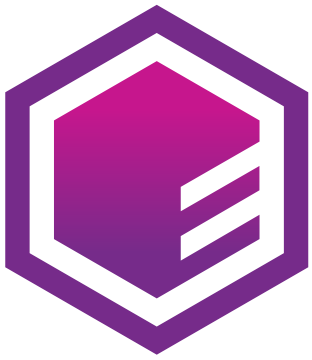


ENTRUST

REMOTE SIGNING SERVICE

DESKTOP VIRTUAL CARD

entrust.com

Document Reference:RSService_DVC

Product Release:2.2.0

Contents

1 Preface

Welcome to the *Entrust Desktop Virtual Card* manual.

1.1 About this Manual

This document explains how to install and configure *Entrust Desktop Virtual Card*.

1.2 Contents

This document is structured in the following chapters:

- The Introduction describes the main aspects of *Entrust Desktop Virtual Card*.
- System Requirements describes the system requirements for installing *Entrust Desktop Virtual Card*.
- Installation and Uninstallation explains how to install and uninstall *Entrust Desktop Virtual Card*.
- Opening the Application explains how to start and use *Entrust Desktop Virtual Card*.
- Application Integrations describes the main uses of *Entrust Desktop Virtual Card*.

1.3 Referenced Documents

Reference is made to the following documents in this manual.

Reference	***Document***
[ORA_PROVIDERS]	Java™ Cryptography Architecture Sun Providers Documentation docs.oracle.com/javase/6/docs/technotes/guides/security/SunPoviders.html

2 Introduction

Entrust Desktop Virtual Card allows locally accessing your remote certificates managed by the *Entrust Remote Signing Service*. Applications running on your computer can use these certificates as if they were local.

Some of the *Entrust Desktop Virtual Card* advantages are the following:

2.1 Ease of Use

Signature operations are executed in the same way as for certificates managed locally by Windows. *Remote Signing Service* operations are totally transparent to you.

2.2 Process Centralization

Entrust Desktop Virtual Card centralizes all the processes related to the use of the certificates, such as those described below.

2.2.1 Certificate Management and Custody

The certificate life-cycle is centralized on the *Entrust Remote Signing Service*, which makes certificate management more straightforward and effective. The process for obtaining the certificates takes place in centralized applications using the Remote Signer Service User Portal.

Certificate custody takes place on the *Entrust Remote Signing Service* with the highest level of security. This provides a more secure cryptographic infrastructure than offered by a certificate installed directly in your computer.

2.2.2 Authentication and Authorization

So that you can access the certificates, the application provides the authentication and authorization methods provided by the *Entrust Remote Signing Service*. This way, you can authenticate in a secure manner and have exclusive control over your certificates, regardless of from where you access them.

2.2.3 Auditing

Generating digital signatures on the server allows registering all users' actions centrally. This makes it easier to audit when you use your certificate using the Remote Signing Service User Portal.

3 System Requirements

This chapter outlines the system requirements for installing and executing *Entrust Desktop Virtual Card*.

3.1 Operating System

Entrust Desktop Virtual Card can be executed on the following versions of the Windows operating system.

3.1.1 Windows 10

Windows 10 64-bit systems.

3.2 Dependencies

Entrust Desktop Virtual Card requires the following dependencies.

3.2.1 .NET Framework

Version 4.6 or higher is required. Keep in mind that it comes with the standard Windows 10 installation.

3.2.2 Microsoft Edge WebView2

The installation of the Microsoft Edge Webview2 Runtime is required. It is recommended to use the latest available update.

If the *Entrust Desktop Virtual Card* installer detects this requirement is not present in the system, it will be downloaded and installed.

3.3 Proxy

Entrust Desktop Virtual Card supports Windows manual proxy setup for connections against the *Entrust Remote Signing Service*.

3.4 Browsers

The keys and certificates of *Entrust Desktop Virtual Card* can be used in the following browsers.

3.4.1 Microsoft Edge

Latest versions of Microsoft Edge.

