Advanced Card Systems Ltd.
Card & Reader Technologies

ACS PocketKey 系列

一次性密码（OTP）身份验证器

应用说明 V1.05

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

目录

图目录

1.0. 背景

ACS PocketKey 系列融合了 FIDO 功能与一次性密码（OTP）的通用优势，旨在实现登录的灵活性。本用户指南将介绍 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，将高级安全特性与用户友好的认证选项相结合。

注：PocketKey USB 令牌（固件 1.00.00.15 及以上版本）需要启用 OTP 功能。

1.1. 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。

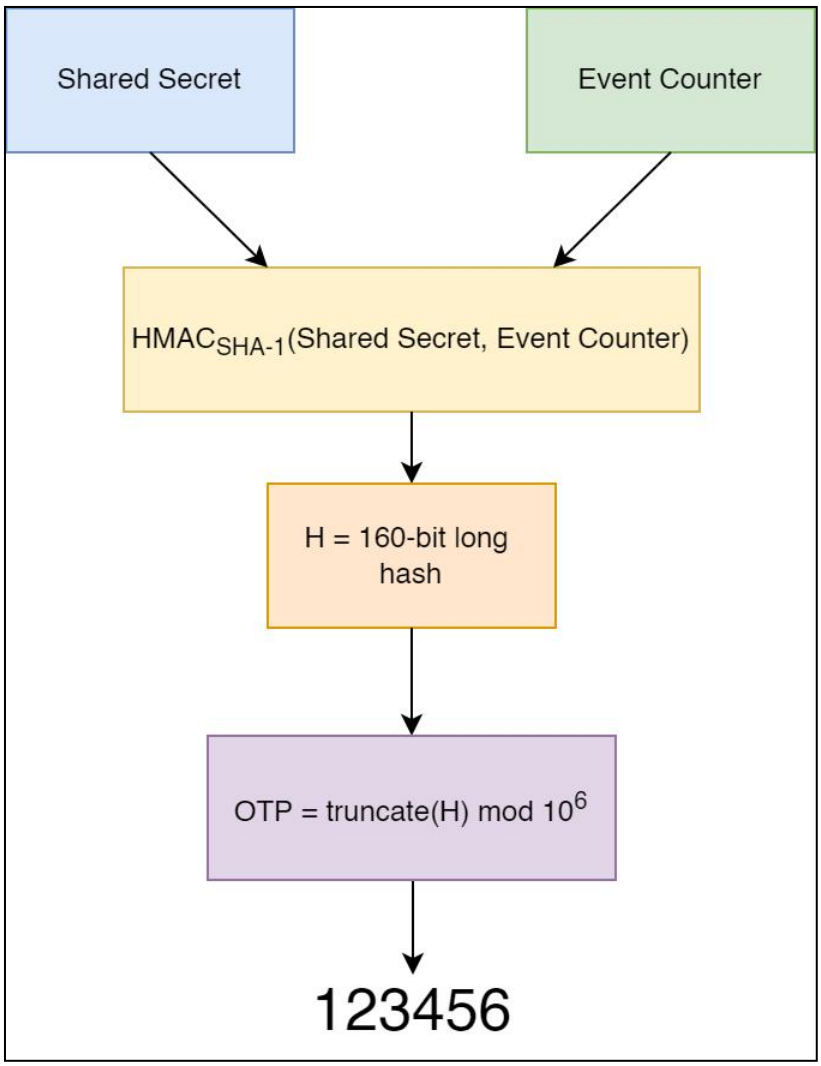


图 1：HOTP

1.2. 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。

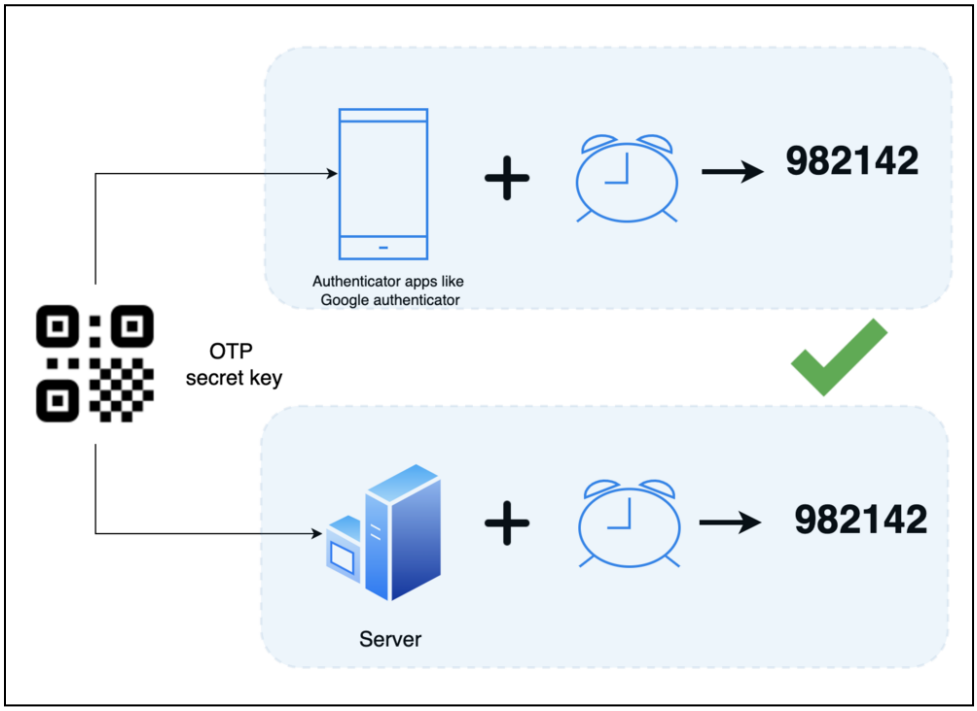


图 2：TOTP

2.0. 设置多重身份验证（MFA）

在使用 ACS PocketKey 系列设备前，需先在各个平台配置好多重身份验证（MFA）。请依照后续章节的说明操作，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。

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**

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**

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**

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**

3.0. PocketKey OTP 工具（OTP Tool）

ACS 的 PocketKey OTP 工具是一款用于 FIDO PocketKey 系列的简易管理工具。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。

3.1. 支持的操作系统

- Windows® & macOS

3.2. 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）。点击 **OTP Tool** 将弹出用户界面，帮助您高效管理和优化 FIDO PocketKey 设备。*

