Advanced Card Systems Ltd.
Card & Reader Technologies

ACS FIDO Device Key Manager

User Manual V2.01

Subject to change without prior notice

info@acs.com.hk
www.acs.com.hk

Table of Contents

List of Figures

1.0. ACS FIDO Device Key Manager Background

The ACS FIDO Device Key Manager* represents a state-of-the-art solution meticulously designed for the effective management of ACS PocketKey Series devices. By seamlessly integrating three core functionalities, this device manager enhances operational efficiency and fortifies security for users harnessing the power of ACS PocketKey technology.

- ACS PocketKey FIDO Management
- ACS PocketKey OTP Tool
- ACS PocketKey PKI Management

The ACS FIDO Device Key Manager addresses the needs of today's users by merging comprehensive security capabilities with an intuitive interface. It stands as an essential tool for organizations striving to enhance their security landscape while delivering a superior user experience.

**The ACS FIDO Device Key Manager is available in English, Simplified Chinese, Spanish and Japanese*

1.1. OS Support

- Windows® & macOS

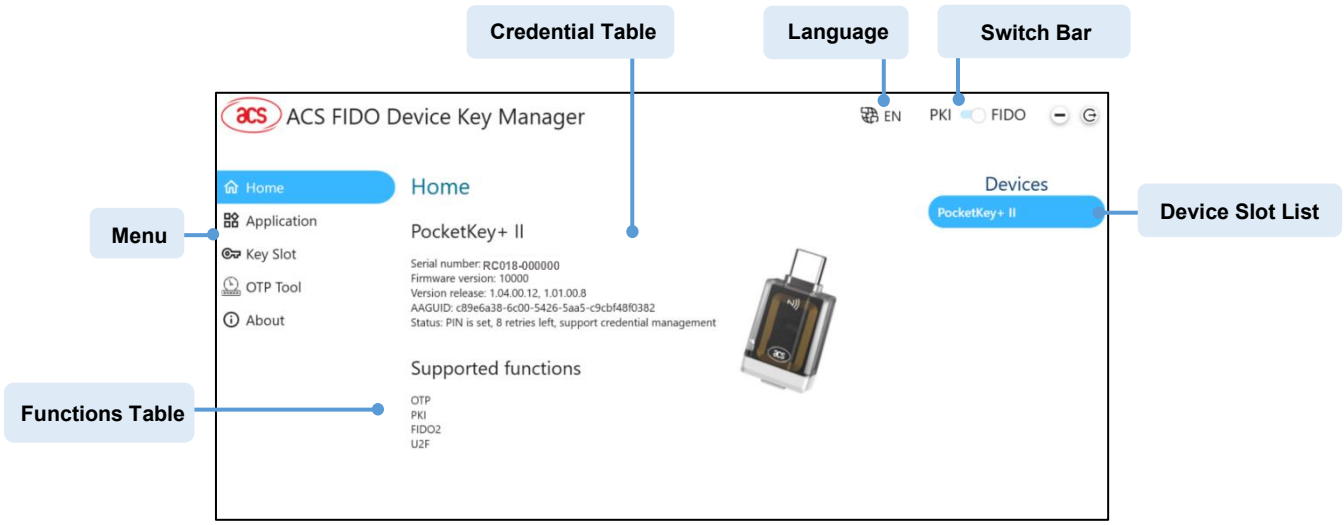


Figure 1: ACS FIDO Device Key Manager User Interface

1.2. Setup Multi-factor Authentication (MFA)

Before utilizing the ACS PocketKey series devices, it is essential to set up Multi-factor Authentication (MFA) across various platforms. Follow the instructions in the subsequent section to ensure seamless integration of this secure authentication device with your existing multi-factor authentication setups.

1.2.1. Microsoft(outlook)

1. Sign-in *Microsoft Account*
2. Go to *Security >> Advanced security options >> Additional security ->> Two-step verification*, Click *Turn on*
3. Click *Next*
4. If you haven't set another authentication method, you may add another authentication method by using an app, an alternate email address or a phone number
5. Click *Next*, then Click *Finish*

1.2.2. Google

1. Sign-in *Google Account*
2. Go to *Security >> How you sign in to Google >> 2-Step Verification*
3. Click Get started
4. If you haven't set another authentication method, you may add another authentication method by using a phone number, a security key or Google prompts.
5. Click *Done*

1.2.3. Yahoo

1. Sign-in *Yahoo Account*
2. Go to *Security >> How you sign in to Yahoo >> 2-step verification*, Click *Turn on*
3. If you haven't set another authentication method, you may add another authentication method by using Any Yahoo app, a phone number, an authenticator app or a security key
4. Click *Done*

1.2.4. Facebook

1. Sign-in *Meta Accounts Centre*
2. Go to *Password and security >> Two-factor authentication*, choose *Facebook account*
3. If you haven't set another authentication method, you may add another authentication method by using an authentication app, a phone number, or a security key.
4. Click *Done*

For more information on how to use PocketKey series to login on various platforms, please refer to the following demonstration video:

- *Facebook Account Sign-In Demo*
- *Google® Account Sign-In Demo*
- *Apple ID® and iCloud® Sign-In Demo*
- *Microsoft® Outlook™ Sign In Demo*

2.0. PocketKey FIDO Management Background

The ACS PocketKey series offers enhanced login flexibility through the integration of FIDO functionality and passwordless authentication. This section serves as a guide to teach you how to effectively manage your PocketKey(s), ensuring optimal performance and security.

2.1. FIDO2 Ecosystem

To better manage your security key, it is essential to understand the FIDO2 architecture and where the PocketKey(s) fits in. The following diagram illustrates the secure authentication flow:

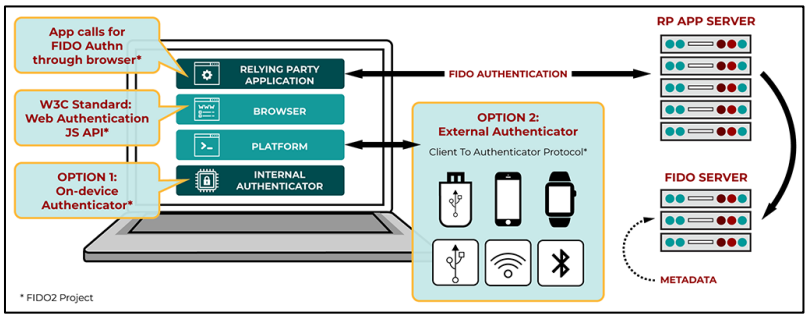


Figure 2: FIDO2 Ecosystem

2.2. Core Components of FIDO2

2.2.1. Passkey

The PocketKey acts as a secure hardware carrier for passkeys, allowing you to sign in to apps and websites without usernames or passwords. By storing these FIDO cryptographic credentials on a physical device, the PocketKey enables a faster, passwordless experience where sign-ins are approved through a simple PIN or biometric touch, ensuring your digital identity remains under your direct physical control.

2.2.2. CTAP2 (Client to Authenticator Protocol)

The PocketKey series functions as an External Authenticator by leveraging the CTAP2 (Client to Authenticator Protocol). This protocol allows the PocketKey to communicate with FIDO2-enabled browsers and operating systems to deliver a secure, passwordless, or multi-factor authentication experience.

2.2.3. CTAP1

PocketKey supports CTAP1 (formerly FIDO U2F) to provide a secure second-factor (2FA) authentication experience. This allows the PocketKey to work over USB or NFC with FIDO2-enabled browsers and operating systems that rely on the established U2F standard.

2.2.4. FIDO UAF

The PocketKey enables a passwordless experience within the UAF framework. It serves as a dedicated authenticator that allows users to log in through local verification—such as a PIN or biometrics—eliminating the need for traditional passwords while maintaining high security for both local and remote services.

2.3. Preparation

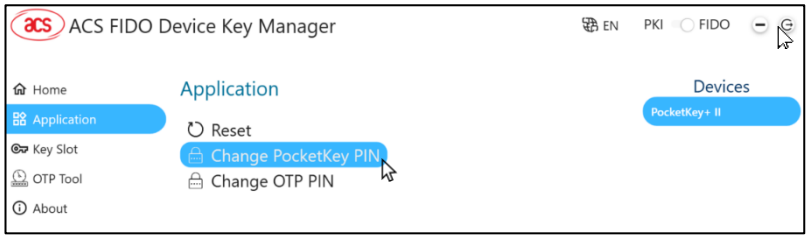
To register credentials, please visit the WebAuthn Specification website. You can also use Webauth.io to try creating credentials.