3.4.2 Google Chrome

Latest versions of 32-bit and 64-bit Google Chrome.

3.4.3 Mozilla Firefox

Latest versions of 32-bit and 64-bit Mozilla Firefox.

3.5 Applications

As well as the above browsers, the following applications can use the keys and certificates of *Entrust Desktop Virtual Card*.

3.5.1 Microsoft Office

32-bit and 64-bit versions from 2007.

3.5.2 Adobe

Versions X, XI and Adobe Reader and Adobe Acrobat DC.

3.6 Integration

Entrust Desktop Virtual Card can be integrated with the following environments.

3.6.1 OpenSC

The OpenSC library supports integrating *Entrust Desktop Virtual Card* with smart cards.

3.6.2 Java SE

Entrust Desktop Virtual Card can be integrated with applications developed with 32-bit and 64-bit Java SE (version 6 or later). For this integration, you need the following providers:

- Sun PKCS #11 Provider
- Sun MSCAPI Provider

4 Installation and uninstallation

This chapter describes the modes supported for installing the *Entrust Desktop Virtual Card* application.

4.1 Installation

4.1.1 Interactive Installation

In this case, you install the application interactively in a wizard.

To install in interactive mode:

1. Log-in in the computer with administrator privileges.
2. Execute the `vc.msi` application installer.
3. In case you do not have the Microsoft Edge WebView2 dependency installed in your system, the installer will proceed with its installation.
4. The installer's wizard will prompt you to accept the license agreement. You must select *I accept the terms in the License Agreement* to continue.
5. The installer's wizard will offer you to continue with the default installation (click **Install** button) or the advanced one (click **Advanced** button).
   a. Default installation will install the application in the destination folder `<ProgramFiles>\Entrust\Desktop Virtual Card` and it will install the **Run Application On Startup** feature (Run automatically the application on Windows startup).
   b. Advanced installation will offer you to change the destination folder and to choose if you want to disable the **Run Application On Startup** feature (Run automatically the application on Windows startup).
6. The installer's wizard will offer you to reboot the computer before using the application if it detects any conflict during the installation.

4.1.2 Unattended Installation

In this case, you install the application in unattended mode, i.e., without a wizard.

To install in unattended mode:

1. Log-in in the computer with administrative privileges.
2. Run the following command line: `msiexec /i vc.msi /quiet [APPLICATIONFOLDER="<path>"] [INSTALLLEVEL="<level>"]`

The optional command `APPLICATIONFOLDER` installs the application in the `<path>` folder. When not used, `<ProgramFiles>\Entrust\Desktop Virtual Card` will be used.

The optional command `INSTALLLEVEL` installs the application with the **Run Application On Startup** feature (Run automatically the application on Windows startup) when defining `<level> 2` or without it (`<level> 1`).

4.1.3 Certificate Chain Installation

After installing the application and before using it, you must have in your computer both the root CA's certificate and the intermediate CA's certificates that form the certification path of the personal certificates you'll virtually have in your system through *Entrust Desktop Virtual Card* so that any application can use them properly. For example, some signing application will take advantage of this in order to include all the certificate chain in the signatures in order to simplify the verification process.

Entrust Desktop Virtual Card does not automatically install the certificate chain.

To install the certificate chain:

- Download the certificates at https://www.entrust.com/resources/certificate-solutions/getting-started-with-remote-signing-getting
- The root certificate from Entrust should be present in any updated trusted certificate store (ie., Windows, Adobe or Firefox). You can check it verifying if the downloaded one is already trusted. Otherwise, you should follow the application instructions for importing it.
- The subordinate certificate from Entrust Remote Signing Service is not included in the list of trusted CAs. Follow each application instructions for importing it as an trusted intermediate CA. For example, in the case of Windows certificate store, open the file, select to import it and indicates the **Intermediate CAs** section for that.

