PIV Smart Card Mini driver

Introduction

The PIV Smart Card Mini driver is applicable to the following products:

- uTrust FIDO GOV Security Key
- uTrust FIDO Card

The mini driver allows you to manage certificates of PIV applet using tools that are already available on Windows. This is typically useful in the absence of full-fledged Card/Credential Management System (CMS) or this can be used to complement the operation of CMS.

Note that some CMS may require the mini driver to be present for their proper operation. Please refer to the CMS documentation for further details.

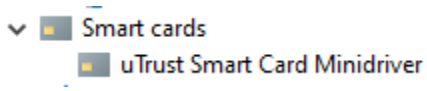
The Hirsch provided mini driver is required to load or delete certificates in different containers. However, the Hirsch provided mini driver is not mandated for normal operation as the Microsoft provided built in PIV mini driver can be used for login, digital signing and encryption once the certificates are loaded.

The mini driver complements the uTrust Token Manager which also allows to manage certificates on PIV applet.

Installation

Run the installer executable. After installing the mini driver, the installer will automatically refresh the device manager so that the mini driver will load for compatible devices that are already available on the host.

The smart card device will show up as *uTrust Smart Card Minidriver* under *Smart cards* in device manager.



Usage

The certificate manipulation operations are done using *certutil* command line utility that is shipped as part of Windows. A minimal subset of *certutil* commands used to manage certificates is explained in subsequent sections. For full documentation, refer to link [certutil | Microsoft Learn]

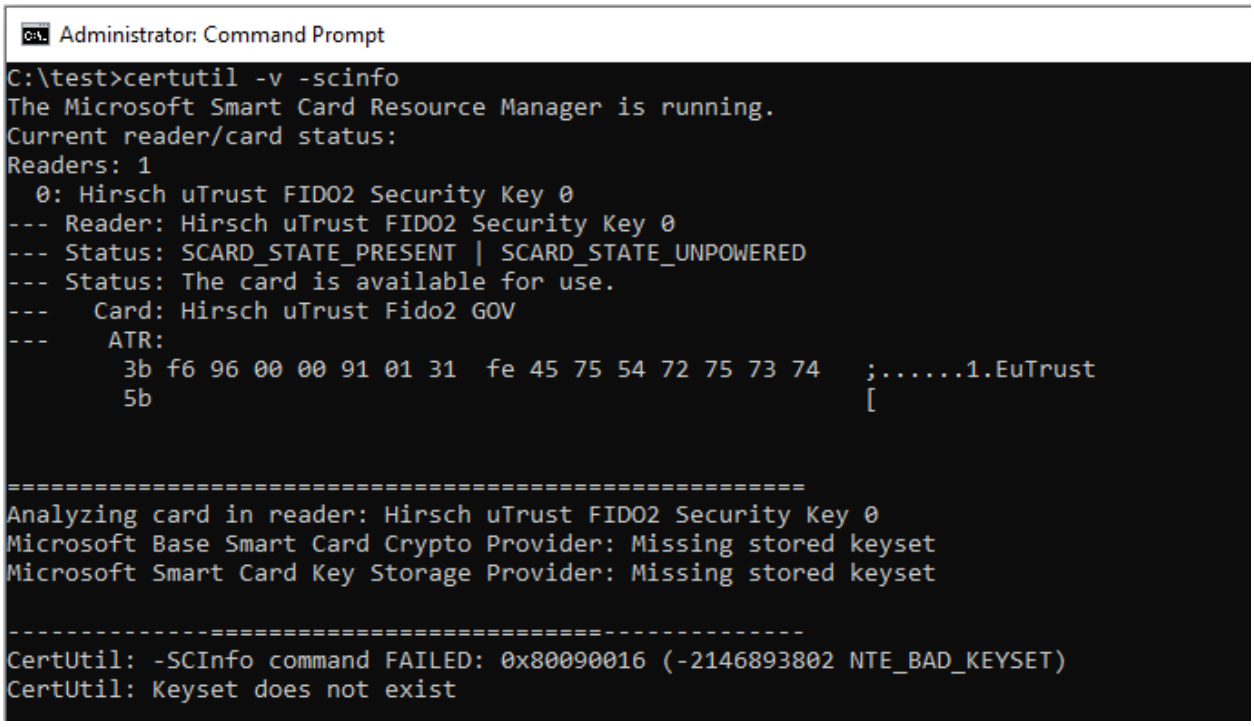
Open a command prompt to work with *certutil*. Some operations (like import and delete) will require the command prompt to be opened with elevated privileges (Run as Administrator).

Displaying Information

The uTrust FIDO GOV Security Key or uTrust FIDO Card does not have any containers populated by default. Type the following at command prompt to display information

```
>certutil -scinfo
```

The following would be the typical output when none of the containers are loaded:



PIV Certificate Container Population Sequence

PIV applet has four certificate slots as detailed below:

Container ID/ Key Reference	Purpose
9A	PIV Authentication or card holder authentication
9C	Digital Signature of documents
9D	Key Management
9E	Card Authentication for physical access

When importing certificates, the mini driver scans the containers in the sequence listed in table above, that is, 9A -> 9C -> 9D -> 9E. The certificate will be placed in the first empty slot that the mini driver encounters. If there are no empty slots, the mini driver will flag an error.

Administrators that manage certificates and CMS software developers that rely on the mini driver need to note the above. For example, there is no way to load 9A, 9C, 9E without loading 9D; there should be some dummy certificate loaded into 9D so container 9E can be populated. (The dummy certificate loaded in 9D can be deleted after 9E is populated.)

