Advanced Card Systems Ltd.
Card & Reader Technologies

ACS FIDO 设备密钥管理器
（ACS FIDO Device Key Manager）

用户手册 V2.01

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

目录

图目录

1.0. ACS FIDO 设备密钥管理器概览

ACS FIDO 设备密钥管理器（ACS FIDO Device Key Manager）*作为一款前沿解决方案，专为有效管理 ACS PocketKey 系列设备而精心设计。该设备管理器通过无缝集成三大核心功能，提升了用户利用 ACS PocketKey 技术的操作效率，并强化了安全性。

- ACS PocketKey FIDO 管理（PocketKey FIDO Management）
- ACS PocketKey OTP 工具（PocketKey OTP Tool）
- ACS PocketKey PKI 管理（ACS PocketKey PKI Management）

ACS FIDO 设备密钥管理器将各类安全功能与直观易用的界面相结合，精准满足当今用户的需求。对于力求提升安全水平，同时追求卓越用户体验的组织和机构而言，是一款必备工具。

**ACS FIDO 设备密钥管理器提供英语、简体中文、西班牙语和日语版本。*

1.1. 支持的操作系统

- Windows® & macOS

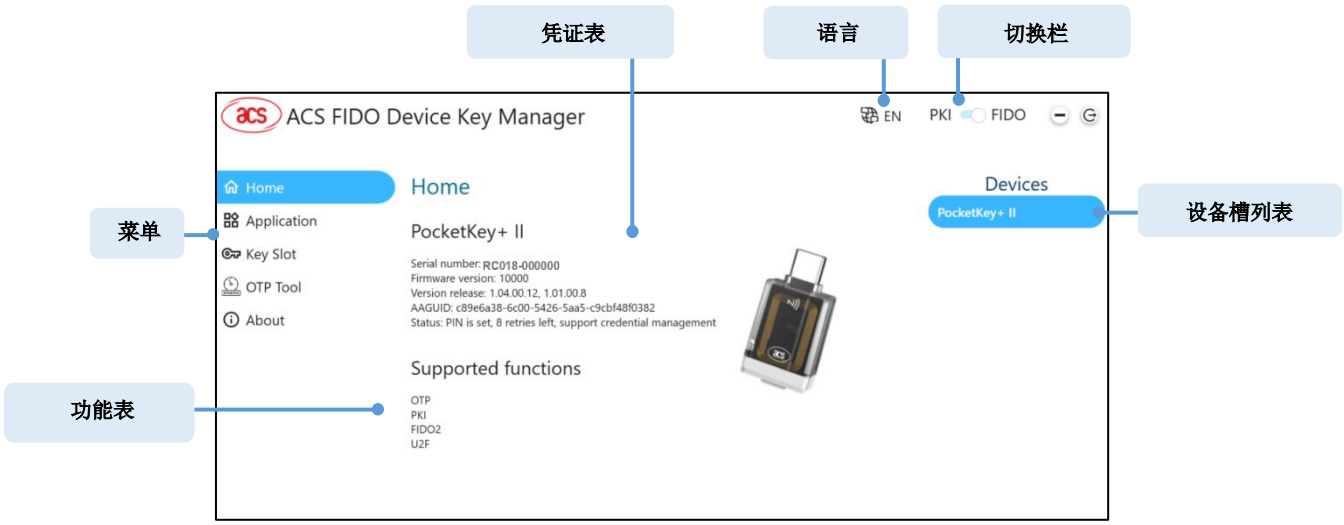


图 1：ACS FIDO 设备密钥管理器用户界面

1.2. 设置多重身份验证（MFA）

在使用 ACS PocketKey 系列设备前，需要先在各个平台配置好多重身份验证（MFA）。请依照后续章节进行操作，以确保该安全设备能无缝集成到现有多重身份验证体系中。

1.2.1. Microsoft(outlook)

1. 登录 *Microsoft 账户*
2. 前往 **Security >> Advanced security options >> Additional security ->> Two-step verification**，点击 **Turn on**
3. 单击 **Next**
4. 若尚未设置其它验证方式，可以通过 APP、其它电子邮箱地址或电话号码进行添加。
5. 点击 **Next**，然后点击 **Finish**

1.2.2. Google

1. 登录 *Google 账户*
2. 前往 **Security >> How you sign in to Google >> 2-Step Verification**
3. 点击 **Get started**
4. 若尚未设置其它验证方式，可以通过电话号码、安全密钥或谷歌提示进行添加。
5. 点击 **Done**

1.2.3. Yahoo

1. 登录 *Yahoo 账户*
2. 前往 **Security >> How you sign in to Yahoo >> 2-step verification**，点击 **Turn on**
3. 若尚未设置其它验证方式，可以通过雅虎应用、电话号码、身份验证器应用或安全密钥进行添加。
4. 点击 **Done**

1.2.4. Facebook

1. 登录 *Meta 账户中心*
2. 前往 **Password and security >> Two-factor authentication**，选择 **Facebook account**
3. 若尚未设置其它验证方式，可以通过身份验证应用、电话号码或安全密钥进行添加。
4. 点击 **Done**

关于如何使用 PocketKey 系列产品登录各个平台的更多信息，请参考下面的演示视频：

- *Facebook 账户登录演示*
- *Google® 账户登录演示*
- *Apple ID® 和 iCloud® 登录演示*
- *Microsoft® Outlook™ 登录演示*

2.0. PocketKey FIDO 管理概览

ACS 的 PocketKey 系列产品通过集成 FIDO 功能与无密码认证方式，提供一种更灵活的登录体验。本节作为使用指南，将介绍如何有效管理 PocketKey 设备，以确保实现最佳的性能和安全性。

2.1. FIDO2 生态系统

为了更好地管理安全密钥，有必要充分了解 FIDO2 架构以及 PocketKey 在体系中的适配定位。下面是安全身份验证的流程示意图：

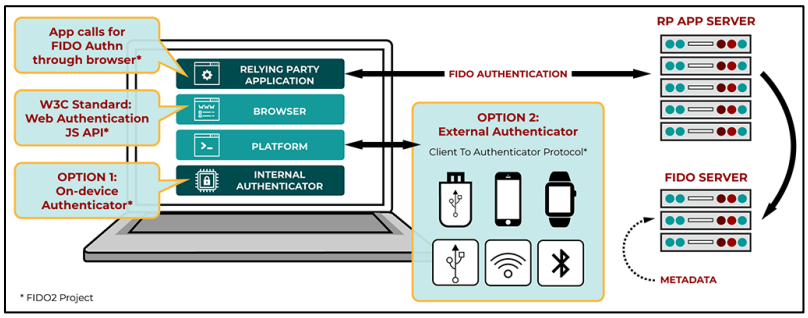


图 2: FIDO2 生态系统

2.2. FIDO2 核心组件

2.2.1. 通行密钥（Passkey）

PocketKey 作为通行密钥（Passkey）的安全硬件载体，使您无需用户名或密码即可登录应用和网站。通过将 FIDO 加密凭证存储在实体设备当中，PocketKey 可实现更快速的无密码体验。用户仅需通过简单的 PIN 码或生物识别触控即可完成登录授权，确保个人数字身份始终在本人的直接物理控制之下。

2.2.2. CTAP2（客户端到验证器协议）

PocketKey 系列产品作为外部身份验证器，基于 CTAP2（客户端到验证器协议）运行。该协议使 PocketKey 能够与支持 FIDO2 的浏览器及操作系统进行通信，从而实现安全的无密码或多因素身份验证体验。

2.2.3. CTAP1

PocketKey 支持 CTAP1（原 FIDO U2F 协议），可提供安全的第二因素（2FA）身份验证体验。因此，PocketKey 能够通过 USB 或 NFC，与依赖现有 U2F 标准并支持 FIDO2 的浏览器及操作系统协同工作。

2.2.4. FIDO UAF

PocketKey 在 UAF 框架内提供无密码登录体验。作为专用身份验证器，PocketKey 支持用户通过本地验证（如 PIN 码或生物识别信息）完成登录，在摒弃传统密码的同时，确保本地及远程服务的高安全性。

2.3. 准备工作

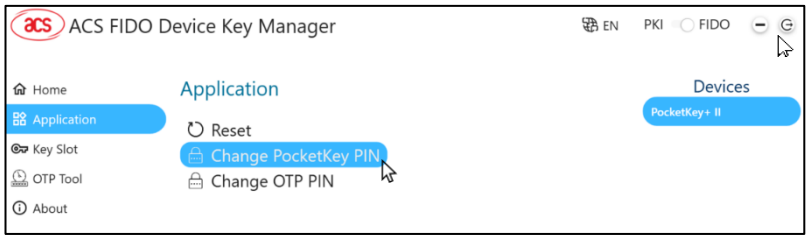
如需注册凭证，请访问 WebAuthn 规范网站。也可以通过 Webauth.io 来尝试创建。