3.0. Get started with PocketKey FIDO Devices Manger

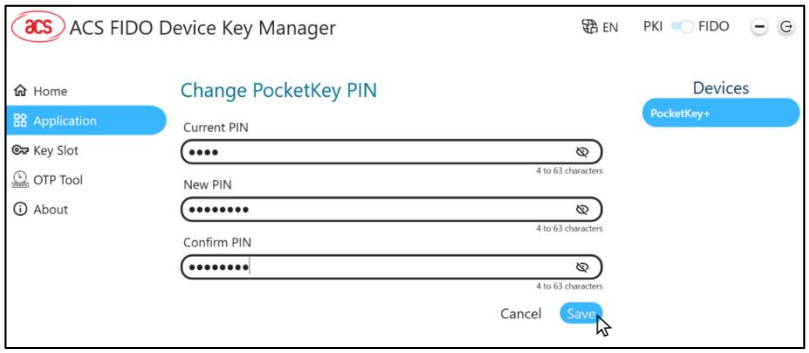
3.1. Change PocketKey PIN

To Change the PocketKey PIN:

1. Click the **Device** to select it.
2. Select **Application** and click **Change PocketKey PIN**.



3. Enter your **Current PIN**, then enter and verify your **New PIN**. Click **Save**.

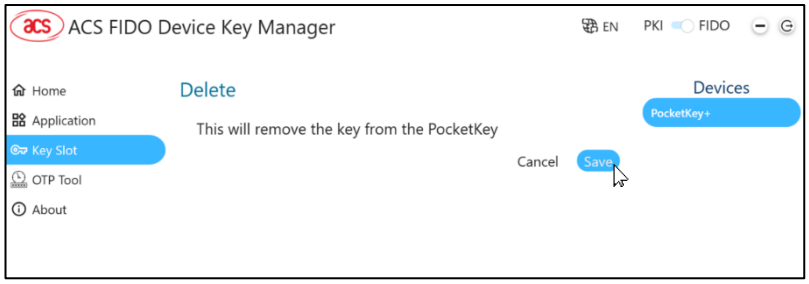


3.2. Delete Passkey Slot

To Delete the Passkey Slot:

1. Select **Key Slot**, and log in to your PocketKey device.
2. Click the checkbox(s) or **Select All** of slot(s) you wish to delete, then click **Delete**.

3. The Tool will confirm the deletion. Click **Save**.

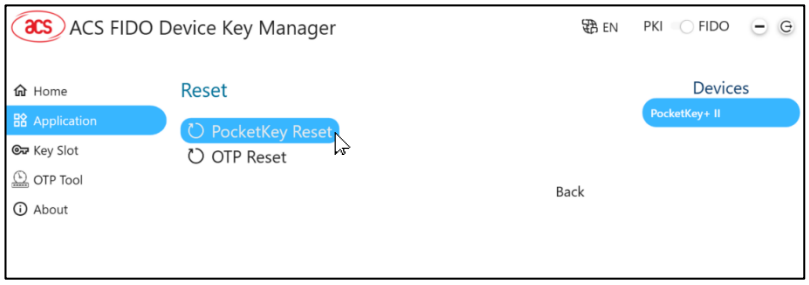


4. The deleted slot(s) will be removed from the slot list.

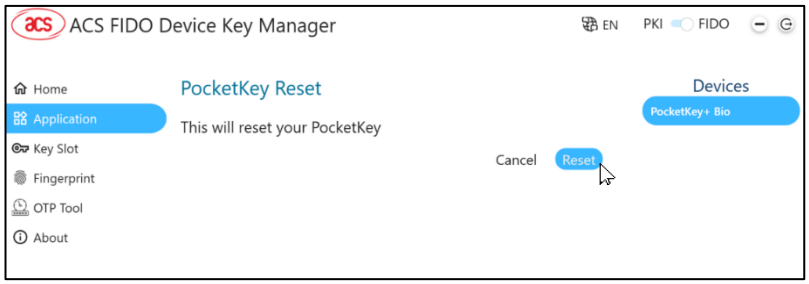
3.3. Reset PocketKey

To reset the PocketKey device:

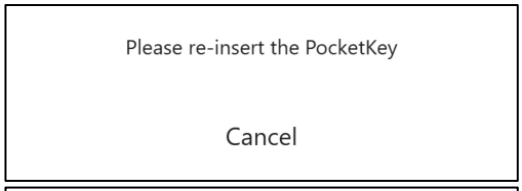
1. Click the **Device** to select it.
2. If you have one or more PocketKey(s), click the **Device Slot List** beside its name or their names to select the device(s).
3. Then click **Application**, select **Reset**, and enter to **PocketKey Reset**.

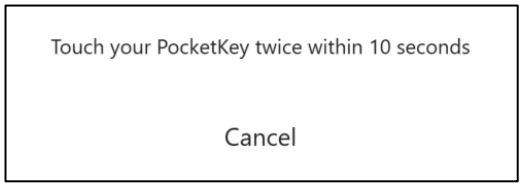


4. This may clean all data (Passkey & Fingerprint) and credentials from the PocketKey(s).



5. Follow the instructions to complete the reset process.





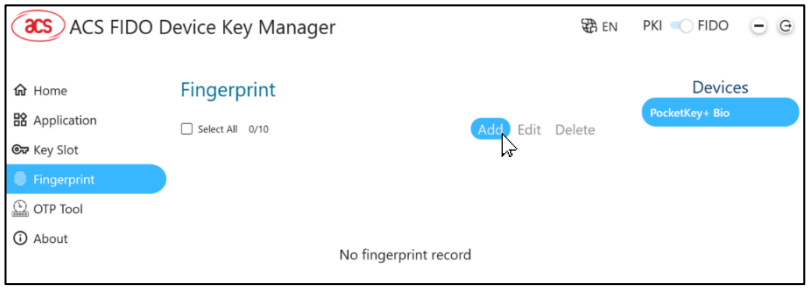
6. The Status will indicate if successful.

3.4. Add Fingerprint

The fingerprint function is only available in **PocketKey+ Bio**.

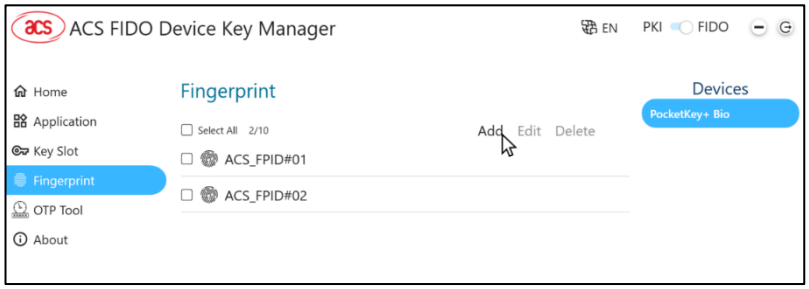
To add the Fingerprint:

1. Click the **Device*** to select it
2. Select **Fingerprint** and log in to the key.
3. Click **Add** on the **Fingerprint** interface.



4. Then **Press your finger to begin** the scan process

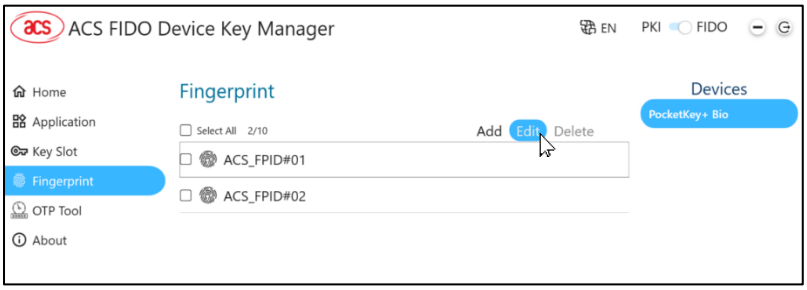
5. The fingerprint list will refresh to include the imported fingerprint(s).



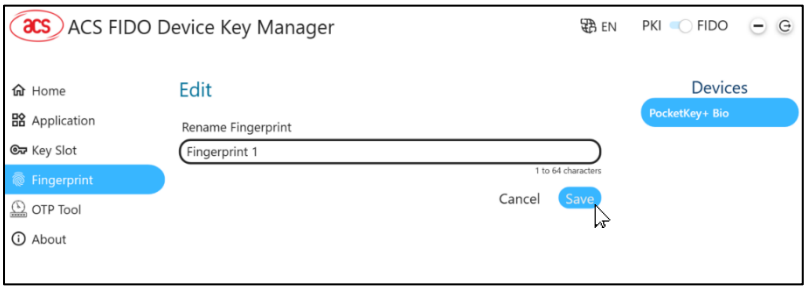
3.5. Edit Fingerprint

To edit the fingerprint

1. Select the fingerprint you want to edit, then press **Edit**.



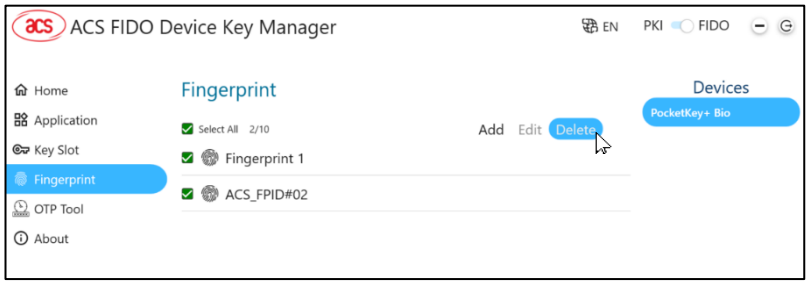
2. Type in your preferred name for the fingerprint(s), then **Save**.



