swissbit®

ユーザーマニュアル

Swissbit iShield Key 2

iShield Key 2 FIDO2
iShield Key 2 FIDO2 MIFARE
iShield Key 2 FIDO2 FIPS
iShield Key 2 Pro
iShield Key 2 Pro MIFARE
iShield Key 2 Pro FIPS

Date: May 2, 2025
Revision: 1.1
File: UserManual_iShield-Key-2-Series_v1.1_JA.pdf

Copyright 2025 Swissbit AG

この文書およびこれに含まれる情報または資料は著作権で保護されています。著作権法で明示的に許可されていない使用には、Swissbit AG の事前の同意が必要です。これは、特に複製、改訂、翻訳、マイクロフィルムへの保存、ならびに電子システムへのインポートおよび処理に適用されます。

この文書に含まれる情報または資料は Swissbit AG の財産であり、この文書の受領者は、Swissbit AG の事前の書面による同意なしに、この文書またはここに含まれる情報または資料を直接的または間接的に開示または漏洩してはなりません。

これに関連するすべての著作権、商標、特許、およびその他の権利は、Swissbit AG に明示的に留保されており、これによりライセンスが付与されることはありません。

ここに記載されているすべてのコンテンツは、技術の進化により変更される可能性があります。

記載されているすべてのブランド名または製品名は、それぞれの所有者の商標または登録商標です。

Contents

1 ドキュメント情報 5

2 ISHIELD KEY 2 シリーズの概要 6

3 ISHIELD KEY シリーズと ISHIELD KEY 2 シリーズの比較 9

4 SWISSBIT 管理ツール 10

4.1 iShield Key Manager 10
4.1.1 インストール 10
4.1.2 ダッシュボード 12
4.1.3 FIDO2 ダッシュボードカード 13
4.1.4 Passcode ダッシュボードカード 17
4.1.5 PIV ダッシュボードカード 26
4.2 iShield Key Manager コマンドラインツール 29
4.2.1 FIDO2 コマンド 29
4.2.2 パスコードコマンド 30
4.2.3 PIV コマンド 33

5 FIDO2 アプリケーション (スタンダード) 35

5.1 概要 35
5.1.1 FIDO2 登録 35
5.1.2 FIDO2 ログイン 36
5.2 FIDO2 アプリケーションを開始する 36
5.2.1 前提条件 36
5.2.2 Swissbit iShield Key 2 の PIN を設定 36
5.2.3 テスト登録 39
5.2.4 テストログイン 40
5.3 Swissbit iShield Key 2 の様々なサービス 41

6 TOTP アプリケーション 41

6.1 概要 41
6.1.1 TOTP シーディング 41
6.1.2 パスワードの生成と認証 42
6.2 Swissbit iShield Key の様々なサービス 42

7 HOTP アプリケーション 43

7.1 概要 43
7.1.1 HOTP シーディング 43
7.1.2 パスワードの生成と認証 44
7.1.3 カウンタの再同期 44
7.2 一括登録 45

8 PIV アプリケーション 46

8.1 ユースケース 46
8.1.1 ログオン 47
8.1.2 Bitlocker 48
8.1.3 Active Directory 48
8.2 基礎的なコンポーネント 49

8.2.1 Windows でのトークンのプロビジョニングと使用 49
8.2.2 認証 49
8.2.3 証明書スロット 49
8.3 要件 50
8.4 iShield Key 2 Pro で PIV を開始する 50
8.4.1 PIV インストールパッケージ 50
8.4.2 OpenSC Minidriver と iShield PIV Module のインストール 50
8.4.3 iShield Key 2 Pro の準備 51
8.4.4 iShield Key 2 Pro のリセット 51
8.5 トラブルシューティング 52
9 GLOSSARY 53
10 DOCUMENT HISTORY 54

1 ドキュメント情報

iShield Key は、シンプル、安全、かつ柔軟性に優れた強力な認証機能を提供します。また、フィッシング、ソーシャルエンジニアリング、アカウント乗っ取りなどのオンライン攻撃からユーザーを保護します。このドキュメントでは、Swissbit iShield Key 2 シリーズ セキュリティキーの使用開始方法について説明します。

iShield Key 2 シリーズは、iShield Key ファミリーの第 2 世代です。第 1 世代の iShield Key シリーズと比較して、iShield Key 2 シリーズは、多様なユーザーニーズに対応するために、強化された機能と拡張されたオプションを提供します。FIPS 140-3 に準拠した最新の FIDO2 CTAP 2.1 および PIV SP 800-73-5 規格、そして MIFARE による物理アクセス制御をサポートするように設計されています。

iShield Key 2 シリーズは、**iShield Key 2 FIDO2** と **iShield Key 2 Pro** の 2 つの製品グループに分類できます: iShield Key 2 FIDO2 は、FIDO2 および U2F 規格をサポートし、オンラインアカウントの安全な保護を実現します。 iShield Key 2 Pro は、様々なユースケースに対応する複数のアプレットを備えたワンチップソリューションを提供します。FIDO2 アプリケーションに加え、iShield Key 2 Pro は、時間ベースおよび HMAC ベースのワンタイムパスワード（TOTP および HOTP）の生成、静的パスワードの保存、そして個人識別認証（PIV）標準に準拠した証明書ベースの認証をサポートします。

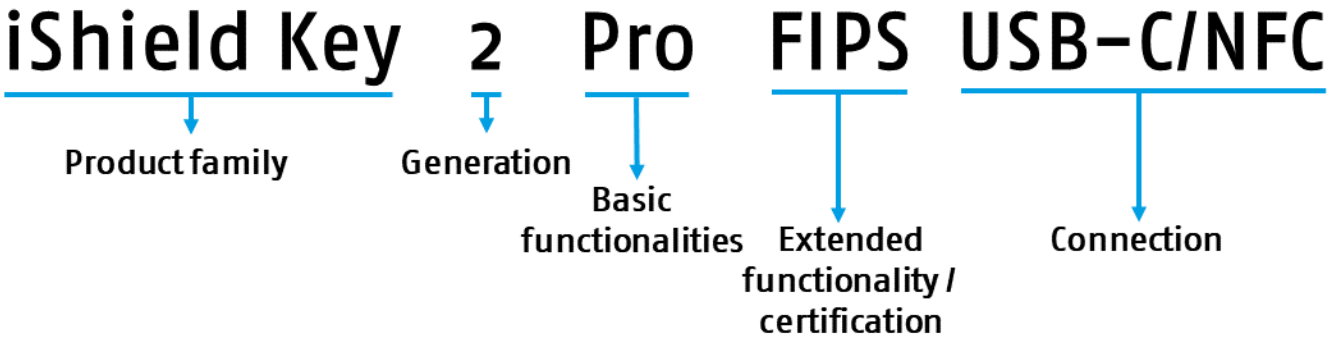
サポートされているユースケースの概要と詳細な説明への参照は、セクション 2 に記載されています。セクション 3 では、iShield Key シリーズと iShield Key 2 シリーズを比較し、セクション 4 ではセキュリティキーに付属する管理ツールを紹介します。以降のセクションでは、アプレットごとにユースケースを詳しく説明します:

- セクション 5 では、FIDO2 機能の使用ガイドを提供します。iShield Key 2 シリーズのすべてのバリアントは同じ FIDO2 機能を共有しているため、あらゆる FIDO2 関連のユースケースにおいて iShield Key 2 FIDO2 を特徴としています。
- セクション 6 と 7 では、iShield Key 2 Pro、iShield Key 2 Pro MIFARE、および iShield Key 2 Pro FIPS にのみ適用される TOTP および HOTP の生成と使用について説明します。
- セクション 8 では、iShield Key 2 Pro を PIV デバイスとしてプロビジョニングおよび使用する方法について説明します。

本書全体を通して、「iShield Key 2」という用語は、製品範囲全体に互換性が適用される場合、シリーズ内のすべてのバリエーションを指します。

2 iShield Key 2 シリーズの概要

iShield Key 2 シリーズには複数の製品バリエーションがあります。製品名をより分かりやすくするために、以下に例を示します:



最初のフィールドは製品ファミリーを示し、2 番目のフィールドは製品の世代を示します。このドキュメントでは、iShield Key 2 シリーズ（製品ファミリー「iShield Key」の第 2 世代）のみについて説明します。

3 番目のフィールドは、製品の基本機能について説明します。製品には「FIDO2」と「Pro」の 2 つのモデルがあります。「**FIDO2**」モデルは FIDO2 機能のみをサポートします。「**Pro**」モデルには、パスコードや PIV アプレットなどの追加機能が含まれています。これにより、時間ベースのワンタイムパスワード（TOTP）、HMAC ベースのワンタイムパスワード（HOTP）の生成、静的パスワードの保存、個人識別および検証（PIV）標準への準拠が可能になります。

iShield Key 2 FIDO2:

- USB-A & NFC
- USB-C & NFC

iShield Key 2 Pro:

