How to use a Yubikey 5 USB with HiCrypt™

Author: digitronic
Release: 27.01.2022

1. Introduction

This documentation shows the preparation of a YubiKey 5 USB token in conjunction with logging on to a network drive encrypted with HiCrypt™. HiCrypt™ professional provides digital confidentiality for groups of employees with a key ownership guarantee. If one wants to deliberately extend access to additional trusted persons, this can be done with the help of a Yubikey.
All it takes is for the HiCrypt™ Professional share manager to pair a YubiKey with another trusted user. After entering the PIN, the YubiKey immediately unlocks the confidential share at the workstation of the new trusted user. If the pairing is to be released again, a click of the share manager is sufficient to end the confidential access.

2. Prerequisites

Please note the following before configuring:

1. Download the installation archive at https://hicrypt.com/download/hicrypt_addon_yubikey.7z.

2. You will find a subfolder "Libraries" in the installation package. All .dll libraries located there must be copied to the standard Windows directory (C:\Windows\System32).

3. Install YubiKey Manager using the setup included in the installation package.

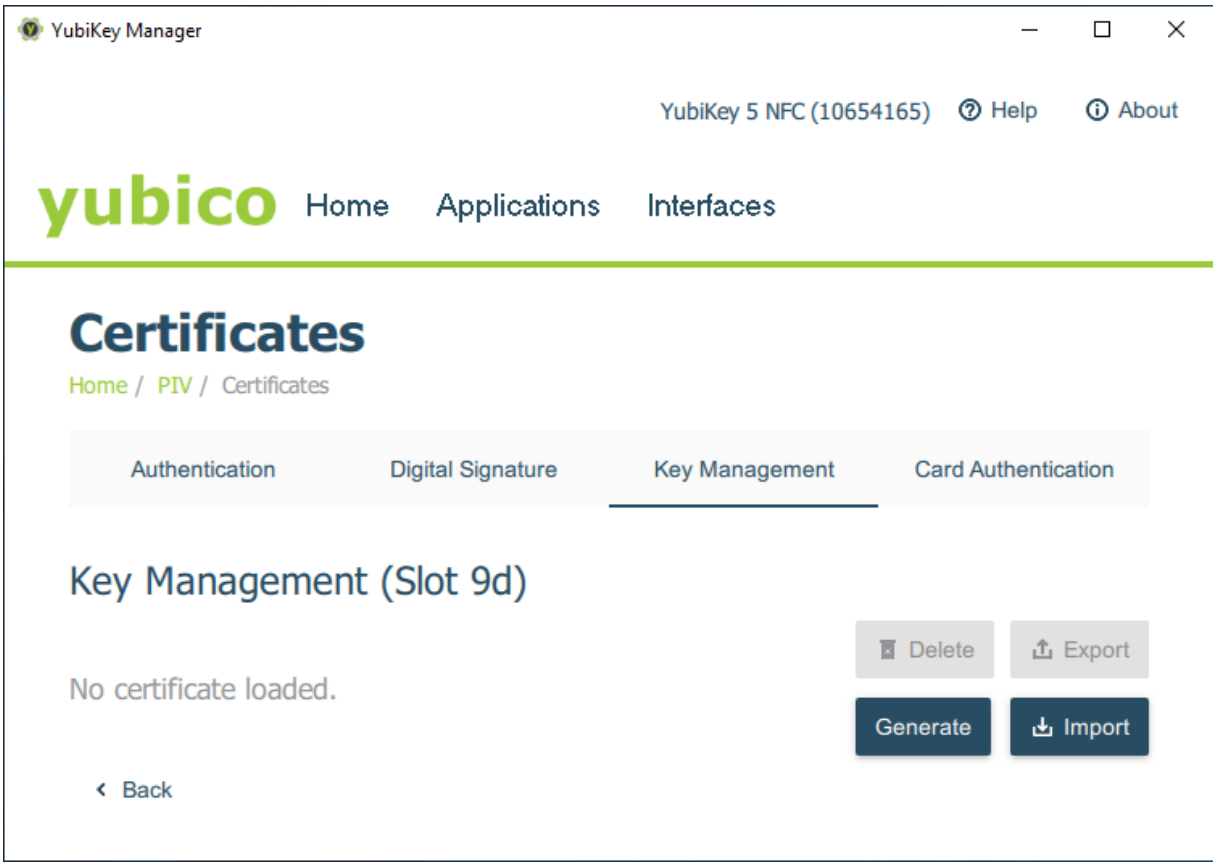
4. Download the Token Engine at https://hicrypt.com/download/TokenEngineSetup.zip.

