DoD Public Key Enablement (PKE) Reference Guide

Configuring Secure Remote Desktop Authentication Using DoD PKI

Contact: dodpke@mail.mil
URL: http://iase.disa.mil/pki-pke

Enabling PKI Technology
for DoD users

Configuring Secure Remote Desktop Web Access Using DoD PKI

17 January 2013

Version 1.0

DoD PKE Team

Revision History

Issue Date	Revision	Change Description
01/17/13	1.0	Initial release

Contents

Introduction

The DoD Public Key Enablement (PKE) Reference Guides are developed to help an organization augment their security posture through the use of the DoD Public Key Infrastructure (PKI). The PKE Reference Guides contain procedures for enabling products and associated technologies to leverage the security services offered by the DoD PKI.

Purpose

This guide provides instructions for configuring Microsoft Remote Desktop Web Access (RWA) for secure authentication and communications using DoD PKI. The guide addresses installing a DoD PKI server certificate on the Remote Desktop Gateway server and configuring security settings to run Remote Desktop Connections (RDC) and Remote Application Connections (RAC) over Transport Layer Security (TLS) with Federal Information Processing Standards (FIPS)-approved ciphers.

Scope

This document is intended for all users of PKI technologies. No in-depth knowledge of PKI is required. Some experience installing and configuring software on Windows platforms is helpful when reading this guide. Additional knowledge of Windows Remote Desktop Services, including Remote Desktop Connection Broker configuration, is recommended. Administrative privileges will be required. **Reference Appendix B for steps to configure Microsoft RemoteApp.**

Getting Started

System Requirements

Windows RDS version 6.0 is the minimum version required to support smart card logon. Windows XP with RDS version 6.0 or later will be able to support TLS and FIPS-compliant smart card logon settings detailed in this configuration guide.

Baseline Environment

This guide was developed using Windows RDS version 7.0 built on a Windows 7 Client machine, with a Windows Server 2008 R2 Session Host server to provide desktops to clients, and Windows Server 2008 R2 Gateway server in a Windows 2008 Functional Level forest on a domain controller.

Architecture

There are various ways RWA can be interconnected with other pieces of the remote desktop infrastructure. For the test architecture, the enablement of the security features applied for all Web Access connections. A RWA Host was PK enabled and connected to a PK enabled 2008 Domain. Connections from the Web Access Host were passed through to a PK enabled Remote Desktop Session Host and to PK enabled Remote Applications. The session host was a single Windows 2008 R2 server. There was no load balancing or clustering used.

Prerequisites

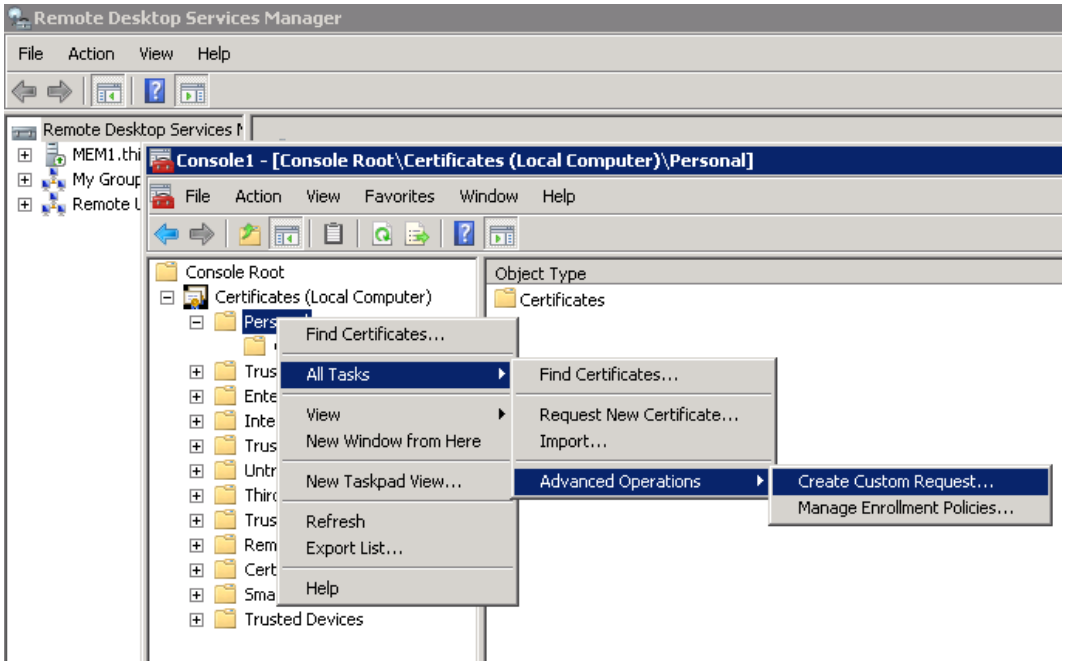
This guide assumes that the Windows domain is configured for smart card logon with DoD PKI credentials. . Refer to the relevant smart card logon guide available from the DoD PKE site under *For Administrators, Integrators, and Developers* > *Network Configuration* for detailed instructions. Additionally, the Windows Server 2008 R2 Session Host must be properly configured and enabled for Remote Desktop PKI operations. For instructions on installing and configuring Windows RDS, see the Microsoft TechNet article titled: *Remote Desktop Services* [i]. For instructions on installing and configuring a Windows Server 2008 R2 Session Host and PK enabling it, please see the DoD PKE *Configuring Microsoft Remote Desktop Services for Authentication using the DoD PKI*[ii]. In addition, if the RD Gateway server is providing access to a selected number of resources on a domain, a group for the target resources must been created in Active Directory as shown in the Technet Article titled: *How to Create a Group in Active Directory*.[iii]

