Raak Technologies Inc.
vSEC:CMS Card Management Utility User Guide v1.01

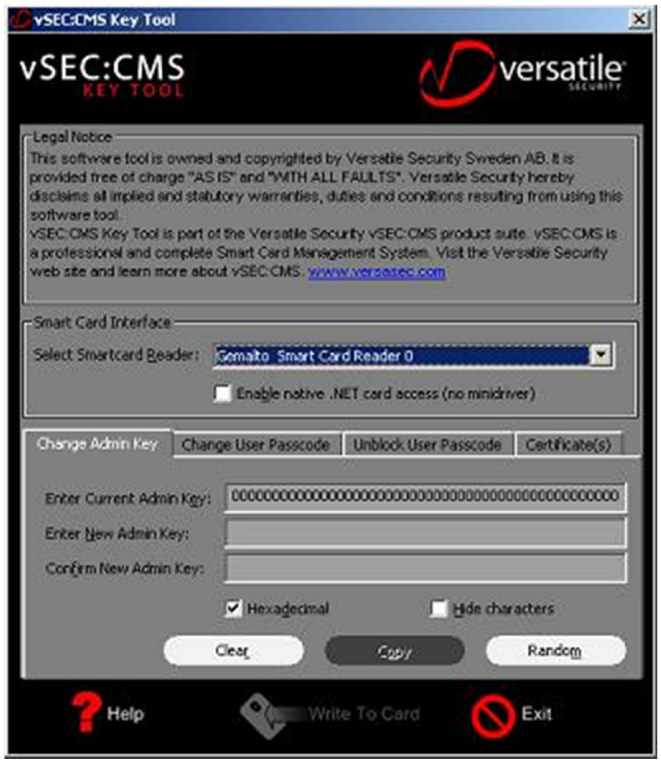
Introduction

The vSEC:CMS Key Tool is a software utility that lets the user manage minidriver enabled smart cards. Actions that can be performed using this tool include:

- Change Smart Card Administration Key
- Change Smart Card User Passcode
- Unblock Smart Card User Passcode
- Manage Smart Card Certificates

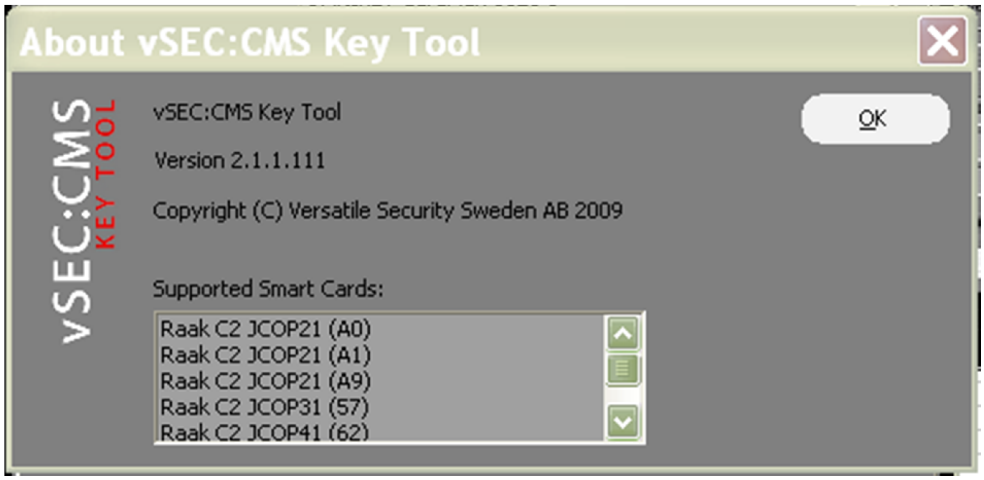
These types of smart cards (including the Raak C2 series smart cards) have their factory default Administration Key set to a null vector (24 bytes, where each byte has the value 0x00). This can be a security issue. The Versatile Security vSEC:CMS Key Tool can be used to remove this security vulnerability.

Smart Card Interface



In the middle section of the main dialog, it is possible to select what smart card reader to use. This is useful if more than one smart card reader with valid smart cards inserted is connected to the system. Selecting the reader is done using the drop down field.

Supported Smart Cards



The types of smart cards supported on the system (as it is currently configured) are displayed in the About dialog. The About dialog is accessed by right clicking on the application window frame and selecting "About Key Tool...".

