

Centrify Infrastructure Services

Smart Card Configuration Guide

October 2018 (release 18.11)

Centrify Corporation





Legal Notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrifly Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrifly Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrifly Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrifly Corporation may make improvements in or changes to the software described in this document at any time.

© **2004-2018 Centrifly Corporation. All rights reserved.** Portions of Centrifly software are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrifly, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrifly for Mobile, Centrifly for SaaS, DirectManage, Centrifly Express, DirectManage Express, Centrifly Suite, Centrifly User Suite, Centrifly Identity Service, Centrifly Privilege Service and Centrifly Server Suite are registered trademarks of Centrifly Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrifly software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,442,962 and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.



Contents

What is Centrify Express for Smart Card?	2
Installing Centrify Express for Smart Card	3
How to install Centrify Express for Smart Card	3
Loading DOD intermediate certificates into the keychain	5
Using the Centrify Express for Smart Card utility	7
Configuring web browsers and mail clients	9
Using Microsoft Outlook 2011 for signed and encrypted mail	9
Using Safari to access protected web sites	11
Using Chrome to access protected web sites	11
Using Firefox to access protected web sites	12
Troubleshooting tips and other topics	13
Downloading certificates from the DoD PKI Management site	15
Validating certificate trusts	16
Checking the certificate revocation list	19
Checking the user principal on the card	21
Removing Centrify Express for Smart Card	23



What is Centrify Express for Smart Card?

Centrify Express for Smart Card enables access to certificate-protected web sites using a smart card. You can download Centrify Express for Smart Card for free from the Centrify web site. It enables you to use a properly provisioned and supported smart card to store credentials and certificates that allow you to access protected web sites and mail servers from Mac OS X computers.

Anyone with a registered Centrify account can download and install Centrify Express for Smart Card.

This guide describes how to install, configure, and uninstall Centrify Express for Smart Card.



Installing Centrify Express for Smart Card

Before installing, you should verify that you have supported hardware and software and the information you need to complete the installation.

To successfully install Centrify Express for Smart Card, check that you have the following:

- An Apple Macintosh computer running OS X 10.6.x or higher with an Intel processor. To check the operating system version and processor, choose the Apple menu, then click **About This Mac**.
- A valid and properly provisioned Department of Defense Common Access Card (CAC), CACNG, or Personal Identity Verification (PIV) card.
- A supported smart card reader with appropriate firmware connected to the Macintosh.
- Administrative access to the computer you are updating.

If you have everything you need, continue to [How to install Centrify Express for Smart Card](#).

How to install Centrify Express for Smart Card

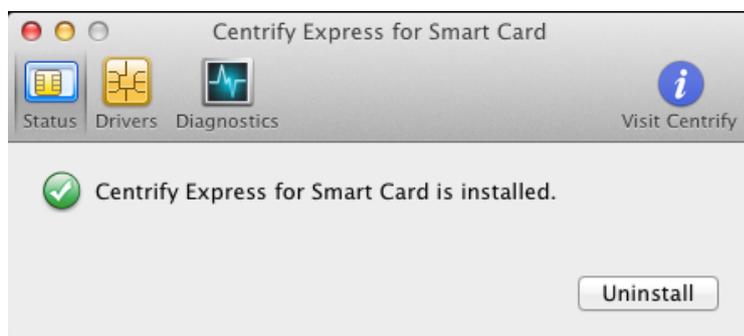
Centrify Express for Smart Card is packaged for distribution in Apple Disk Image (.pkg) files. There are separate Disk Image files for different Mac OS X architecture (Intel and PowerPC) and different operating system versions. You can download the appropriate Disk Image file for your environment from the Centrify web site. You can then open the Disk Image and run the Centrify Express for Smart Card installer. The installer provides an intuitive interface that guides you through the rest of the setup process.



To install Centrify Express for Smart Card on a Mac OS X computer:

1. Power on the Mac OS X computer and log in with the local administrator account.
2. Double-click the .pkg file to extract the contents of the file. For example:
`Express for Smart Card-release-mac10.6.pkg`
3. Double-click `centrify Express for Smart Card.pkg` to start the installer.
4. Review the information on the Welcome page, then click **Continue**.
5. Review, print, or save the terms of the license agreement and click **Continue**, then click **Agree** to agree to the terms of the license agreement.
6. If there are no conflicts, click **Continue**.
7. Select a volume for installing Centrify Express for Smart Card, then click **Continue**.
8. Click **Install** to begin installing Centrify Express for Smart Card.
9. Type the user name and password, then click **OK**.
10. Click **Close** after you see confirmation that files have been successfully installed.