Requesting and Installing A Certificate for the Remote Web Access Server

This section details installing a server certificate on the RWA server to enable clients to establish a TLS connection with the RWA server during Remote Desktop Protocol (RDP) connections.

Generating the Certificate Request

1) On the RWA server, open the Microsoft Management Console (MMC) by selecting **Start > Run** and entering *mmc*. Click **OK**.
2) Select **File > Add/Remove Snap-in**.
3) At the Add/Remove Snap-in screen, select **Add**.
4) Select the **Certificates** snap-in and click **Add**.
5) Select **Computer Account** for the type of certificates to manage. Click **Next**.
6) When returned to the Add/Remove Snap-in screen, click **OK**.
7) At the main MMC window, the **Certificates (Local Computer)** snap-in should appear. Expand **Certificates (Local Computer) > Personal.** Right-click **Certificates** and select **All Tasks > Advanced Operations > Create custom request.**



8) On the Before You Begin screen, read over the brief descriptions and click **Next**.

9) On the Certificate Enrollment Policy screen, select **Proceed without enrollment policy** under **Custom Request** and click **Next.**

10) Select the **(No template) Legacy key** template. Check the **Suppress default extensions** box. Ensure **PKCS #10** is selected. Click **Next**.

    NOTE: For Windows Server 2008 R2, select the (No Template) CNG Key.

11) Click the **expansion arrow** to the right of **Details** and click the **Properties** button.

12) Select the **Subject** tab. In the **Subject Name** box, select Type **Common name**. In the **Value** field, enter the member server's **Fully Qualified Domain Name (FQDN)** (e.g., dc1.mydomain.mil).

13) Click the **Add** button and the subject will appear on the right side in the form **CN=FQDN** (e.g., CN=mem1.mydomain.mil).

14) Select the **Private Key** tab and expand **Key options** by clicking the **expansion arrow** at the right of the **Key options** row. Select the **Key size** "2048".. Click **OK**.

15) At the Certificate Information screen, click **Next.**

    NOTE: For Windows Server 2008 R2, select the (No Template) CNG Key. The details will display blank values, and will be set by the DoD CA upon certificate issuance.

16) Click the **Browse** button to select the location to which you would like to save the certificate signing request (CSR) file and enter a **file name** with a **.txt** extension. Select **Save as Type** "All Files" and click **Save**. Ensure the **Base 64** radio button is selected and click **Finish** to save the request and exit the certificate request wizard.

Requesting a DoD-Signed Certificate

Follow the instructions in the *Obtaining a PKI Certificate for a DoD Server*[iv] guide, available on the DoD PKE website under *For Administrators, Integrators & Developers* > *Web Servers*, to submit the CSR and retrieve the certificate for the request generated above. Make a note of the name and path to the retrieved certificate file.