3.0. 使用 PocketKey FIDO 设备管理器

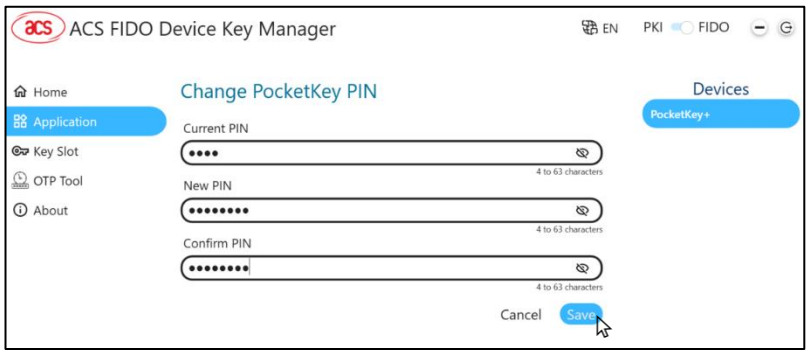
3.1. 修改 PocketKey PIN 码

修改 PocketKey PIN 的步骤如下：

1. 点击 **Device** 并选择设备。
2. 选择 **Application**，然后点击 **Change PocketKey PIN**。



3. 在 **Current PIN** 中输入您当前的 PIN，然后在 **New PIN** 输入并验证您的新 PIN。点击 **Save**。

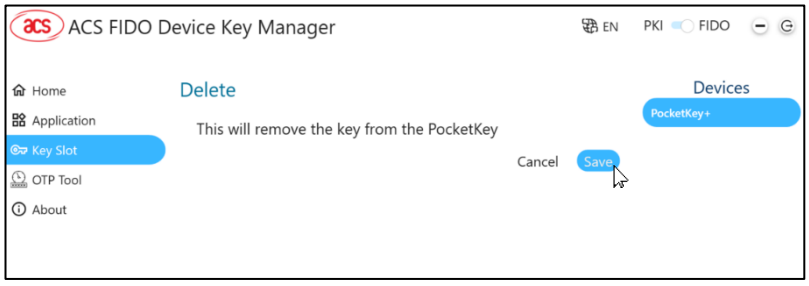


3.2. 删除通行密钥槽

删除通行密钥槽的步骤如下：

1. 选择 **Key Slot**，并登录您的 PocketKey 设备。
2. 勾选需要删除的槽对应的复选框，或 **Select All**，然后点击 **Delete**。

3. 工具会确认删除操作。点击 **Save**。

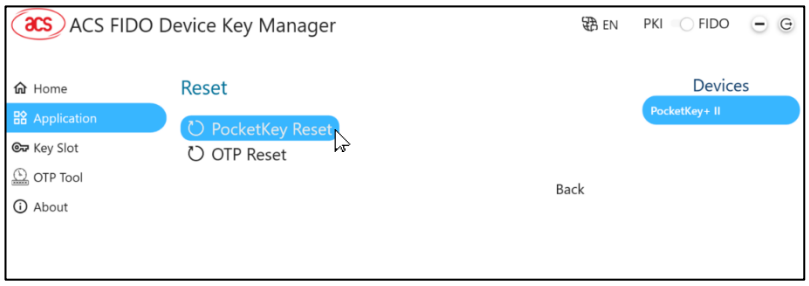


4. 已删除的槽将从槽列表中移除。

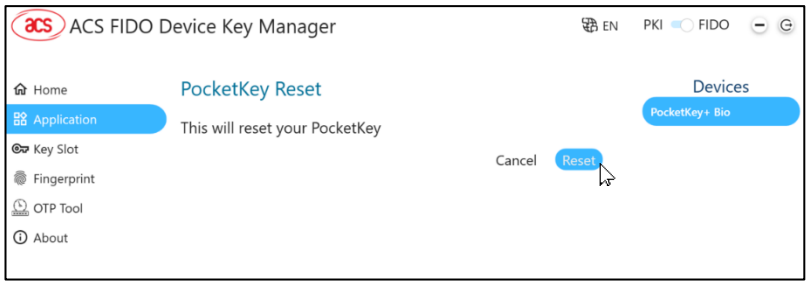
3.3. 重置 PocketKey

重置 PocketKey 设备的步骤如下：

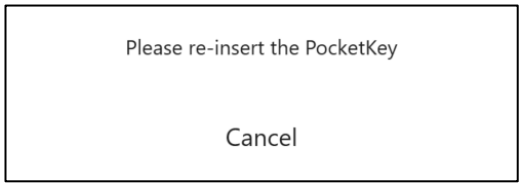
1. 点击 **Device** 并选择设备。
2. 如果您拥有一台或多台 PocketKey 设备，请点击设备名称旁边的设备槽列表并选择设备。
3. 然后点击 **Application**，选择 **Reset**，进入 **PocketKey Reset**。