4.2 Uninstallation

4.2.1 Interactive Uninstallation

To uninstall in interactive mode:

1. Log-in in the computer with administrative privileges.
2. In the Windows panel for removing programs, select **Entrust Desktop Virtual Card**.
3. Click **Remove** option.

4.2.2 Unattended Uninstallation

To uninstall in unattended mode:

1. Log-in in the computer with administrative privileges.
2. Execute the following command: `msiexec /x vc.msi /quiet`

5 Opening the Application

This chapter explains how start and use the *Entrust Desktop Virtual Card* application.

5.1 Status of the Application

5.1.1 Accessing the Certificates

For having your RSS certificates visible as certificates on your computer, *Entrust Desktop Virtual Card* must be up and running. In addition, you must have logged in to it.

5.1.2 Starting the Application

To start the application, in the Windows **Start** menu, click on the **Entrust Desktop Virtual Card** shortcut.

When the application is started, login is not automatically requested.

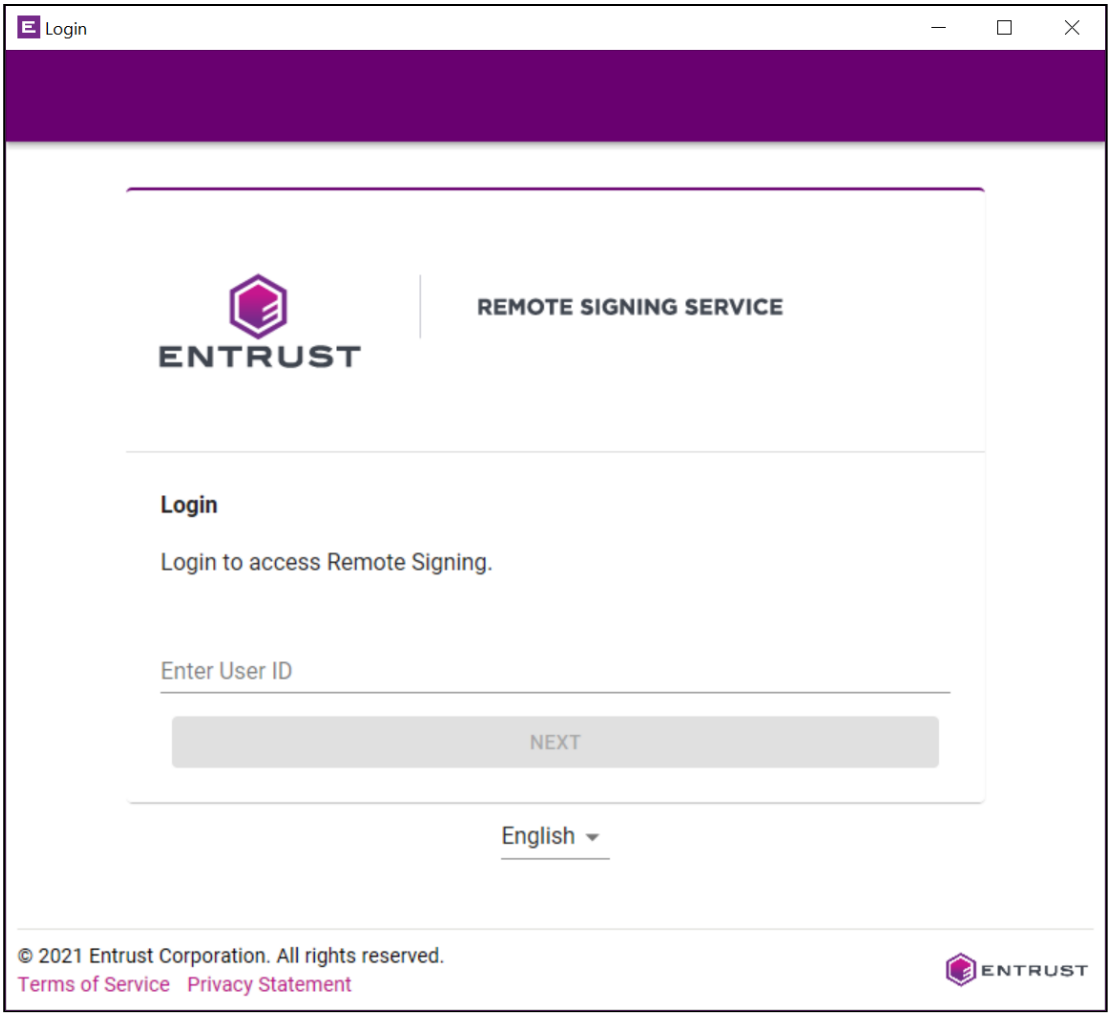
5.1.3 Exiting the Application

To close the *Entrust Desktop Virtual Card* application, right-click on the application icon in the taskbar and select the **Exit** command. This will close your ongoing session in *Entrust Desktop Virtual Card*, and the RSS certificates will become invisible to the computer.

5.2 Session Management

5.2.1 Logging in

To start a session, right-click on the application's icon in the taskbar and select the **Login** contextual command or double-click on the icon. This way, *Entrust Desktop Virtual Card* will display a login form according to the authentication options set for it by the Entrust Remote Signing Service. For example, the following one:



When *Entrust Desktop Virtual Card* is running, an icon is displayed in the Windows taskbar. As discussed below, both the appearance and the notifications of this icon allow easily checking the session status.

5.2.2 Status Icons

The taskbar icon may display the following elements, depending on the application's status.


The *Entrust Desktop Virtual Card* application is running but there is no ongoing user session. When you hover the cursor over the icon, the following message is shown:

```
Desktop Virtual Card: Session closed
```


There is an ongoing user session. When you hover the cursor over the icon, the following message is shown:

```
Desktop Virtual Card: <user>
```

-

Where:

- `<user>` your name.

5.2.3 Status Change Notifications

When you select the options described in this chapter, changes in the application's status are notified via the following alerts in the Windows taskbar.

5.2.3.1 *Logging in*

A session is being started with the credentials entered by you.

5.2.3.2 *Logged in*

The user session was successfully started.

5.2.3.3 *Logged out*

The session was ended.

5.2.4 Logging out

To log out, right-click on the icon in the taskbar (when a session is open) and select the **Log out** contextual command. After you log out, the certificates managed by *Entrust Desktop Virtual Card* are no longer available to your computer.

5.3 Using the Certificates

5.3.1 Accessing the Certificates

Once you log in to *Entrust Desktop Virtual Card*, all your remote certificates become available to applications using the Windows certificate store.

Alternatively, some desktop applications (e.g., the Firefox browser) may require use of the PKCS #11 interface for accessing the certificates. In this case, in addition to logging in to the *Entrust Desktop Virtual Card* application, you also need to register it in the application as a PKCS #11 device. See Application Integrations for details on this case.