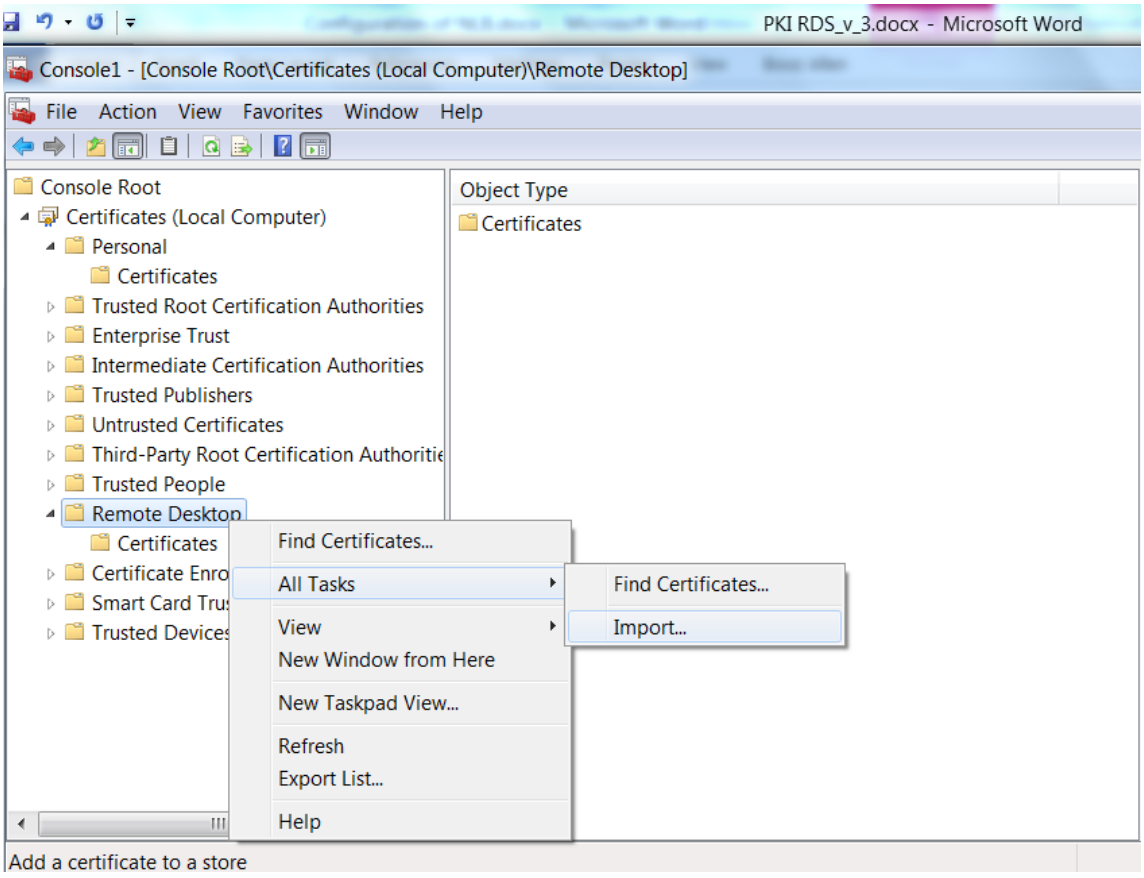
Installing the Issued Certificate

Import the certificate issued in the previous section into the RWA server.

1) On the RWA server, navigate to the MMC window containing the Local Computer Certificates snap-in. If it has been closed, re-open it by following steps 1-6 in the **Generating the Certificate Request** section.

2) Right-click the **Personal** store and select **All Tasks > Import** to import the issued server certificate.

3) Click **Next** on the Welcome screen.
4) On the File to Import screen, click **Browse** and navigate to the directory where the issued certificate was saved (noted in the previous section).
5) Select the **issued certificate file** and click **Next**.
6) Ensure that **Place all certificates in the following store** "Personal" is selected. Click **Next**.
7) Click **Finish** to import the certificate.
8) Repeat steps 1-7 of this section for the **Remote Desktop** store to make the certificate available for RDS functions.



Configuring Web Access Server Settings

The following sections detail how to configure an RWA environment to use TLS with FIPS-approved ciphers for RDG connections. The TechNet article *Remote Desktop Services* [v] includes details about basic setup procedures for RWA as well as other RD components. There are several options that need to be modified during installation to configure the web access server for DoD PKI. The cert requested earlier in the document should already be installed on the machine before beginning these steps. Reference Appendix B for steps to configure Microsoft RemoteApp.

1) Refer to the Technet Article titled: *Install the Remote Desktop Web Access Role Service* [vi] to add the Required Web Access Role Services .

   NOTE: Under Role Services during the selection step check the box for Client Certificate Authentication Mapping.

2) Once the Role Services are installed, open **IIS manager** and navigate to **Default Web Site**. Navigate to **Bindings** and set **https binding** to the certificate you created earlier.