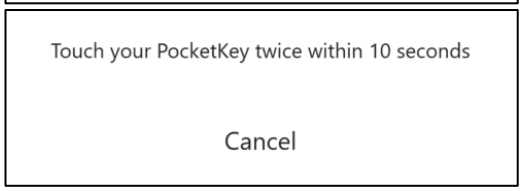


4. 此操作会清除 PocketKey 的所有数据（通行密钥和指纹）及凭证。



5. 按照指示完成重置流程。





6. 状态信息显示操作是否成功。

3.4. 添加指纹

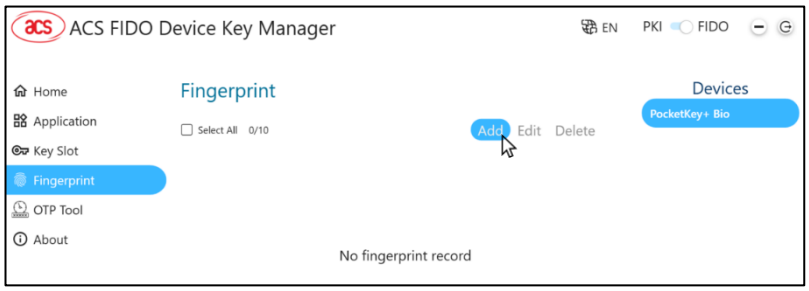
指纹功能仅适用于 **PocketKey+ Bio**。

添加指纹的步骤如下：

1. 点击 **Device***并选择设备

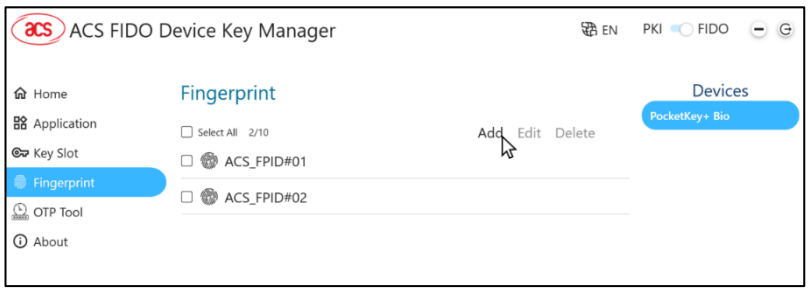
   指纹功能仅在 **PocketKey+ Bio 中提供*

2. 选择 **Fingerprint** 并登录密钥。
3. 在 **Fingerprint** 界面点击 **Add**。



4. 然后将手指按压传感器（**Press your finger to begin**），开始指纹录入过程。

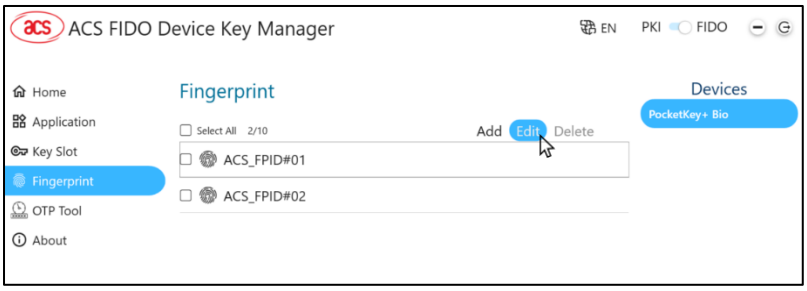
5. 指纹列表将更新，显示录入的指纹。



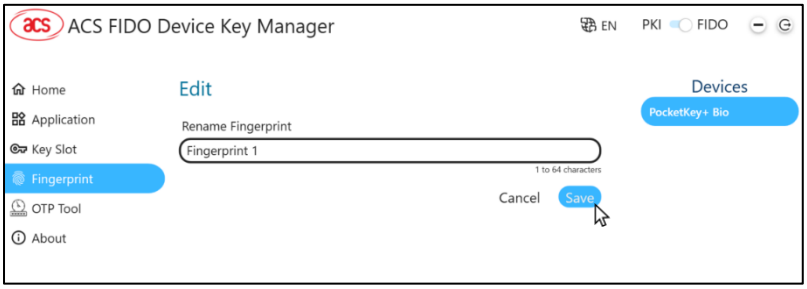
3.5. 编辑指纹

编辑指纹的步骤如下：

1. 选中要编辑的指纹，然后点击 **Edit**。



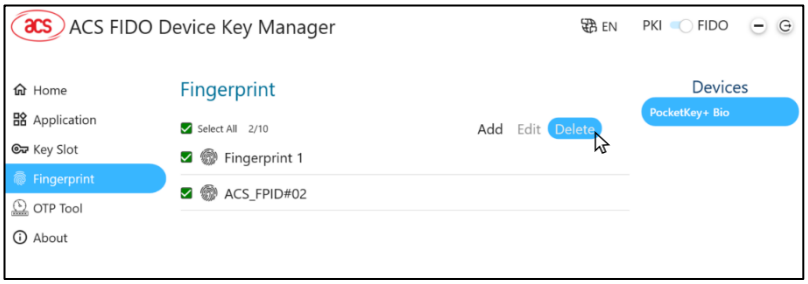
2. 为指纹输入名称，然后点击 **Save**。



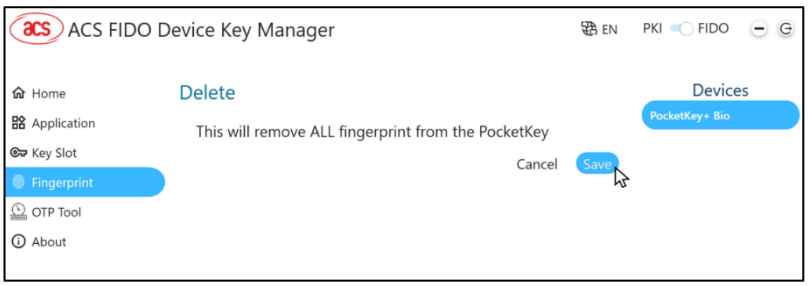
3.6. 删除指纹

删除一个或多个指纹的步骤如下：

1. 勾选需要删除的指纹对应的复选框，或 **Select All**，然后点击 **Delete**。



2. 管理器再次确认删除操作。点击 **Save**。



3. 已删除的指纹将从指纹列表中移除。

4.0. ACS PocketKey OTP 验证器概览

ACS PocketKey 系列设备融合了 FIDO 功能与一次性密码（OTP）的多功能性优势，旨在实现登录的灵活性。本节将介绍 OTP 工具及其在安全登录流程中的设置方法，为用户提供一种无缝认证体验，将高级的安全特性与用户友好的认证选项相结合。

***注：**PocketKey USB 令牌要启用 OTP 功能，固件必须是 1.00.00.15 及以上版本。*

4.1. HOTP：基于事件的一次性密码

基于事件的一次性密码（Event-based OTP，又称 HOTP，即基于 HMAC 的一次性密码）是最初的一次性密码算法，其依赖两项信息。第一项是仅由令牌和 OTP 验证服务器共享的密钥，称为“种子”。第二项信息是动态因子，在基于事件的 OTP 中，该因子为计数器。计数器同时存在于令牌和服务器中。当令牌上的按钮被按下时，令牌内的计数器会递增；而服务器端的计数器仅在一次性密码（OTP）成功验证后才会递增。

计算 OTP 时，令牌会以“种子”作为密钥，将计数器值输入到 HMAC 算法。HOTP 在 HMAC 算法中采用 SHA-1 哈希函数，生成一个 160 位的值，随后将其缩减为 6 位（或 8 位）的十进制数字，在令牌上显示。

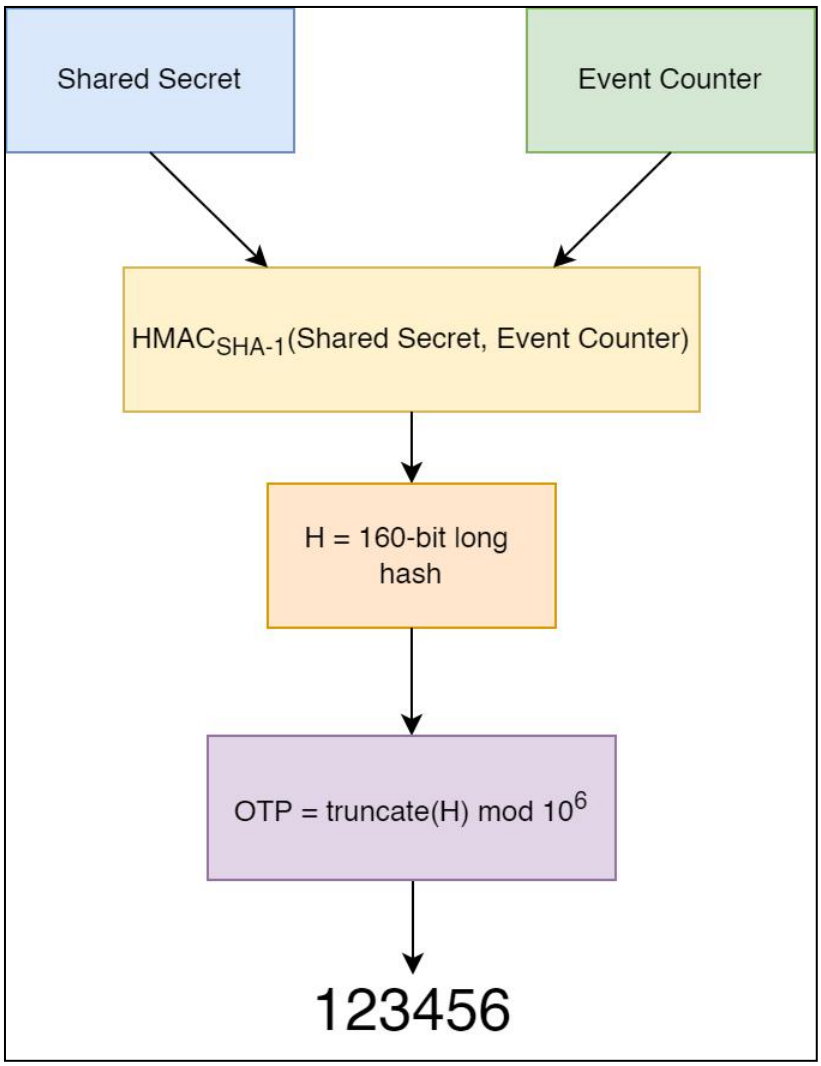


图 3：HOTP

4.2. TOTP：基于时间的一次性密码

基于时间的一次性密码（Time-based OTP，又称 TOTP）以 HOTP 为基础，其动态因子采用时间而非计数器。TOTP 以时间步长（Timestep）为单位的递增时间，时间步长通常为 30 秒或 60 秒。这意味着每个 OTP 仅在对应的时间步长内有效。

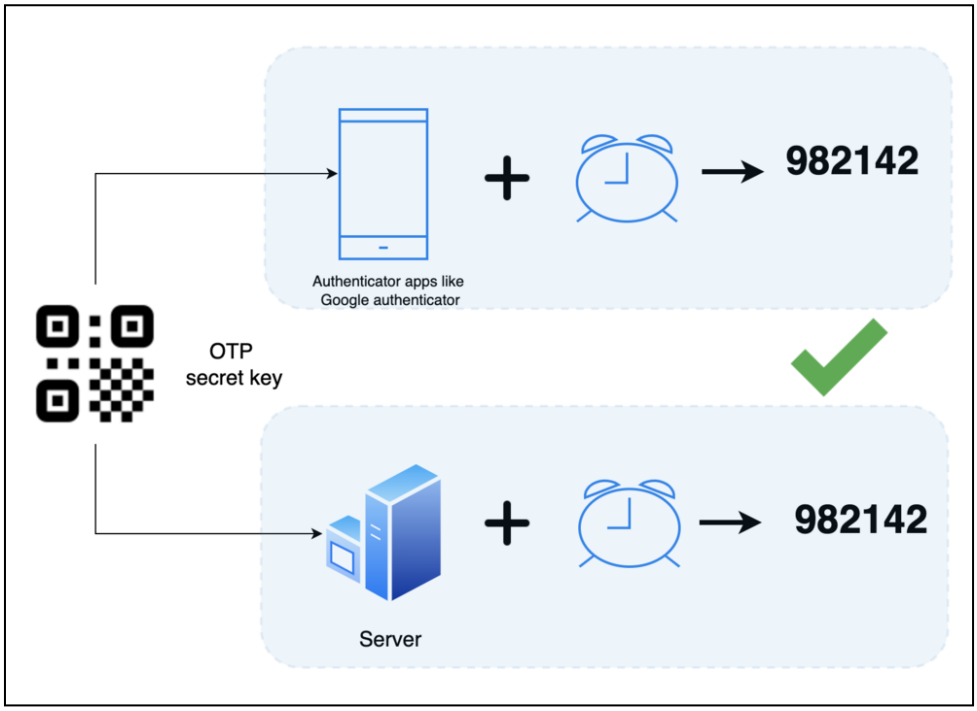


图 4：TOTP

5.0. PocketKey OTP 工具

OTP 工具（OTP Tool）是一款用于管理 ACS FIDO PocketKey 系列产品的简易工具。该工具主要提供两项功能，一项是管理多功能安全密钥的协议；另外一项是管理可选的 OATH HOTP 功能。

5.1. 准备工作

在使用 OTP 工具前，需先安装并启动 ACS FIDO 设备密钥管理器（ACS FIDO Device Key Manager）。在设备槽列表中选择好 PocketKey 之后，点击"OTP Tool”进入用户界面，即可有效管理和充分利用 FIDO PocketKey 设备。