After you confirm the installation, the Centrify Express for Smart Card utility starts and displays the current status. For example:



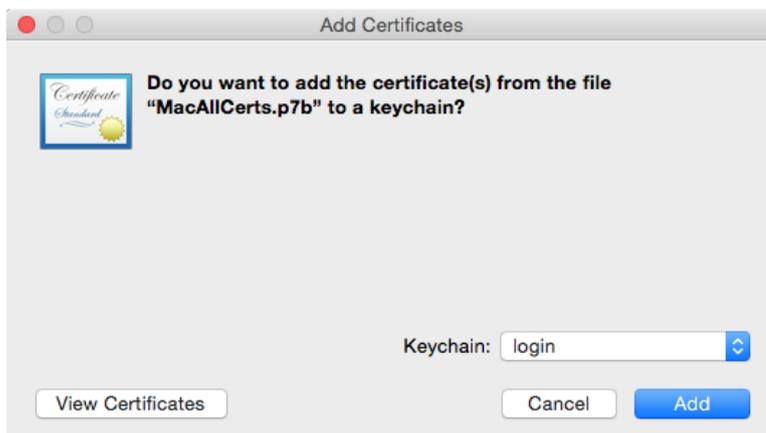
Loading DOD intermediate certificates into the keychain

You need to download the DOD intermediate certificates and load them into the keychain.

To load these intermediate certificates and make them available:

1. Download the DOD intermediate certificates from <https://militarycac.com/maccerts/MacAllCerts.p7b>, then open the MacAllCerts.p7b file.

The Add Certificates window appears.

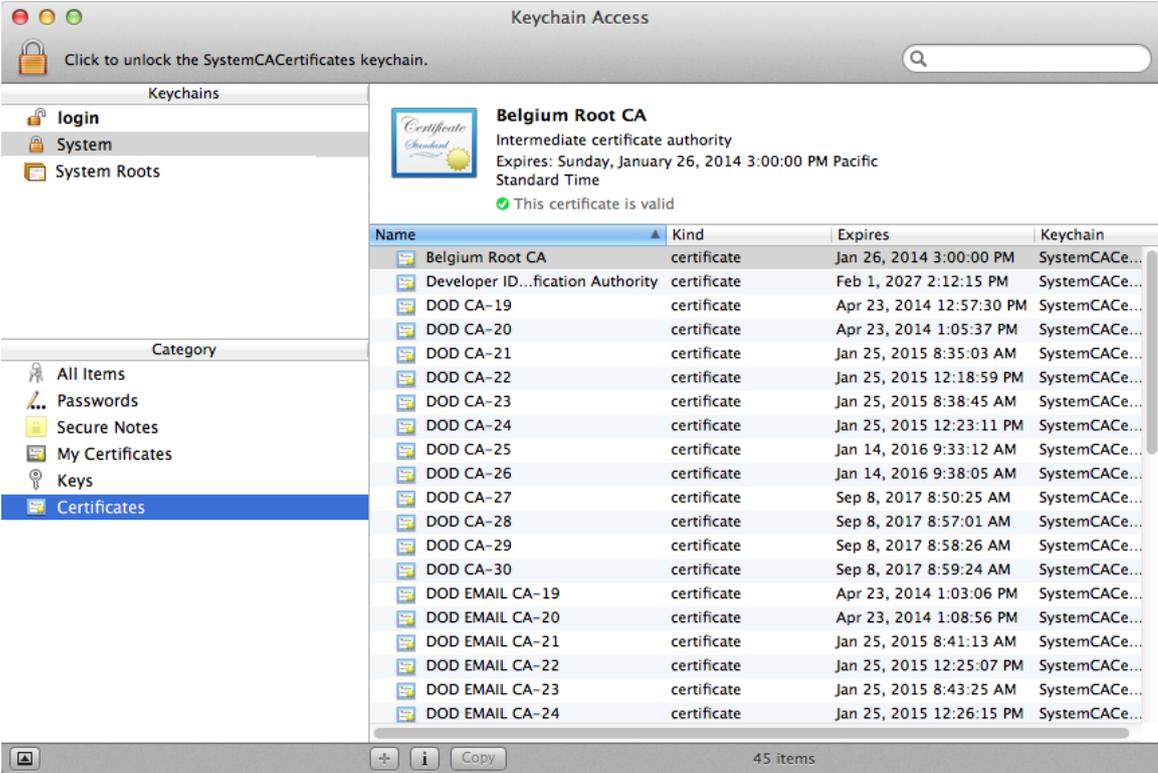


2. In the Keychain dropdown menu, select System if you have admin privileges, or login if you do not have admin privileges, then click **Add**. The DOD intermediate certificates are add to the selected keychain.
3. Open Applications, then open the Utilities folder and double-click **Keychain Access**.
4. Select the keychain that you added the certificates to, then select the



Certificates category to verify that the certificates were successfully added.

For example:

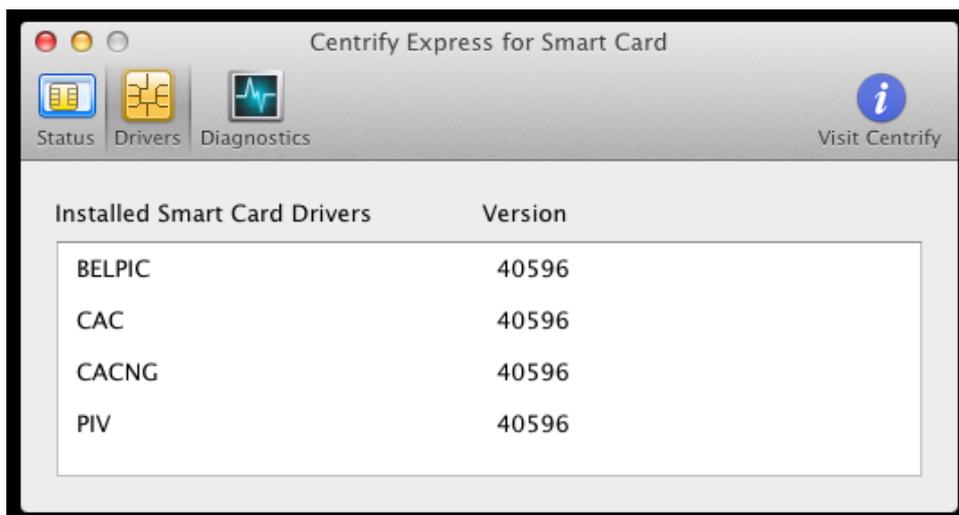


Using the Centrifly Express for Smart Card utility

You can use the Centrifly Express for Smart Card utility to check the current status of Centrifly Express for Smart Card, check the list of drivers installed on your computer, or run diagnostics on your computer.

To open and use the Centrifly Express for Smart Card utility:

1. Insert the card into the smart card reader.
2. From the Finder, open Applications, Utilities, then open the Centrifly folder and double-click **Centrifly Express for Smart Card**. The current status is displayed by default.
3. Click **Drivers** to view the list of drivers installed on your computer in the /System/Library/Security/token directory. For example:



The drivers are also known as tokend drivers



4. Click **Diagnostics** to examine the certificates on your card.

After you click **Diagnostics**, follow the instructions displayed to get a listing of all certificates on the card. You can then click **Save to Desktop** to save the output to disk.





Configuring web browsers and mail clients

The topics in this section provide tips for configuring different web browsers and mail clients to work with Centrify Express for Smart Card on Mac OS X computers. The following topics are covered:

- Using Microsoft Outlook 2011 for signed and encrypted mail
- Using Safari to access protected web sites
- Using Firefox to access protected web sites
- Using Chrome to access protected web sites

Using Microsoft Outlook 2011 for signed and encrypted mail

To use Outlook for Mac 2011 to send and receive encrypted email, you must have a valid digital certificate. After you have downloaded and imported the appropriate intermediate certificates for your smart card, you can configure Microsoft Outlook 2011 to sign email with your certificate and send encrypted mail.

To send a digitally signed message:

1. Log on the Mac and open Microsoft Outlook.
2. On the Tools menu, click **Accounts**.
3. Select the account from which you want to send a digitally signed message.



4. Click **Advanced**, then click the **Security** tab.
5. Under **Digital signing**, click the **Certificate** menu, then select the certificate that you want to use.
6. Click **Include my certificates in signed messages** check box if all of your recipients have email that supports digital signing and encryption.
7. Click **OK**, then close the Accounts dialog box.
8. When composing email messages, click the Options tab, click Security, then click **Digitally Sign Message**.

To send an encrypted message:

1. Log on the Mac and open Microsoft Outlook.
2. On the Tools menu, click **Accounts**.
3. Select the account from which you want to send an encrypted message.
4. Click **Advanced**, then click the **Security** tab.
5. Under **Encryption**, click the **Certificate** menu, then select the certificate that you want to use.
6. Click **OK**, then close the Accounts dialog box.
7. When composing email messages, click the Options tab, click Security, then click **Encrypt Message**.

To send an encrypted message, you must have the public certificate of the user to whom you are sending the mail message. If the recipient is a contact in your address book, this certificate is typically available on the Certificates tab in Outlook. If you do not have the certificate, Outlook will not create an encrypted mail message. However, if the name of the person matches a contact in your address book, Outlook encrypts the message before sending it.

For more information about managing digital certificates and sending and receiving encrypted email in Outlook for Mac 2011, see the [Microsoft topic How users manage digital certificates in Outlook for Mac 2011](#). *How users manage digital certificates in Outlook for Mac 2011*.



Using Safari to access protected web sites

If you want to use a smart card to access Department of Defense (DOD) web sites using Safari as your web browser, you should configure the certificate to use for authentication.

To configure a certificate for the smart card:

1. If you have Safari open, choose the Safari menu, then click **Quit Safari**.
2. Insert your smart card in the reader, then navigate to Utilities and open **Keychain Access**.
3. Select the provisioned CAC keychain for your smart card.
4. From Category list, select **My Certificates**.
5. Right-click the certificate you want to use to authenticate your identity. In most cases, you should select the **Authentication Private Key** certificate or the **Digital Signature Private Key** certificate, depending on the web site you want to view.
6. Select **New Identity Preference**.
7. Type the complete URL for the web site you want to access, then click **Add**. For example:

```
https://akocac.us.army.mil/
```

```
https://www.jtfgno.mil/
```

Using Chrome to access protected web sites

If you want to use a smart card to access Department of Defense (DOD) web sites using Google Chrome as your web browser, you should configure the certificate to use for authentication.