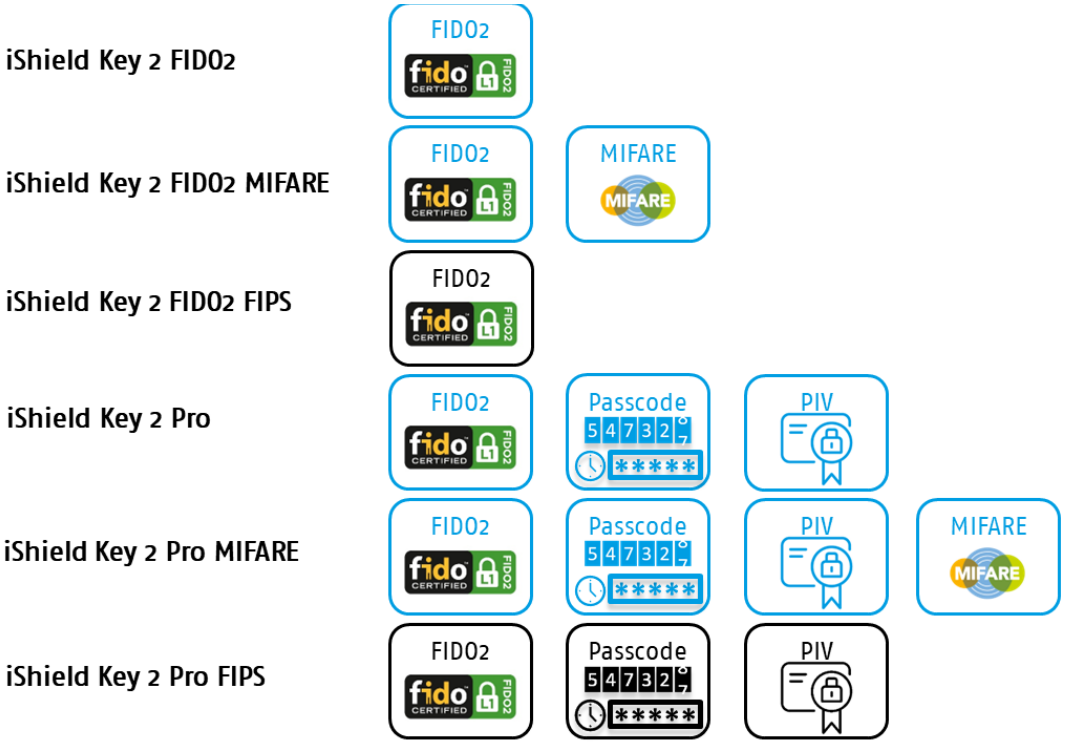
- USB-A & NFC
- USB-C & NFC

どちらのモデルも前面は同一です。iShield Key 2 Pro の背面には「P」の文字が刻印されており、これらを区別することができます。

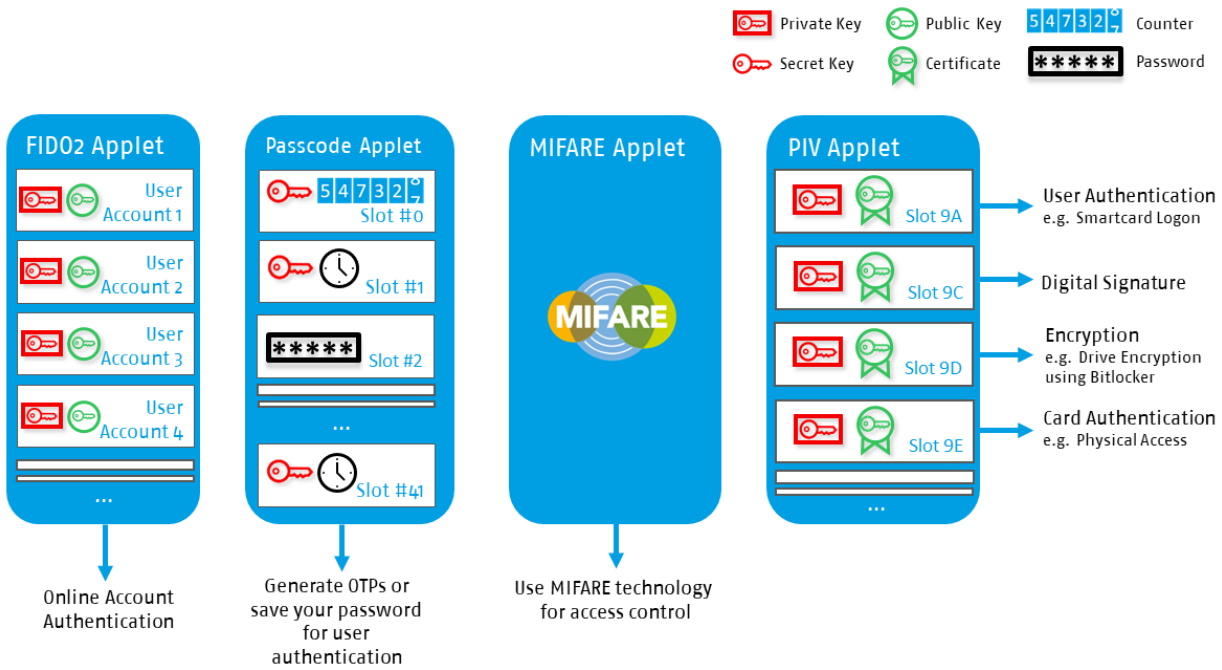
4 番目の欄は、拡張機能または認証（オプション）の概要を示しています。一部の製品モデルは、追加の規格（例：MIFARE）をサポートしているか、FIPS 140-3 の認証を受けています。該当する場合は、その旨が明記されています。

最後の欄は接続インターフェースを示しています。各製品モデルは **USB-A** または **USB-C** インターフェースのいずれかで提供されており、**すべてのモデルで NFC 接続をサポートしています**。

現在、以下の製品モデルが利用可能です:



Swissbit iShield Key 2 FIDO2 には FIDO2 アプレットのみがインストールされていますが、iShield Key 2 Pro には FIDO2、パスコード、PIV アプレットが含まれています。さらに、iShield Key 2 FIDO2 MIFARE と iShield Key 2 Pro MIFARE は MIFARE 規格をサポートし、iShield Key 2 FIDO2 FIPS と iShield Key 2 Pro FIPS は FIPS 140-3 規格に準拠していることが認定されています。



以下の表に記載されているユースケースの詳細については、Swissbit コミュニティポータル（https://community.swissbit.com/c/ishield-key/）をご覧ください。

ユースケース	説明	アプレット
オンライン認証	FIDO2 対応のウェブサイトおよびサービスでのユーザー認証	FIDO2
検出可能な認証情報（レジデントキー/パスキー）	iShield Key 2 で検出可能な認証情報（パスキーまたはレジデントキーとも呼ばれます）を生成	FIDO2（FIDO 2.1）
オンラインアカウント/VPN の 2FA	TOTP 対応のウェブサイト、サービス、または VPN での 2 要素認証	Passcode (TOTP)
オンラインアカウント/VPN の 2FA	HOTP 対応のウェブサイト、サービス、または VPN での 2 要素認証	Passcode (HOTP)
BitLocker – ローカルアカウント	ローカル Windows アカウントでの BitLocker を使用したドライブ暗号化	PIV
BitLocker – Active Directory	Windows Active Directory ドメインアカウントでの BitLocker を使用したドライブ暗号化	PIV
Windows アカウントログオン – Active Directory	Windows Active Directory ドメインアカウントへのログオン	PIV

3 iShield Key シリーズと iShield Key 2 シリーズの比較

機能	iShield Key	iShield Key 2
筐体	従来型	新型
FIDO2 バージョン	CTAP 2.0	CTAP 2.1
パスワード（パスコードアプレット）	-	サポート
タッチジェスチャー	HOTP に 1 ジェスチャ	HOTP や password に 2 ジェスチャ
HOTP	1 スロット	42 スロットまで
MIFARE	-	サポート [1]
FIPS	-	FIPS 140-3 [2]

モダンなデザインを採用した新世代製品は、お客様にとって一目で見分けがつきます。FIDO Client to Authenticator Protocol (CTAP) 2.1 の実装により、FIDO2 PIN 管理の改善、PIN の強制変更、パスキー管理など、大幅な機能強化が図られ、実用的なユーザーニーズに効果的に対応しています。iShield Key 2 Pro は静的パスワードの保存もサポートしており、ユーザーは OTP とパスワードを 1 つのトークンで管理できます。さらに、HOTP スロットとパスワードスロットに 2 つのジェスチャを割り当てることができるため、追加のドライバーやツールを必要とせずに、ホスト上で HOTP コードとパスワードを迅速に出力できます。

さらに、NXP Semiconductors が開発した非接触型スマートカードおよびリーダー向けの先進ソリューションである MIFARE テクノロジーを必要とするお客様向けに、特注バージョンもご用意しています。MIFARE は、様々なアプリケーションで安全かつ便利なデータ保存と通信に広く利用されています。さらに、当社は、高度な改ざん防止メカニズムと ID ベースの認証を実証し、最高レベルのセキュリティと信頼性を保証する FIPS 140-3 認定を取得した iShield Key 2 Pro バージョンを提供しています。

[1] iShield Key 2 Pro MIFARE のみ
[2] iShield Key 2 Pro FIPS のみ

4 Swissbit 管理ツール

iShield Key Manager (iKM) と iShield Key Manager コマンドライン (iKMcli) は、iShield Key2 を管理および設定するためのツールです。どちらのツールも、Swissbit iShield Key のランディングページからダウンロードできます。iShield Key Manager を使用する場合、ユーザーはライセンス条項に同意したものとみなされます。ライセンスは、アプリケーションのインストールディレクトリにあります。