注：*PocketKey USB 令牌（固件 1.00.00.15 及以上版本）需要启用 OTP 功能。*

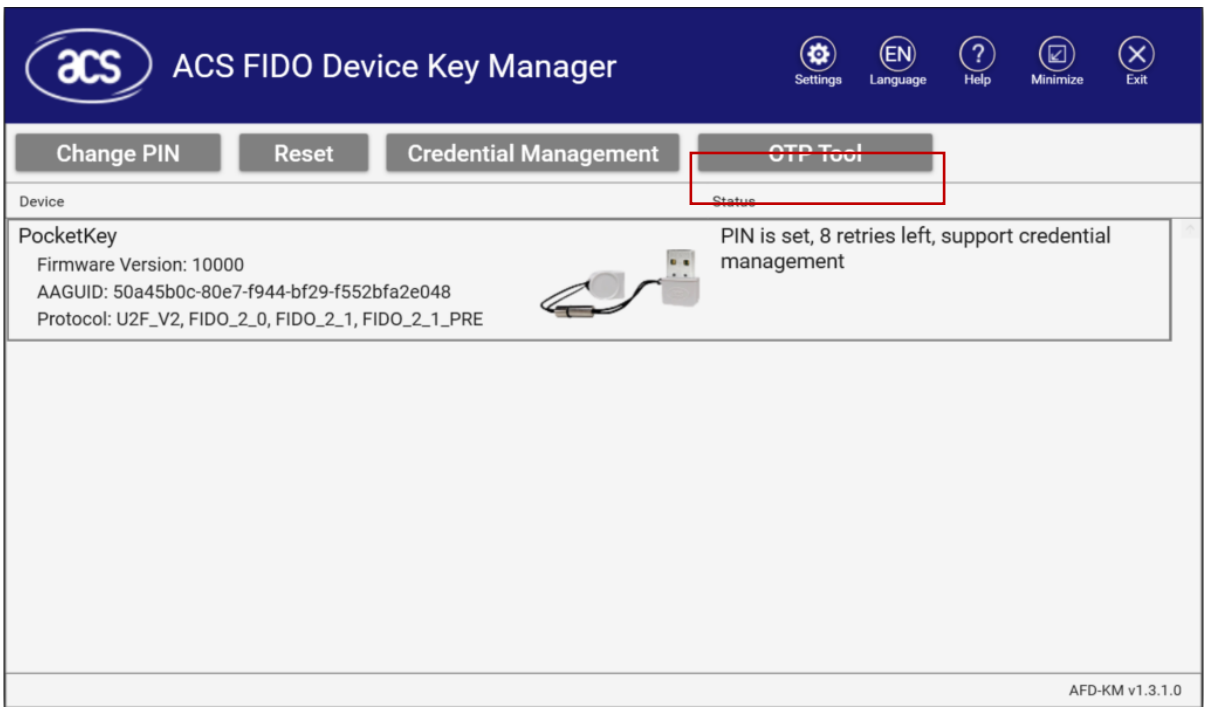


图 3：ACS FIDO 设备密钥管理器

3.3. 用户界面

图 4： PocketKey OTP 工具

3.3.1. 主功能栏

主功能栏位于 PocketKey OTP 工具顶部，用户可通过主功能栏快速调用常用功能。

3.3.1.1. 设备列表

点击列表可选择 PocketKey 设备

PocketKey USB 安全密钥/ Pocketkey+ NFC USB 安全密钥：

- 选择 AFD FIDO

PocketKey NFC 卡：

- 如果使用接触式接口，选择 ICC device
- 如果使用非接触接口，选择 PICC device

3.3.1.2. 修改 PIN 码

修改 PocketKey 的 PIN。默认 PIN：00000000

3.3.1.3. 恢复出厂设置

输入管理员密钥可以将 PocketKey 设备恢复出厂设置，此操作会清除数据槽中的所有数据，并将 PIN 码恢复为默认值。管理员密钥：5B1D11969B22F10CD4004ACA30DE99E3