To configure a certificate for the smart card:

1. If you have Chrome open, choose the Chrome menu, then click **Quit Google Chrome**.



2. Insert your smart card in the reader, then navigate to Utilities and open **Keychain Access**.
3. Select the provisioned CAC keychain for your smart card.
4. From Category list, select **My Certificates**.
5. Right-click the certificate you want to use to authenticate your identity. In most cases, you should select the **Authentication Private Key** certificate or the **Digital Signature Private Key** certificate, depending on the web site you want to view.
6. Select **New Identity Preference**.
7. Type the complete URL for the web site you want to access, then click **Add**. For example:

`https://akocac.us.army.mil/`

`https://www.jtfgno.mil/`

Using Firefox to access protected web sites

Firefox is not supported for smart card to access Department of Defense (DOD) web sites. If you want to use a smart card to access Department of Defense (DOD) web sites using Mozilla Firefox as your web browser, you must download and install a package from www.militarycac.com and modify the configuration of the Firefox browser. For more information, see http://www.militarycac.com/MacVideos.htm#Firefox_6.



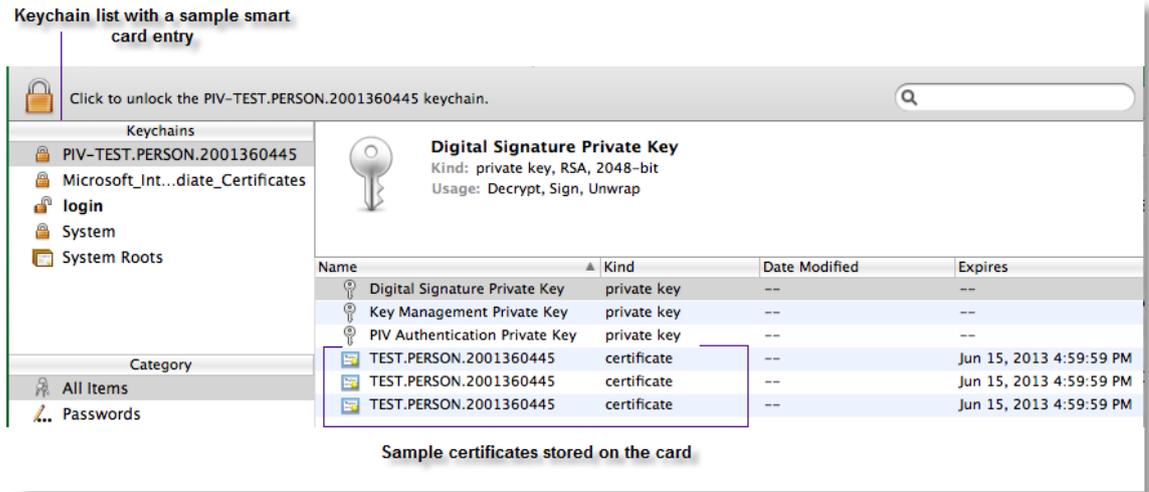
Troubleshooting tips and other topics

Before you can access protected web sites or send encrypted email, you should check the certificates on your smart to determine whether they are signed by a trusted certificate authority and ready to use. In most cases, you will need to determine the appropriate issuing authority, then import one or more intermediate certificates manually to make the existing certificates trusted.

To check the issuing authority and whether a certificate is trusted:

1. Insert your card into the smart card reader.
2. From the Finder, open Applications, then open the Utilities folder and double-click **Keychain Access**.
3. In the list of Keychains on the left, select the keychain entry for the smart card.

The keychain entry is typically labeled as CAC or PIV with a unique number and is usually listed first. For example:



You should see one to four certificates listed, depending on the type of card. You can get more information about each certificate by clicking the triangle next to the certificate name. The common certificate types are:

- PIV Authentication
 - Digital Signature
 - Key Management
 - Email Signing
 - Email Encryption
4. Select the first certificate, and check the Issued by information to verify the certificate has been issued by a legitimate Certificate Authority and check the Expires field to determine when the certificate on the card expires.

The top right panel indicates whether the certificate is valid. For example:

✔ This certificate is valid

If the certificate is valid, no further action is necessary and you can check additional certificates stored in the keychain.

If the certificate on your smart card is not signed by a trusted authority, it displays a message similar to this in the Keychain Access application:

✘ This certificate was signed by an unknown authority

5. Identify the issuing Certificate Authority so that you can download the appropriate intermediate root certificate to enable the certificate on your smart card to be trusted.



For example, if you have certificates issued by DOD CA-25 and DOD EMAIL CA-25 certificates, display you must download the DOD CA-25 and DOD EMAIL CA-25 intermediate certificate files for the certificates on the card to be trusted.