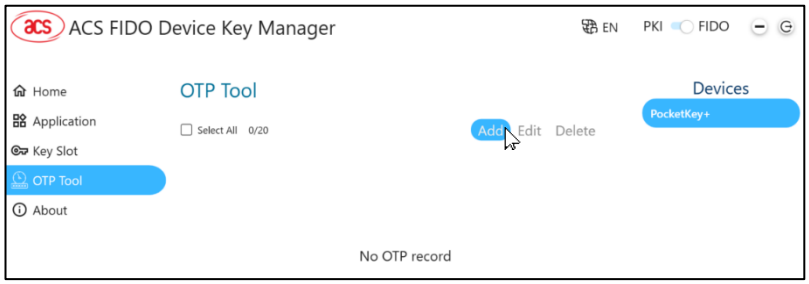
图 5：PocketKey OTP 工具用户界面

6.0. 使用 Pocketkey OTP 工具

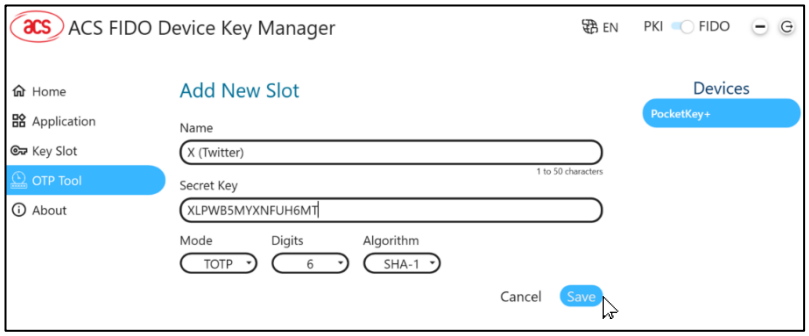
6.1. 添加 OTP

添加 OTP 槽的步骤如下：

1. 登录 **OTP 工具***。
   默认 PIN：00000000
2. 在 OTP 界面点击 **Add**。



3. 输入要添加的槽的信息，并保存。

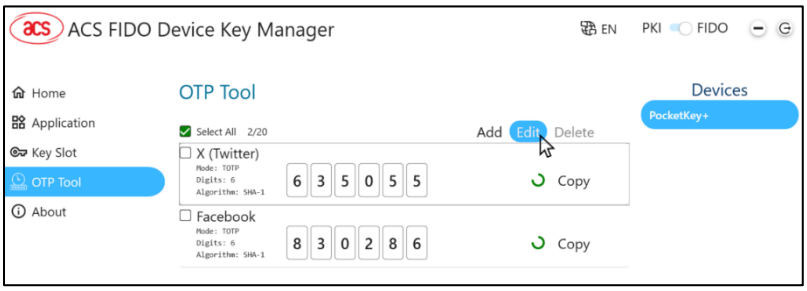


4. 等待添加 OTP 槽。
5. 槽列表将更新，显示已经添加的 OTP 槽。

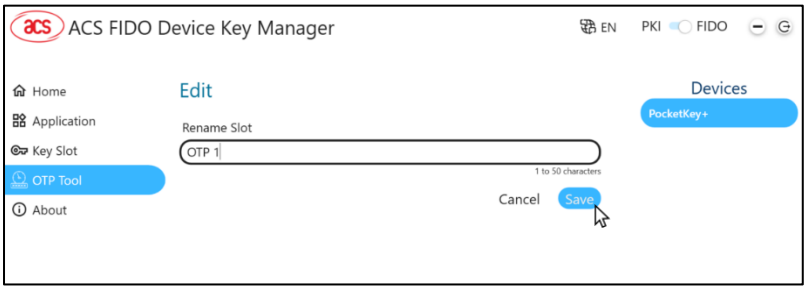
6.2. 编辑 OTP

编辑 OTP 名称的步骤如下：

1. 选中要编辑的 OTP 槽，然后点击 **Edit**。



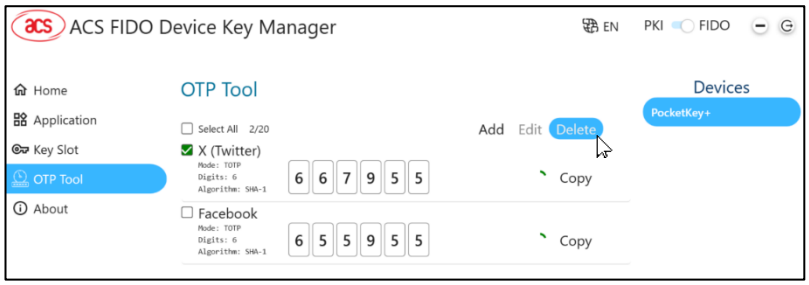
2. 输入要设置的槽名称，然后点击 **Save**。



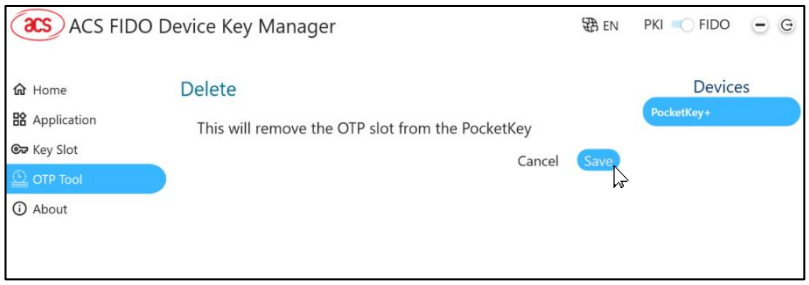
6.3. 删除 OTP

删除 OTP 槽的步骤如下：

1. 勾选需要删除的 OTP 槽对应的复选框，或 **Select All**，然后点击 **Delete**。



2. 工具会确认删除操作。点击 **Save**。

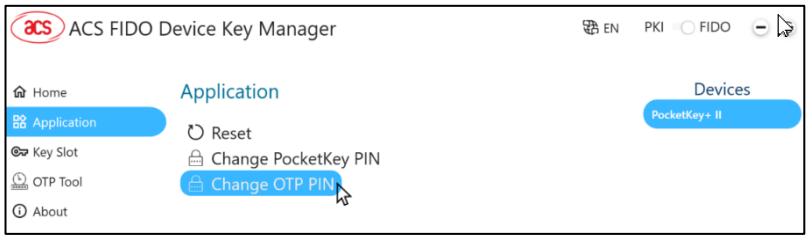


3. 已删除的 OTP 槽将从槽列表中移除。

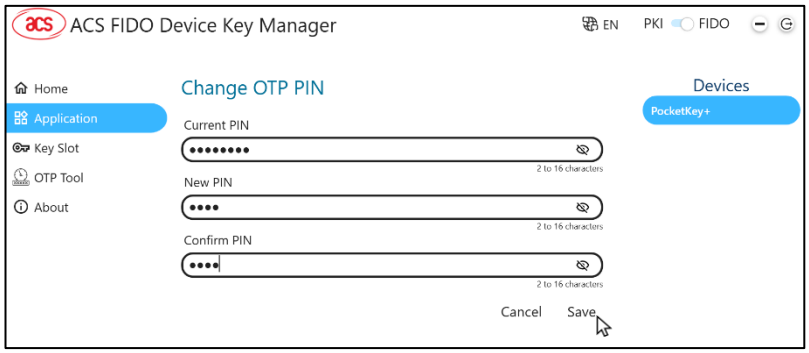
6.4. 修改 OTP PIN 码

修改 OTP PIN 的步骤如下：

1. 点击 **Device** 并选择设备。
2. 选择 **Application**，然后点击 **Change OTP PIN**。



3. 在 **Current PIN** 中输入您当前的 PIN，然后在 **New PIN** 输入并验证您的新 PIN。点击 **Save**。

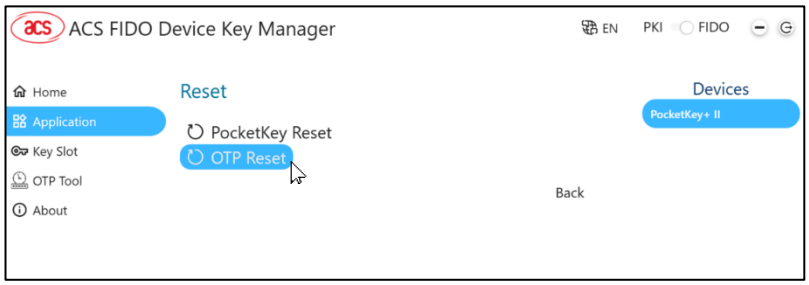


默认 PIN：00000000

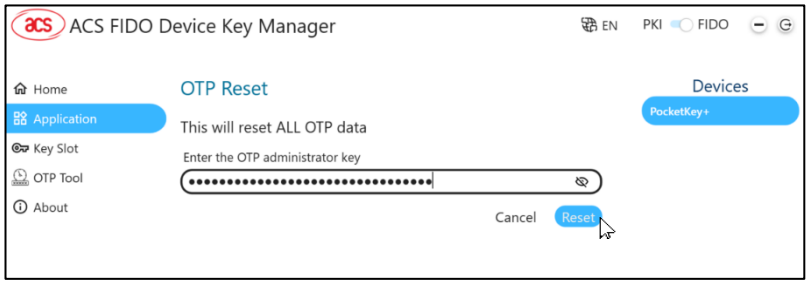
6.5. OTP 重置

重置 OTP 的步骤如下：

1. 将令牌连接到系统。等待工具加载令牌。
2. 如果有一个或多个空白或已初始化的令牌，请点击令牌名称旁边的设备槽列表并选择令牌。
3. 然后点击 **Application**，选择 **Reset**，进入 **OTP Reset**。