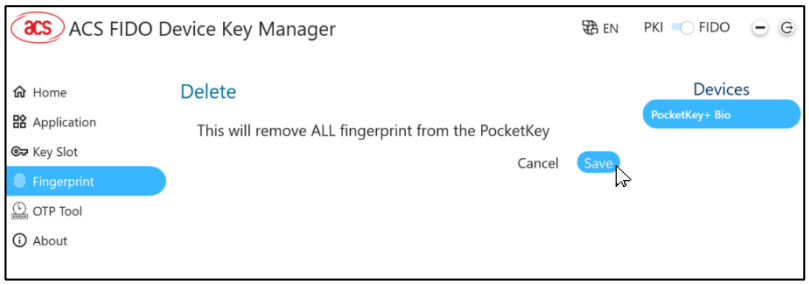
3.6. Delete Fingerprint

To delete one or more fingerprint(s):

1. Click the checkbox or **Select All** of fingerprint(s) you wish to delete, then click **Delete**.



2. Manager will confirm the deletion. Click **Save**.



3. The deleted fingerprint(s) will be removed from the fingerprint list.

4.0. ACS PocketKey OTP Authenticator Background

ACS PocketKey series combine FIDO functionality with the versatility of One-Time Password (OTP) for login flexibility. This section serves as a guide to introduce the OTP tool and its setup for secure login procedures, providing users with a seamless authentication experience that blends advanced security features with user-friendly authentication options.

Note: *For PocketKey USB token, Firmware 1.00.00.15 or above is required to enable OTP function.*

4.1. HOTP: Event-based One-Time Password

Event-based OTP (also called HOTP meaning HMAC-based One-Time Password) is the original One-Time Password algorithm and relies on two pieces of information. The first is the secret key, called the "seed", which is known only by the token and the server that validates submitted OTP codes. The second piece of information is the moving factor which, in event-based OTP, is a counter. The counter is stored in the token and on the server. The counter in the token increments when the button on the token is pressed, while the counter on the server is incremented only when an OTP is successfully validated.

To calculate an OTP the token feeds the counter into the HMAC algorithm using the token seed as the key. HOTP uses the SHA-1 hash function in the HMAC. This produces a 160-bit value which is then reduced down to the 6 (or 8) decimal digits displayed by the token.

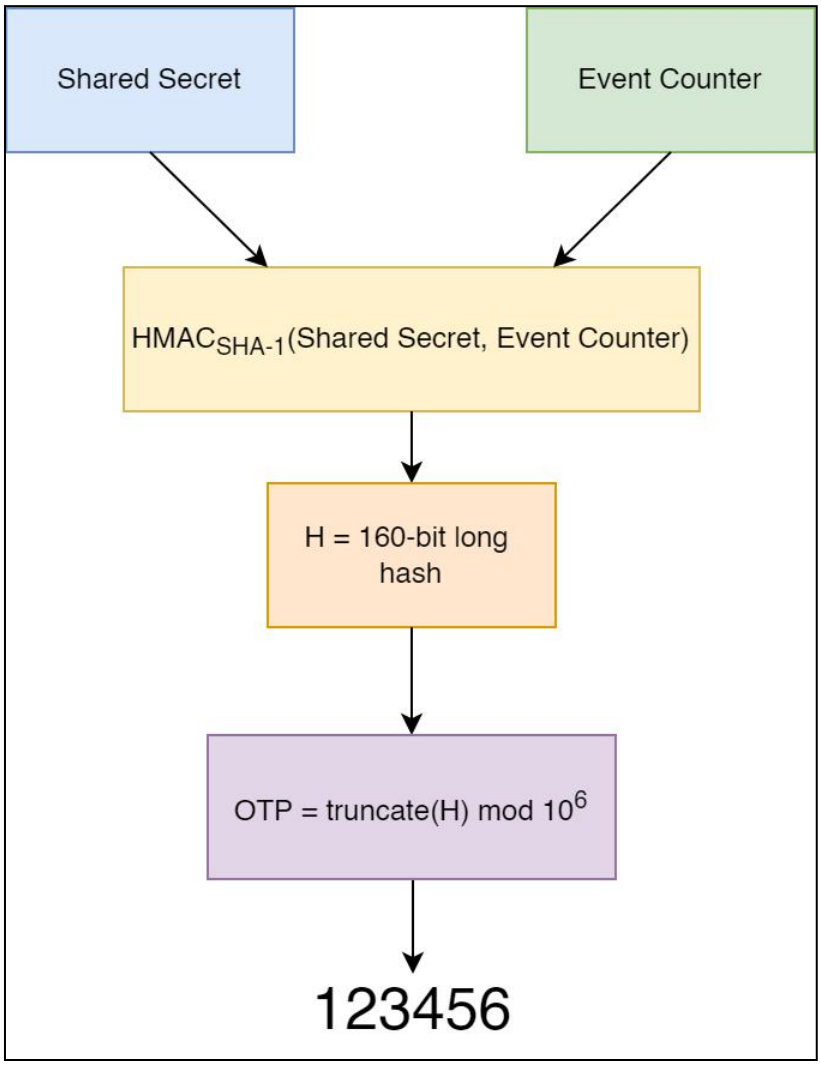


Figure 3: HOTP

4.2. TOTP: Time-based One-Time Password

Time-based OTP (TOTP for short), is based on HOTP but where the moving factor is time instead of the counter. TOTP uses time in increments called the timestep, which is usually 30 or 60 seconds. This means that each OTP is valid for the duration of the timestep.

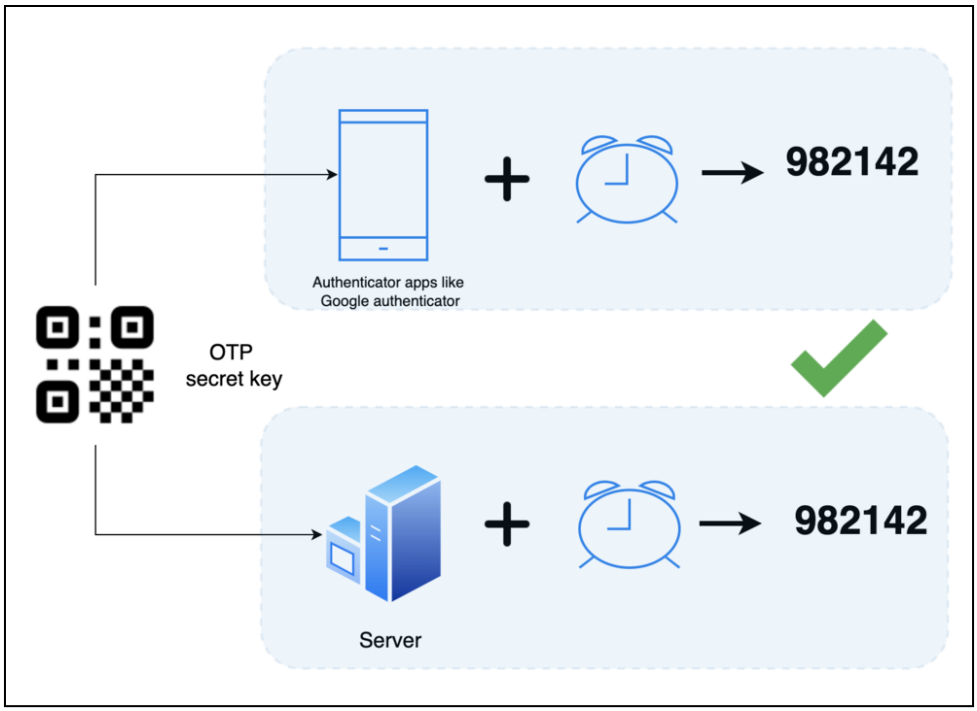


Figure 4: TOTP

5.0. PocketKey OTP Tool

OTP Tool is designed to be a simple management tool used for ACS FIDO PocketKey series. This tool mainly provides 2 functions, one is protocol management of multi-functional security keys; the other is to manage the optional OATH HOTP function.

5.1. Preparation

Before using the OTP tool, it is crucial to install and launch the ACS FIDO Device Key Manager. After selecting the PocketKey from the “Devices” slot list, clicking on "OTP Tool" will take you to the User Interface, enabling you to effectively manage and optimize your FIDO PocketKey devices.