6. Double-click the certificate or click **Get Info** to display details about the certificate. For example:

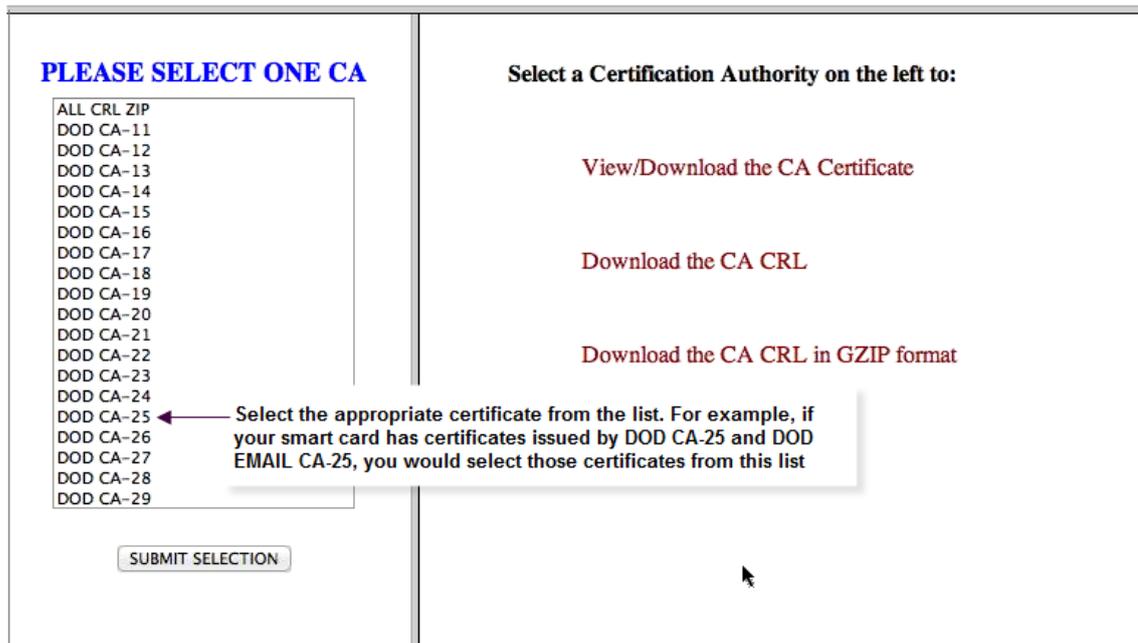


Downloading certificates from the DoD PKI Management site

As an alternative to downloading intermediate certificates from within Keychain Access, if you have access to the Department of Defense PKI Management site, you can navigate to the site and download the appropriate intermediate certificates from that site.

To download the intermediate root certificates from the PKI Management site:

1. Go to the following URL in a web browser:
<https://crl.gds.disa.mil/>
2. Scroll to locate the certificate for the certificate authorities that issued the certificates on your smart card. For example:



3. Select the appropriate certificate, then click **View/Download the CA Certificate**.

Depending on the browser you use and preference settings, you may be prompted to Open or Save the file or have a warning message displayed.

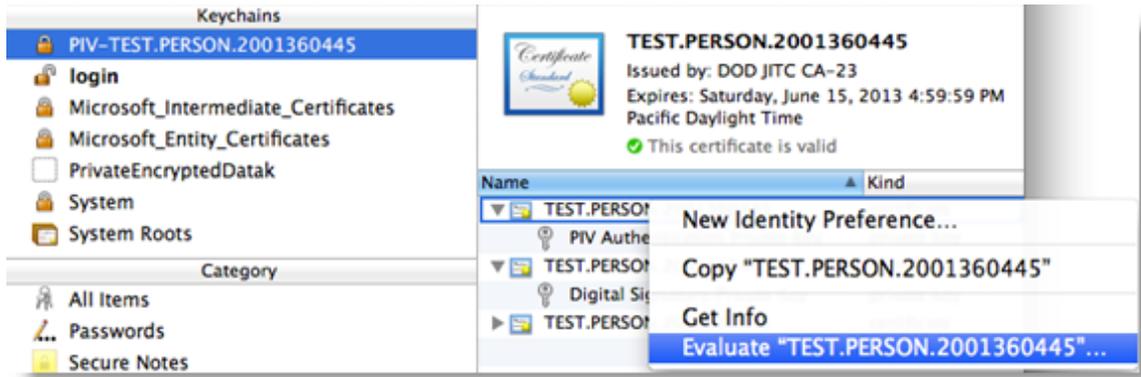
4. Click **Save File** and select the Downloads folder or another location, then click **OK**.

Validating certificate trusts

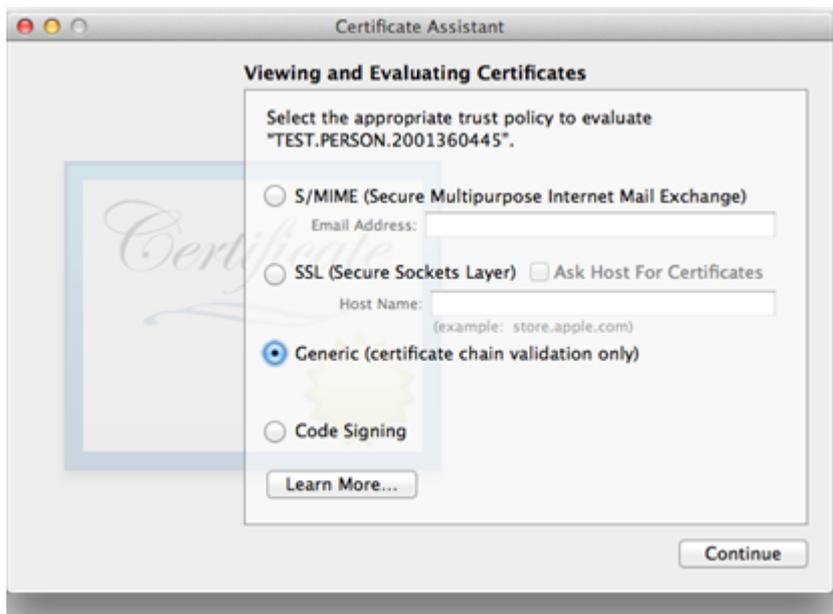
After you have imported the appropriate root and intermediate certificates, you can validate the trust chain.