4. 输入管理员密钥可以将 OTP 工具恢复到出厂设置，此操作会清除所有的 OTP 槽数据，并将 PIN 码恢复为默认值。



管理员密钥：5B1D11969B22F10CD4004ACA30DE99E3

5. 状态信息显示操作是否成功

7.0. ACS PocketKey PKI 管理页概览

ACS PocketKey PKI 管理页是一个安全便捷的管理工具，可帮助 PKI 系统管理员准备/管理普通用户的卡片及令牌。

- 证书管理器（CM）：此应用协助管理存储在 PocketKey 中的数字证书。
- 初始化管理器（IM）：此应用协助初始化要分发给终端用户的 PocketKey 设备。

7.1. 准备工作

使用 PKI 工具前，需要先安装并启动 ACS FIDO 设备密钥管理器（ACS FIDO Device Key Manager）。在右侧切换到“PKI”，进入 **PKI 用户界面**，即可有效管理并充分利用设备。*

注：针对 *PocketKey 系列设备，PKI 功能仅支援 PocketKey+ II*。

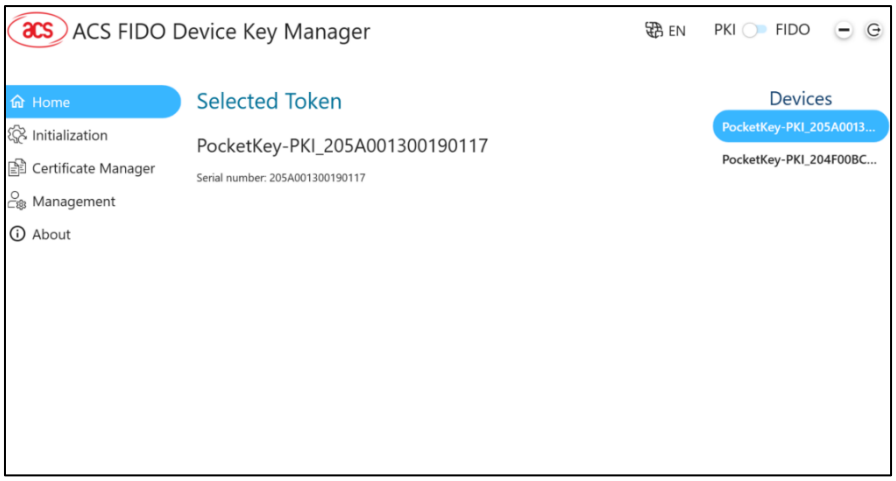


图 6：ACS FIDO 设备密钥管理器

7.2. 令牌分类

ACS FIDO 设备密钥管理器将令牌分为以下类型：

- **已初始化令牌** - CM 将显示该令牌的指定名称（如"PocketKey-PKI"）。您可在此令牌上安装证书，并通过 CM 对其进行管理。
- **空白令牌** - 未初始化的令牌。当前状态下无法在该令牌上安装证书，请联系管理员完成令牌初始化。
- **未知令牌** - 通过其它应用程序完成初始化的令牌。当前状态下无法在该令牌上安装证书，请联系管理员重新初始化。
- **无法识别的令牌** - 表示 CM 未能加载该令牌的全部信息。请移除该令牌，然后重新正确插入。

8.0. 使用证书管理器

8.1. 快速入门指南

证书管理器（CM）是由龙杰智能卡有限公司开发的应用程序，用于轻松管理数字证书，以便在各类 PKI 应用（例如：文档加密或解密）中进行使用。通过 CM，能够查看自己的证书，同时还可导出、添加或删除现有证书。