3.3.2. 数据槽

显示槽的状态：灰色代表未使用，蓝色代表已使用。当数据槽状态为已使用时，点击数据槽背景可以生成 OTP。

默认值：灰色

3.3.2.1. 槽号

数据槽的编号，每个 PocketKey 有 20 个数据槽用于存储 OTP 数据。

3.3.2.2. 槽名

数据槽的名称，可由用户自定义。默认值：空

3.3.2.3. 清除数据

输入 PIN 码后可以清除槽中的数据，此操作可能会清除槽中所有数据并恢复默认设置。

3.3.2.4. 编辑槽名

输入 PIN 码后可以编辑槽名。

3.3.2.5. 数据槽设置

进入 OTP 设置，该操作会将空的数据槽更改为 OTP 槽。

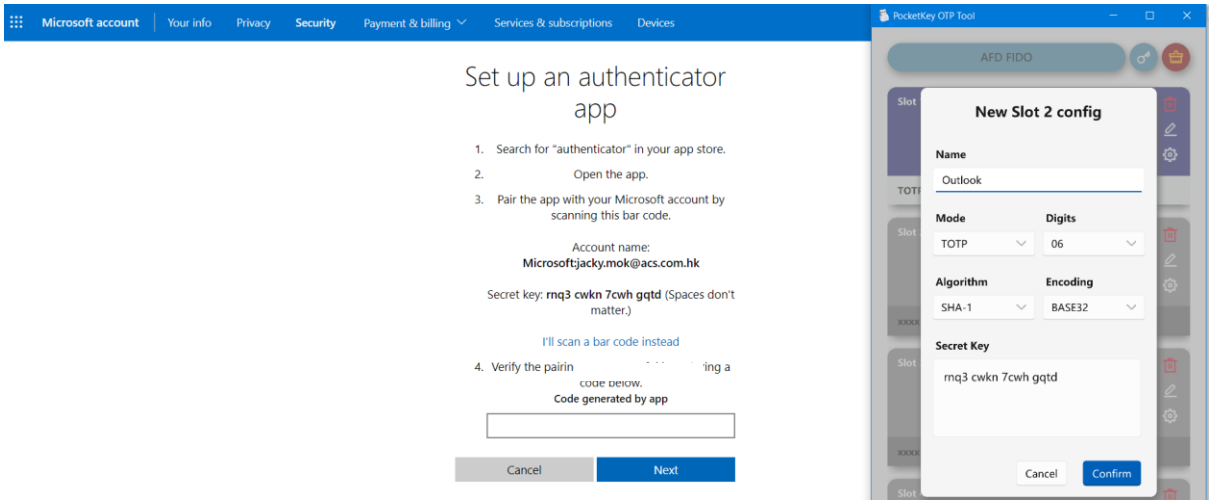
3.3.2.6. OTP 类型

显示槽内存储的 OTP 类型。默认值：XXXX

4.0. 设置 PocketKey 作为 TOTP 身份验证器的步骤

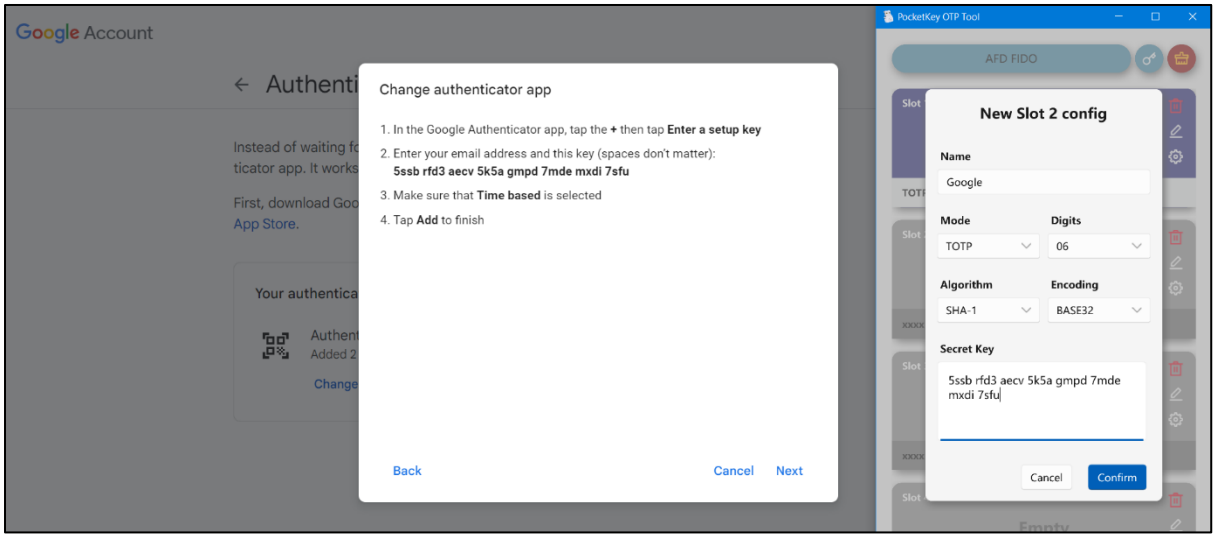
本节介绍如何为常用网站配置 TOTP 选项。请插入 PocketKey 并打开 PocketKey OTP 工具，为 TOTP 验证流程做好准备。有关 PocketKey OTP 工具各项功能的详细信息，请参阅*用户界面*章节。