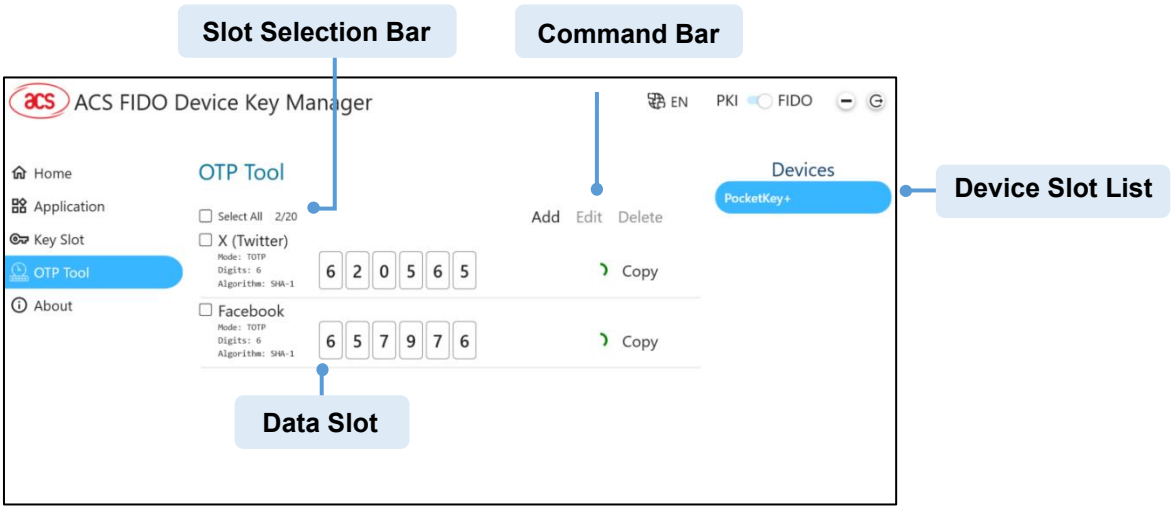


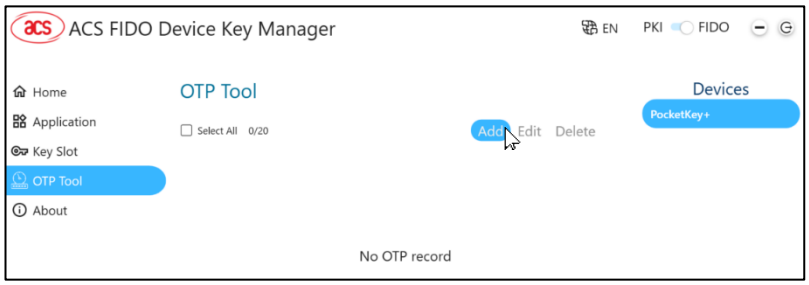
Figure 5: PocketKey OTP Tool User Interface

6.0. Get started with Pocketkey OTP Tool

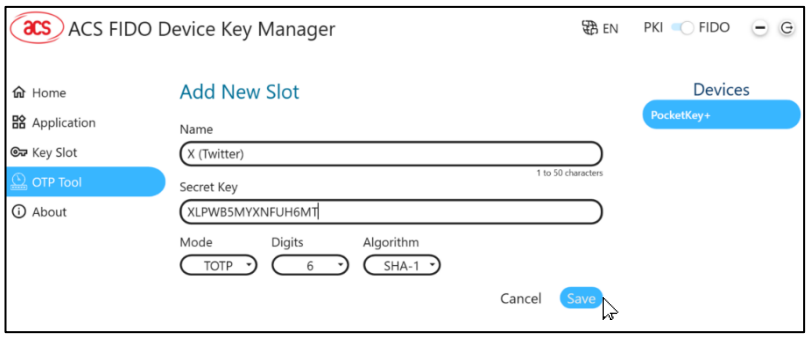
6.1. Add OTP

To add the OTP slot(s):

1. Log in to OTP Tool.
   Default PIN: 00000000
2. Click **Add** on the OTP interface.



3. Enter the Slot information, and Save

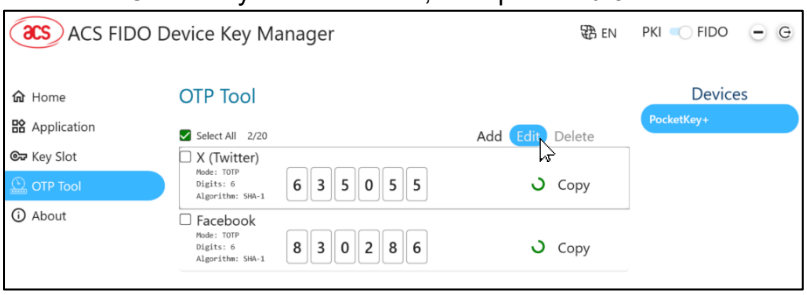


4. Wait while the slot(s) is added.
5. The Slot list will refresh to include the added slot(s).

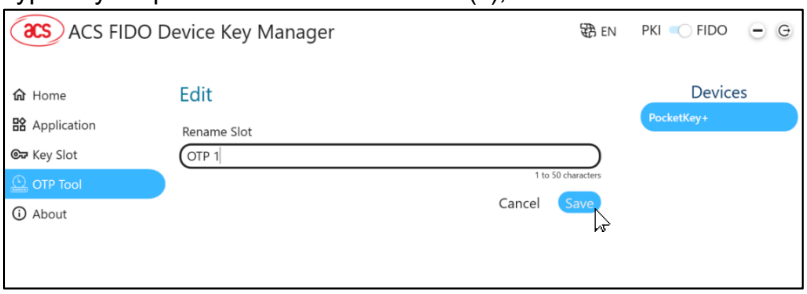
6.2. Edit OTP

To edit the OTP name

1. Select the OTP slot you want to edit, then press **Edit**.



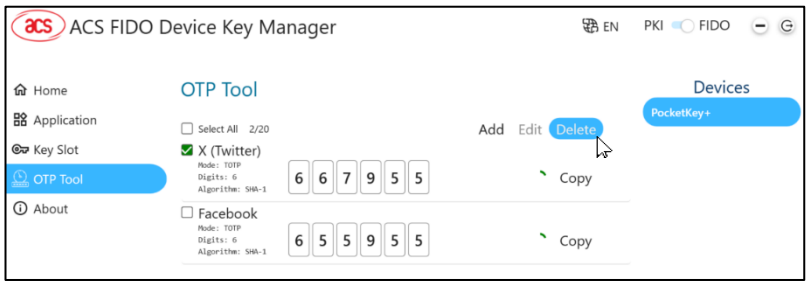
2. Type in your preferred name for the slot(s), then **Save**.



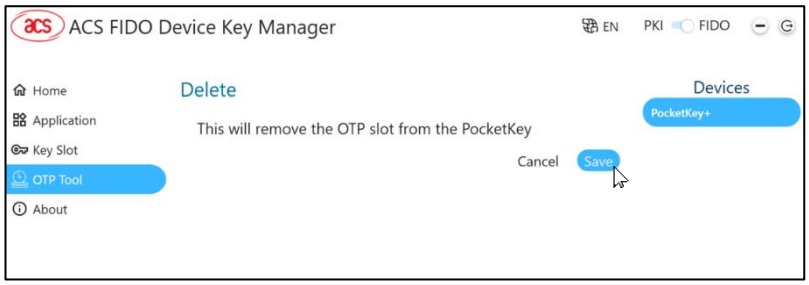
6.3. Delete OTP

Delete the OTP Slot(s):

1. Click the checkbox(s) or **Select All** of slot(s) you wish to delete, then click **Delete**.



2. The Tool will confirm the deletion. Click **Save**.

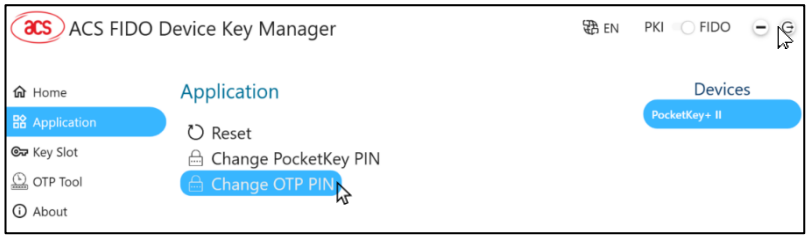


3. The deleted slot(s) will be removed from the slot list.

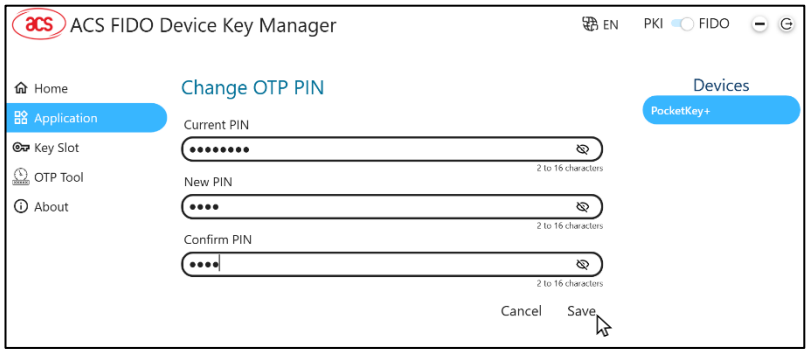
6.4. Change OTP PIN

To Change the OTP PIN:

1. Click the **Device** to select it.
2. Select **Application** and click **Change OTP PIN**.



3. Enter your **Current PIN***, then enter and verify your **New PIN**. Click **Save**.

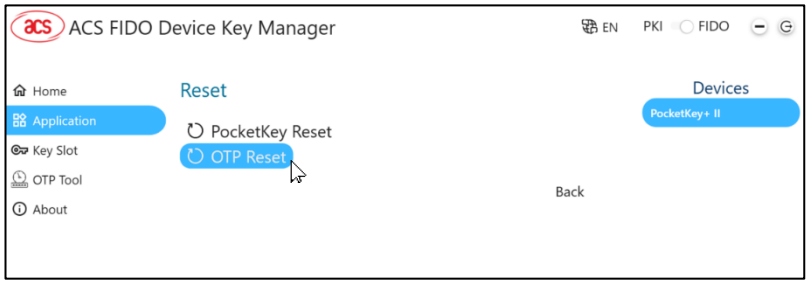


Default PIN: *00000000*

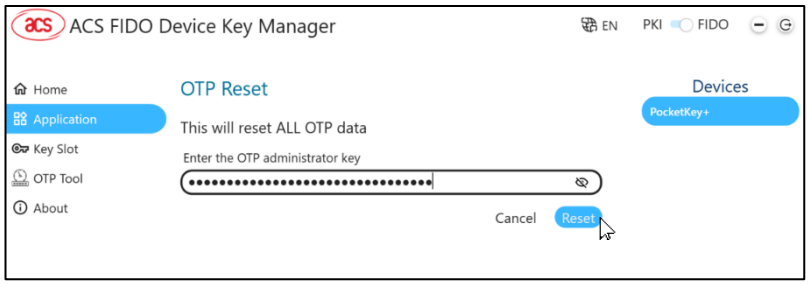
6.5. OTP Reset

To Rest the OTP:

1. Connect the token(s) to your system. Wait while Tool loads the token(s).
2. If you have one or more blank or initialized token(s), click the **Device Slot List** beside its name or their names to select the token(s).
3. Then click **Application**, select **Reset**, and enter to **OTP Rest**.



4. Enter the Admin key to restore the OTP Tool to factory default, this may clean all OTP slots' data and restore PIN to default.



Admin key: *5B1D11969B22F10CD4004ACA30DE99E3*

5. The Status will indicate if successful

7.0. ACS PocketKey PKI Management Page Background

ACS PocketKey PKI Management Page is a secure and easy-to-use manager that enables administrators in a public-key infrastructure (PKI) system to prepare and manage the cards and tokens of their standard users.

- Certificate Manager: This application helps you manage the digital certificates stored in PocketKey.
- Initialization Manager: This application helps you initialize PocketKey that will be issued to end-users.

7.1. Preparation

Switch to "PKI" on the right side and will take you to the PKI User Interface, enabling you to effectively manage and optimize your devices.*

Note: *For PocketKey series devices, the PKI Tool is only supported on the PocketKey+ II.*

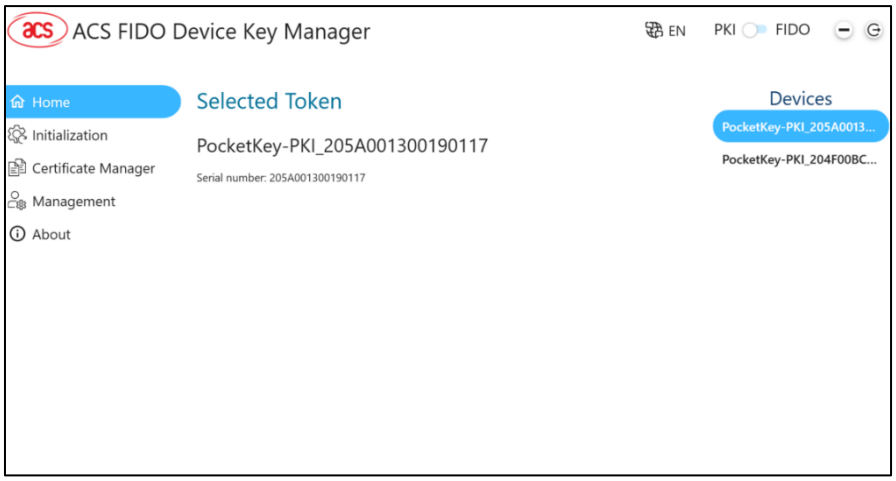


Figure 6: ACS FIDO Device Key Manager

7.2. Token Classification

ACS FIDO Device Key Manager identifies token(s) as one of the following:

- **Initialized Token** - CM will display the token's given name, such as "PocketKey-PKI." You can install certificates on this token and manage it using CM.
- **Blank Token** - A blank token. You cannot install certificates on this token as it is. Contact your Administrator to have this token initialized.
- **Unknown Token** - A token that may have been initialized using other applications. You cannot install certificates on this token as it is. Contact your Administrator to have this token re-initialized.
- **Unrecognized Token** - This means that CM failed to load all the token's details. Remove the token then re-insert it properly.

8.0. Get started with Certificate Manager

8.1. Quick Start Guide

Certificate Manager (CM) is an application developed by Advanced Card Systems Ltd. It allows you to easily manage your digital certificates for use in various PKI applications (e.g., encrypting or decrypting documents). Through this manager, you can view your certificates, as well as export, add or delete existing ones.

This help file will use the term "Token" to refer to the PocketKey series devices.

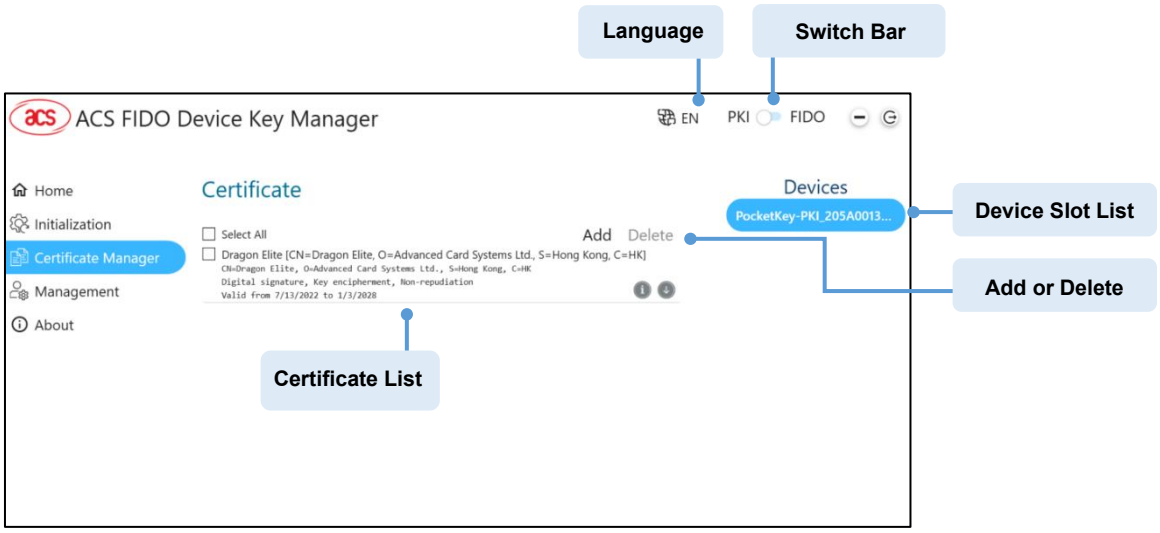


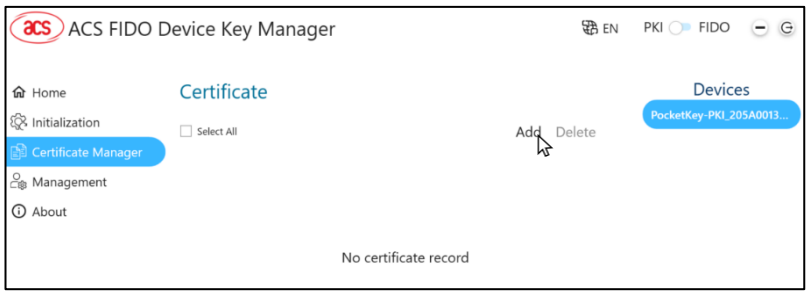
Figure 7: Certificate Manager User Interface

8.2. Import certificate

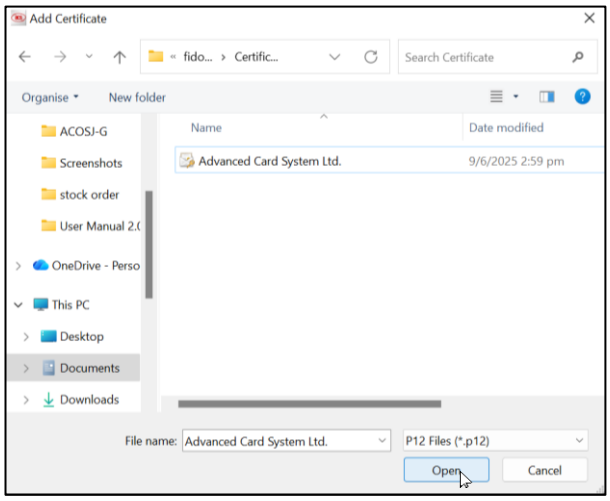
CM can import certificates that are in .p12 and .pfx file format.

