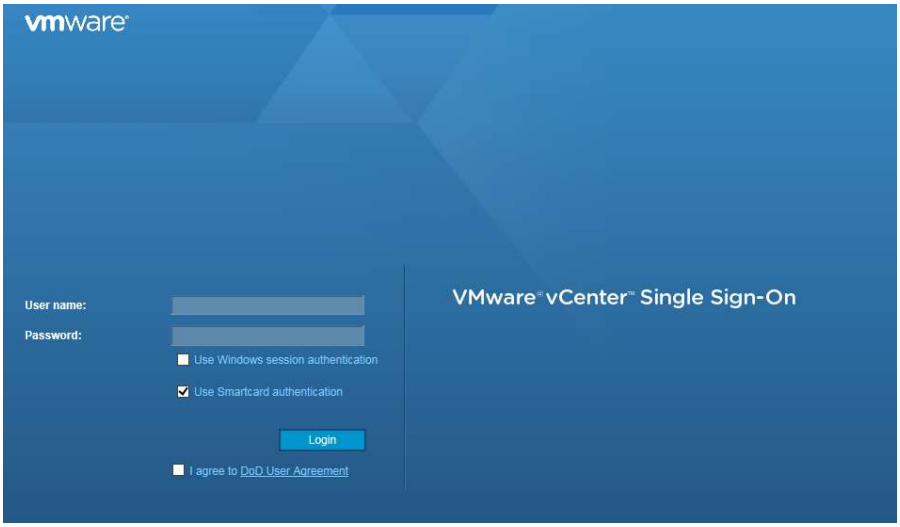


Figure 6. vCenter Web Client Login Page after Smart Card Authentication is Enabled.



2.2 Option 2 : Configure smart card authentication from the command line

1. SSH or log on to the console of the PSC.
2. Skip this step if the default shell has already been changed. SCP will not work with the default root shell. Enable SCP by changing the shell for root from “/bin/appliancesh” to “/bin/bash” by running the following commands:

```
a. shell

b. chsh -s /bin/bash root
```

3. Option 1 : To add all DoD root certs easily:
   a. Navigate to http://iase.disa.mil/pki-pke/Pages/tools.aspx
   b. Click the ‘Trust Store’ tab
   c. Scroll to the bottom until you see "PKI CA Certificate Bundles: PKCS#7"
   d. Click the download link that says "For DoD PKI Only - Version X.X"
   e. Open the zip, extract the PEM p7b file, in our case Certificates_PKCS7_v5.4_DoD.pem.p7b
   f. SCP the p7b file to /tmp on the PSC

```
g. cd /tmp
```

```
h. openssl pkcs7 -inform PEM -print_certs -in
   ./Certificates_PKCS7_v5.4_DoD.pem.p7b | awk '/subject=/ {++n} {print >
   "dodcert" n ".cer"} END {print n " certificates split out"}'

i. list="";for i in dodcert*.cer; do
   list="$list,$i";done;list=${list:1};/opt/vmware/bin/sso-config.sh -
   set_authn_policy -certAuthn true -cacerts "$list" -t vsphere.local
```

4. Option 2 : Upload the desired certificates individually.
   a. SCP your PEM/Base64 trusted root certificates to /tmp on the PSC.
   b. Run the following command to add the trusted roots to SSO. This command is not additive, all certificates must be specified at once.

```
i. /opt/vmware/bin/sso-config.sh -set_authn_policy -certAuthn true -
   cacerts "/tmp/MySmartCA1.cer,/tmp/MySmartCA2.cer"  -t
   vsphere.local
```

5. Turn off Integrated Windows Authentication and SecurID.

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -winAuthn false -
   securIDAuthn false -t vsphere.local
```

6. Add your smart card enabled AD account to the SSO Administrators group.
7. Make sure that logins are working correctly before continuing.
   a. Disable revocation checking (on by default) to make sure logins work without checks.

```
i. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -
   revocationCheck false
```

   b. When logins are working turn revocation checking on and continue configuration.