Importing Certificate to PIV Container

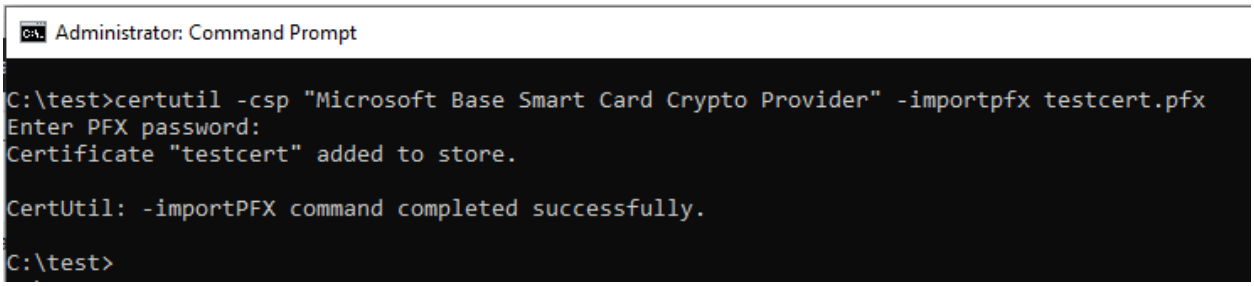
Certificates need to be generated off-card and stored in a file along with private key; this is usually the PFX file. PFX files are always secured by password since they include the private key. Note that a certificate can also be stored as CER or PEM, but these will have only the certificate with public key without the private key.

Let us assume that the certificate and private key were generated off-card and stored in the file *testcert.pfx*. Use the following command line to import the certificate and private key into the first available container.

```
>certutil -csp "Microsoft Base Smart Card Crypto Provider" -importpfx testcert.pfx
```

When executing this command, *certutil* will prompt to enter the password for the PFX file. Then *certutil* will prompt with a GUI pop-up requesting the PIN to access the PIV container on the card/token. After the PIN is entered, the certificate will be imported into the card/token.

The command window will look as below



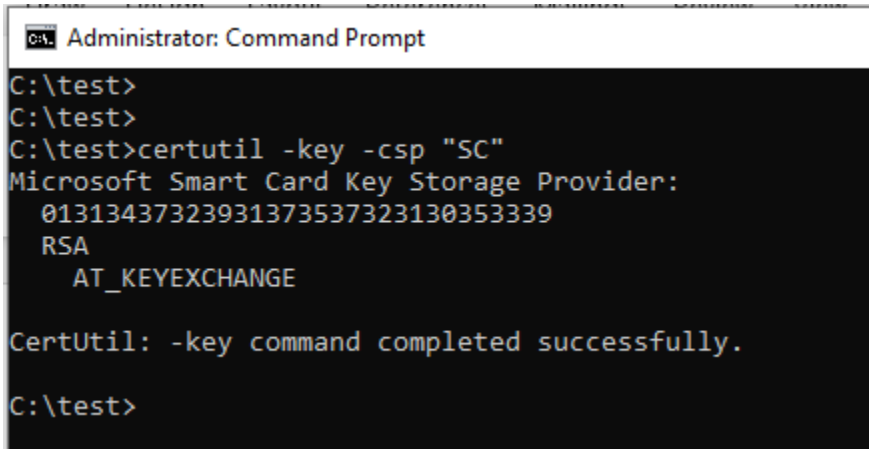
Certificates can be imported into other containers with the same procedure.

Displaying Key Identifier of Certificate in PIV Containers

The key identifier of a certificate in PIV container can be displayed with the following command:

```
>certutil -key -csp "SC"
```

The output would look as below:



The number 013134373239313735373231303533 39 is the key identifier.

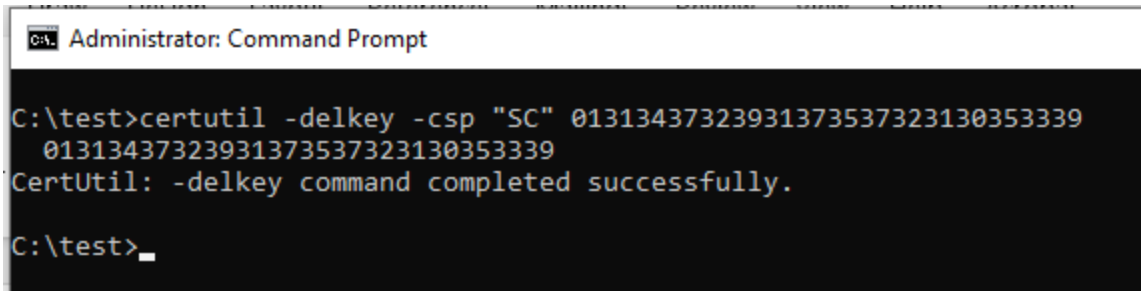
The key identifiers are listed in the same sequence of containers: 9A, 9C, 9D, 9E; if a container is empty, then nothing will be displayed.

Deleting Certificate from PIV Container

Certificate in a PIV container can be deleted once its key identifier has been determined. For example, the following command will delete the key listed with key identifier 013134373239313735373231303533 39

```
>certutil -delkey -csp "SC" 013134373239313735373231303533 39
```

Certutil will prompt for PIN; the certificate will be deleted after authenticating with card using the PIN. The command window will look as below


Administrator: Command Prompt
C:\test>certutil -delkey -csp "SC" 013134373239313735373231303533339
013134373239313735373231303533339
CertUtil: -delkey command completed successfully.
C:\test>