4.1. Microsoft(outlook)



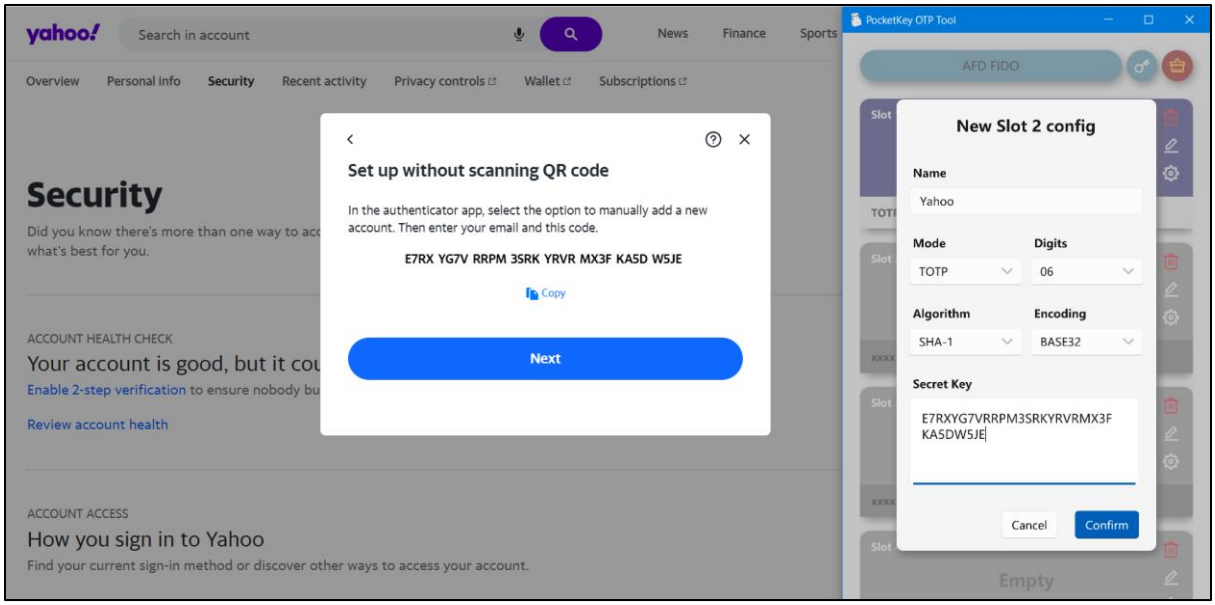
1. 登录 *Microsoft 账户*
2. 前往 **Security >> Manage how I sign in >> Add a new way to sign in or verify**
3. 选择 **Use an app**
4. 点击 **set up a different Authenticator app**
5. 选择 **I can't scan the bar code**
6. 将 **Key** 复制粘贴到 **PocketKey OTP Tool**，然后点击 **Confirm**
7. 进入 Verify PIN，点击 **Confirm**（首次登录时需操作）
8. 点击 **Slot Background**
9. 返回 *Microsoft 账户*页，将 **code** 粘贴到 **Code generated by app** 的下方
10. 点击 **Next**

