Verwendung eines YubiKey 5 mit HiCrypt™

© 2022 digitronic computersysteme gmbh

Dieses Dokument ist urheberrechtlich geschützt, und seine Verbreitung unterliegt den Lizenzen, die seine Verwendung, Vervielfältigung und Verbreitung einschränken. Kein Teil dieses Produkts oder Dokuments darf ohne vorherige schriftliche Genehmigung von digitronic in irgendeiner Art und Weise reproduziert werden.

Verfasser: digitronic
Stand: 27.01.2022

1. Einleitung

Diese Dokumentation zeigt die Vorbereitung eines YubiKey 5 USB Tokens in Verbindung mit der Anmeldung an einem mit HiCrypt™ verschlüsselten Netzlaufwerk. HiCrypt™ professional bietet für Gruppen von Mitarbeitern digitale Vertraulichkeit mit Schlüsselalleinbesitzgarantie. Will man bewusst den Zugriff auf weitere Vertrauenspersonen erweitern, so kann dies mit Hilfe eines YubiKeys erfolgen.
Es reicht aus, wenn der HiCrypt™ Professional-Sharemanager einen YubiKey mit einem weiteren Vertrauensnutzer koppelt. Ab sofort schaltet der YubiKey nach erfolgter PIN-Eingabe das vertrauliche Share auch am Arbeitsplatz der neuen Vertrauensperson frei. Soll die Kopplung wieder gelöst werden, reicht ein Klick des Sharemanagers aus, den vertraulichen Zugriff zu beenden.

2. Voraussetzungen

Bitte beachten Sie vor der Konfiguration folgende Hinweise:

1. Laden Sie das Installationspaket unter https://hicrypt.com/download/hicrypt_addon_yubikey.7z herunter.

2. Sie finden im Installationspaket einen Unterordner "Bibliotheken". Es müssen **alle** dort befindlichen .dll-Bibliotheken in das Standard-Windows-Verzeichnis (C:\Windows\System32) kopiert werden.

3. Installieren Sie den YubiKey Manager mit Hilfe des im Installationspaket befindlichen Setups.

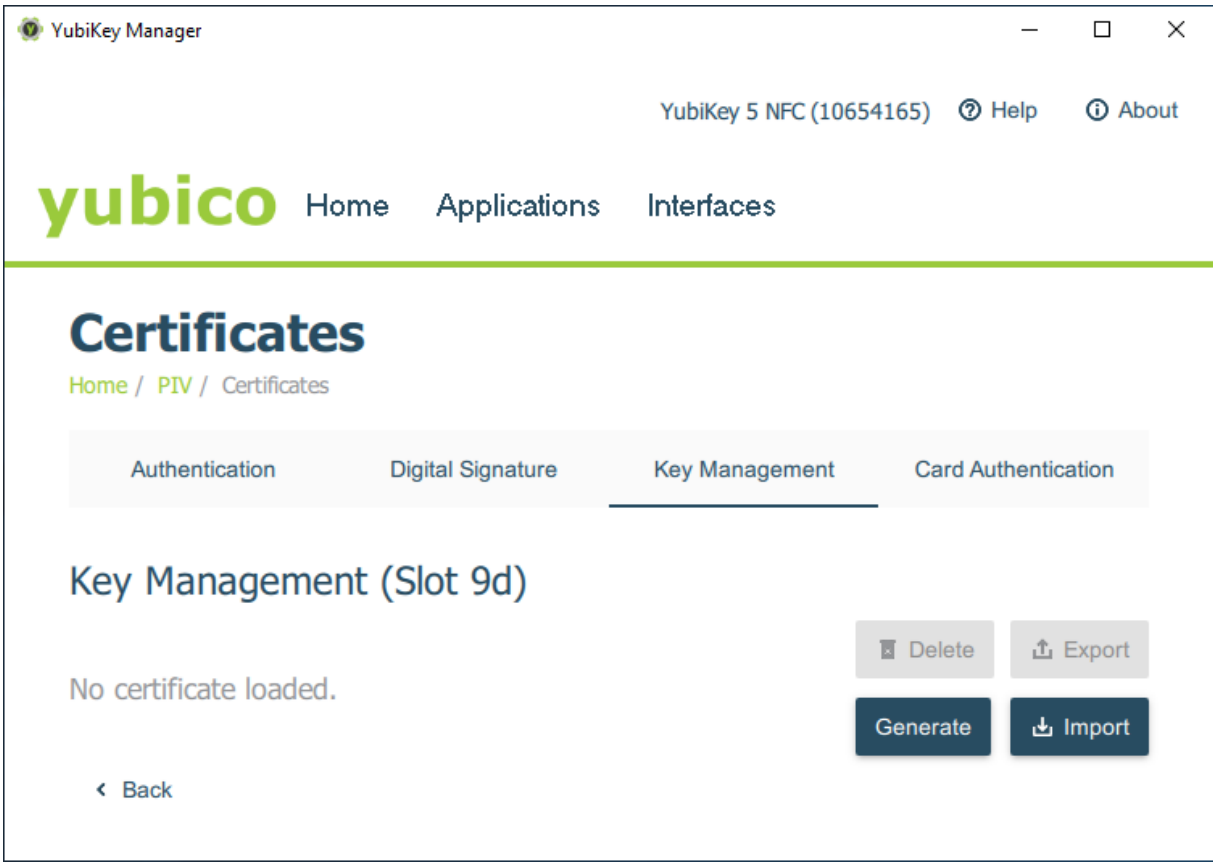
4. Laden Sie die Token Engine unter https://hicrypt.com/download/TokenEngineSetup.zip herunter.