3) Under **SSL Settings** still under Default Web Site, set SSL to **Require SSL** and **Require Client Certificates**. Be aware that once this is set you will require a smart card to log in to the website.

4) Select the server under the IIS manager list, just above Application Pools. Under the **Authentication** section in IIS settings in the middle pane, enable **Active Directory Client Certificate Authentication**.

5) Log in to the **Active Directory Domain Controller** and add any smart card enabled accounts to the **TS Web Access Administrators group** for accounts that require administrative rights on the RWA server.

6) Log on to the **RD Web Access Server** as an administrative account using username and password and configure **Remote App and Remote Desktop Sources.**

7) For any **RD Session Host** that requires use as a Remote App source, add the **RWA server** to the **TS Web Access Computers group** as well as other configuration for **Remote Apps**. More info can be found in Appendix C.

8) For security purposes, the **Remote Desktop Connection** dialogue should be **disabled** for non-administrative users.

   NOTE: Users will still be able to Remote Desktop to desktops published for them, but not to any ip address/FQDN. Disable this option by navigating to Default Web Site->RDWeb->Pages in IIS manager and then selecting Application settings under ASP.net settings. Change the Show Desktops option to false.

NOTE: Additional configuration for the RDWeb Access website includes the option to route non-local traffic through an RD Gateway server. These options are explained in the Microsoft Technet article "*Configure Remote Desktop Web Connection Behavior*"[vii]).

9) By default the only authentication method available for RWA accounts is **Forms** which only allows the use of username/password. However, Microsoft provides a mechanism to allow Smartcard usage by utilizing Windows authentication. This option can be enabled by modifying the **Web.config** configuration file located at **%WinDir%\Web\RDWeb\Pages**

10) Inside the web.config file there is a section that by default has:

```
<!--
        To turn on Windows Authentication:
          - uncomment <authentication mode="Windows"/> section
          - and comment out:
          1) <authentication mode="Forms"> section.
          2) <modules> and <security> sections in <system.webServer> section at the end of the file.
 3) Optional: Windows Authentication will work in https.  However, to turn off https, disable 'Require SSL'
for both RDWeb and RDWeb/Pages VDIR.
            Launch IIS Manager UI, click on RDWeb VDIR, double click on SSL Settings in the middle pane,
uncheck 'Require SSL' and
            click Apply in the top right in the right pane.  Repeat the steps for RDWeb/Pages VDIR.
    -->
    <!--
    <authentication mode="Windows"/>
    -->
    <authentication mode="Forms">
      <forms loginUrl="default.aspx" name="TSWAAuthHttpOnlyCookie" protection="All"
requireSSL="true" />
    </authentication>

    <webParts>
      <personalization defaultProvider="TSPortalProvider">
       <providers>
        <add name="TSPortalProvider"
type="Microsoft.TerminalServices.Publishing.Portal.TSPortalProvider"/>
       </providers>
       <authorization>
        <allow users="*" verbs="enterSharedScope">
        </allow>
       </authorization>
      </personalization>
    </webParts>
  </system.web>

   <system.webServer>
    <modules runAllManagedModulesForAllRequests="true">
  <remove name="FormsAuthentication" />
  <add name="RDWAFormsAuthenticationModule"
type="Microsoft.TerminalServices.Publishing.Portal.FormAuthentication.TSFormsAuthentication" />
 </modules>
 <security>
```

```
      <authentication>
        <windowsAuthentication enabled="false" />
        <anonymousAuthentication enabled="true" />
      </authentication>
    </security>
    <httpRedirect enabled="false" />
  </system.webServer>
```

11) Modify it as follows:

```
<!--
        To turn on Windows Authentication:
          - uncomment <authentication mode="Windows"/> section
          - and comment out:
          1) <authentication mode="Forms"> section.
          2) <modules> and <security> sections in <system.webServer> section at the end of the file.
          3) Optional: Windows Authentication will work in https.  However, to turn off https, disable 'Require
             SSL' for both RDWeb and RDWeb/Pages VDIR. Launch IIS Manager UI, click on RDWeb VDIR,
             double click on SSL Settings in the middle pane, uncheck 'Require SSL' and  click Apply in the top
             right in the right pane.  Repeat the steps for RDWeb/Pages VDIR.
    -->


    <authentication mode="Windows"/>
<!--
    <authentication mode="Forms">
      <forms loginUrl="default.aspx" name="TSWAAuthHttpOnlyCookie" protection="All" requireSSL="true"
/>
    </authentication>
    -->

    <webParts>
      <personalization defaultProvider="TSPortalProvider">
        <providers>
          <add name="TSPortalProvider"
type="Microsoft.TerminalServices.Publishing.Portal.TSPortalProvider"/>
        </providers>
        <authorization>
          <allow users="*" verbs="enterSharedScope">
          </allow>
        </authorization>
      </personalization>
    </webParts>
  </system.web>

  <system.webServer>
<!--
    <modules runAllManagedModulesForAllRequests="true">
      <remove name="FormsAuthentication" />
      <add name="RDWAFormsAuthenticationModule"
type="Microsoft.TerminalServices.Publishing.Portal.FormAuthentication.TSFormsAuthentication" />
    </modules>

    <security>
      <authentication>
        <windowsAuthentication enabled="false" />
```

```
        <anonymousAuthentication enabled="true" />
      </authentication>
    </security>
-->
    <httpRedirect enabled="false" />
  </system.webServer>
```