5. After you have installed the Token Engine, select the "SafeSign" module in the Token Manager of the Token Engine under "Settings". A restart is then required.

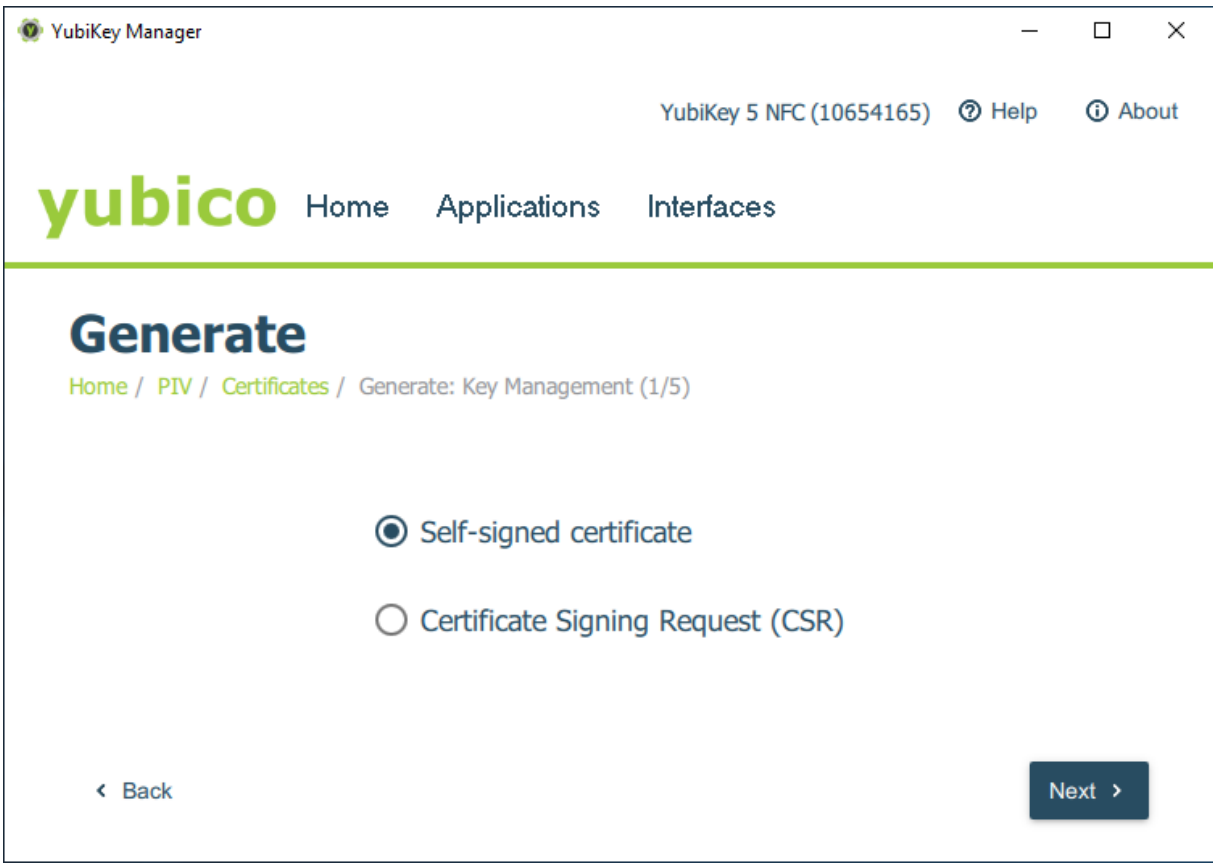
6. Then execute the "Use_YubiKey" registry file. It is possible to switch back to the original state at any time using the "Reset_YubiKey" registry file.