5. Wählen Sie nach der Installation der Token Engine im Token Manager der Token Engine unter "Einstellungen" das Modul "SafeSign" aus.

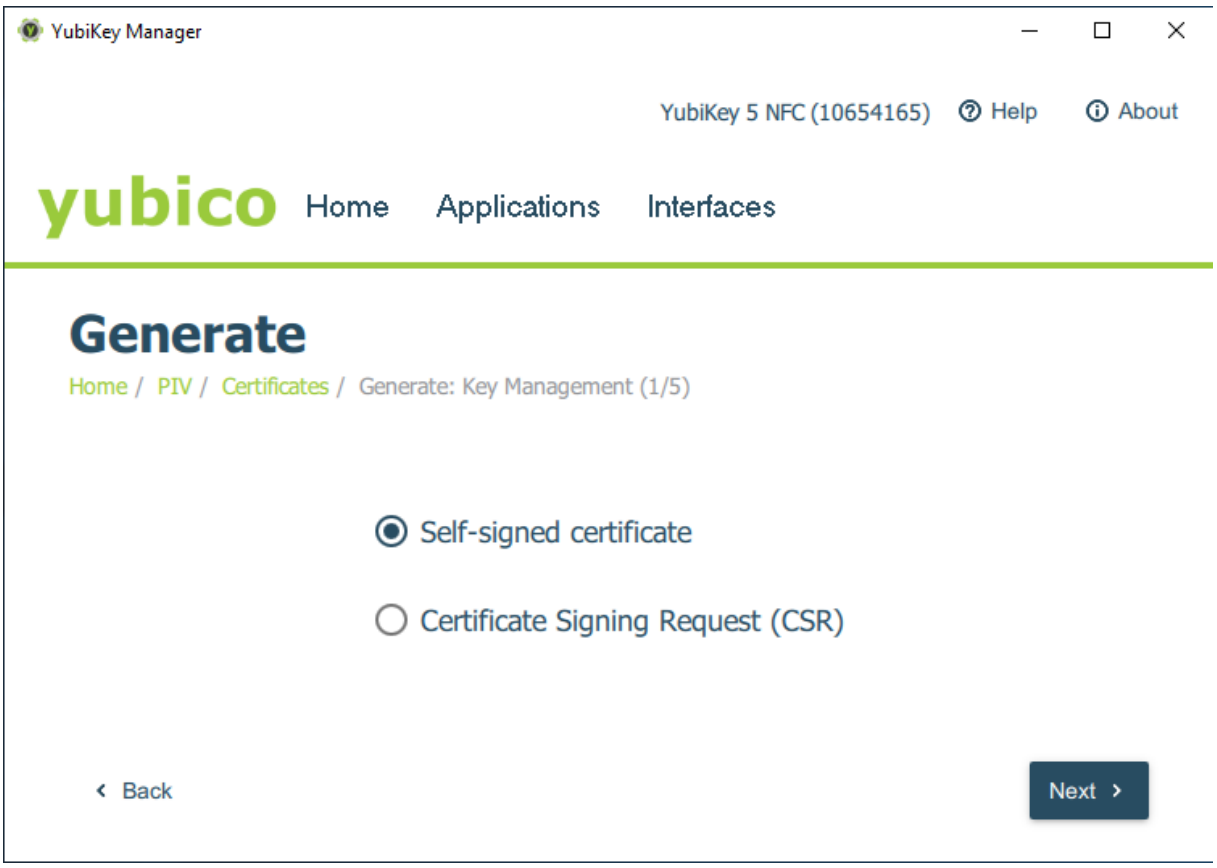
6. Anschließend führen Sie bitte die Registrierungs-Datei "Use_YubiKey" aus. Ein Wechsel in den Ursprungszustand ist mit der Registrierungs-Datei "Reset_YubiKey" jederzeit möglich.