```
i. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -
   revocationCheck true
```

8. (**Optional**) Turn off password authentication and mandate smart card authentication. This includes vsphere.local accounts but it can easily be re-enabled.

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn false -t
   vsphere.local
```

9. By default OCSP is off and CRL from the distribution points on the certificate is used. It is recommend to turn on OCSP and use CRL as fallback but this will depend on your environment.

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -useOcsp
   true

b. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -
   failoverToCrl true
```

10. (**Optional**) It is further recommended to configure alternate, local OCSP responders and CRL repositories to limit WAN traffic. Site ID is optional and will default to the default site. Responders can be configured to be site-specific, for example to force your Boston site to use the Boston responder and your Seattle site to use the Seattle responder. Once this again, this is optional and will depend on your environment.

```
a. /opt/vmware/bin/sso-config.sh -t vsphere.local -add_alt_ocsp  [-siteID
   yourPSCClusterID] -ocspUrl http://local.ocsp.url -ocspSigningCert
   /path/to/yourOCSPSigningCA.cer

b. If you need to find the SiteID for a given PSC, run this command
```

```
i. /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-guid --server-name
   PSC.FQDN.or.localhost
```

11. (**Optional**) Now we override the CRL URL with a local repository.

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -
   useCertCrl false -crlUrl http://local.crl.url
```

12. (**Optional**) Set the login banner.

```
a. /opt/vmware/bin/sso-config.sh -set_logon_banner -title "Banner title" -
   enable_checkbox Y <path-to-banner-file>
```

2.3 Individual Configuration Items

2.3.1 Enable password authentication

a. /opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn true -t vsphere.local

2.3.2 Get a summary of the current configuration

b. /opt/vmware/bin/sso-config.sh -get_authn_policy -t vsphere.local

2.3.3 Enable or disable revocation checking

a. /opt/vmware/bin/sso-config.sh -set_authn_policy -revocationCheck **<true/false>** -t vsphere.local

2.3.4 Enable or disable OCSP

a. /opt/vmware/bin/sso-config.sh -set_authn_policy -useOcsp **<true/false>** -t vsphere.local

2.3.5 Set OCSP responder override

a. /opt/vmware/bin/sso-config.sh -t vsphere.local -add_alt_ocsp [-siteID yourPSCClusterID] -ocspUrl http://responder.FDQN.or.IP -ocspSigningCert /path/to/yourOCSPSigningCA.cer

b. If you need to find the SiteID for a given PSC, run this command

i. /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-guid --server-name PSC.FQDN.or.localhost

2.3.6 Show OCSP responder override

a. /opt/vmware/bin/sso-config.sh -t vsphere.local -get_alt_ocsp [-siteID yourPSCClusterID]

2.3.7 Remove OCSP responder override

a. `/opt/vmware/bin/sso-config.sh -t vsphere.local -delete_alt_ocsp [-allSite] [-siteID yourPSCClusterID]`

2.3.8 Enable or disable CRL failover after OCSP fails

a. `/opt/vmware/bin/sso-config.sh -set_authn_policy -failoverToCrl <true/false> -t vsphere.local`

2.3.9 Set logon banner from the command line

a. `/opt/vmware/bin/sso-config.sh -set_logon_banner -title "Banner title" -enable_checkbox Y <path-to-banner-file>`

3. FAQ

1. Is the Enhanced Authentication Plugin (EAP) required for smart card authentication?
    a. No. The documentation that says as such is incorrect. The EAP enables Windows Integration Authentication, it passes Windows Kerberos session credentials.
2. What is the format required for the trusted certificates?
    a. Base64 / PEM
3. Does the order that the certificates are added via sso-config.sh or the PSC UI matter?
    a. No
4. Do I need to specify an OCSP URL?
    a. No. By default the OCSP responder URL is pulled from the client certificate itself. If you have a local responder you can specify that local service with “-add_alt_ocsp” above and override the certificate fields.
5. Can I have username and password on with smart card authentication at the same time?
    a. Yes
6. What if I mandated smart card authentication but I cannot login, how do I get access to vCenter?
    a. Disable smart card authentication and re-enable username and password

```
/opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn true -winAuthn false -
certAuthn false -securIDAuthn false -t vsphere.local
```