7. Now a restart is required.

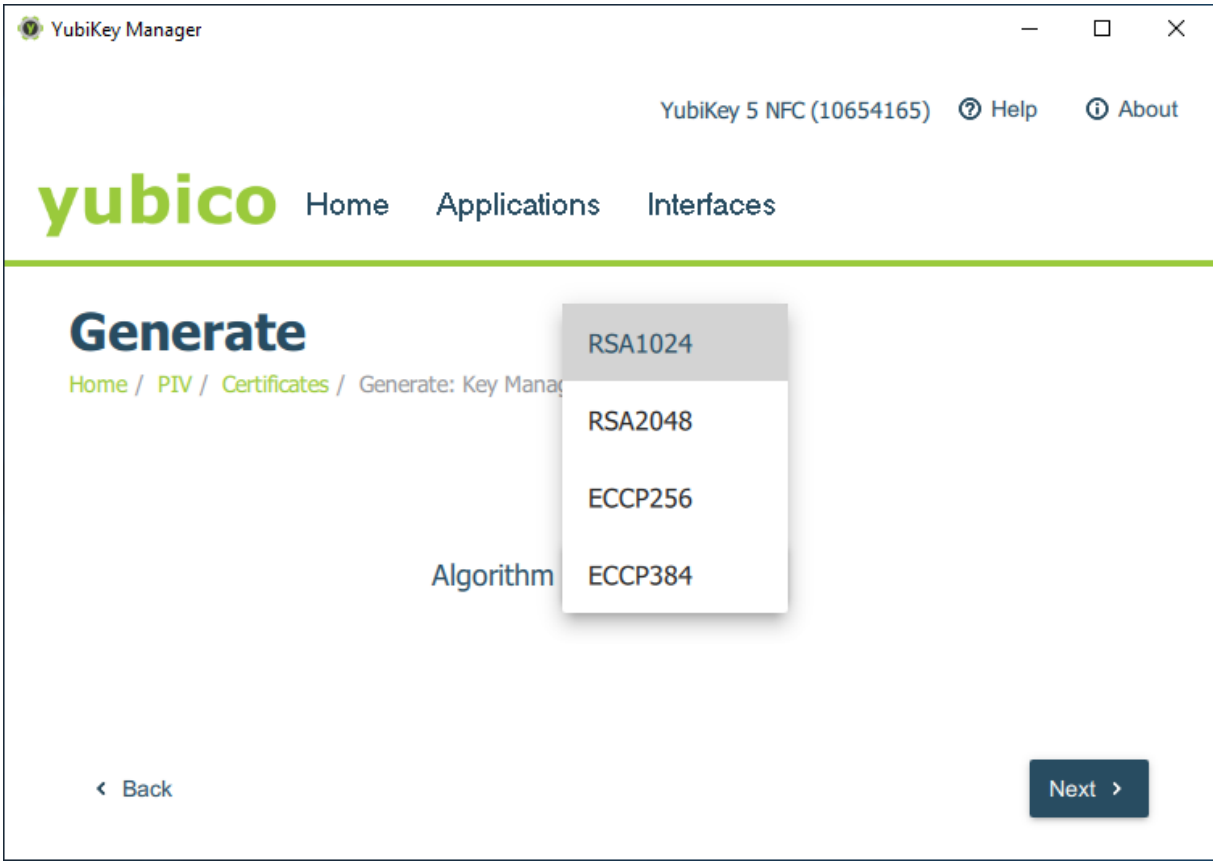
3. Step by Step



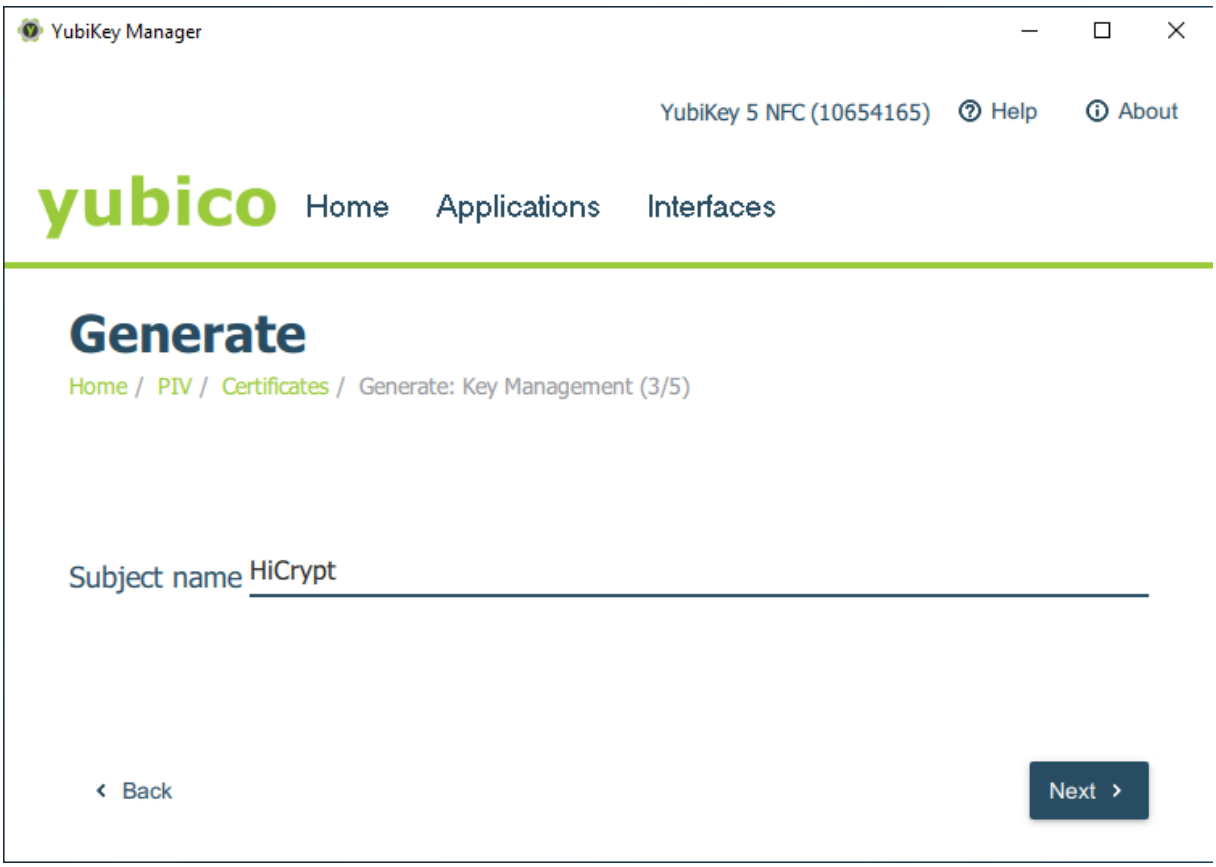