セクション 4.1 では iKM の使用方法について説明し、セクション 4.2 では IKMcli でサポートされているコマンドの一覧を示します。

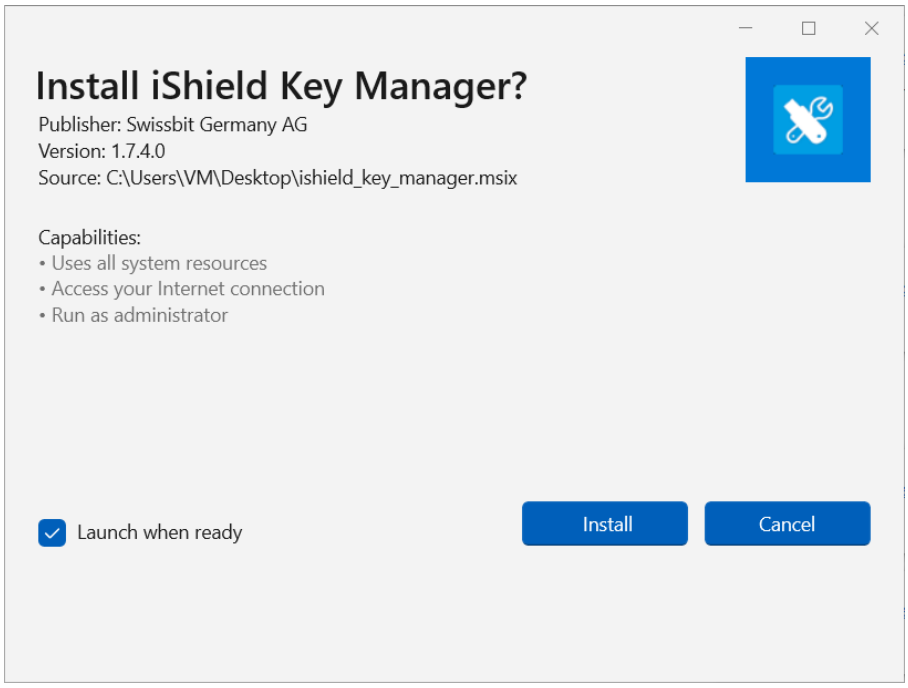
注: iShield Key 2 をサポートするには、iKM または iKMcli バージョン 1.7.4 以上が必要です。iKMcli は、HOTP 一括登録機能などの追加の設定オプションをサポートしています。.

4.1 iShield Key Manager

4.1.1 インストール

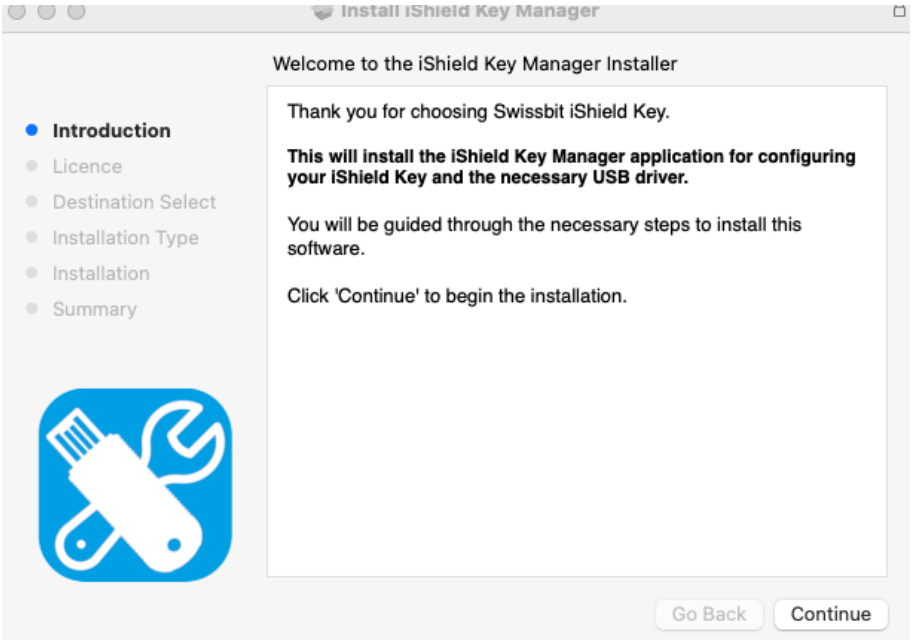
4.1.1.1 Windows でのインストール

アプリケーションをインストールするには、ishield_key_manager.msix パッケージをダブルクリックし、インストーラーの手順に従う必要があります。



4.1.1.2 macOS でのインストール

アプリケーションをインストールするには、**iShieldKeyManagerInstaller.pkg** パッケージをダブルクリックしてください。インストーラーが、アプリケーションのインストールに必要な手順を案内します。



「Continue」をクリックしてインストールを開始します。使用許諾契約に同意した後、画面の指示に従ってください。インストールが完了したら、「アプリケーション」から「iShield Key Manager」をクリックしてアプリケーションを起動できます。

4.1.1.3 Linux でのインストール

Linux に iShield Key Manager をインストールするコマンドを実行します

```
sudo dpkg -i ishield-key-manager.deb
```

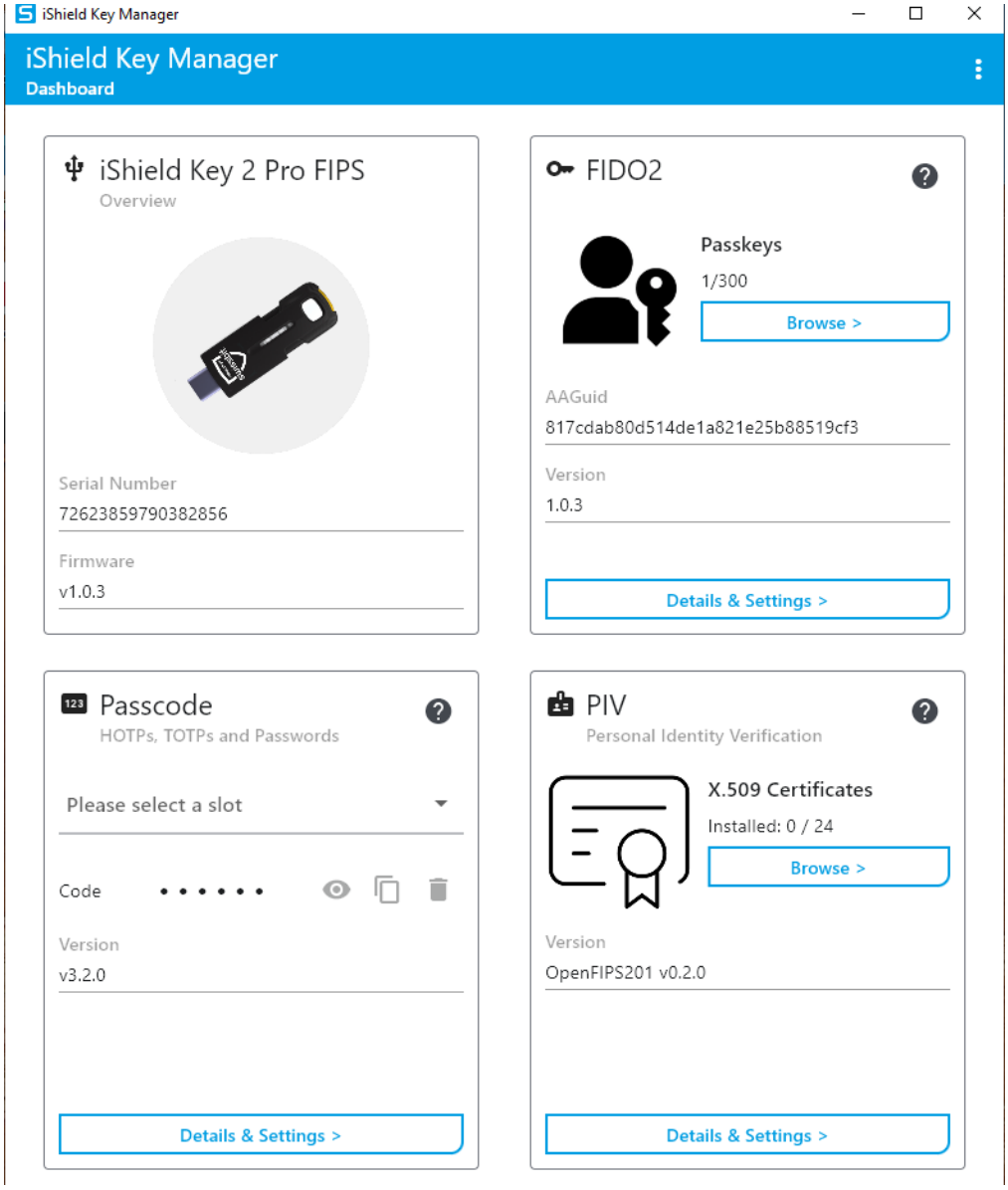
アプリケーションを起動するには次のコマンドを実行します:

```
ishield-key-manager
```

4.1.2 ダッシュボード

iShield Key Manager は、ホスト PC に接続された 1 台の iShield Key 2 のみをサポートします。アプリを起動すると、iShield Key 2 のデータが読み込まれ、概要と iShield Key 2 上のアプレットを管理するためのカードを含むダッシュボードが表示されます。