7. Anschließend ist ein Neustart erforderlich.

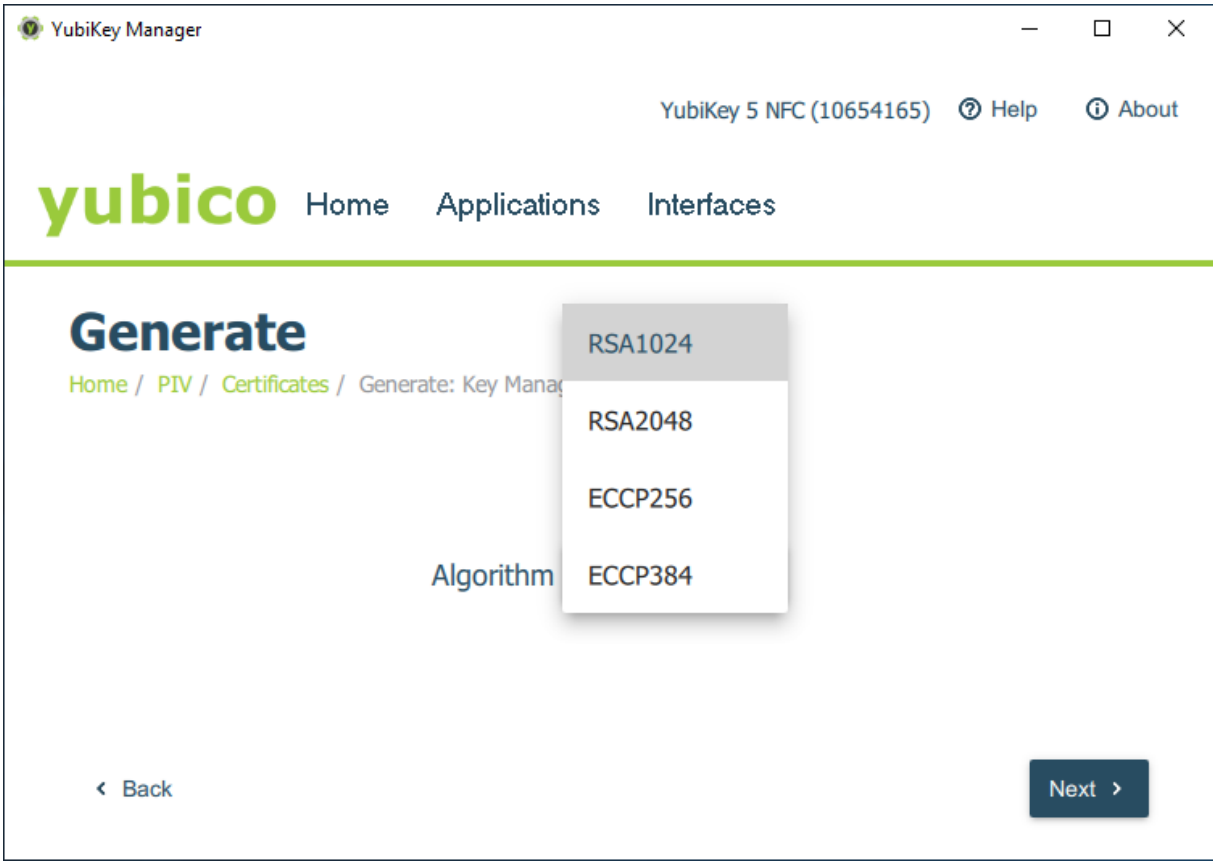
3. Schritt für Schritt Anleitung