本文档中，“令牌（Token）”均指 PocketKey 系列设备。

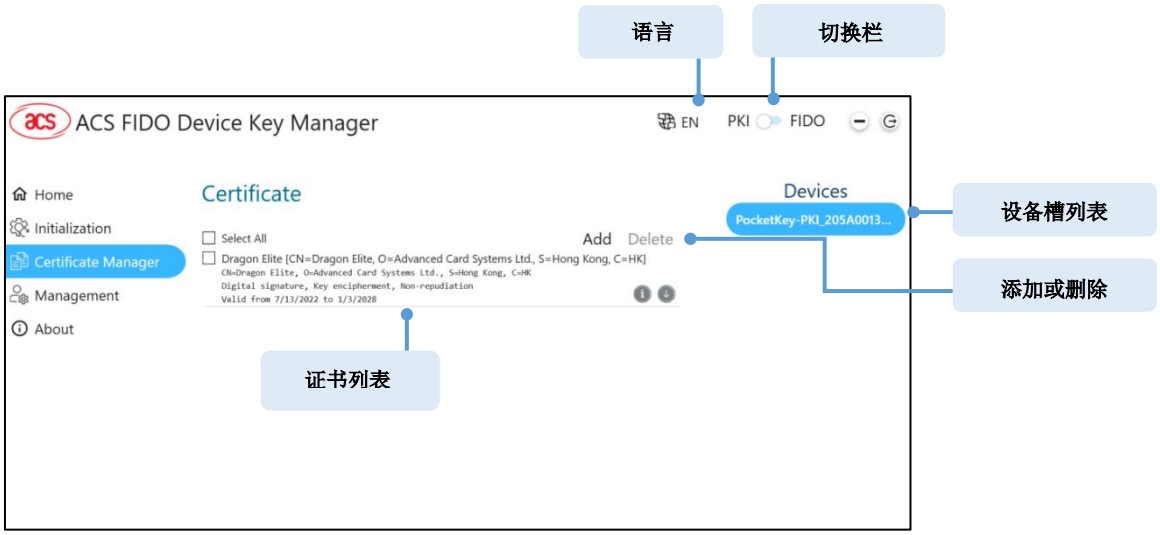


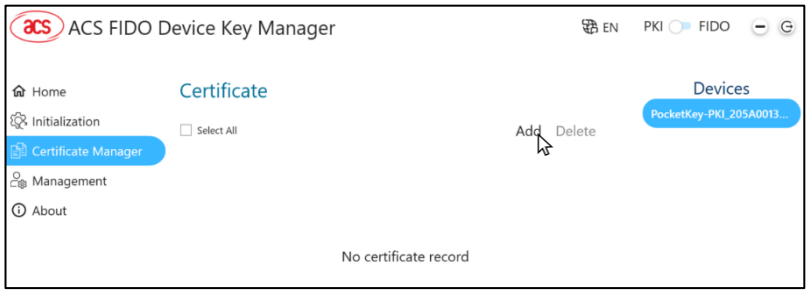
图 7：证书管理器（CM）用户界面

8.2. 导入证书

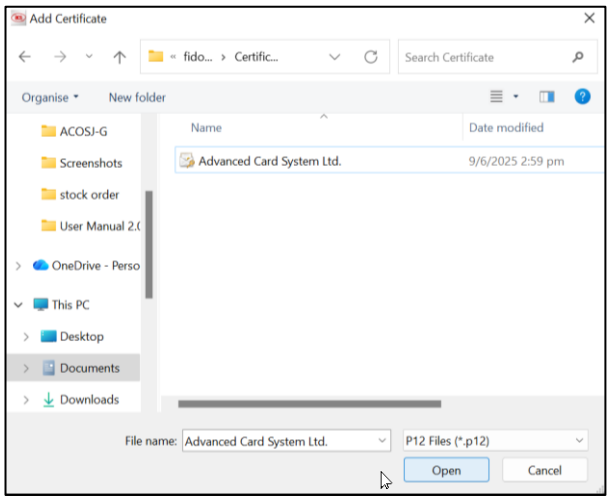
CM 支持导入. p12 及.pfx 文件格式的证书。

导入证书的步骤如下：

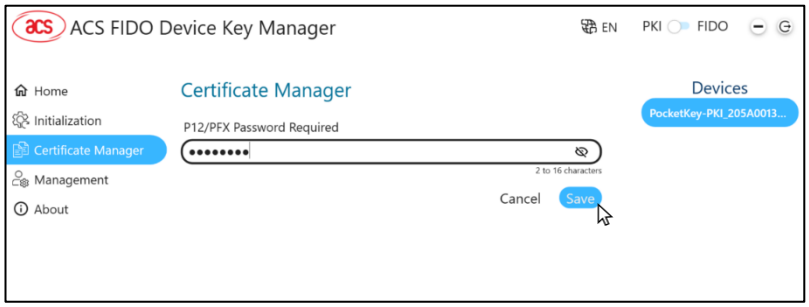
1. 登录令牌。
2. 在 CM 界面中点击 **Add**。



3. 找到要导入的证书，然后点击 **Open**。可能需要点击文件名输入框旁的文件类型下拉菜单，选择正确的文件类型，证书才会显示。

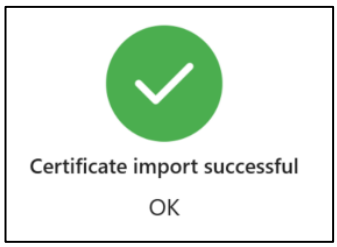


4. 若证书设有密码，请输入密码，然后点击 **Save**。

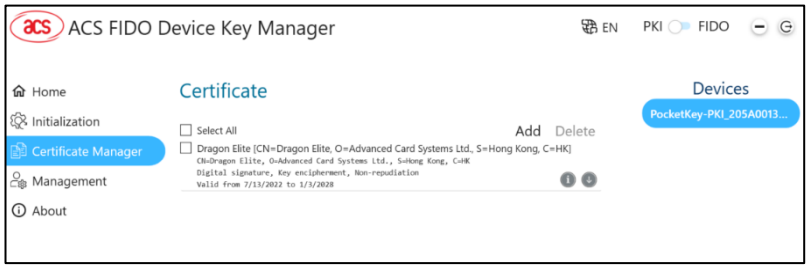


导入证书时，管理器将自动检测并提示您安装**根证书**。请根据需要選擇相關項目。

5. 等待证书导入完成。



6. 证书列表将自动刷新，显示已导入的证书。



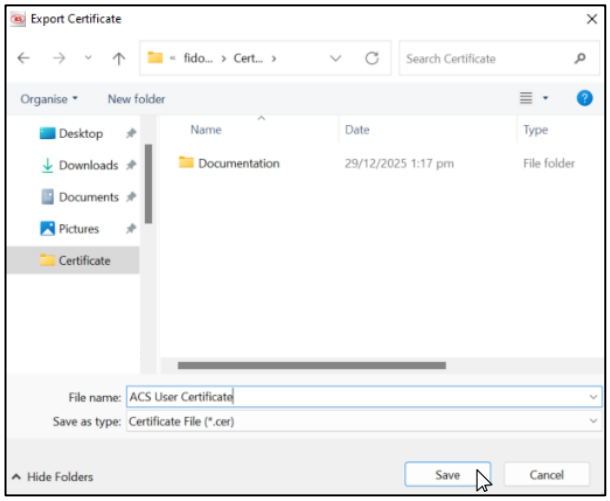
8.3. 导出证书

CM 可将证书导出为.cer 格式文件。

导出证书的步骤如下：

1. 点击证书名称右下角的图标。

2. 选择目标文件夹，然后点击 **Save**。

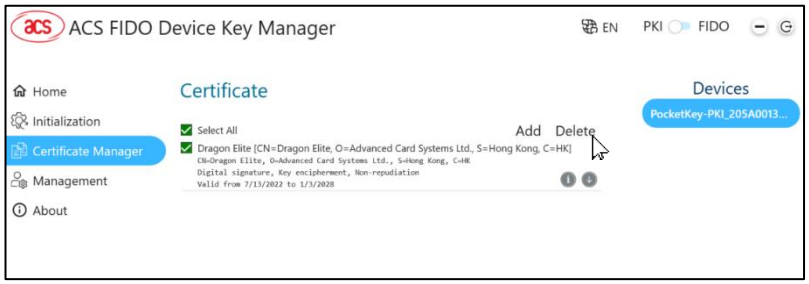


3. 证书将以.cer 格式导出。

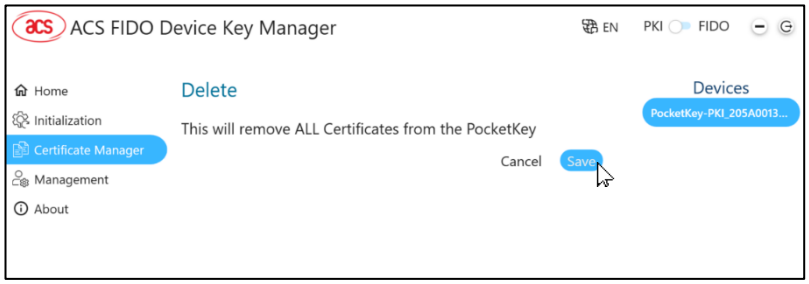
8.4. 删除证书

删除一个或多个证书的步骤如下：

4. 勾选需要删除的证书对应的复选框，或 **Select All**，然后点击 **Delete**。



5. CM 确认删除操作。点击 **Save**。

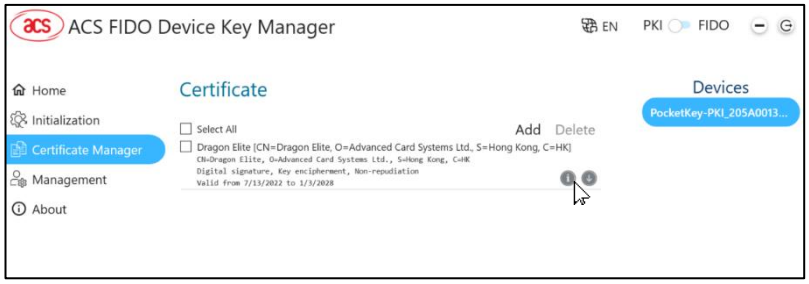


6. 已删除的证书将从证书列表中移除。

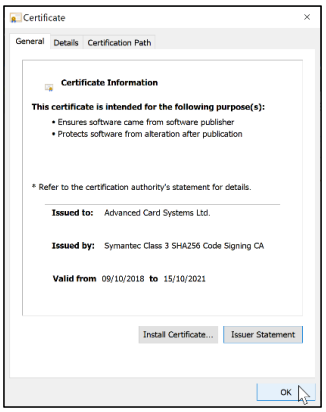
8.5. 查看证书信息

查看证书详细信息的步骤如下：

1. 点击证书名称右下角的ⓘ图标。



2. 弹出 Certificate 窗口。

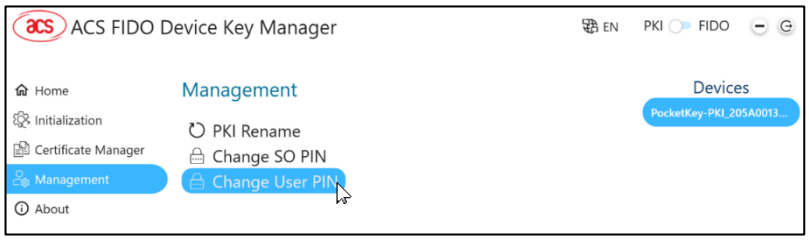


8.6. 修改用户 PIN 码

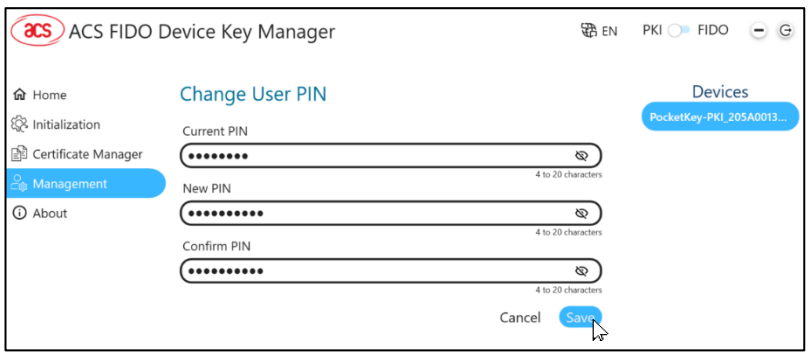
修改用户 PIN 的步骤如下：

4. 点击令牌名称并选中。

5. 选择 **Management**，然后点击 **Change User PIN**。



6. 输入当前 PIN，然后输入并验证新的 PIN。点击 **Save**。



9.0. 使用初始化管理器

9.1. 快速入门指南