概要ダッシュボードカードには、iShield Key のシリアル番号やファームウェアバージョンなどの一般的な情報が表示されます。



PIN のルール

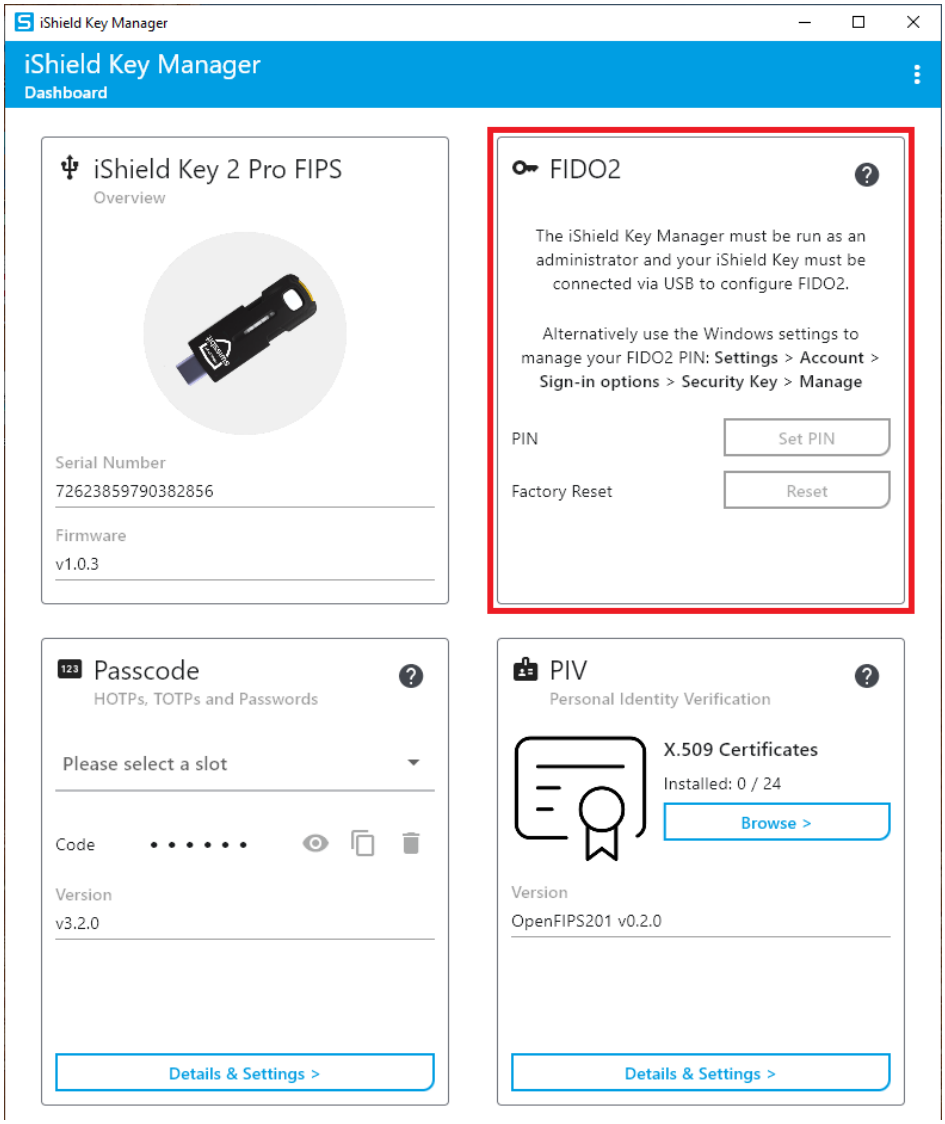
別途指定がない限り、iShield Key 2 の各アプレットの PIN/PUK は以下の規則に従う必要があります:

- PIN は 6 文字以上である必要があります。
- つの文字が同一の文字で構成される PIN (例: 2222as) は許可されませんが、3 つの文字が同一の PIN (例: 222asd) は許可されます。
- 数字または文字の連続 (例: 123456、abcdef) は許可されません。

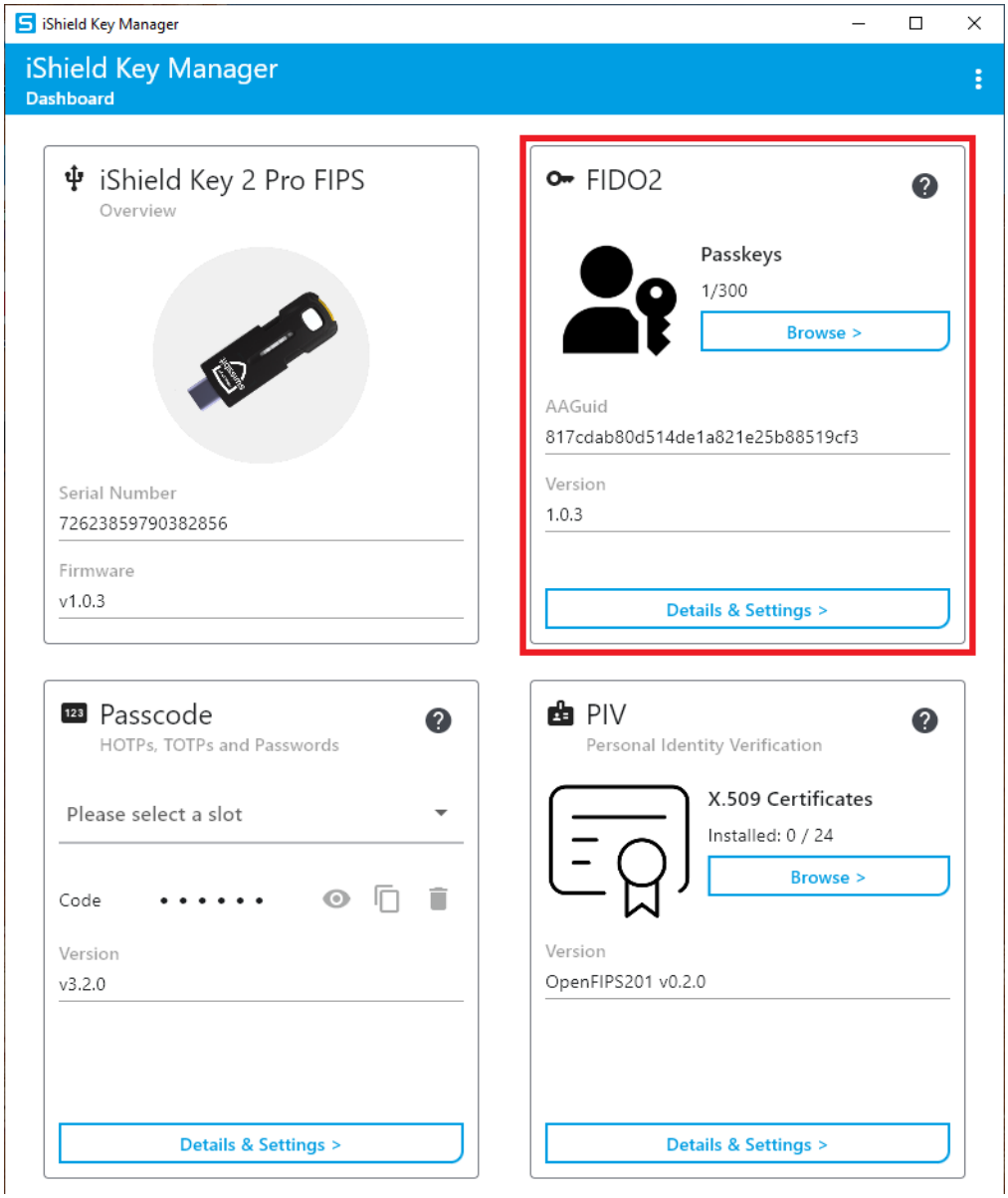
4.1.3 FIDO2 ダッシュボードカード

Windows で iShield Key の FIDO2 機能を管理するには、iShield Key Manager を管理者として起動する必要があります。管理者権限なしでツールを起動した場合は、Windows の設定で PIN の設定またはリセットを行う必要があります。新しい FIDO PIN は 4～8 文字でなければなりません。

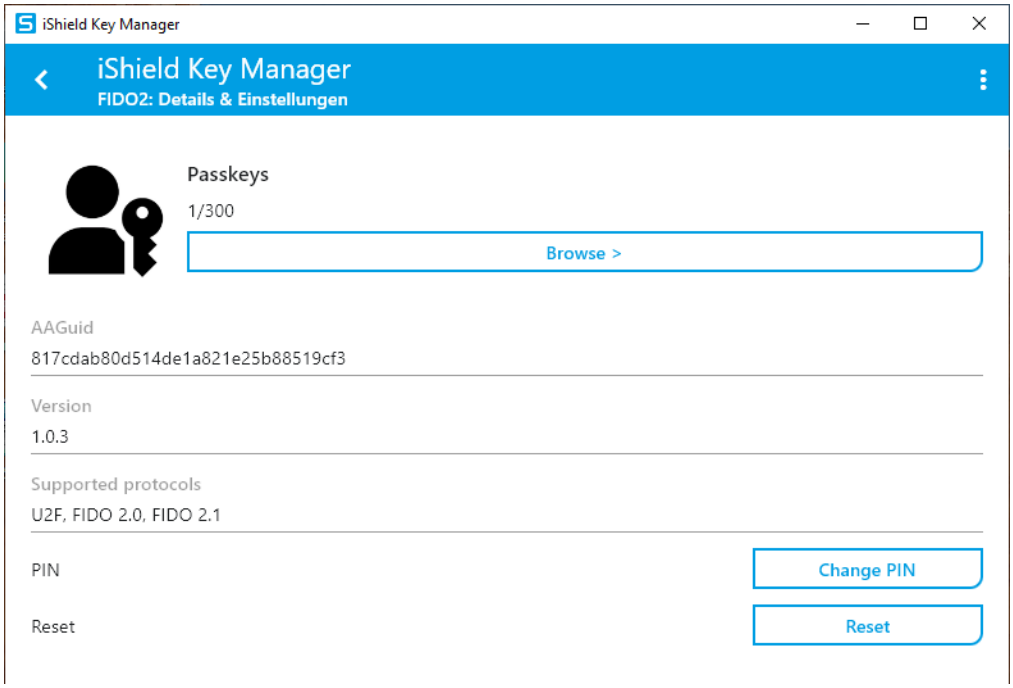
注: FIPS 準拠のため、**iShield Key 2 Pro FIPS** の新しい FIDO2 PIN は PIN のルールに準拠する必要があります。