Start the YubiKey Manager and navigate to "Key Management".



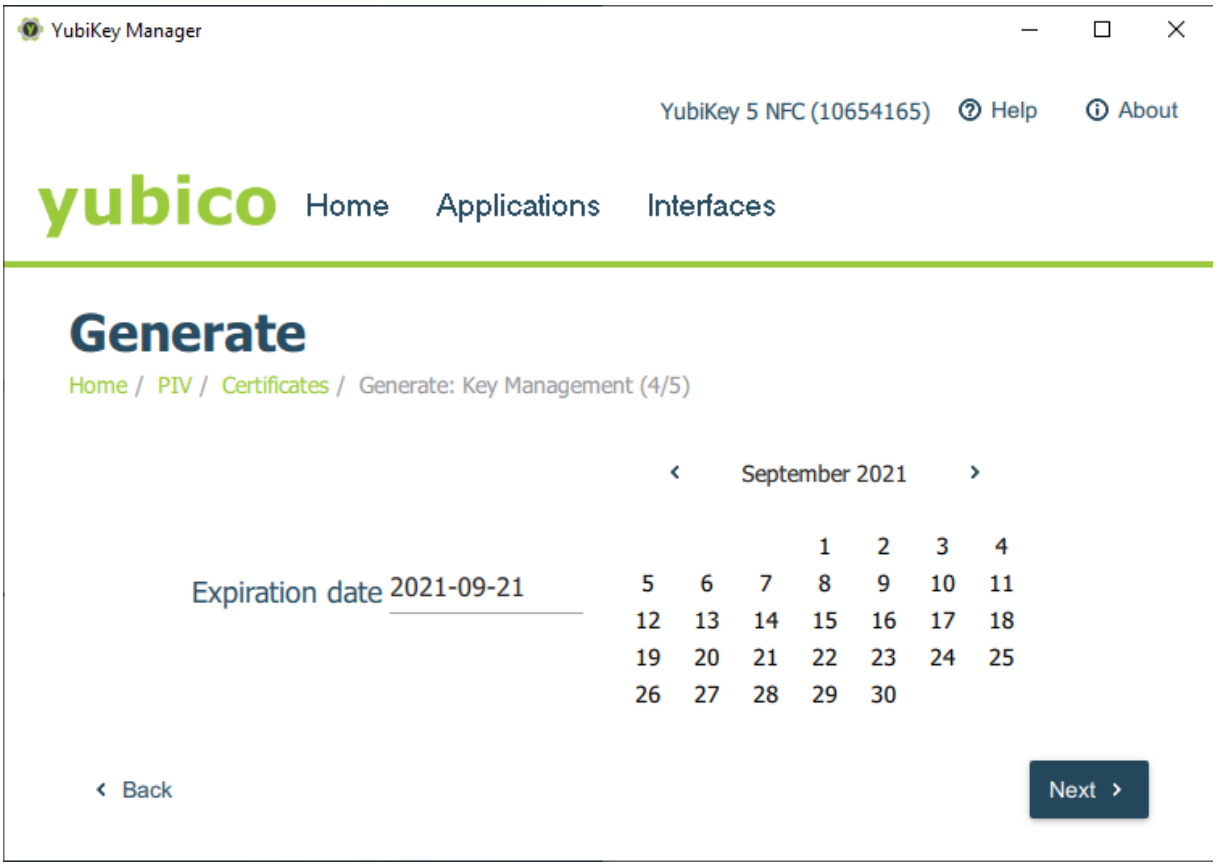
Check the option "Self-signed certificate" and go on with "Next".