4.2. Google



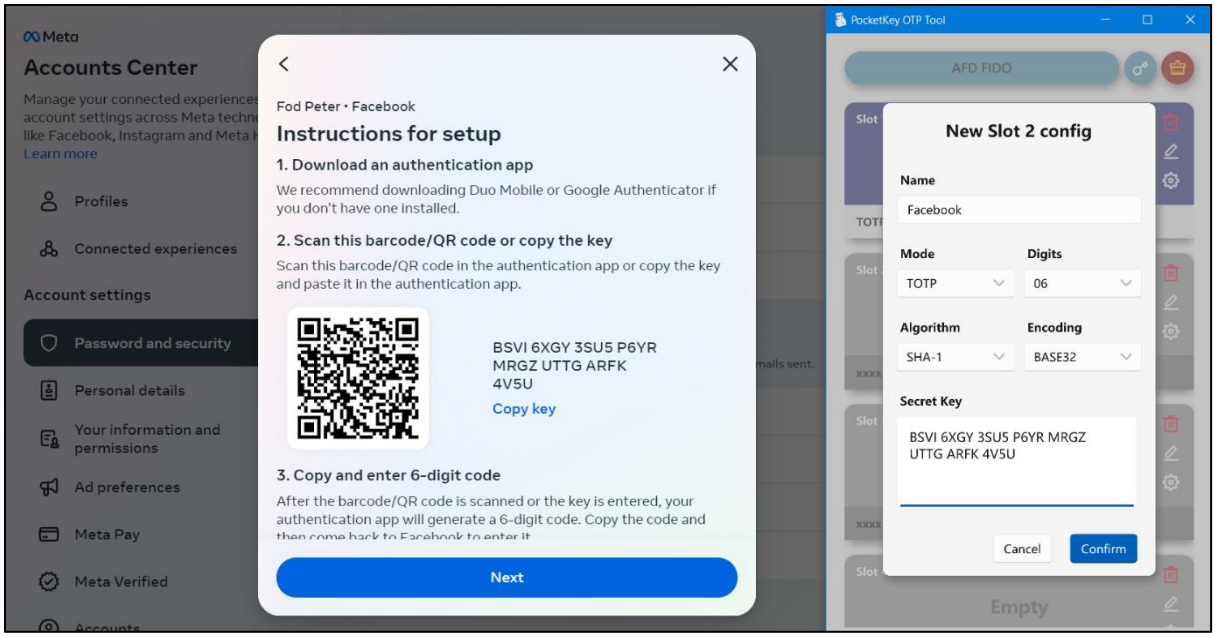
1. 登录 *Google 账户*
2. 前往 **Security >> How you sign in to Google >> 2-Step Verification**
3. 选择 **Authenticator app**
4. 点击 **Set up authenticator**
5. 点击 **Can't scan it**
6. 将 **Secret Key** 复制粘贴到 **PocketKey OTP Tool**，然后点击 **Confirm**
7. 进入 Verify PIN，点击 **Confirm**（首次登录时需操作）
8. 点击 **Slot Background**
9. 返回 *Google 账户* 页，将 **code** 粘贴到 **Enter code** 中
10. 开始 **Verify**