初始化管理器（IM）是由龙杰智能卡有限公司开发的应用程序，专为证书颁发机构、安全管理员或系统管理员设计，用于为终端用户准备和定制令牌。

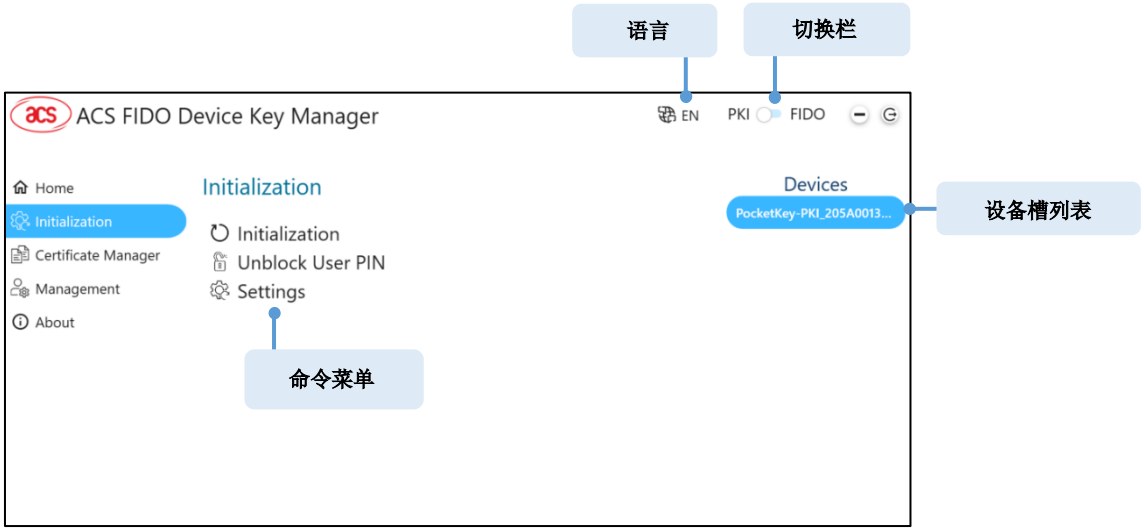
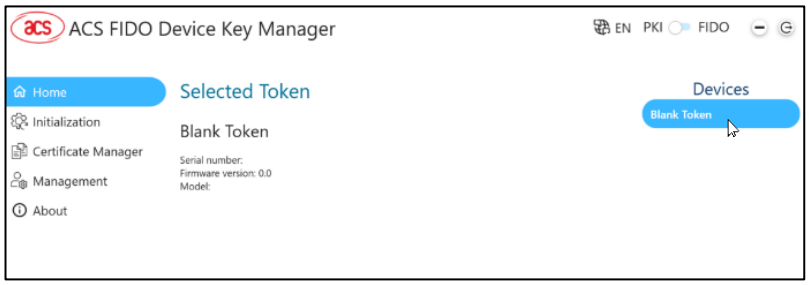


图 8：初始化管理器（IM）用户界面

9.2. 初始化令牌

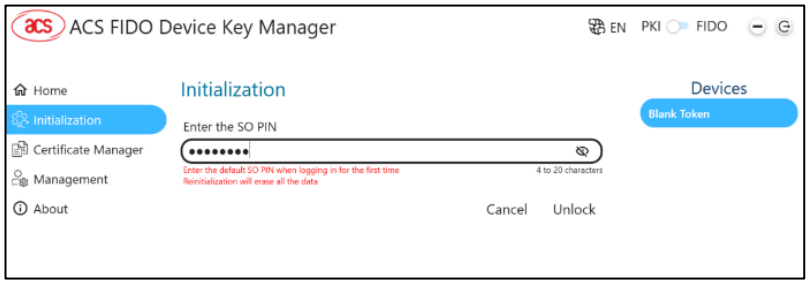
初始化令牌的步骤如下：

1. 将令牌连接到系统。等待 IM 加载令牌。

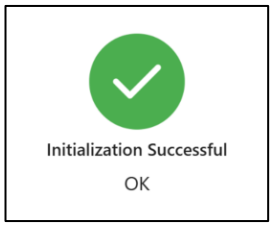


2. 如果有一个或多个空白或已初始化的令牌，请点击令牌名称旁边的设备槽列表并选择令牌。
3. 然后点击 **Initialization**。

若对已初始化的令牌进行重新初始化操作，系统将显示警告提示，要求为每个已初始化的令牌输入安全管理员（SO）PIN 码，方可继续执行初始化操作。



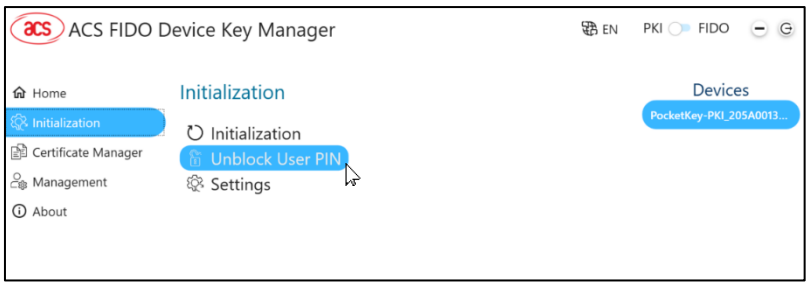
4. 等待 IM 初始化令牌。
   重要提示：*初始化过程中，请勿从系统中移除令牌。*
5. 状态信息显示是否初始化成功。



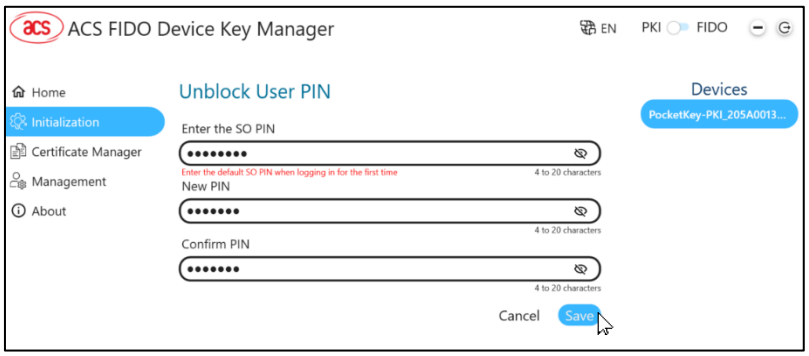
9.3. 解锁用户 PIN

若用户输入 PIN 错误次数超过允许重试次数，用户 PIN 码将被锁定。解锁用户 PIN 的步骤如下：

1. 将令牌连接到系统。等待 IM 加载令牌。
2. 点击 **Unblock User PIN**。



3. 在弹出的窗口中输入 SO PIN 码和新的用户 PIN。点击 **Save**。



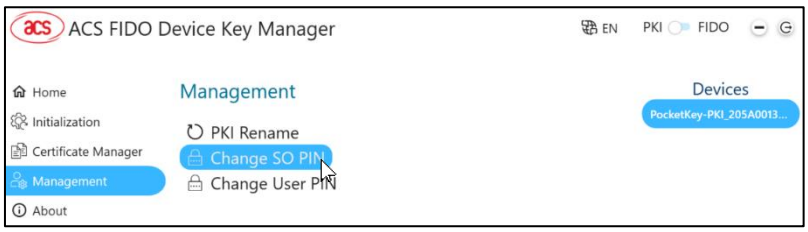
4. 等待 IM 解锁用户 PIN。
5. 状态信息显示用户 PIN 码是否已成功解锁。

9.4. 修改 SO PIN/密钥

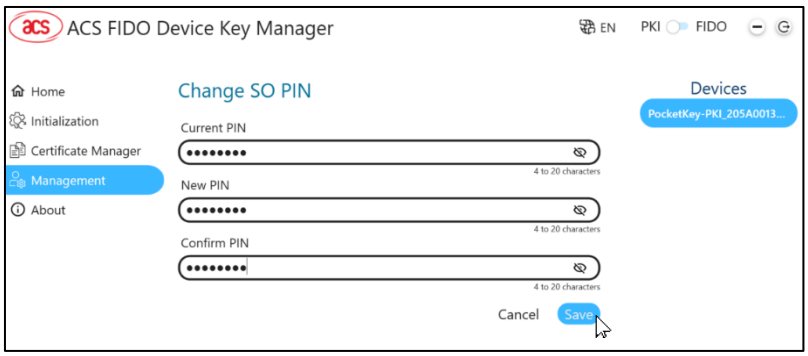
安全管理员（SO）PIN/密钥也称为 **PIN 解锁密钥（PUK）**。当用户 PIN 码因输入错误次数超过允许重试次数而被锁定时，可通过该密钥重置用户 PIN 码。

修改 SO PIN/密钥的步骤如下：

1. 将令牌连接到系统。等待 IM 加载令牌。
2. 选择 **Management**，然后点击 **Change SO PIN**.



3. 输入当前密码，然后输入并验证新的密码。点击 **Save**。



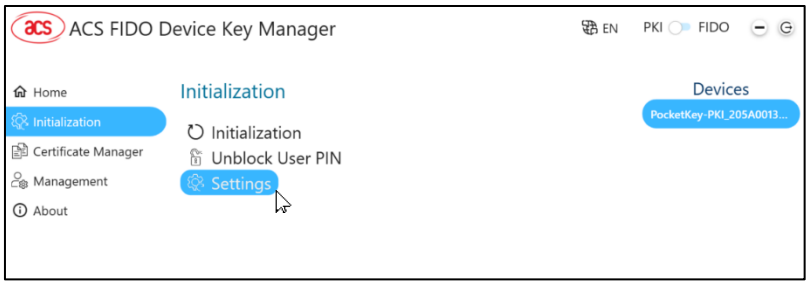
10.0. 更改应用设置

您可以更改或启用某些设置来调整 CM/IM 的操作。

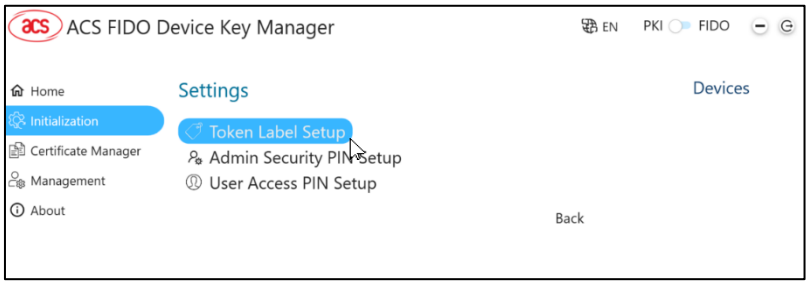
10.1. 自定义令牌设置

自定义令牌设置的步骤如下：

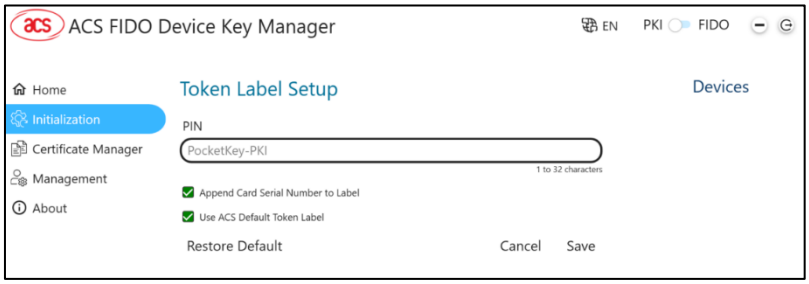
1. 将令牌连接至系统，等待 IM 加载令牌。
2. 在 IM 界面中，点击 **Settings**。