12) Restart the **web server** from the IIS manager panel. This should enable the RWA server correctly with Smart Card Enabled logon.

Appendix A: Supplemental Information

Web Site

Please visit the URL below for additional information.
http://iase.disa.mil/pki-pke

Technical Support

Contact technical support at the email address below.
dodpke@mail.mil

Acronyms

CN	Common Name
CSR	Certificate Signing Request
DoD	Department of Defense
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
MMC	Microsoft Management Console
PKE	Public Key Enablement
PKI	Public Key Infrastructure
RAC	Remote Application Connection
RD	Remote Desktop
RDC	Remote Desktop Connection
RDS	Remote Desktop Services
RDSH	Remote Desktop Session Host
RDG	Remote Desktop Gateway
RWA	Remote Desktop Web Access
SSL	Secure Socket Layer
TLS	Transport Layer Security

Appendix B: Remote Application Configuration

1) Please refer to *Configuring Microsoft Remote Desktop Services for Authentication using DoD PKI*[viii] for instructions on configuring a Remote Desktop Session Host (RDSH).
2) Utilizing the Microsoft Technet Guide: *Installing and Configuring RemoteApp*[ix], configure the RDSH to support remote applications.
3) Make sure the RDSH's local **TS Web Access Computers** group is populated with the **computer account** for the **RD Web Access Server**.
4) Install any applications to be delivered through the Remote Application system on the RDSH.
5) From **Server manager** on the RDSH host, select **Remote App Manager**. From here, click **Add Remote App Programs** and add any applications that should be available to remote users.
6) If utilizing a remote desktop gateway, configure the remote desktop gateway options in the Remote App configuration panel. For more information, reference the *Configuring Remote Desktop Gateway Authentication Using DoD PKI*[x] located at

   NOTE: Remote desktop gateway will only be active for non-local connections.
7) Configure the **RD Session Host server settings** in the RD Session Host Server Setting dialogue. Check the **Remote Desktop Access** box to allow the RDSH to present session-based desktops to users over the RWA server.

   NOTE: Do not set the Access to unlisted programs option to allow. This will grant users the ability to execute any program on the host remotely.
8) Set the **RDSH hostname** and **RDP port** to use if they are not set. This RDSH hostname might be the DNS name of a farm if utilizing a farm of multiple RDSH hosts.

Appendix C: References

The resources below were used to help develop the content of this document.

---

[i]"Remote Desktop Services", Microsoft TechNet, http://technet.microsoft.com/en-us/library/cc770412.aspx (2011).
ii "Configuring Microsoft Remote Desktop Services for Authentication using the DoD PKI", http://iase.disa.mil/pki-pke
iii "How to Create a Group in Active Directory", Microsoft TechNet, http://msdn.microsoft.com/en-us/library/aa545347%28v=cs.70%29.aspx
iv "Obtaining a PKI Certificate for a DoD Server", http://iase.disa.mil/pki-pke
v "Remote Desktop Services", http://technet.microsoft.com/en-us/library/cc772214.aspx
vi "Install the Remote Desktop Web Access Role Service", http://technet.microsoft.com/en-us/library/cc772214.aspx
vii "Configure Remote Desktop Web Connection Behavior", http://technet.microsoft.com/en-us/library/cc731465.aspx
viii Configuring Microsoft Remote Desktop Services for Authentication using the DoD PKI", http://iase.disa.mil/pki-pke
ix "Installing and Configuring RemoteApp", http://technet.microsoft.com/en-us/library/dd772730%28v=ws.10%29.aspx
x "Configuring Remote Desktop Gateway Authentication Using DoD PKI", http://iase.disa.mil/pki-pke