To import certificate(s):

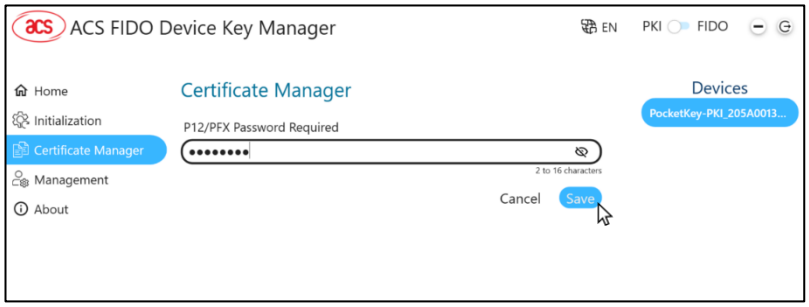
1. Log in to your token.
2. Click **Add** on the CM interface.



3. Locate the certificate(s) you wish to import, then click Open. You may have to click the file type dropdown menu beside the file name field and choose the correct file type to make the certificate(s) visible.

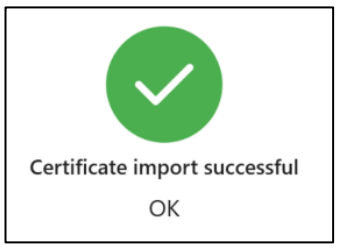


4. If the certificate has a password, type in the password then click **Save**.



When loading a certificate, the Manager will automatically detect and prompt you to install the **Root Certificate**. Please select the required items as needed.

5. Wait while the certificate is imported.



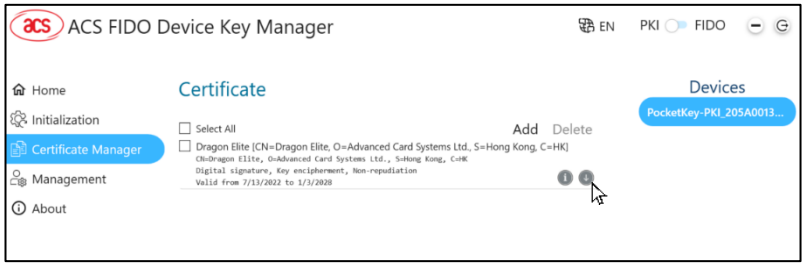
6. The certificate list will refresh to include the imported certificate(s).

8.3. Export certificate

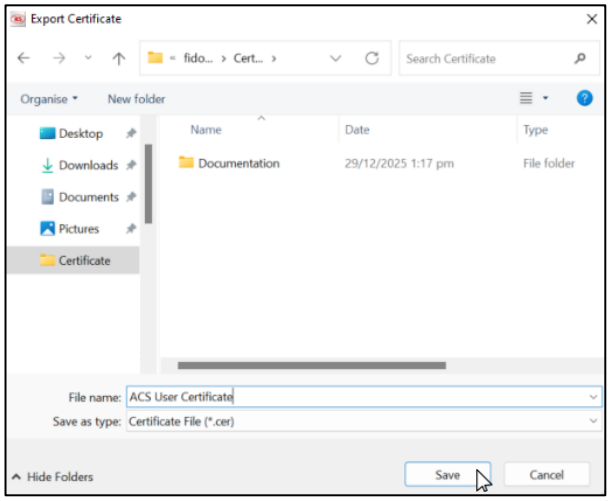
CM can export certificates as .cer files.

To export a certificate:

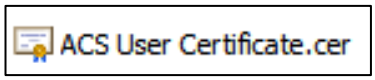
1. Click the icon on the lower-right portion of the certificate's name.



2. Navigate to your preferred destination folder, then click **Save**.



3. The certificate will be exported as a .cer file.

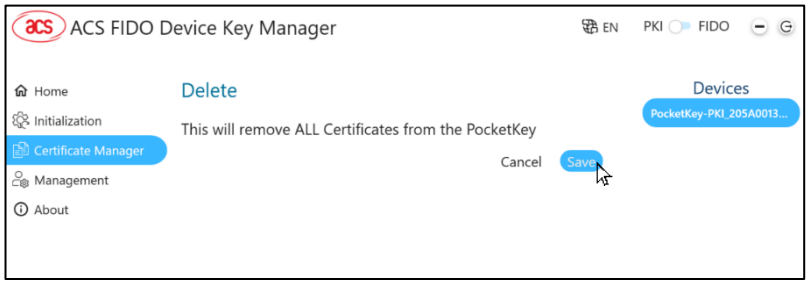


8.4. Delete certificate

To delete one or more certificates:

4. Click the checkbox or **Select All** of certificate(s) you wish to delete, then click **Delete**.

5. CM will confirm the deletion. Click **Save**.

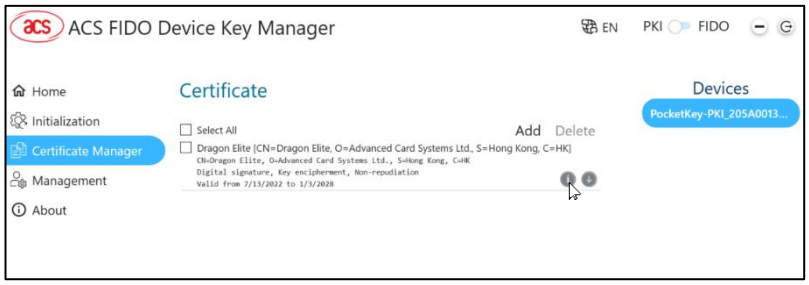


6. The deleted certificate(s) will be removed from the certificate list.

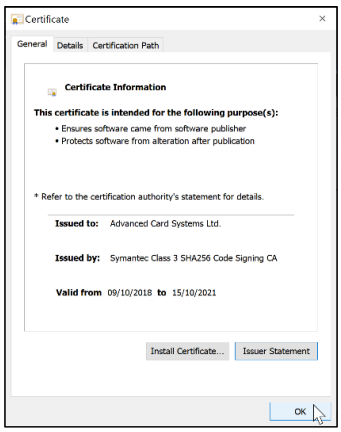
8.5. View certificate details

To view the details of a certificate:

1. Click the ⓘ icon on the lower right portion of the certificate's name.



2. The Certificate window will appear.

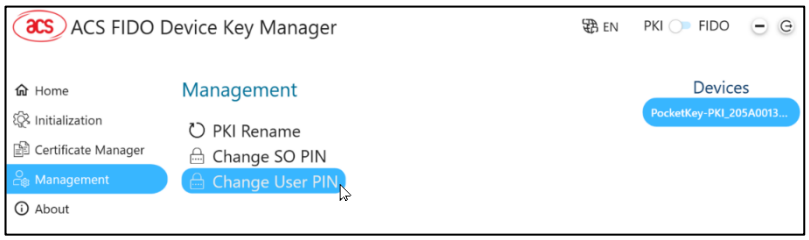


8.6. Change User PIN

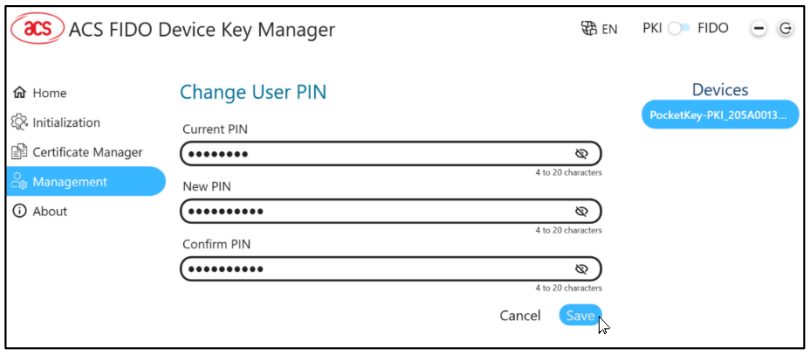
To change the User PIN:

4. Click the token's name to select it.

5. Select **Management** and click **Change User PIN**.



6. Enter your current PIN, then enter and verify your new PIN. Click **Save**.



9.0. Get started with Initialization Manager

9.1. Quick Start Guide

Initialization Manager (IM) is an application developed by Advanced Card Systems Ltd. It is designed for the use of Certificate Authorities, Security Officers, or Administrators to prepare and customize tokens for their intended end-users.