To verify your smart card certificates are trusted:

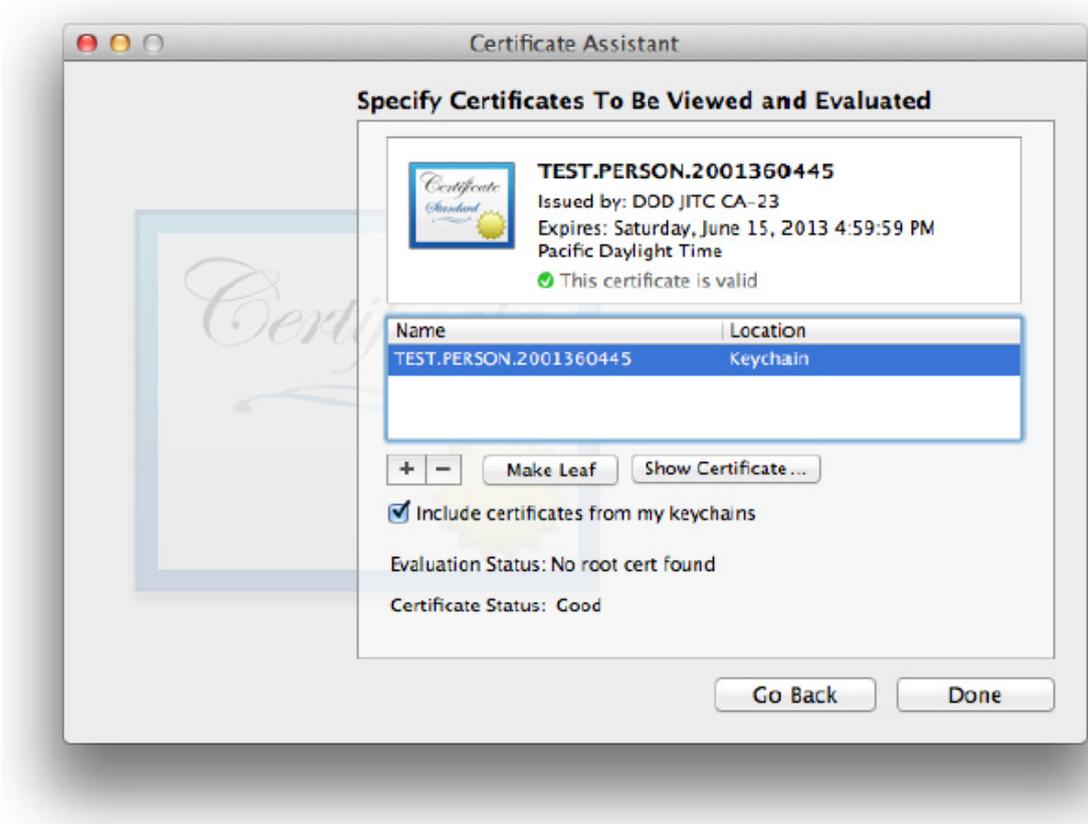
1. Insert your card into the smart card reader.
2. From the Finder, open Applications, then open the Utilities folder and double-click **Keychain Access**.
3. Select the keychain entry for the smart card.
4. Select the certificate to test, right-click, then click **Evaluate "certificate_name"**.



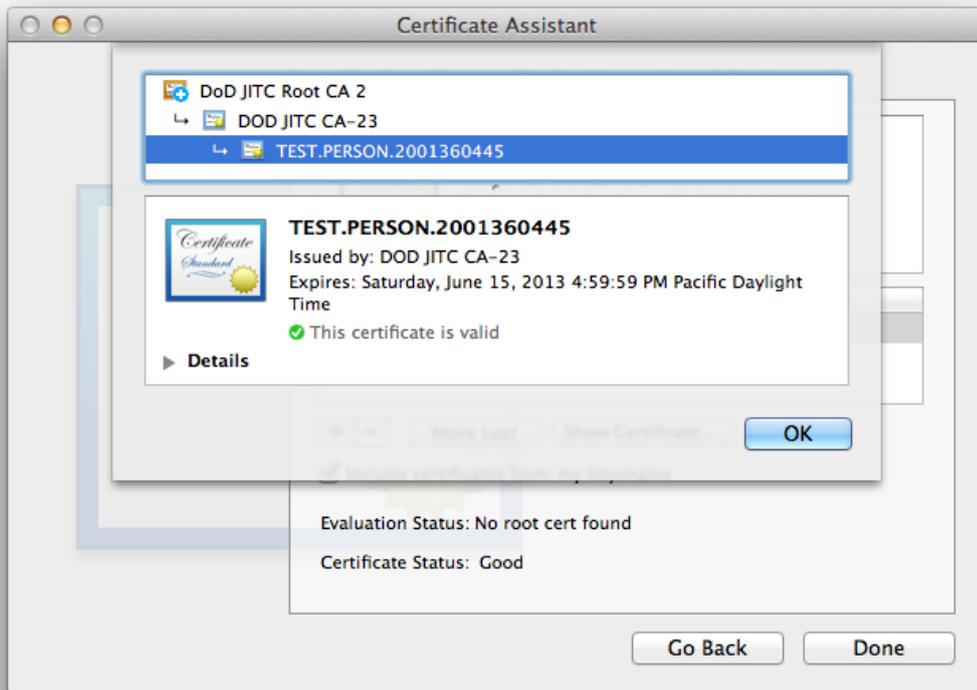
5. Select the **Generic (certificate chain validation only)** option, then click **Continue**.