4.3. Yahoo



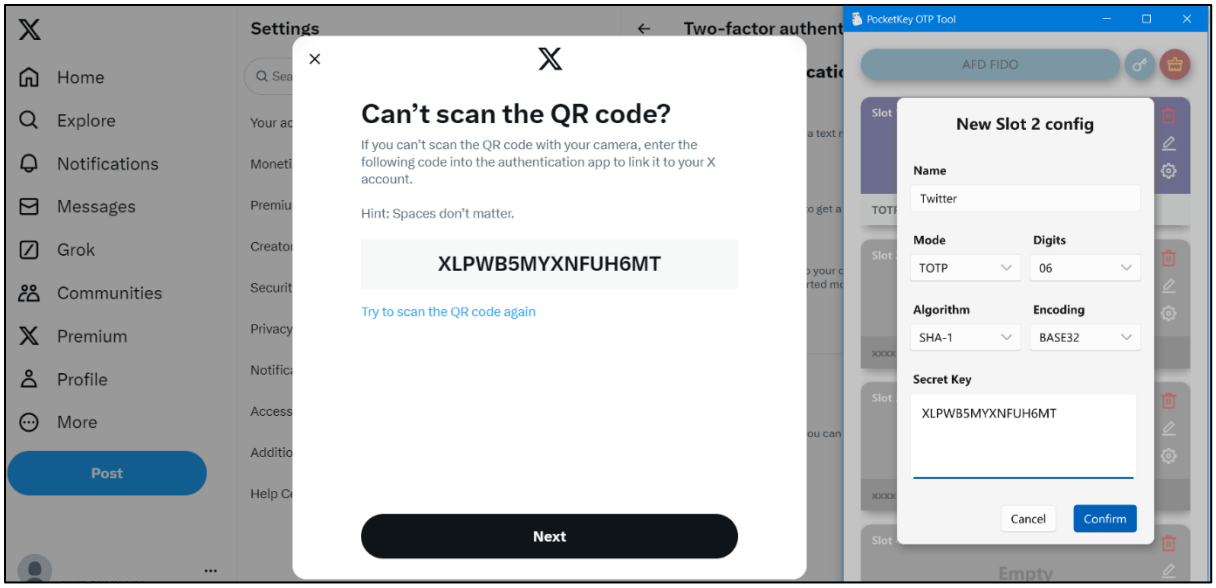
1. 登录*雅虎账户*
2. 前往 **Security >> Enable 2-step verification >> Authenticator app**
3. 选择 ***Can't scan?***
4. 然后将 **Key** 复制到 **PocketKey OTP Tool**，点击 **Confirm**
5. 进入 Verify PIN，点击 **Confirm**（首次登录时需操作）
6. 点击 **Slot Background**
7. 返回 *Yahoo 账户*，将 **code** 粘贴到 **Enter verification code**
8. 点击 **Next**

4.4. Facebook



1. 登录 *Meta 账户中心*
2. 前往 **Settings & privacy >> Setting >> Password and security >> Two-factor authentication**
3. 选择 **Authentication app**，然后将 **key** 复制到 **PocketKey OTP Tool**，点击 **Confirm**
4. 进入 Verify PIN，点击 **Confirm**（首次登录时需操作）
5. 点击 **Slot Background**
6. 返回 *Meta 账户中心*，将 **code** 粘贴到 **Enter the code**，之后点击 **Next**
7. 点击 **Done**

4.5. X (Twitter)



1. 登录 *Twitter*
2. 前往 **More >> Setting and privacy >> Security and account access >> Security >> Two-factor authentication**
3. 点击 **Authentication app**
4. 再点击 **Get started**
5. 选择 **Can't scan the QR code?**
6. 将 **Key** 复制粘贴到 **PocketKey OTP Tool**，然后点击 **Confirm**
7. 进入 Verify PIN，点击 **Confirm**（首次登录时需操作）
8. 点击 **Slot Background**
9. 返回 *Twitter* 页面，将 **code** 粘贴到 **Enter the confirmation code**，然后点击 **Next**
10. 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*