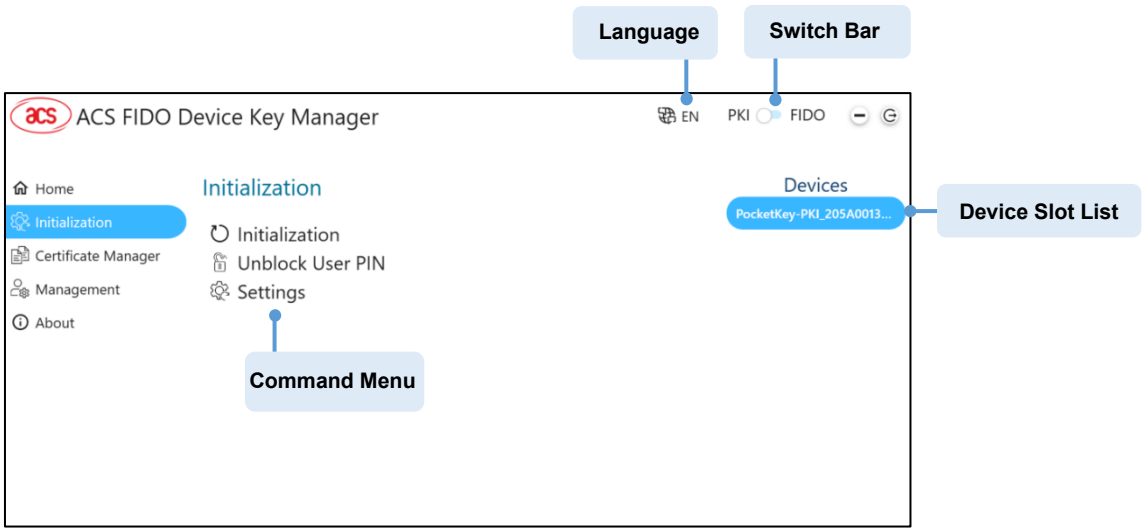
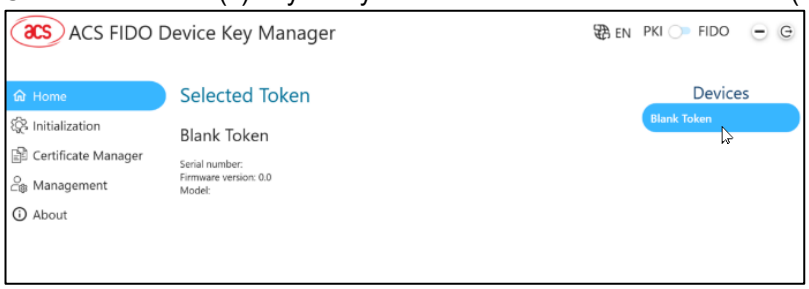


Figure 8: Initialization Manager User Interface

9.2. Initialize Token

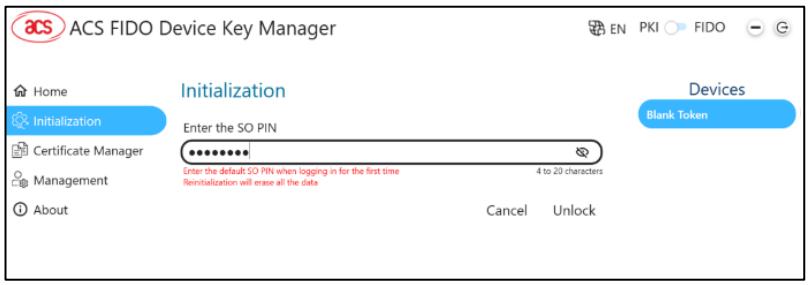
To initialize tokens:

1. Connect the token(s) to your system. Wait while IM loads the token(s).

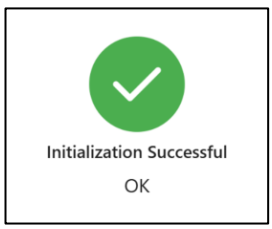


2. If you have one or more blank or initialized token(s), click the **Device Slot List** beside its name or their names to select the token(s).
3. Then click **Initialization**.

If you are re-initializing initialized tokens, a warning sign will display and ask you to enter the SO PIN for each previously initialized token before you can proceed with initialization.



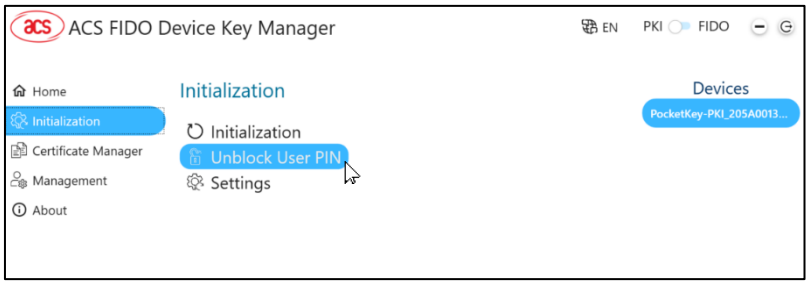
4. Wait while IM initializes the token(s).
   IMPORTANT: *Do not remove the token(s) from your system during initialization.*
5. The Status will indicate if the initialization was successful.



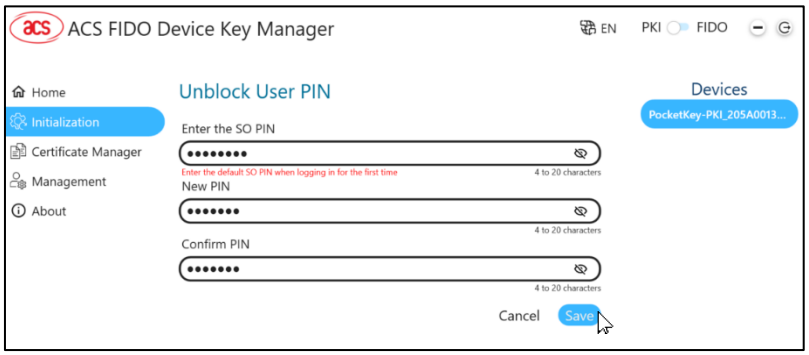
9.3. Unblock User PIN

The User PIN will be blocked if the user enters the incorrect value beyond the permitted number of retries. To unblock a User PIN:

1. Connect the token(s) to your system. Wait while IM loads the token(s).
2. Click **Unblock User PIN**.



3. Type in the SO PIN and a new User PIN in the window that appears. Click **Save**.



4. Wait while IM unblocks the User PIN.
5. The Status will show if the User PIN was successfully unblocked.

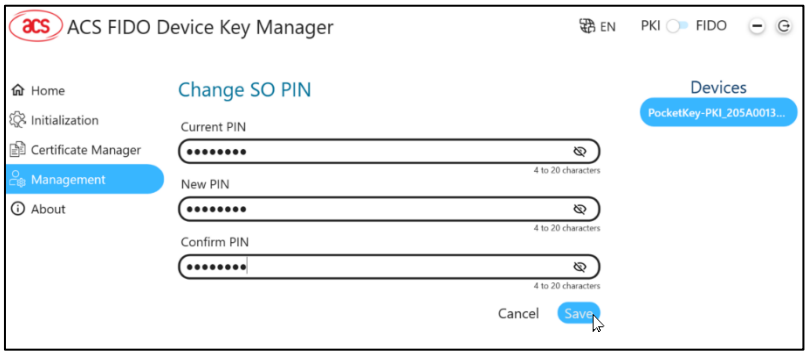
9.4. Change SO PIN/SO Key

The **SO (Security Officer) PIN/Key** is also known as the **PIN Unblocking Key (PUK)**. It is used to set a new User PIN if the current one has been blocked, which happens when the incorrect User PIN was entered beyond the permitted number of retries.

To change the SO PIN/SO Key:

1. Connect the token(s) to your system. Wait while IM loads the token(s).
2. Select **Management** and click **Change SO PIN**.

3. Enter your current PIN, then enter and verify your new PIN. Click **Save**.



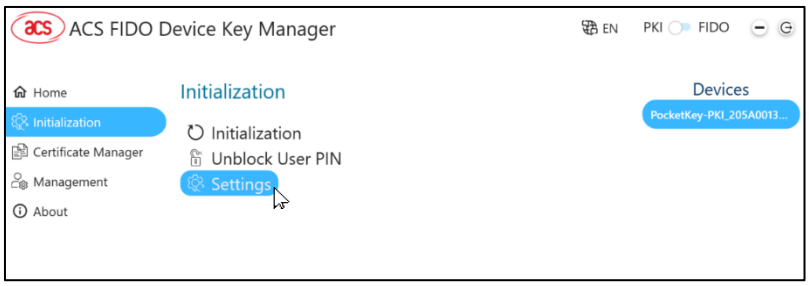
10.0. Change Application Settings

You can change or enable certain settings that affect how CM/IM behaves.