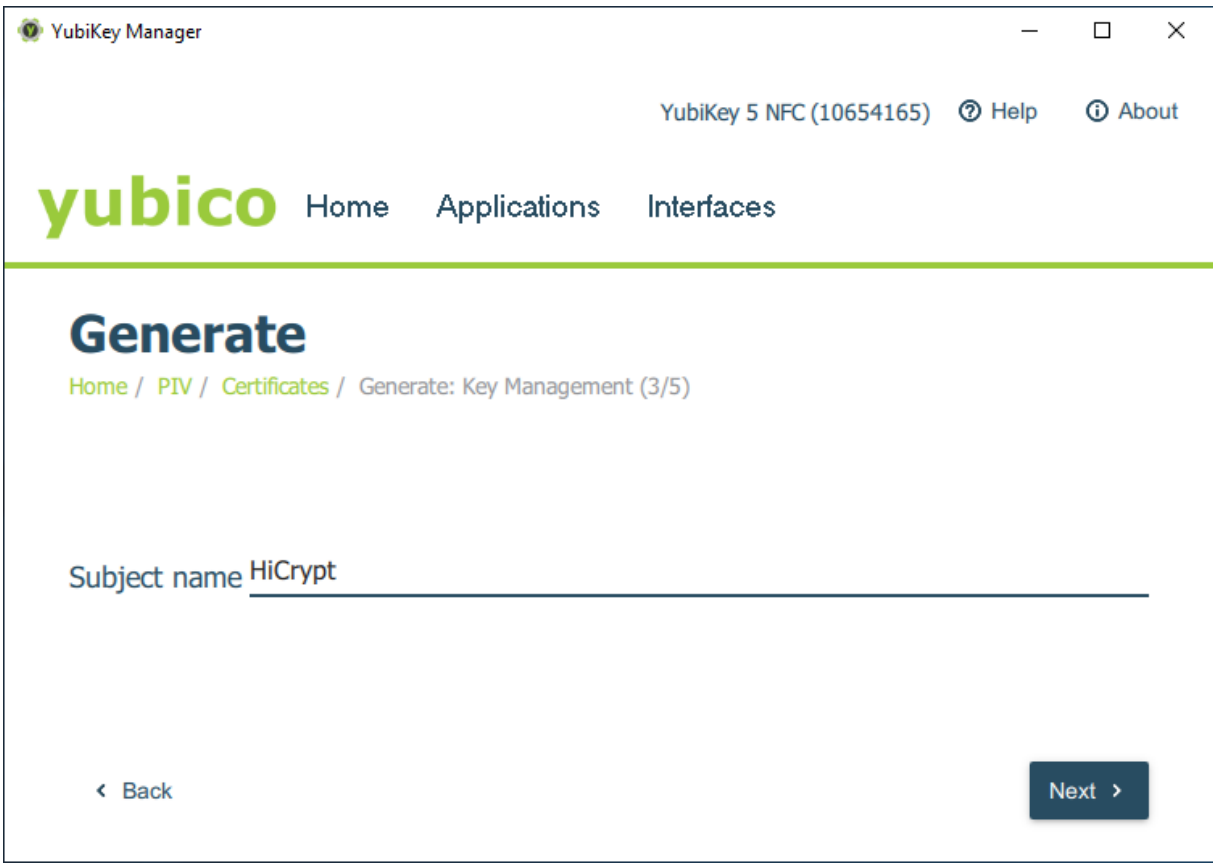
Öffnen Sie den YubiKey Manager und klicken Sie auf den Reiter "Key Management".