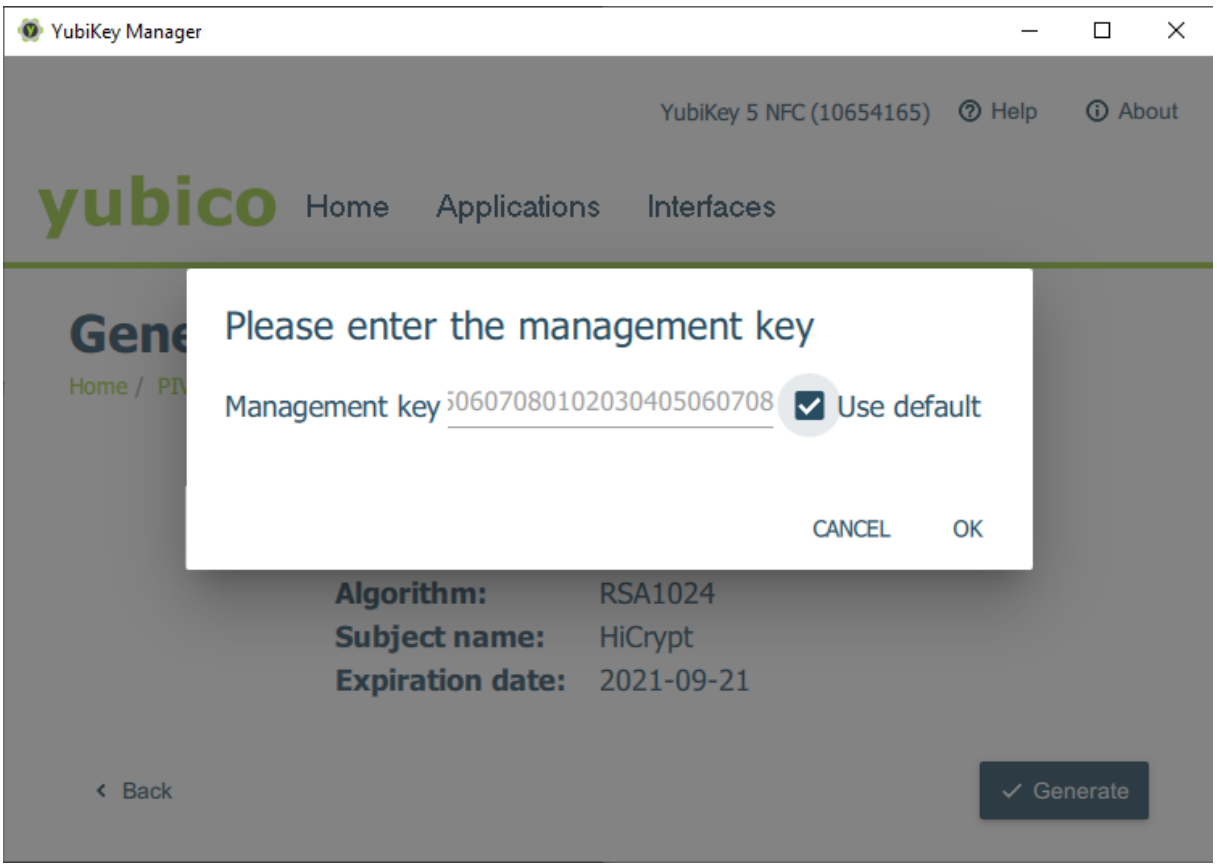
Change the algorithm to RSA1024 and click "Next".