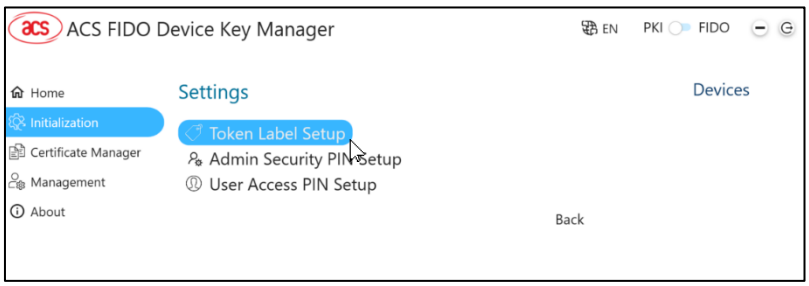
10.1. Customize Token Settings

To customize token settings:

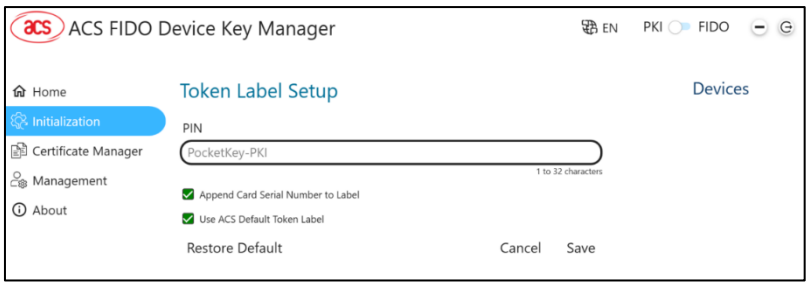
1. Connect the token(s) to your system, Wait while IM loads the token(s).
2. On the IM interface, click **Settings**



3. In the **Settings** interface, click the **Table Label Setup** tab.



4. Under Token Label, type in your preferred name for tokens. If you will be creating multiple tokens, this label will be applied to all tokens.



You can customize the token label with the following options, both of which are enabled by default:

- Append Card Serial Number to Label
- Use ACS Default Token Label (ACOS5-EVO/ PocketKey-PKI)

Appending the card's serial number will result in a much longer label. But it will make the card easier to identify, especially if there are multiple cards connected to the PC.

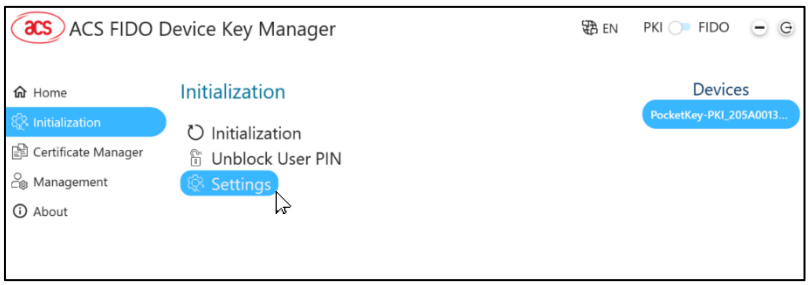
5. Click **Save**.
6. To set the properties back to their default values, click **Restore Default**.

10.2. Change Default SO PIN/SO Key

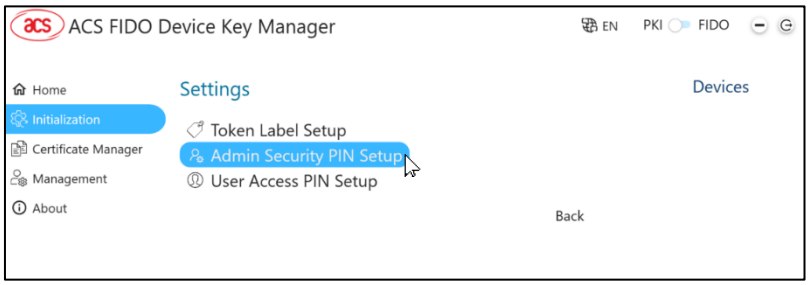
You can change the default SO PIN or SO Key in the Settings menu.

To change the default SO PIN:

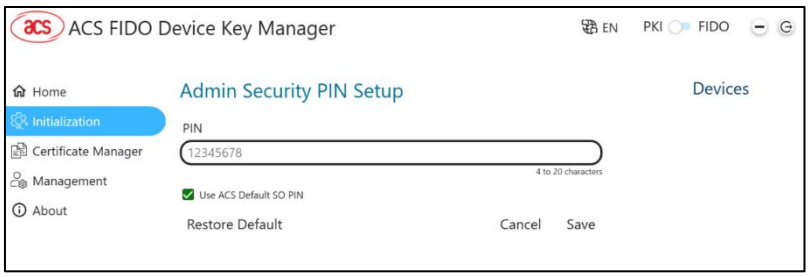
1. Connect the token(s) to your system, Wait while IM loads the token(s).
2. On the IM interface, click **Settings**.



3. Click the **Admin Security PIN Setup** tab.



4. Under SO PIN/Key Settings, enter your preferred default PIN value.
   The "Use ACS Default SO PIN" option is enabled by default. It sets the default PIN to **12345678**.

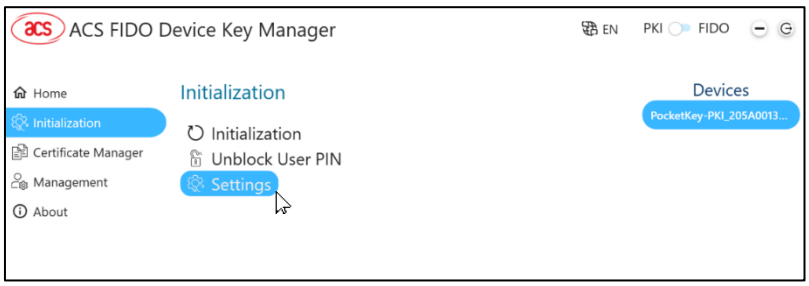


5. Click **Save**.
6. To set the properties back to their default values, click **Restore Default**.

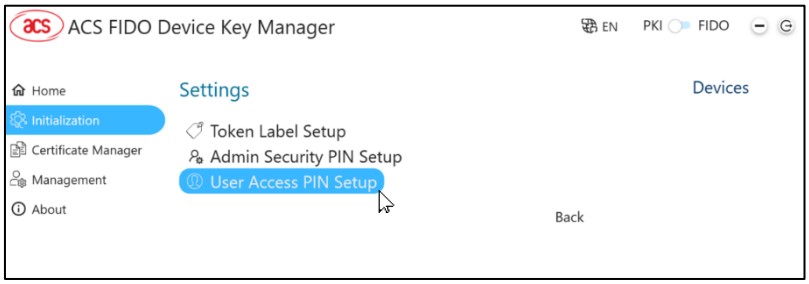
10.3. Customize Token Settings

To customize the User PIN settings:

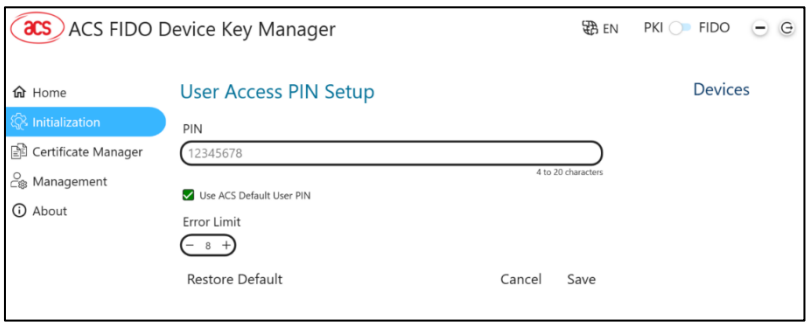
1. Connect the token(s) to your system, Wait while IM loads the token(s).
2. On the IM interface, click **Settings**.



3. Click the **Access PIN Setup** tab.



4. Under User PIN Value, type in your preferred default User PIN.
   The "Use ACS Default User PIN" option is enabled by default. It sets the default PIN to **12345678**.

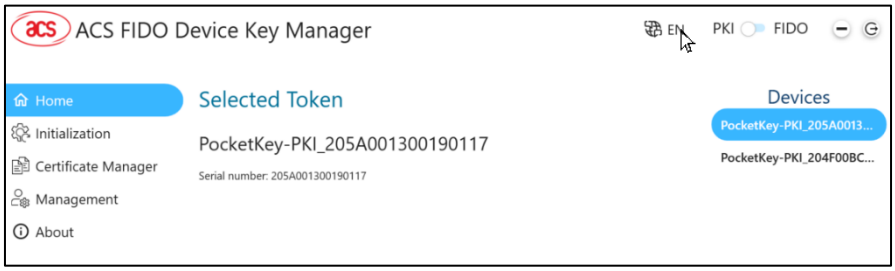


5. Under User PIN Attributes, set your preferred error limit. This specifies the maximum number of failed user PIN entries before the user is locked out.
6. Click **Save**.
7. To set the properties back to their default values, click **Restore Default**.

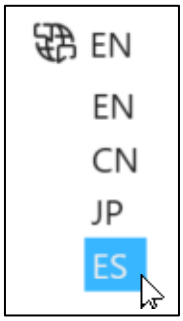
11.0. Change application language

To change the language:

1. On the ACS FIDO Device Key Manager interface, click icon.



2. Select your preferred language.



3. The interface will be displayed in your selected language.