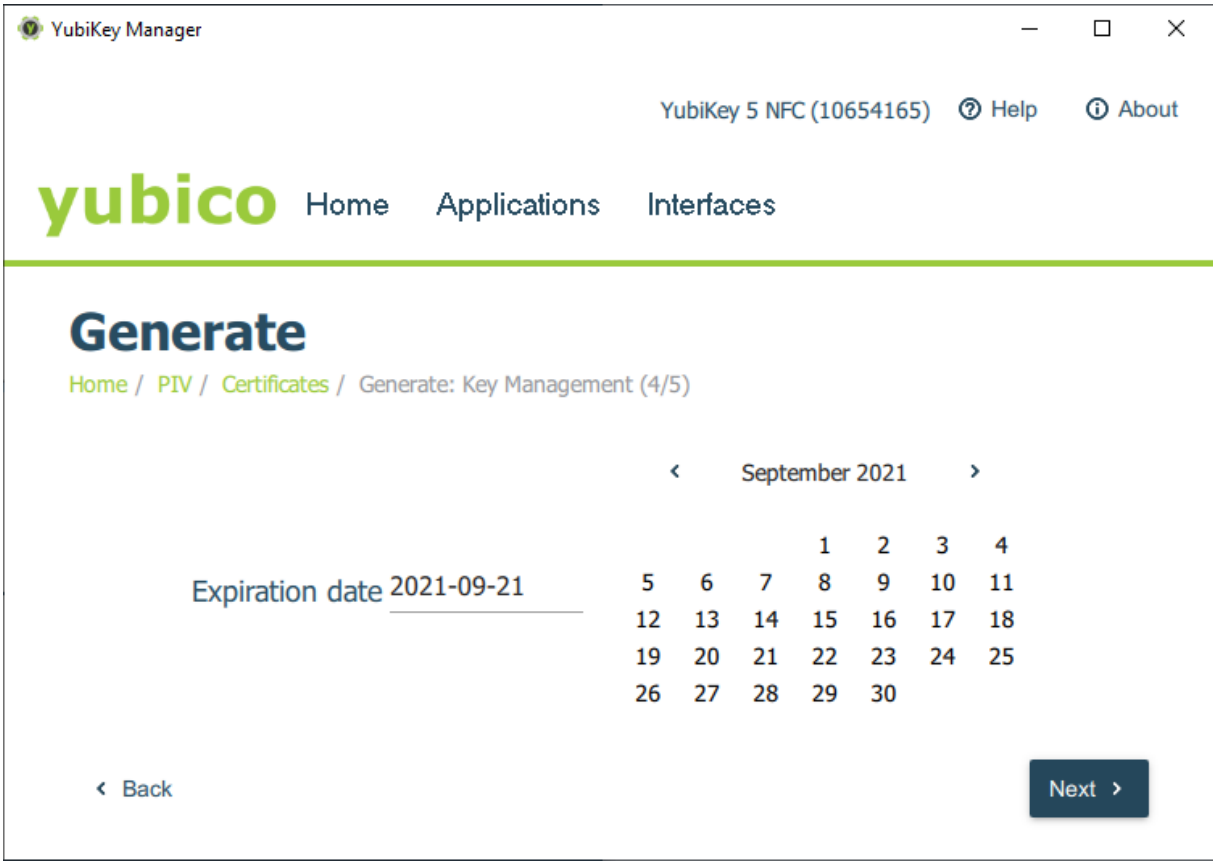
Wählen Sie die Option "Self-signed cerificate" aus und bestätigen Sie mit "Next".