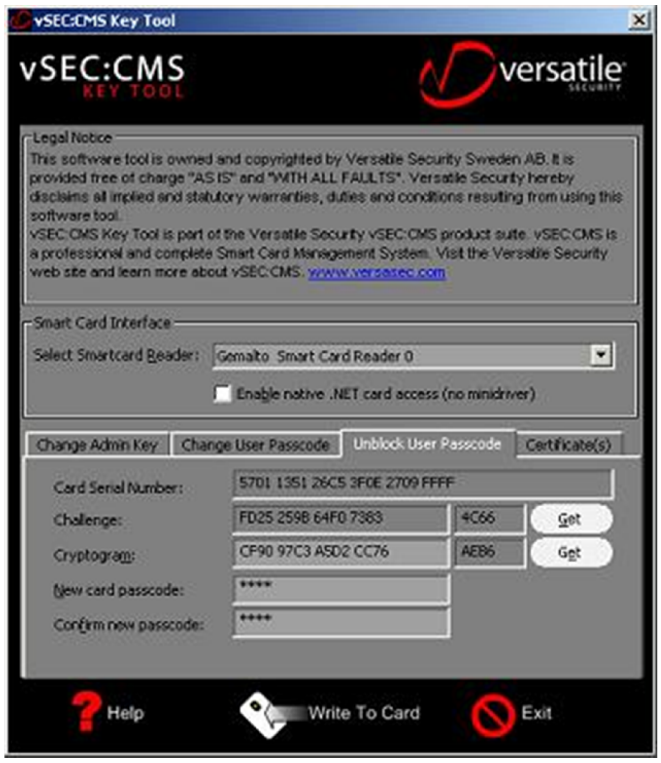
Changing the Administration Key

To change the smart card administration key, select the "Change Admin Key" tab. First the Current key needs to be provided. If the card inserted is a new card, the current key is normally the factory default

key (all zeros), this value is also by default entered when the application is started or when the "Clear" button is used. Second, the New key needs to be provided (twice). This can be done by entering the key manually or by letting the application create a random key using the "Random" button. If the "Random" button is used, it is recommended to copy the key value to a secure location for storage. This can be done by using of the "Copy" button - this puts the key value and the CSN of the smart card into the copy buffer so it can be pasted into a file for storage.

When the Current and the New key have been provided and the card is connected, the "Write To Card" button gets activated and can be used to complete the transaction. The format that the key values are entered and displayed in can be changed using the checkboxes under the input fields. The "Hexadecimal" checkbox should be used if the keys are in hexadecimal format, otherwise the keys must be in ASCII format. If the "Hide characters" checkbox is checked each character of the key value is displayed as a "*" character.

Change Smart Card User Passcode/PIN



To change the smart card user passcode (also known as PIN) the "Change User Passcode" tab is used. The Current and the New (twice) passcodes must be provided. If the smart card is a new smart card the Current passcode is often "0000" or “12345”. When the Current and the New passcodes have been provided and the smart card is connected, the "Write To Card" button gets activated and can be used to complete the transaction.

Unblock Smart Card User Passcode

If the smart card user passcode (also known as PIN) has been blocked (for example by entering the wrong passcode several times), it can be unblocked by using the functionality available on the "Unblock User Passcode" tab.

Card Serial Number: This field should be entered automatically if the card is inserted.

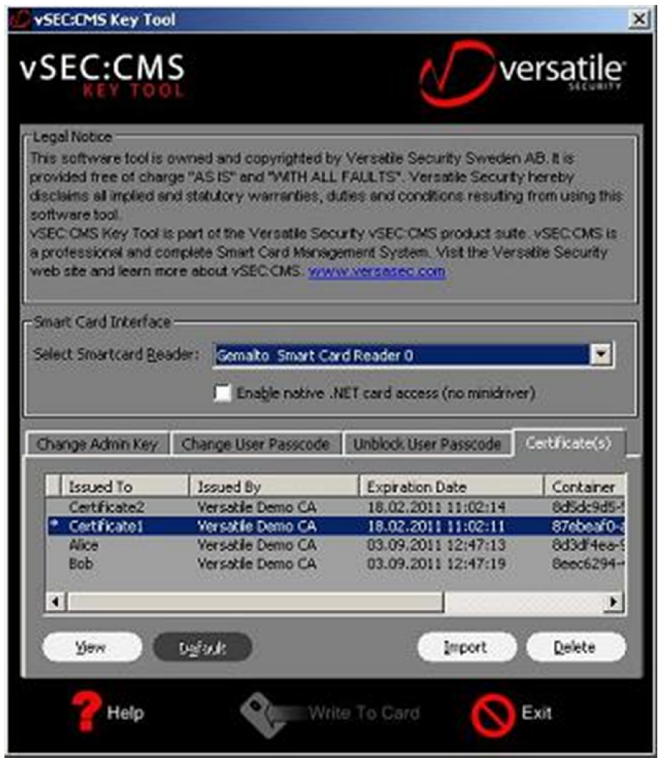
Challenge: This field is entered by clicking the "Get" button next to it. Next to the field there is also a checksum of the Challenge value displayed.

Cryptogram: The cryptogram is calculated by the manager of the smart card. The manager of the smart card knows the Administration key for this card. If you are the manager of the card, you can use the "Get" button to calculate the Cryptogram using the Administration key. If you are not the manager of the smart card, you need to provide the Challenge to the manager of the smart card and then the manager of the smart card will give you the Cryptogram back.

Note that it is important that the card is not removed and that the tab remains open during the process as it is a one to one relationship between the Challenge and Cryptogram.

New passcode: When the Card Serial Number, the Challenge and the Cryptogram have been filled you may enter the new passcode (twice). After that the "Write To Card" button is activated and can be used to complete the transaction.

User Certificates



Using the "Certificate(s)" tab it is possible to manage the certificates on the smart card. In the certificate list (on top) all the certificates that are loaded on the smart card are listed. For most of the operations available in this tab, the smart card PIN is needed and is prompted for.

View: The "View" button displays details of the certificate selected in the certificate list.

Default: The "Default" button sets the currently selected certificate (selected in the certificate list) to be the smart card default certificate. The default certificate is indicated with an asterisk in the certificate list.

Import: The "Import" button makes it possible to load certificate files onto the smart card. For User credentials (certificates associated with a user key) it is necessary to use a PFX file.

Delete: The "Delete" button deletes the currently selected certificate (selected in the list above) from the smart card.