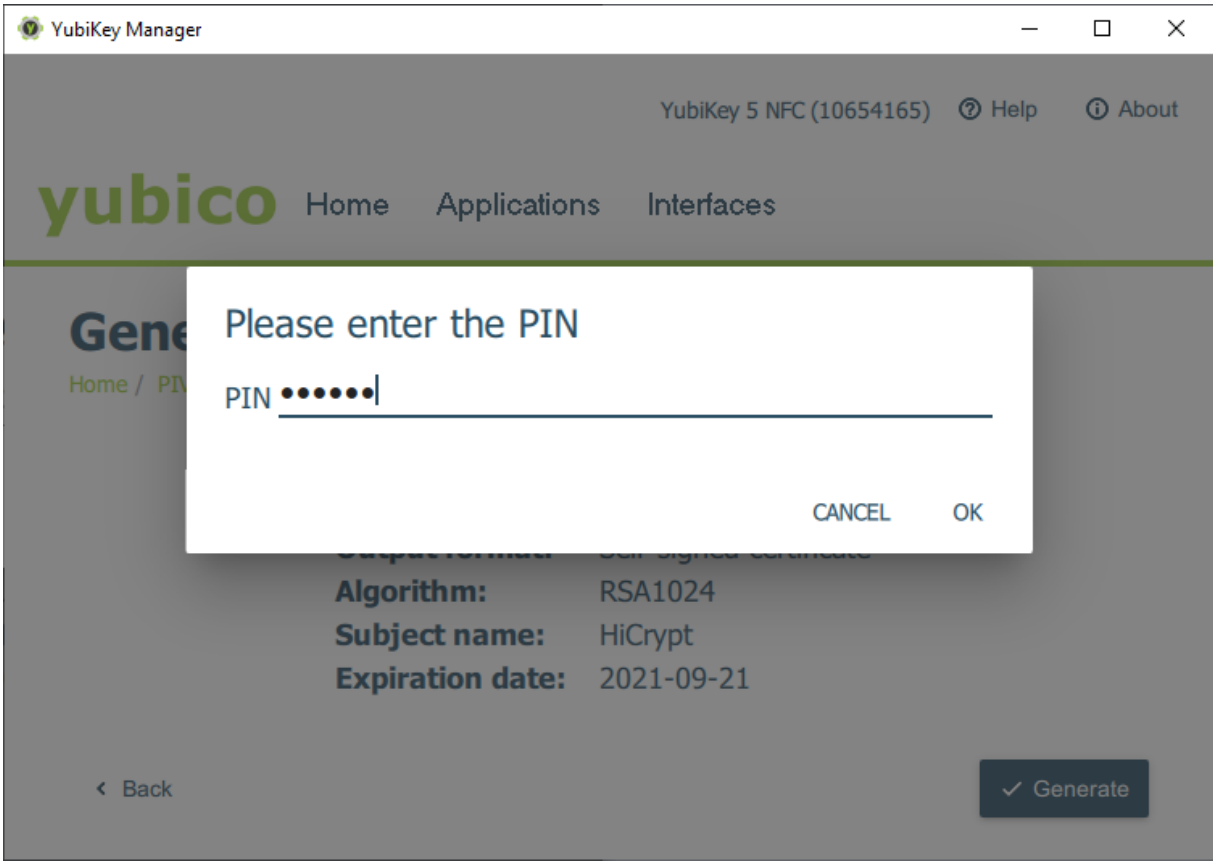
Set a name for your key which will be created in the following step. Go on by clicking "Next".