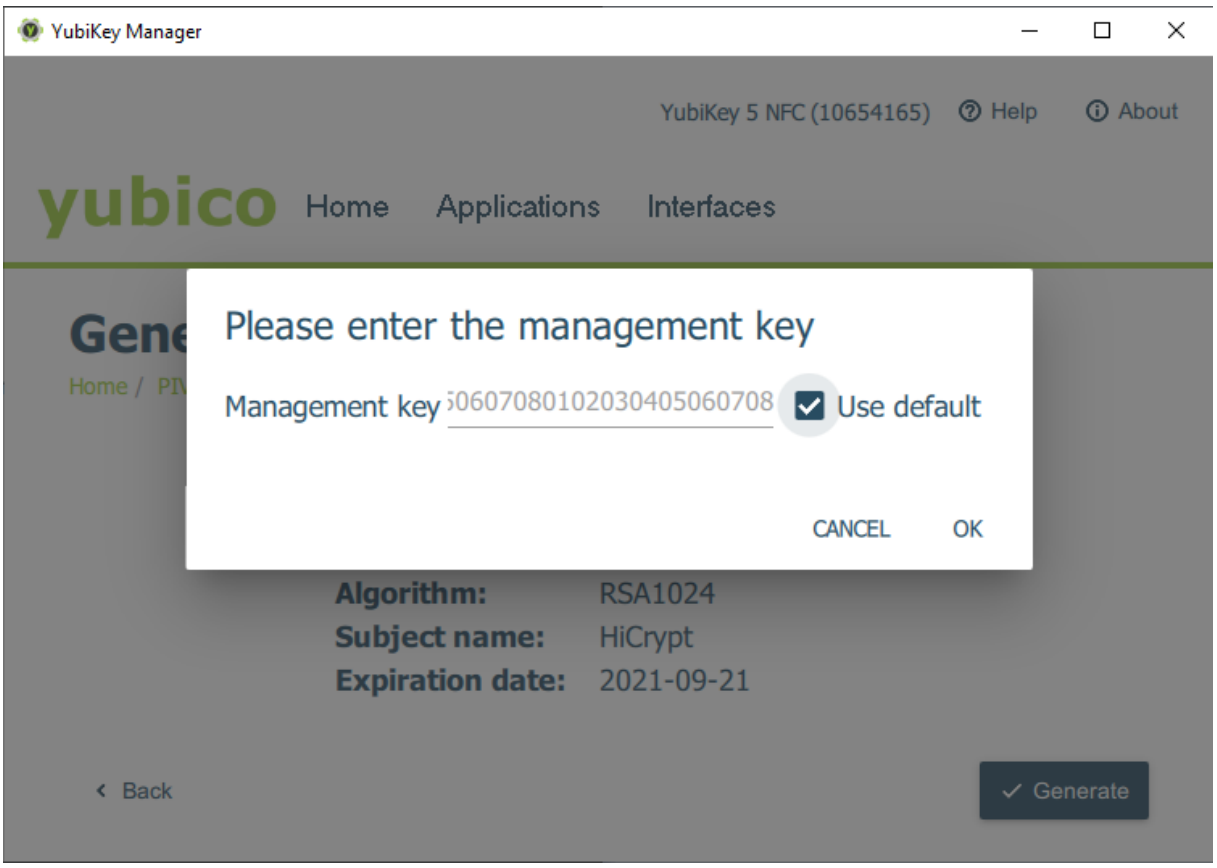
Wechseln Sie in diesem Dialog den Algorithmus auf RSA1024 und bestätigen Sie mit "Next"