6. Double-click the certificate that is displayed to see if all the certificates in the chain of trust are properly installed.



7. If the certificates in the keychain are all valid, you can click **OK**, then click **Done**. For example:



If there are any certificates that are not signed by a trusted authority, you must import the appropriate intermediate certificates to allow your smart card certificates to be trusted.

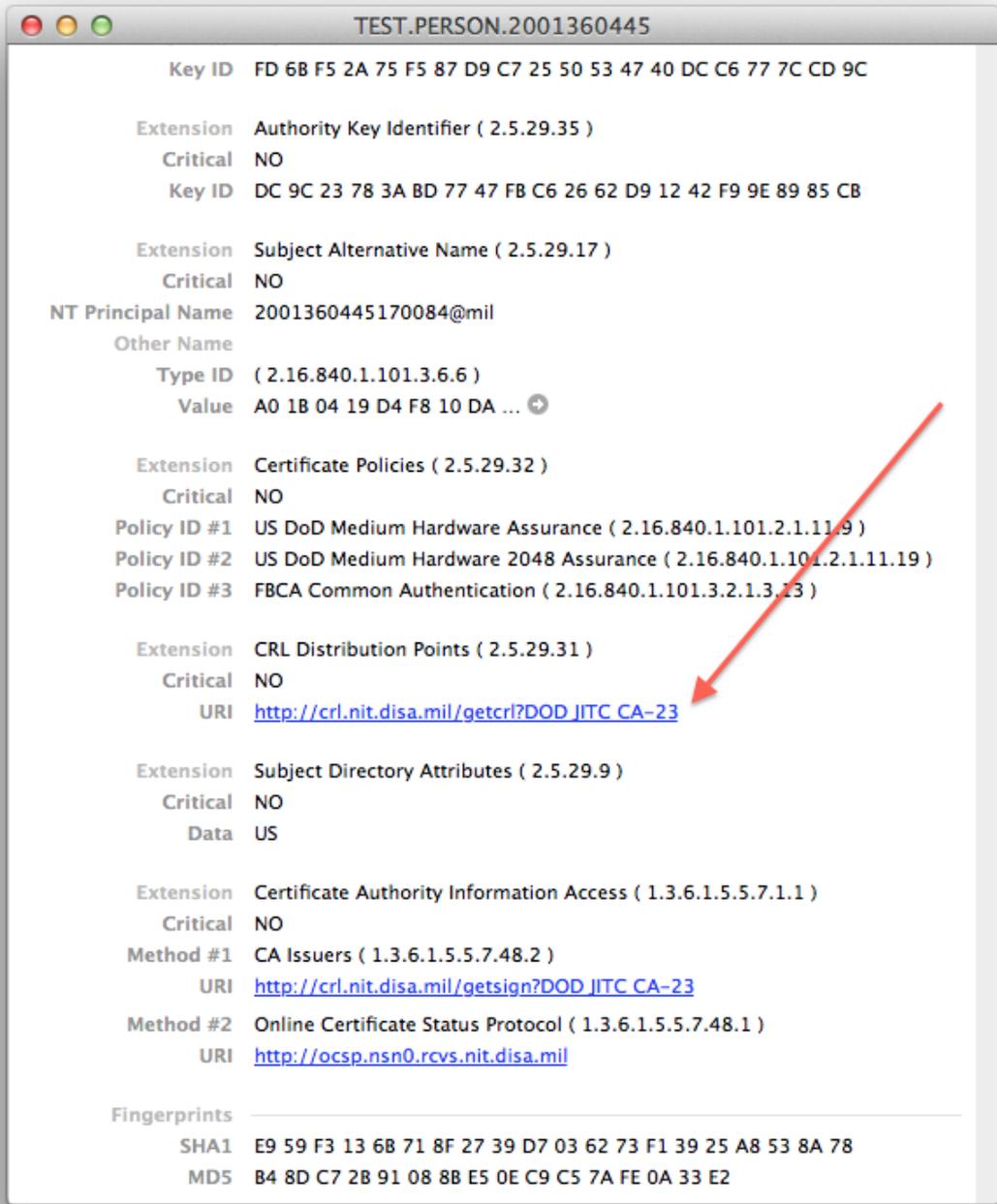
Checking the certificate revocation list

A Certificate Revocation List (CRL) is a URL that lists all certificates that have been revoked. If you are troubleshooting problems with your smart card, you should check whether your CRL links are valid and test the CRL links for all of your certificates. At a minimum, you should verify that the CRL for the authentication certificate is valid.