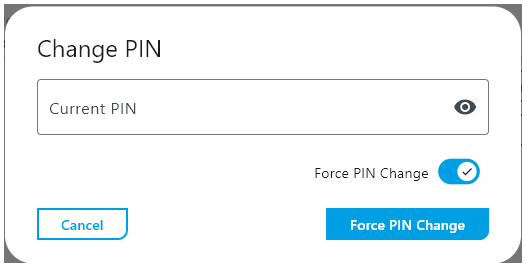
macOS、Linux、または Windows で管理者権限を使用してアプリを起動すると、FIDO2 ダッシュボード カードに AAGUID、FIDO2 アプレットのバージョン、保存されているパスキーの数が表示され、iShield Key 2 のパスキーを管理できるようになります。

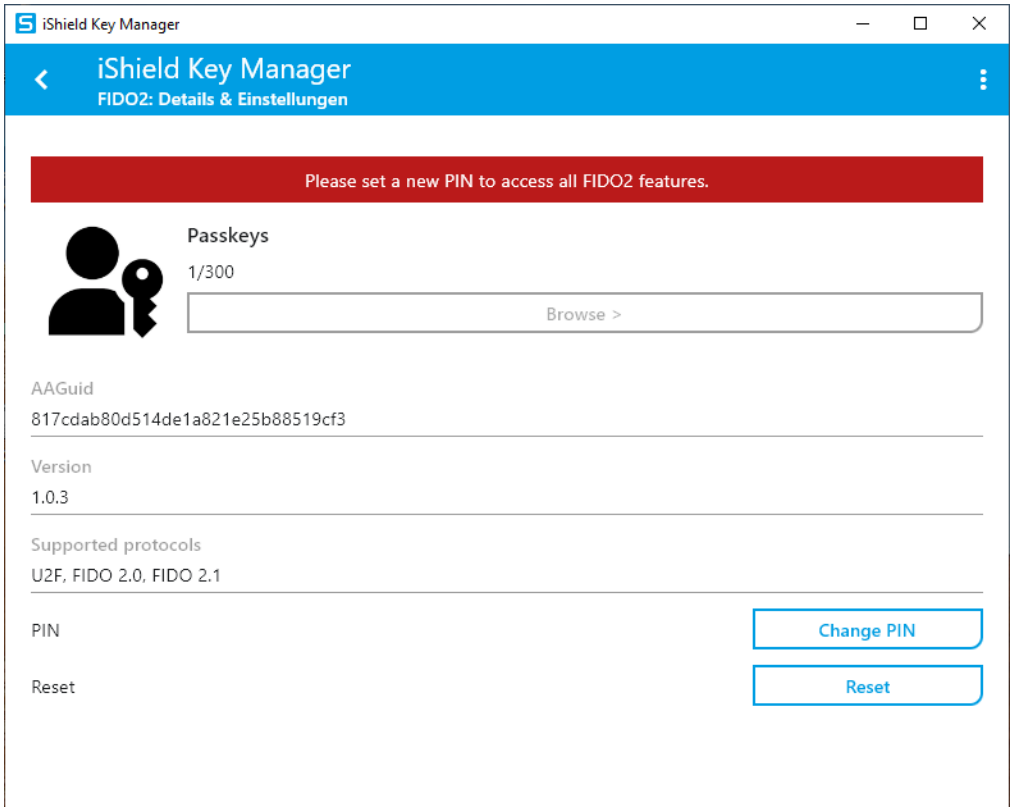


「Details & Settings」をクリックすると、FIDO2 アプレットでサポートされているプロトコルの情報を確認し、新しい PIN を設定したり、後で変更したりできます。PIN を忘れた場合は、iShield Key 2 の FIDO2 アプレットを工場出荷時の設定にリセットできます。これにより、すべてのパスキーが消去されます。.



「PIN の変更」ウィンドウでは、次回使用時に PIN を強制的に変更するオプションがあります。現在の PIN でこの設定を有効にすると、FIDO2 アプレットを次回使用する際に、新しいパスキーを作成する場合でも、既存のパスキーを管理する場合でも、PIN の変更が求められます。



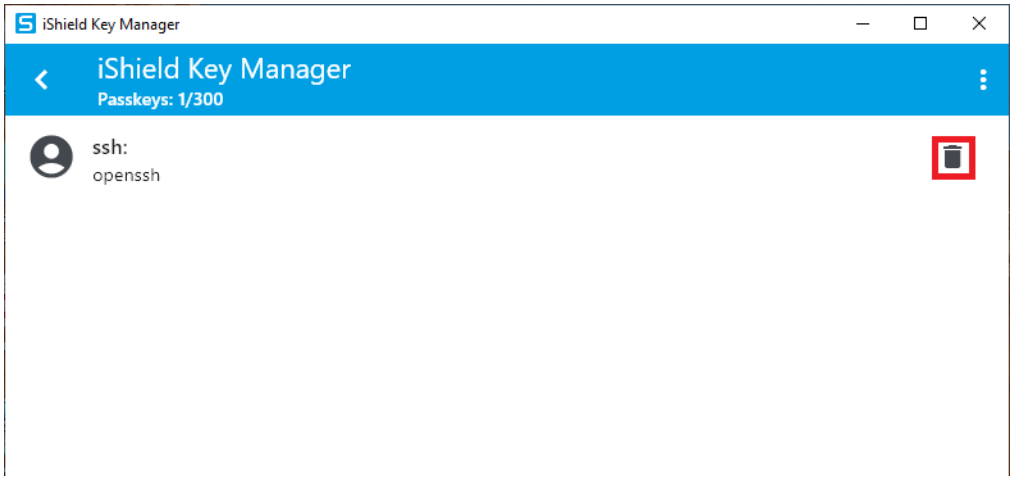


iShield Key 2 は FIDO 2.1（CTAP2.1）規格に対応しており、各パスキーを個別に管理できます。

注：パスキー管理を許可するには、FIDO2 PIN を設定する必要があります。

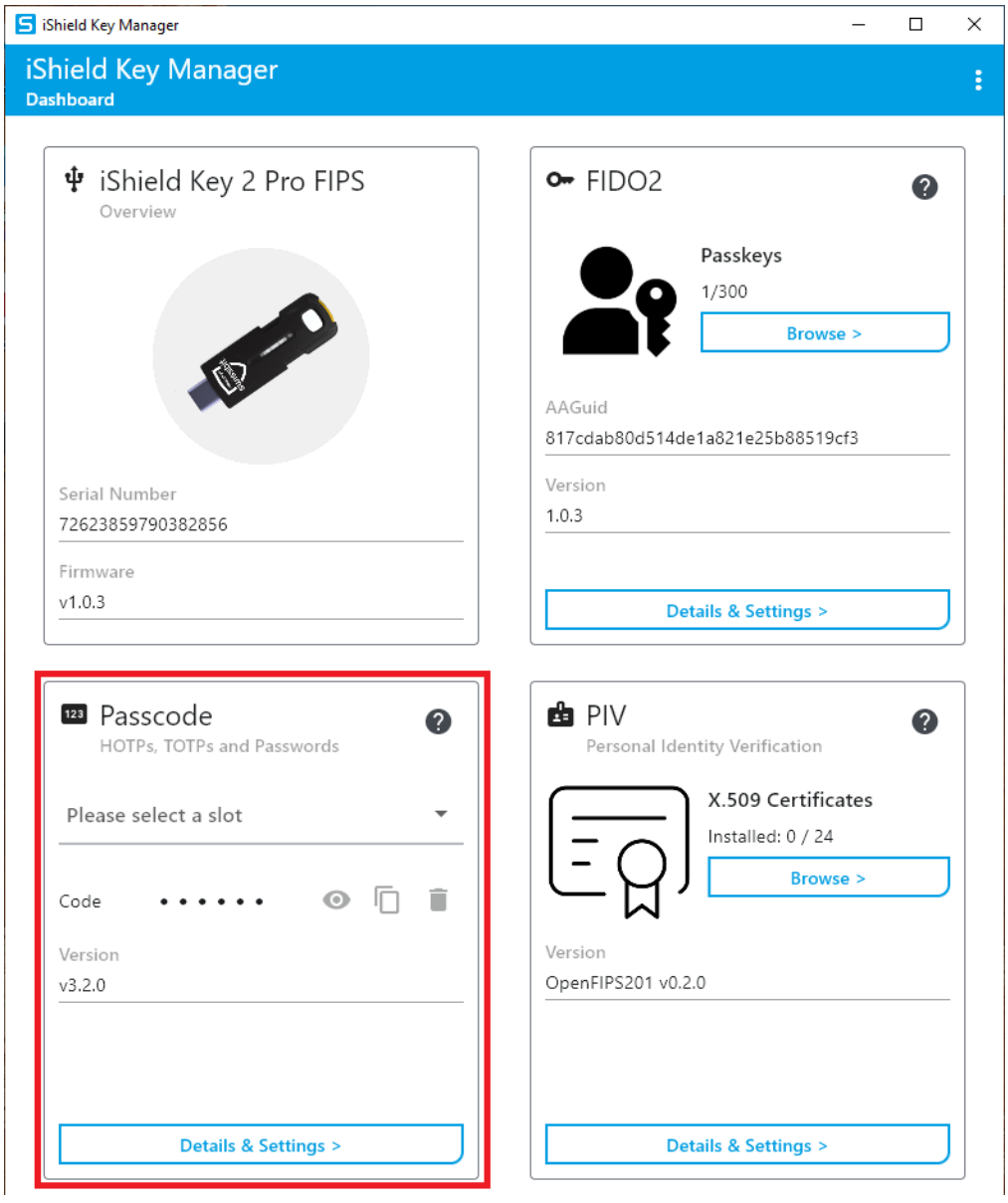
「参照」ボタンをクリックして FIDO2 PIN を入力すると、iShield Key 2 に保存されているすべてのパスキーを確認・管理できます。