3. 在 **Settings** 界面，点击 **Token Label Setup** 选项卡。



4. 在令牌标签下，输入您希望使用的令牌名称。若需创建多个令牌，该标签将应用于所有令牌。



您可以通过以下选项自定义令牌标签（两项均默认处于启用状态）：

- 在标签后附加卡片序列号
- 使用 ACS 默认令牌标签（ACOS5-EVO/PocketKey-PKI）

附加卡片序列号会使标签变长，但更方便识别卡片，尤其是有多张卡片同时连接电脑时。

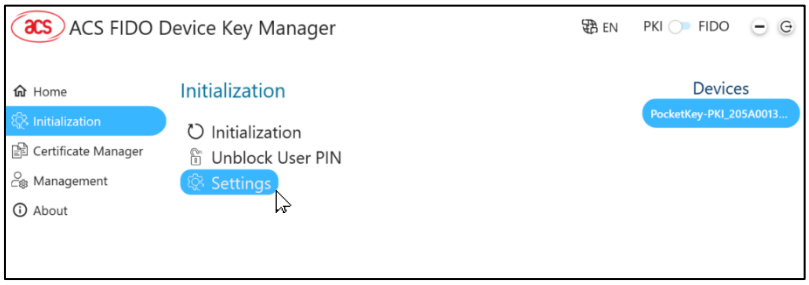
5. 点击 **Save**。
6. 如需将属性恢复为默认值，请点击 **Restore Default**。

10.2. 修改默认 SO PIN/密钥

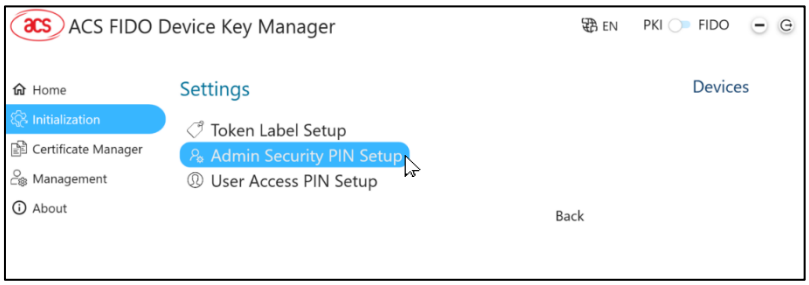
您可以在 Settings 菜单中修改默认的 SO PIN 或密钥。

修改默认 SO PIN 的步骤如下：

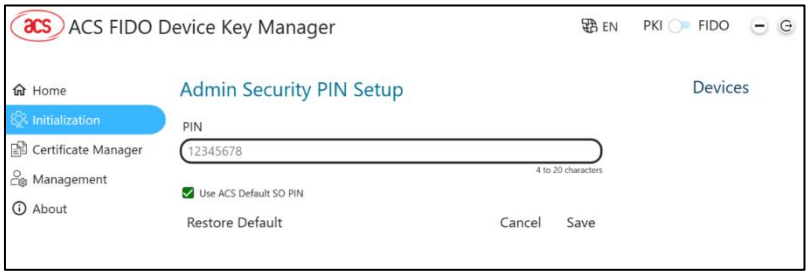
1. 将令牌连接至系统，等待 IM 加载令牌。
2. 在 IM 界面中，点击 **Settings**。



3. 点击 **Admin Security PIN Setup** 选项卡。



4. 在 SO PIN/密钥设置下，输入您首选的默认 PIN 值。
   默认启用“Use ACS Default SO PIN”选项，此时默认 PIN 设置为 **12345678**。

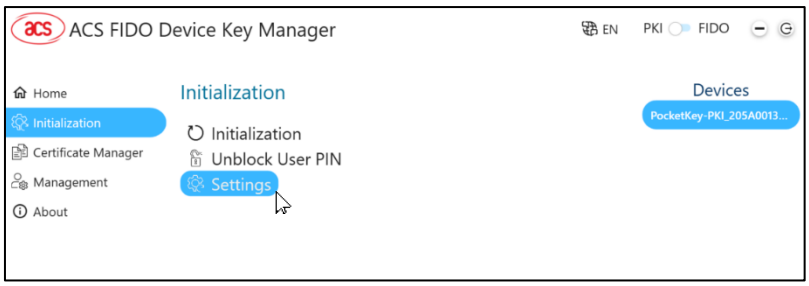


5. 点击 **Save**。
6. 如需将属性恢复为默认值，请点击 **Restore Default**。

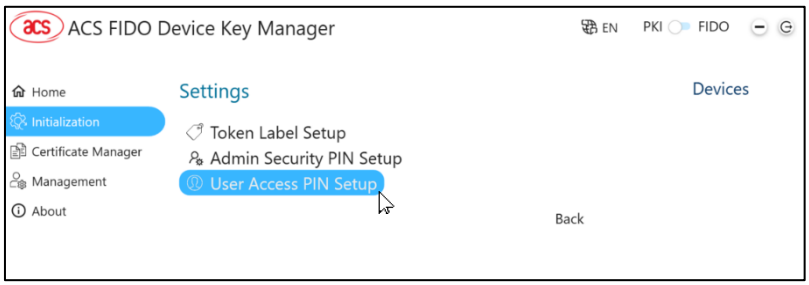
10.3. 自定义令牌设置

自定义用户 PIN 设置的步骤如下：

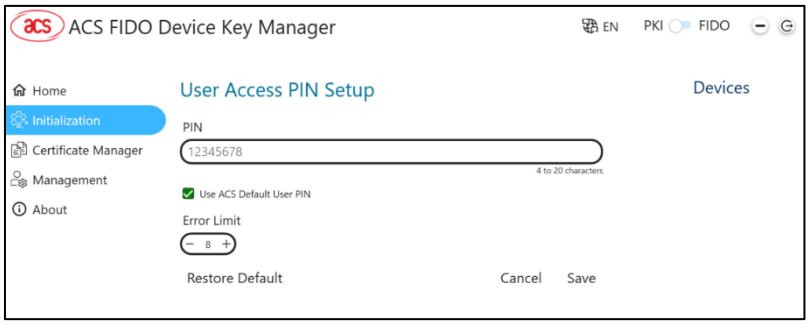
1. 将令牌连接至系统，等待 IM 加载令牌。
2. 在 IM 界面中，点击 **Settings**。



3. 点击 **Access PIN Setup** 选项卡。



4. 在用户 PIN 值的下方，输入您首选的默认用户 PIN。
   默认启用“Use ACS Default User PIN”选项，此时默认 PIN 设置为 **12345678**。

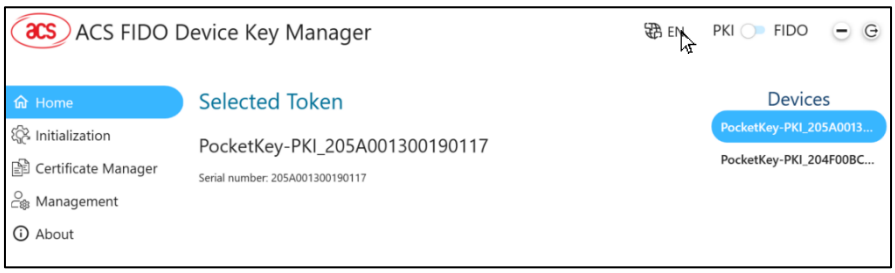


5. 在用户 PIN 属性下方，可以设置错误重试次数的上限，指定用户 PIN 输入错误的最大次数，超出后用户将被锁定。
6. 点击 **Save**。
7. 如需将属性恢复为默认值，请点击 **Restore Default**。

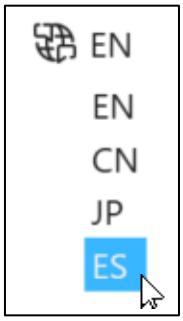
11.0. 更改语言设置

更改语言设置的步骤如下：

1. 在 ACS FIDO Device Key Manager 界面上，点击图标。



2. 选择所需语言



3. 界面将切换为所选语言。