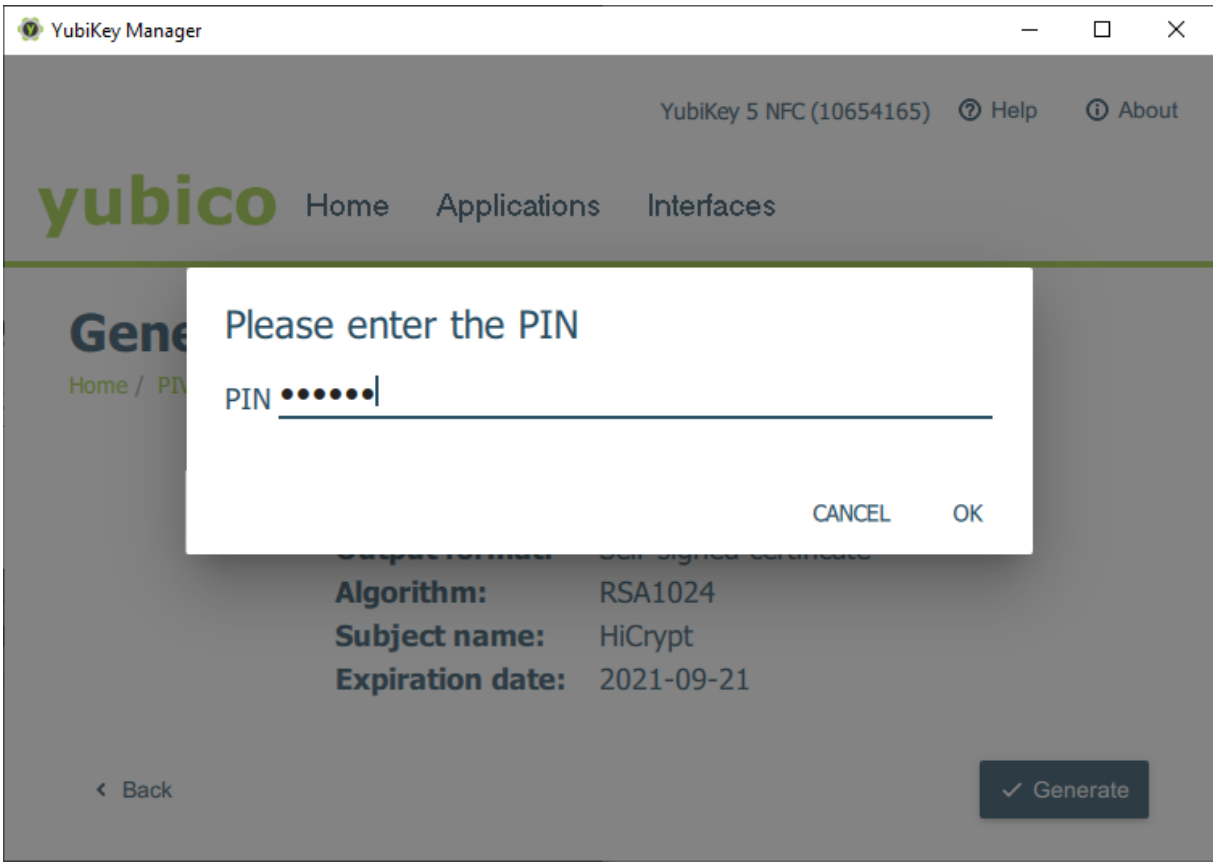
Benennen Sie den Schlüssel, der generiert werden soll und bestätigen Sie ihre Eingabe mit "Next".