さらに、「ゴミ箱」アイコンをクリックすると、パスキーを削除できます。



4.1.4 Passcode ダッシュボードカード

iShield Key 2 Pro は、HOTP/TOTP および静的パスワードをサポートしています。このアプレットは、パスコードカードの iKM で管理されます。このアプレットを使用すると、ユーザーは 2 要素認証（2FA）用の HOTP および TOTP コードを保存したり、静的パスワードを保存したりできます。最大 42 個のスロットをサポートし、HOTP、TOTP、および静的パスワードを自由に設定できます。スロットはオプションでユーザーPIN で保護できます。ユーザーPIN で保護されていない HOTP またはパスワードスロットには、2 種類のタッチジェスチャ（ショートタッチとロングタッチ）を割り当てることができます。



Passcode ダッシュボード カードには、パスコード アプレットのバージョンが表示され、ドロップダウンでは、対応するアイコンを認識してさまざまなタイプのスロットをすばやく選択できます。

HOTP スロット

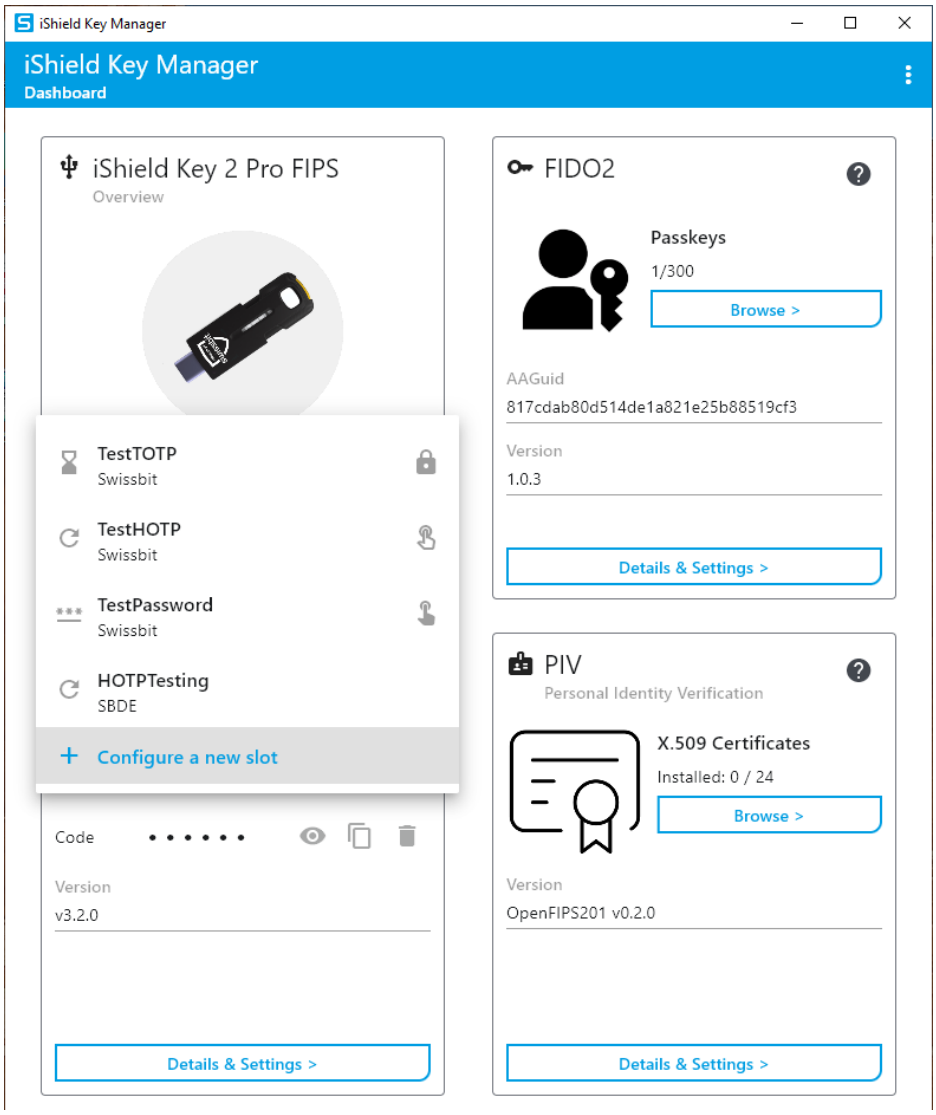
TOTP スロット

Password スロット

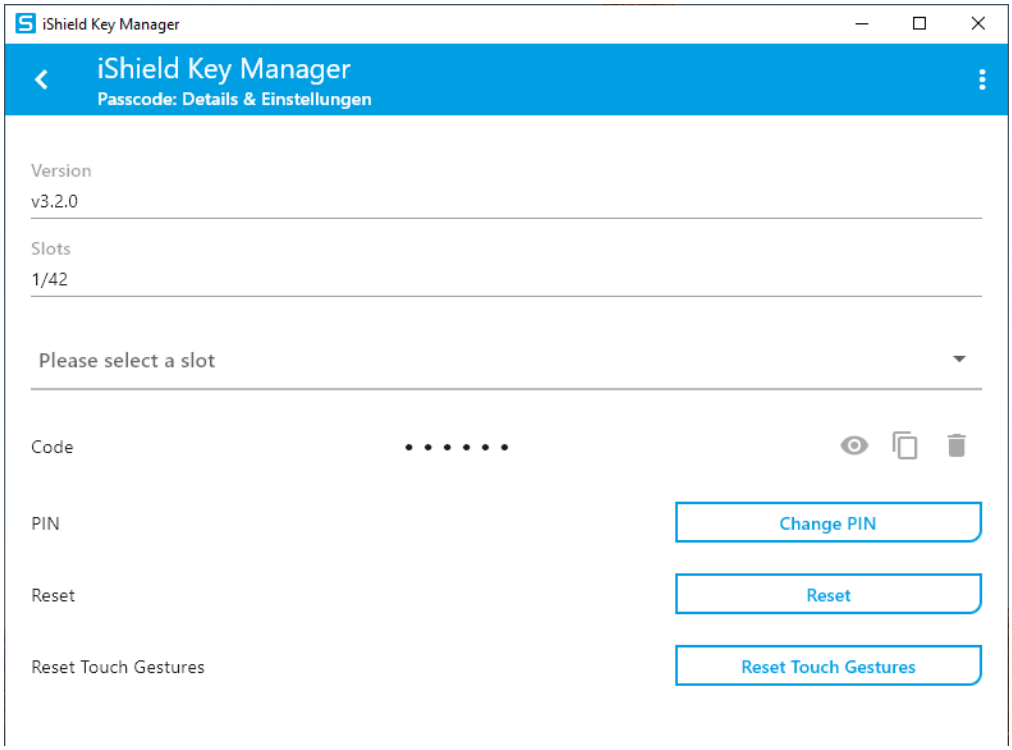
ショートタッチジェスチャ

ロングタッチジェスチャ

スロットがユーザーPIN で保護されている



「Details & Settings」をクリックすると、保存されているスロットの数に関する情報を確認したり、ユーザーPIN を設定または変更したりできます。また、設定済みのスロットに割り当てられたタッチジェスチャをリセットすることもできます。



ユーザーPIN 保護

オプションで、ユーザーPIN を使用してスロットをセキュリティ保護できます。有効にすると、そのスロットから OTP またはパスワードを取得する前にユーザーPIN を入力する必要があります。この機能を有効にするには、まず **PIN のルール**を満たす新しい PIN を設定する必要があります。

ユーザーPIN を 10 回間違えて入力すると、永久にブロックされます！ブロックされると、ユーザーPIN で保護されたスロットからワンタイムパスワードを生成したり、パスワードを取得したりできなくなります。ユーザーPIN 機能へのアクセスを復元するには、**ユーザーPIN のリセット**を実行する必要があります。リセットにより、以下の処理が行われます。

- PIN で保護されたスロットに保存されているすべての認証情報が削除されます。
- ユーザーPIN が削除されます。
- 新しいユーザーPIN を設定できます。