To check your certificate revocation list links:

1. Insert your card into the smart card reader.
2. Open **Keychain Access** and double-click the certificate to check to display its details.

- 3. Scroll down the certificate details to locate the Extension for CRL Distribution Point attribute.



- 4. Click the URI for the CRL Distribution Point.

If the connection is successful, the web browser should display a page, but you may not be able to read the contents. If you get any type of browser error, such as web site not found or file not found, then the CRL distribution point is invalid.



If the CRL distribution point is not valid, contact the card issuer for information.

Checking the user principal on the card

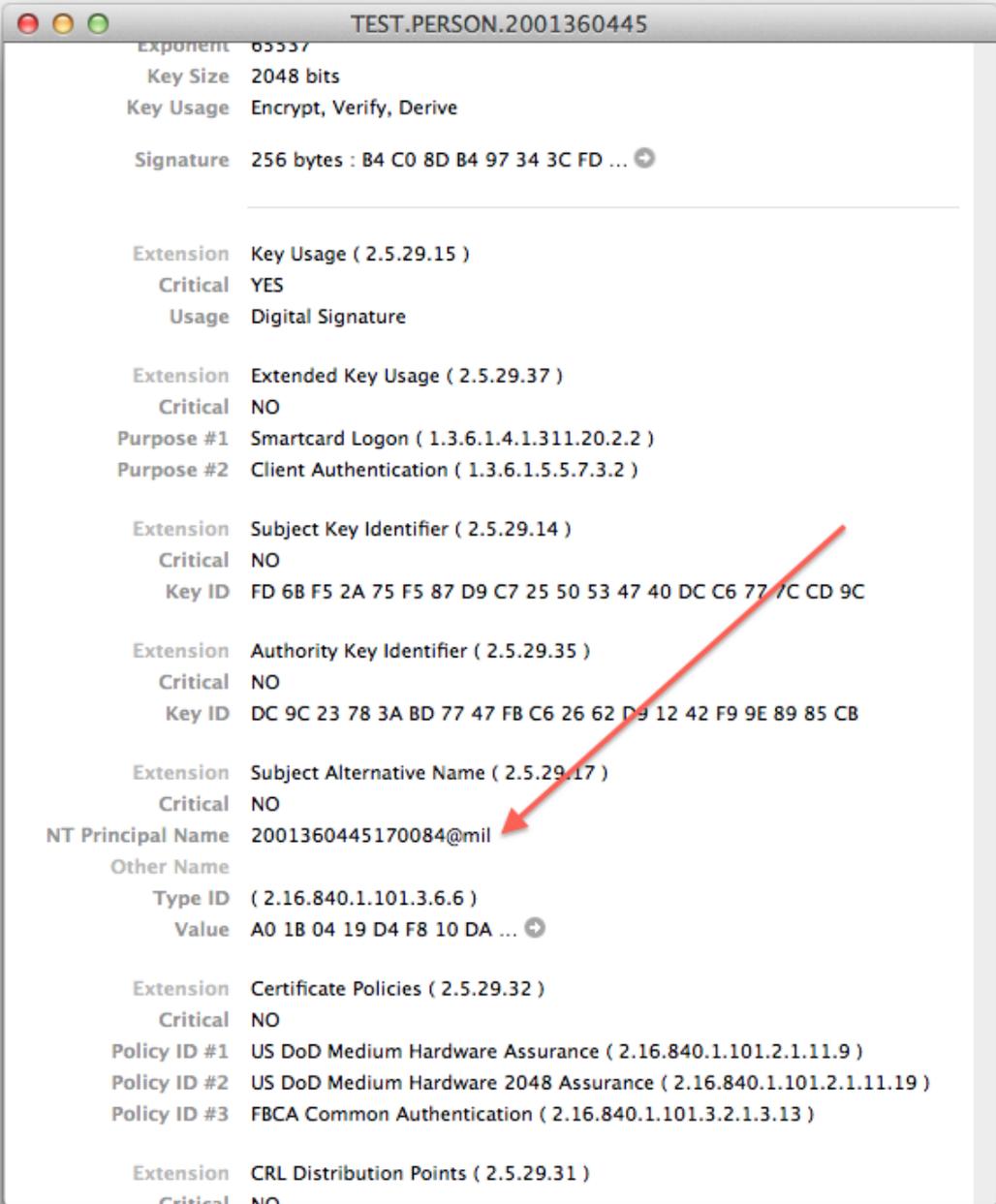
If you are issued a card without a photographic identifier, you may want to check the user account principal name to verify that the card is yours.

To check the user principal name on a card:

1. Insert your card into the smart card reader.
2. Open **Keychain Access** and double-click the certificate to display its details.
3. Scroll down the certificate details to locate the NT Principal Name



attribute.





Removing Centrify Express for Smart Card

To remove Centrify Express for Smart Card, open the Centrify Express for Smart Card program, then click **Uninstall**.