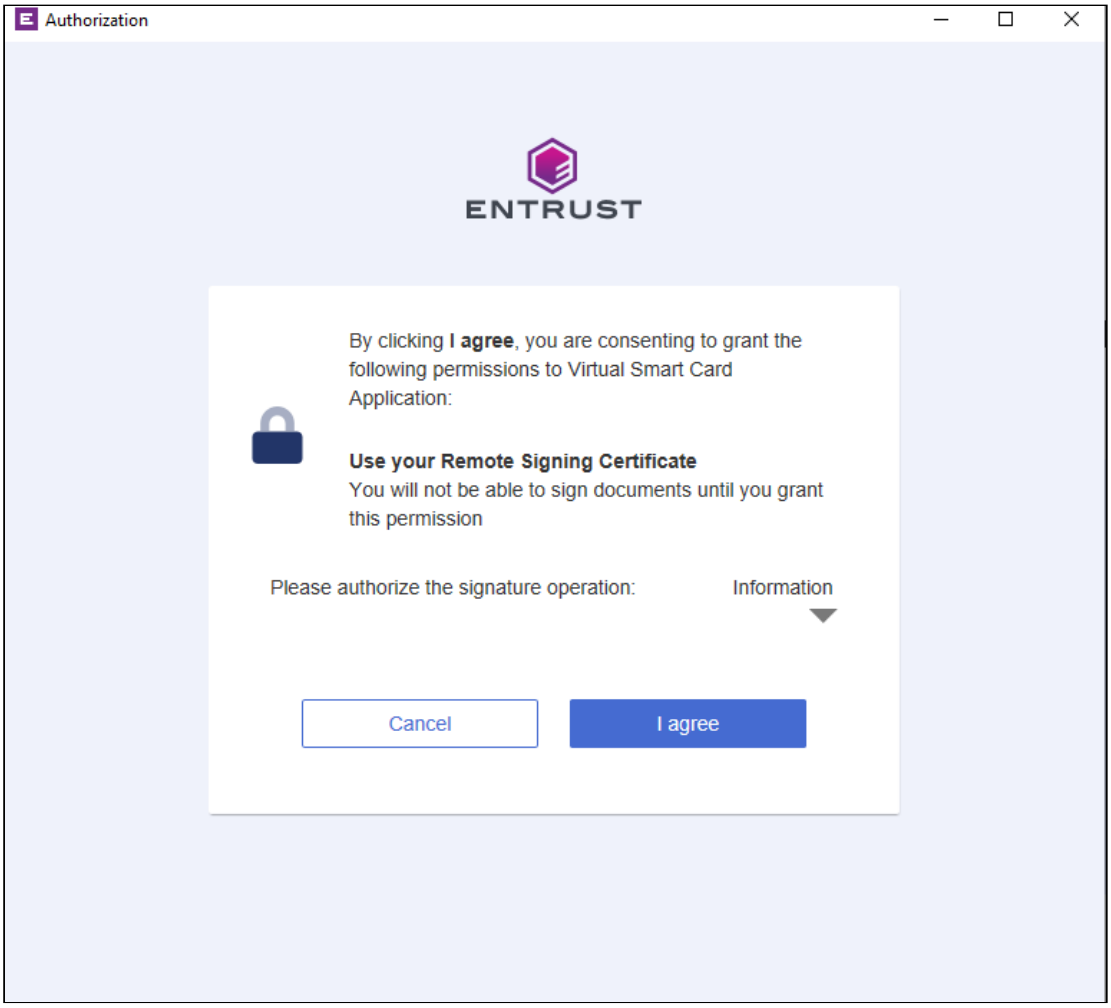
The applications that allow choosing the certificate to be used in a signature process (when there are several certificates available to your computer) also display the certificates stored in the *Remote Signing Service*. If the descriptive name of the certificate registered in Windows is used, the CN field of the subject of the certificate is displayed.

Important

Entrust Desktop Virtual Card does not install the certificates included in your certificates' certification paths in your computer. Some applications may require the installation of these certificates to complete the signing process. See Installation and Uninstallation for more details.

5.3.2 Using the Private Key

If you select to use an RSS certificate to generate a signature, *Entrust Desktop Virtual Card* will prompt you to authorize access to the corresponding private key. It will display a form to capture your consent to the signature operation and will request you to enter your credentials to authenticate this consent.



Following authorization, the signature process requested by the application is performed in the same way as if the certificate were installed in your computer or available on a cryptographic card.

Note

Before requesting authorization for the operation from you, if the *Entrust Desktop Virtual Card* application detects that the session has been inactive for over an hour, it automatically displays the login form and prompts you to log in again.

5.4 Other Options of the Application

The application allows performing other operations. In particular:

To view your certificates:

1. In the Windows taskbar, right-click on the logged-in icon.
2. Select the **Show Certificates** contextual command to access the **Certificates** dialog box.
3. In the **Certificates** dialog box, click on the certificates to browse their properties.