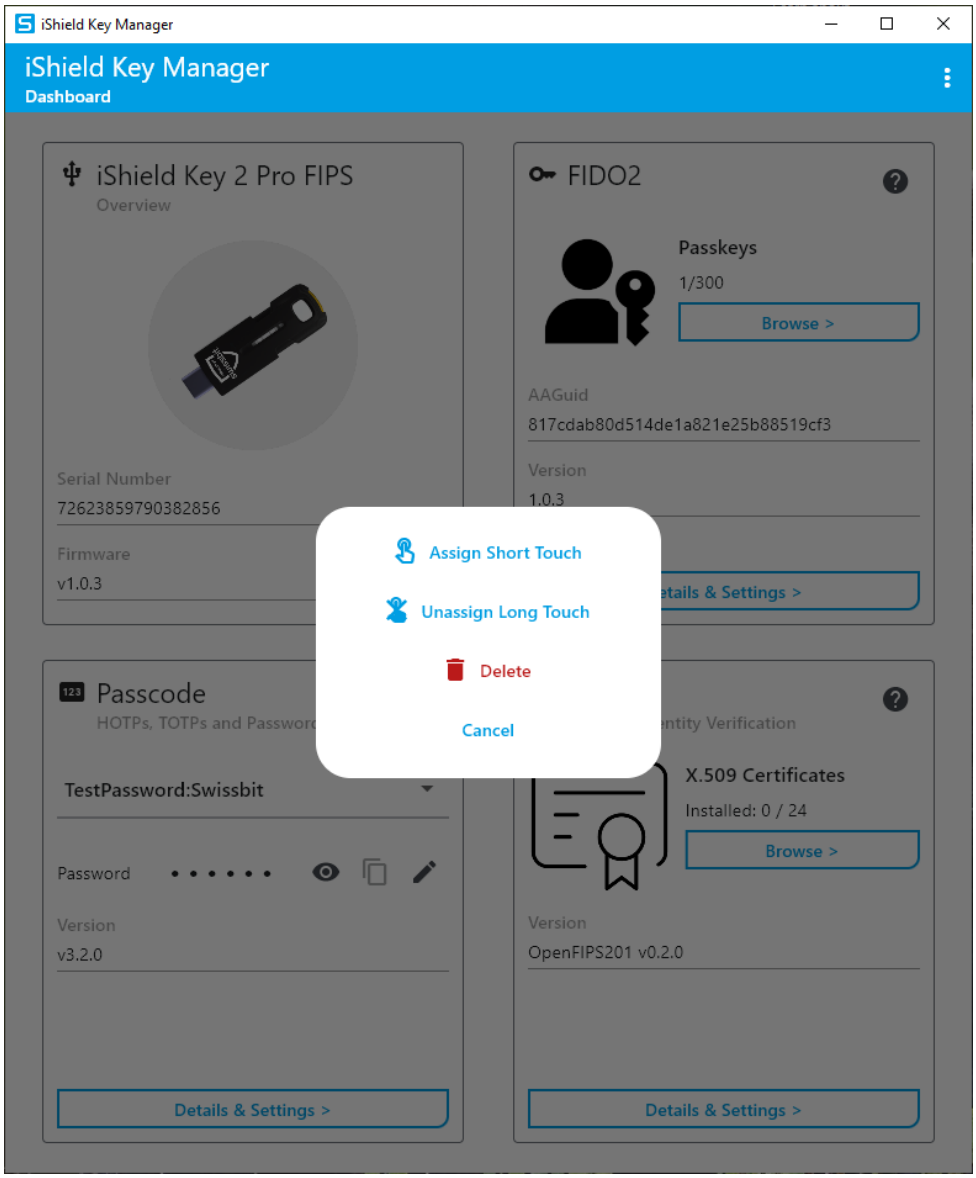
ユーザーPIN による認証に成功すると、再試行カウンターがリセットされます。

Factory Reset を実行すると、iShield Key 2 のパスコードアプレットが元の状態に戻ります。このプロセスにより、すべてのパスコードデータと認証情報が永久に削除されます。

注： ユーザーPIN 保護は、スロットの初期設定時にのみ有効にできます。

ユーザーPIN で保護された HOTP スロットには、タッチジェスチャを割り当てることはできません。

「タッチ」ジェスチャ



iShield Key 2 は、新機能として設定可能なタッチジェスチャーを導入しました。ショートタッチとロングタッチの 2 種類のジェスチャをそれぞれスロットに割り当てることができます。

- ショートタッチ（約 1 秒）すると、割り当てられたスロットに保存されている HOTP またはパスワードが出力されます。
- ロングタッチ（約 3 秒）すると、割り当てられたスロットに保存されている HOTP またはパスワードが出力されます。

これらのジェスチャは、**ユーザーPIN で保護されていない HOTP またはパスワード**スロットにのみ割り当てることができます。

タッチジェスチャが認識されると、iShield Key 2 Pro は USB-HID キーボードインターフェースを介して接続されたデバイスに対応する HOTP またはパスワードを送信し、キーストロークをエミュレートします。

ジェスチャを割り当てるには、設定された HOTP またはパスワードスロットの横にある「鉛筆」アイコンをクリックするだけです。

割り当てられたタッチジェスチャ両方を削除するには、「Details & Settings」に移動し、「Reset Touch Gestures」をクリックします。

注：タッチ時に HOTP またはパスワード出力に「Enter」キーストロークが自動的に追加されます。

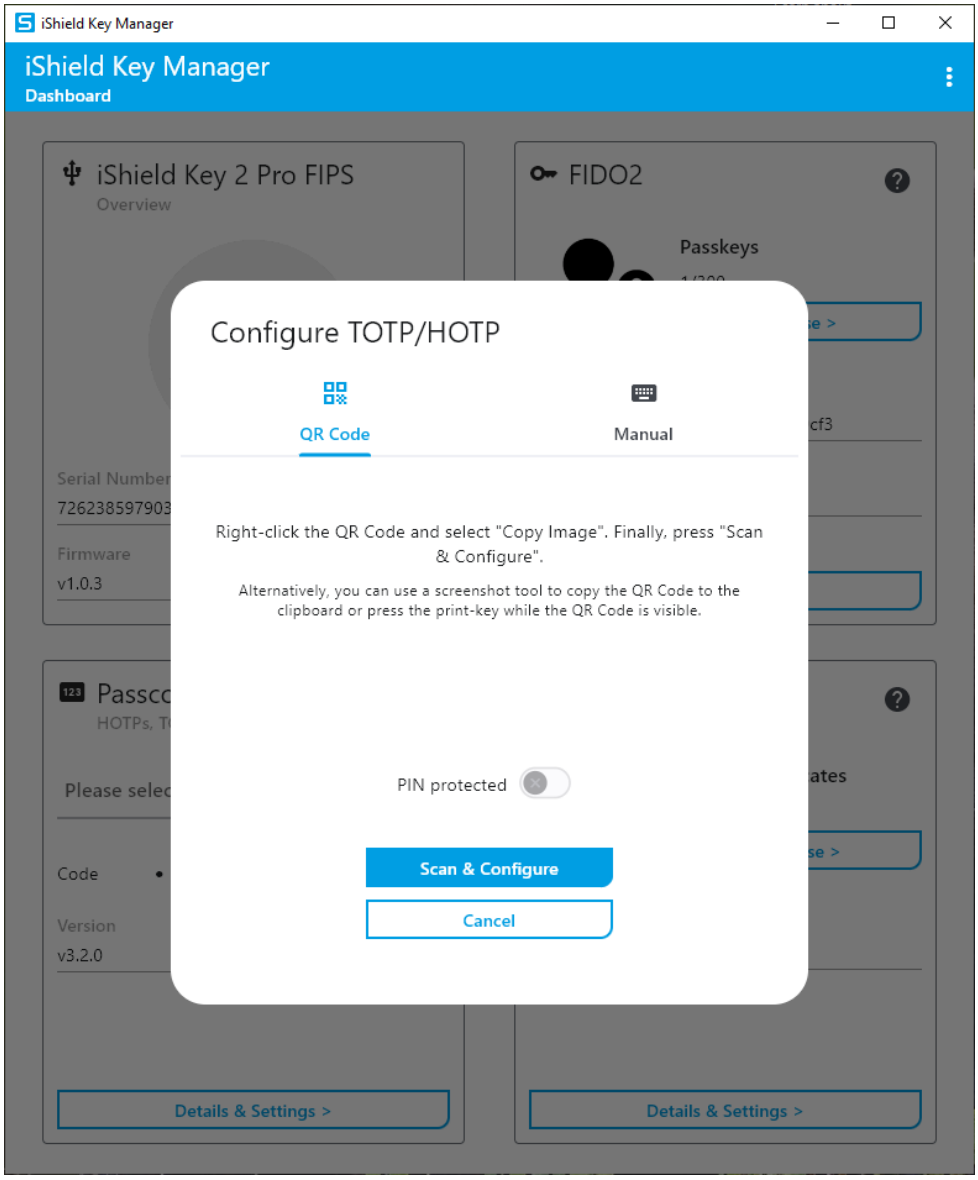
TOTP & HOTP

1. iShield Key 2 Pro を TOTP または HOTP による 2 要素認証に使用するには、まず新しい OTP スロットを設定して、希望のサービスまたはアカウントに登録する必要があります。ドロップダウンメニューを開き、「+ Configure a new slot」を選択してください。