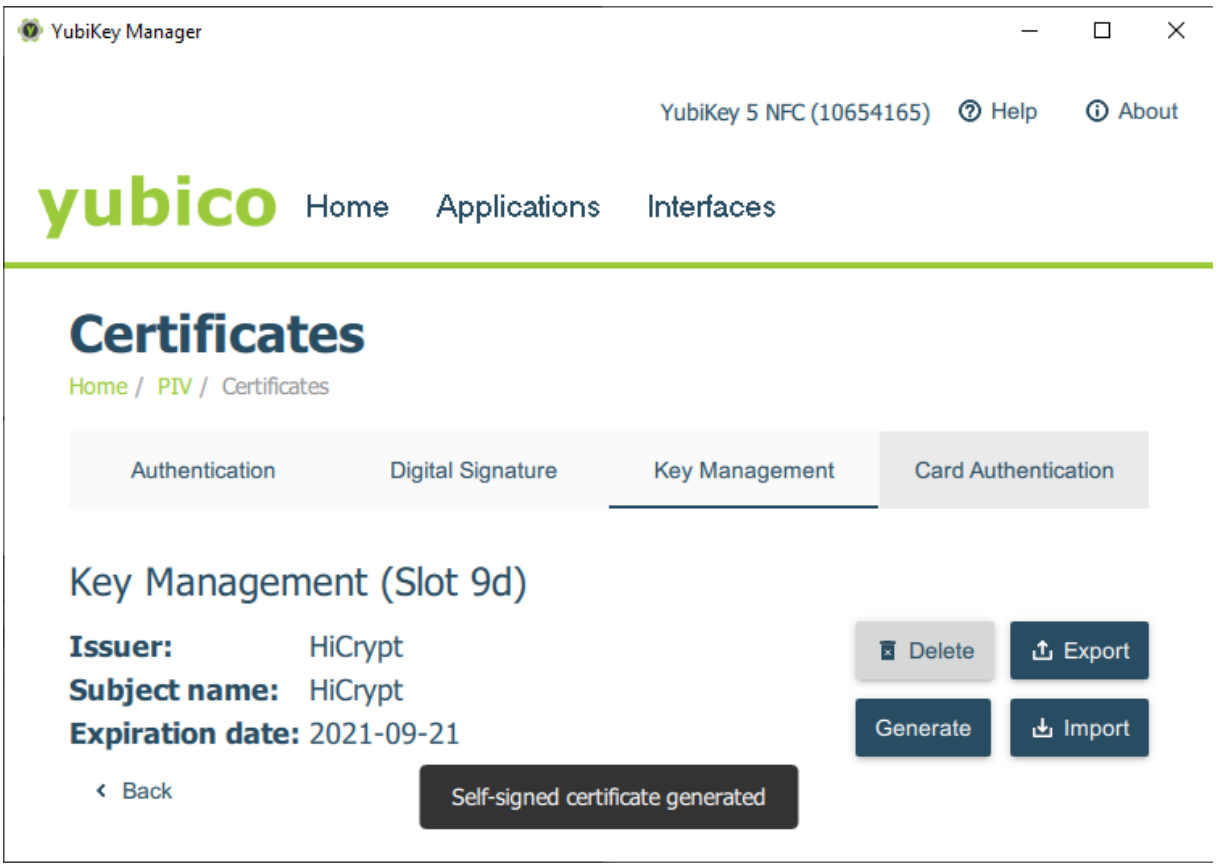
Wählen Sie ein Ablaufdatum für den Schlüssel. Derzeit hat dies keine Auswirkung auf die Nutzung des Schlüssels für die Anmeldung an einem mit HiCrypt™ verschlüsselten Laufwerk.



Wählen Sie in diesem Dialog "Use Default", um den standardmäßigen Management Schlüssel zu nutzen. Bestätigen Sie mit einem Klick auf "OK".



Geben Sie anschließend die PIN des YubiKey ein (Standard: 123456). Bestätigen Sie die Eingabe mit "OK".



Der Schlüssel wird nun generiert und nachfolgend in der Übersicht angezeigt. Zusätzlich finden Sie noch einmal den Namen und das Ablaufdatum. Über die Schaltflächen rechts kann der Schlüssel exportiert oder gelöscht werden.

Nachdem die Vorbereitung des YubiKey abgeschlossen ist, kann der Token über die HiCrypt™-Oberfläche für die Nutzung mit einem Benutzer vorbereitet und mit dem Konto verknüpft werden. Folgen Sie dafür den Hinweisen in der HiCrypt™-Dokumentation.