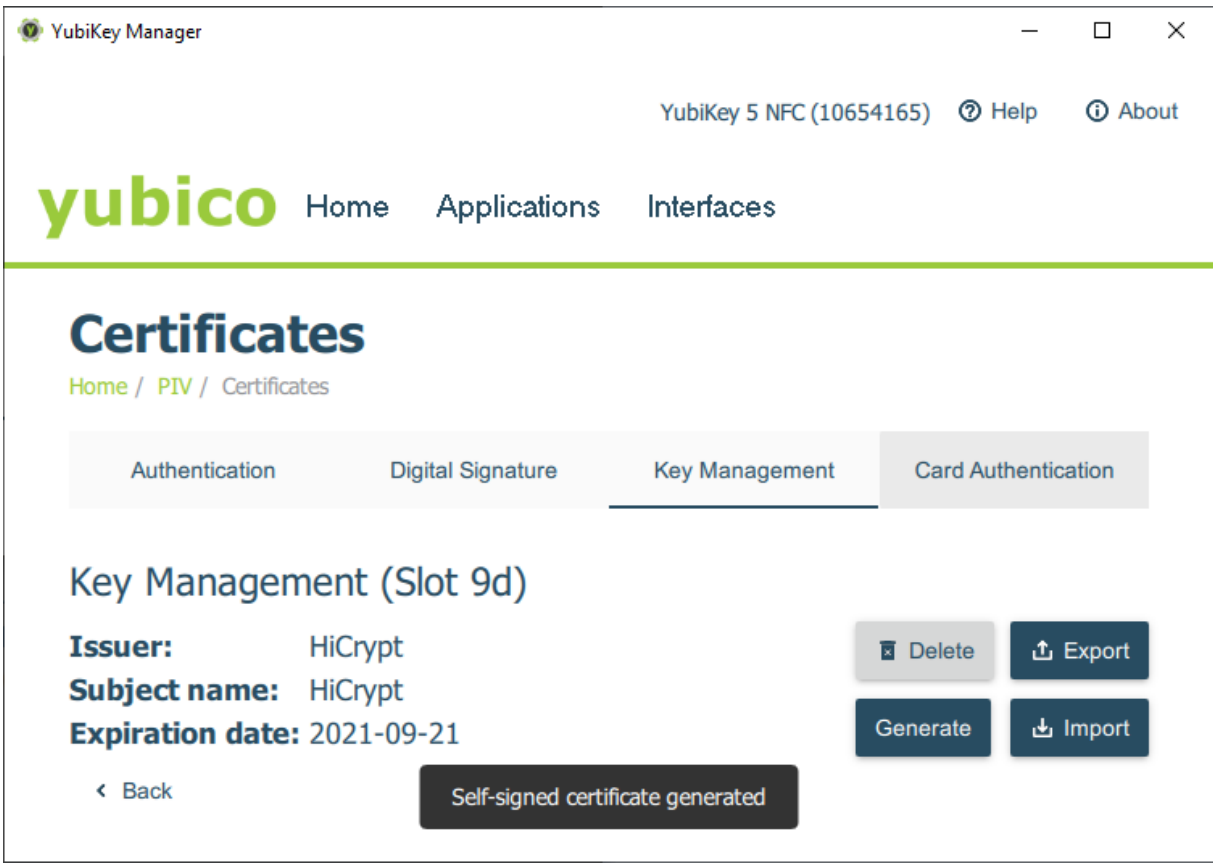
In this dialogue you have to set an expiration date, but it won´t have any influence of using the key with HiCrypt™ at the moment.



Choose "Use default" to use the default Management Key. Go on by clicking "OK".



Enter your Yubikey PIN (default 123456) and confirm by clicking "OK".



The key is now generated and subsequently displayed in the overview. Additionally you will find once again the name and the expiration date. The key can be exported or deleted via the buttons on the right.

After the preparation of the YubiKey has been completed, the token can be prepared for use with a user and linked to the account via the HiCrypt™ interface with a user and associate it with the account. Follow the instructions in the HiCrypt™ documentation for this.