To view the Entrust Desktop Virtual Card's version:

1. In the Windows taskbar, right-click on the icon.
2. Select the **About** contextual command to access the view with information on the application.
3. In the lower bar of the view, the version of the application is displayed.

6 Application Integrations

This chapter describes the main use cases of the virtual card.

6.1 Windows Certificate Store

As explained in the Introduction, after starting a session in Entrust Desktop Virtual Card, your certificates managed remotely by *Entrust Remote Signing Service* appear available as certificates of your Windows user account.

The certificates can be used by any desktop application that uses the Windows certificate store. The remote management of certificates is completely transparent. The only difference is that you are prompted for the authorization for accessing the keys by Desktop Virtual Card instead of the Windows certificate store.

Important

Certificates managed by the virtual card cannot be imported or deleted with the Windows certificate store.

See the following sections for examples of using Entrust Desktop Virtual Card with applications that have access to the Windows certificate store.

6.1.1 Signing Documents and Forms

Signing documents with Microsoft Office (e.g., Word or Excel) or Adobe (Acrobat or Reader) tools.

Signing documents or Web forms with signature components executed in browsers such as Google Chrome or Edge.

6.1.2 Signing Email

Signing emails with client applications such as Microsoft Outlook.

6.2 PKCS #11 Certificate Store

Applications without access to the Windows keystore can access your certificates with the PKCS #11 client provided with *Entrust Desktop Virtual Card*.

When you configure the application, specify the path of the `p11rss.dll` library.

- 32-bit applications: `C:\Windows\SysWOW64\p11rss.dll`
- 64-bit applications: `C:\Windows\System32\p11rss.dll`

The following sections illustrate examples of using the PKCS #11 client.

6.2.1 Signing Documents and Forms

Signing documents and Web forms with signature components executed in browsers such as Mozilla Firefox.

6.2.2 Signing Email

Signing emails with client applications such as Mozilla Thunderbird.

Important

Certificates managed by the virtual card cannot be imported or deleted with the browser.

6.3 Integration

Certificates managed by the virtual card can be used by applications with interfaces such as the following:

6.3.1 Network Security Services

The virtual card integrates with the Network Security Services (NSS) cryptographic libraries. To do this, in applications that use these libraries, the virtual card can be registered as a PKCS #11 device.

Integration with NSS supports registering the virtual card as a security device of Mozilla applications (e.g., Firefox, Thunderbird). This means that through these application you can use the certificates on the virtual card.

To register the virtual card as a Firefox device:

1. In the Firefox browser, select the **Settings** to access the configuration box.
2. In the configuration menu, click on the **Privacy & Security** icon.
3. In the **Security > Certificates** option, click on the **Security Devices** button to access the cryptographic device administrator.
4. In the device administrator, click on **Load** to add a device with the properties described below.

6.3.1.1 Module Name

Name of the new security device (e.g., DesktopCard).

Important

Owing to browser limitations, it is advisable not to leave any blank spaces in the module name.

6.3.1.2 Module Filename

Provide the path of the installed `p11rss.dll` library (32 or 64 bits) as explained in PKCS #11 Certificate Store.

6.3.2 OpenSC

The virtual card integrates with the OpenSC cryptographic libraries. In applications that use these libraries, the virtual card can be registered as a PKCS #11 device. For example, the following command line generates a key pair via the PKCS #11 interface of the virtual card:

```
pkcs11-tool.exe --module "C:\Windows\SysWOW64\p11rss.dll" -l -k --key-type rsa:1024
```

Note that the `--module` command argument is the path of the `p11rss.dll` library.

Note

OpenSC's `engine_pkcs11` supports integrating the virtual card with OpenSSL.

6.3.3 Java

The virtual card can be integrated with applications developed with Java SE (version 6 or later), e.g., desktop applications. For this integration, the following cryptographic providers must be used that allow access to the virtual card via PKCS #11 or the Windows store (see [ORA_PROVIDERS] for a description of the cryptography providers):

- `SunPKCS11`
- `SunMSCAPI`


ENTRUST