7. Why are we specifying certificates two times?
    a. There are two components involved in smart card authentication, the reverse proxy and SSO itself. The reverse proxy sits in front of a number of vCenter/PSC services and its configuration is not currently exposed by API, all modifications must be made by hand. The certs for the reverse proxy are to aid the browser in client cert selection by providing an acceptable white list. The certs configured in SSO via GUI or sso-config.sh are for the verifying that client certificates are issued by one of the specified trusted roots.
8. I want to go back to the stock configuration, how do I do that?
    a. Set the authentication policy back to windows and username/password.

```
i.  /opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn true -
    winAuthn true -certAuthn false -securIDAuthn false -t vsphere.local
```

    b. Open `/etc/vmware-rhttpproxy/config.xml` in your editor of choice and replace the `<requestClientCertificate>` block with:

```
i.  <!-- <requestClientCertificate>true</requestClientCertificate> -->
```

c. Restart the service:

```
i.  /usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy
```

9. I have multiple AD domains that I want to smart card authenticate to, how do I do pick my target domain? How do I know which one is being used by default?
    a. You cannot currently specify the domain to target for smart card login. This will likely change in future releases.
    b. If you have multiple domains then SSO will start at the top of the list of identity sources and try each one until the user is found. SSO currently assumes a smart card user will be unique across domains.
    c. DoD users have the @mil domain in their UPN. For other types that may have "user@actual-domain.com" SSO will attempt to authenticate against "actual-domain.com" if that domain is configured or discovered through AD trust.
10. If I mandate smart card authentication on the web client can't I bypass this with the C# client?
    a. The authentication methods allowed by AD come in to play here. Generally speaking, accounts that are smart card enabled should not have a user-defined password. The C# client is fully deprecated in vSphere 6.5.
11. I have multiple PSCs linked in the same SSO domain, can I configure CAC authentication on one and have it replicate to the rest?
    a. Partially. The reverse proxy must be configured on each PSC manually. All other changes through the PSC GUI or using sso-config.sh are replicated via vmdir and only need to be done on one PSC.
12. Where is the public documentation for this feature?
    a. https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.psc.doc/GUID-08DF3B90-85C6-4CBB-B87C-CEF380844B95.html
13. Where are the relevant logs on the PSC?
    a. `/var/log/vmware/sso/vmware-sts-idmd.log`
    b. `/var/log/vmware/sso/ssoAdminServer.log`

4. Troubleshooting

Issue: You get an error “Unable to validate the submitted credential” when trying to login to the vSphere Web Client with Smart Card authentication.

Resolution: All root and intermediate certificates in the chain must be specified.

Check the logs under `/var/log/vmware/sso/vmware-sts-idmd.log` for

“com.vmware.identity.idm.CertificateRevocationCheckException: CertPath building failed. unable to find valid certification path to requested target”

You are probably missing a certificate in the path of the user’s certificate. There are many DoD root and intermediate CAs so verify the path on the user’s certificate and add any missing from the chain.

Resolution: This error can also indicate a problem after the raw certificate validation, an issue finding the user in AD. For example, it could be that a certificate without a subject alternative name was selected, resulting is the following logs entries:

Check the logs under `/var/log/vmware/sso/vmware-sts-idmd.log` for

“ERROR] [IdmClientCertificateValidator] No subject alternative name found in the cert.”

Or

“ERROR] [ServerUtils] Exception 'com.vmware.identity.idm.IdmClientCertificateParsingException: Empty Subject Alternative Names'”

Resolution: Look at `/var/log/vmware/sso/vmware-sts-idmd.log` for details on where the authentication is failing. Otherwise, generally make sure that the AD identity source is working, that the base DNs are correct and that the user exists. The Web Client login is actually an LDAP lookup by the PSC (after certificate validation) so it must be able to find and read the user account or the login will fail. In the case of integrated authentication if the user is located in a trusted domain make sure that the machine account is able to enumerate that other domain.