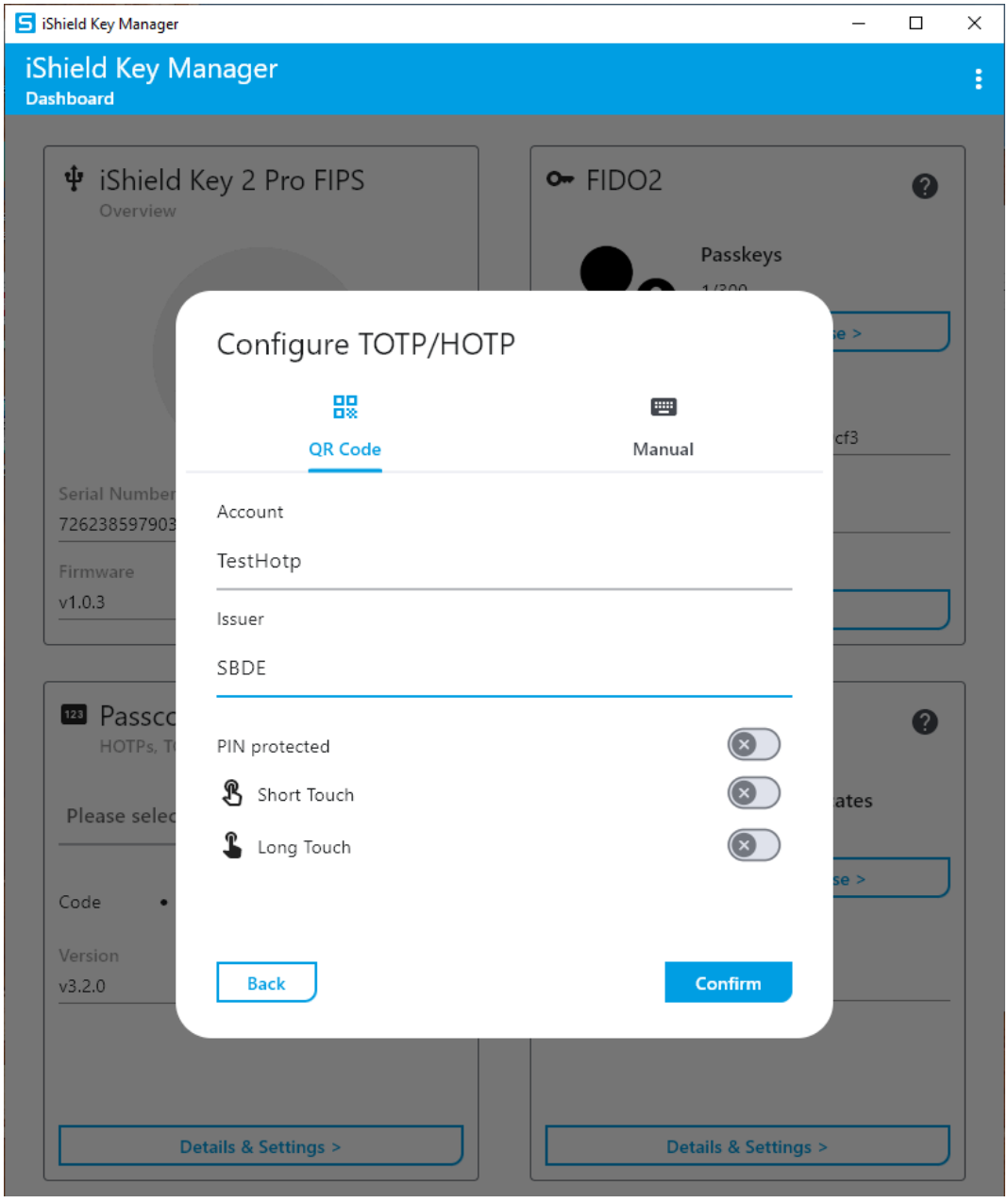
2. スロットの設定は、以下の 2 つの方法のいずれかで行えます:

    a. サービスから提供された QR コードをスキャンする

    b. 必要な情報を手動で入力する



QR コードをスキャンして「Scan & Configure」を押し、OTP スロットを設定すると、QR コードに埋め込まれたアカウント名と発行者情報が次の画面に表示されます。これらの情報は必要に応じて確認・編集できます。同じ画面で、ユーザーPIN 保護の有効化や、ショート / ロングタッチジェスチャの割り当ても行えます。



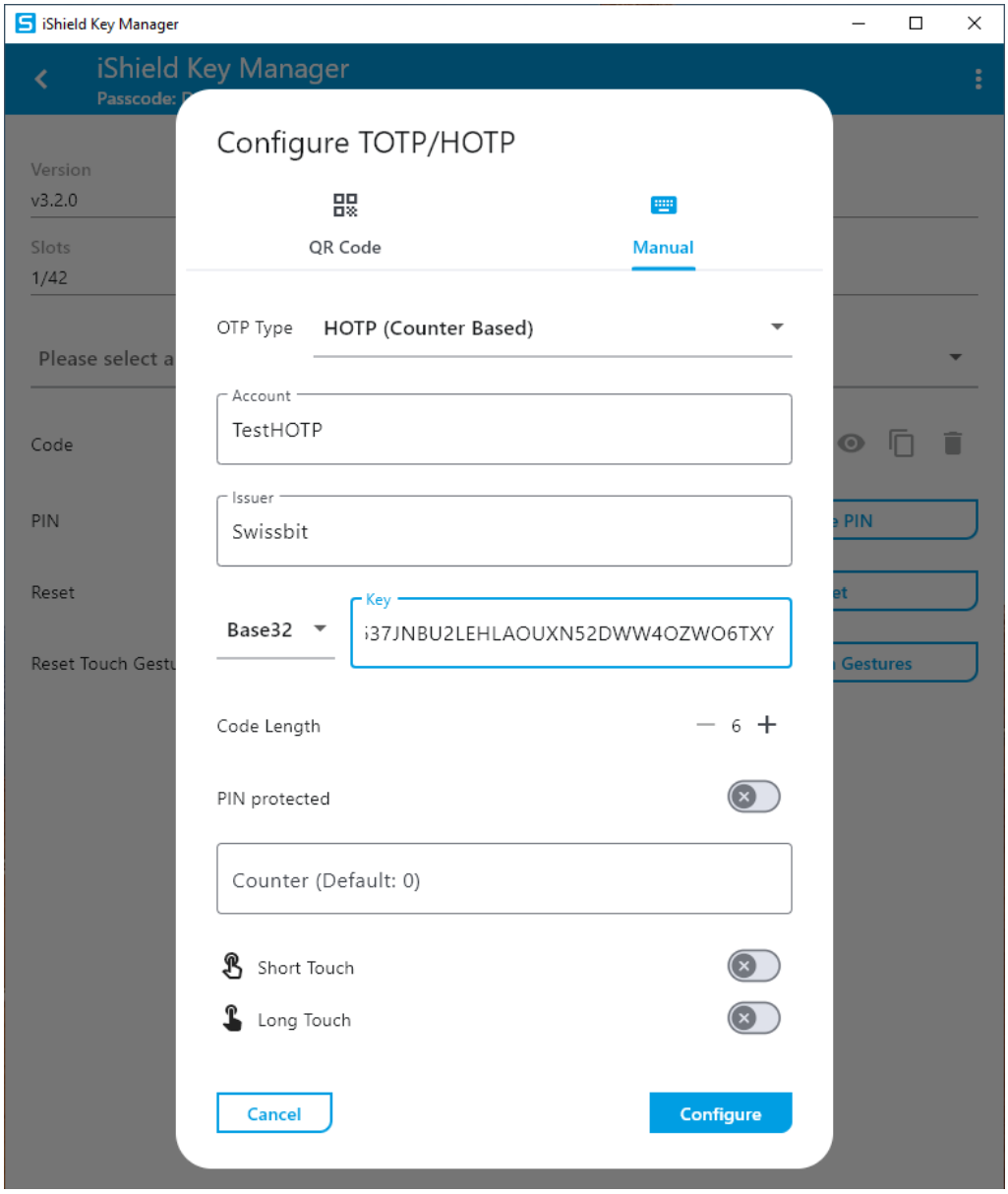
新しいスロットを手動で設定する場合は、新しい HOTP/TOTP スロットのアカウント名と、サービスから提供される秘密鍵（16～64 バイト）を入力する必要があります。デフォルトでは秘密鍵は Base32 形式ですが、鍵入力フィールドの横にあるドロップダウンメニューを使用して 16 進形式に切り替えることができます。また、サービスで使用されているパラメータに合わせて、追加のパラメータを設定する必要がある場合もあります:

- コード長（6～9 桁）
- 初期カウンタ（HOTP の場合。パスコードバージョンが 3.2 未満の場合 0 である必要があります）
- 時間間隔（TOTP の場合）

- アルゴリズム（TOTP の場合）

これらの値がプロバイダーの設定と一致していることを確認することは、認証を成功させるために不可欠です。

必要に応じて発行者名を入力できます。発行者名は、スロットを特定のアカウントまたはサービスに関連付けるのに役立ち、後で識別しやすくなります。



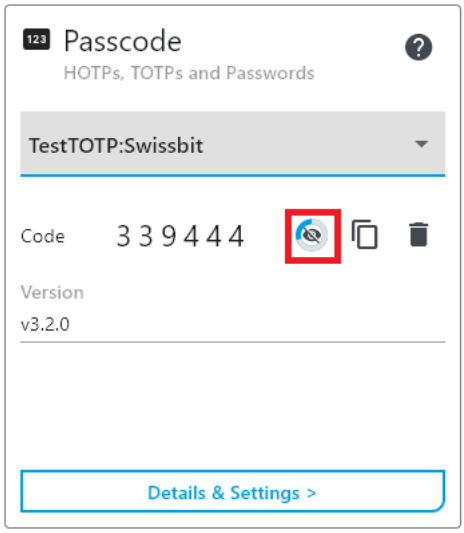
セットアッププロセスを完了するには、通常、サービスからワンタイムパスワード（OTP）の入力を求められます。新しく設定したスロットを選択して OTP コードを生成し、有効期限内にサービスに送信してください。

TOTP スロットの場合、ダッシュボードのカウントダウンバーに TOTP が無効になるまでの残り時間が表示されます。期限が切れると、新しい TOTP が自動的に生成されます。

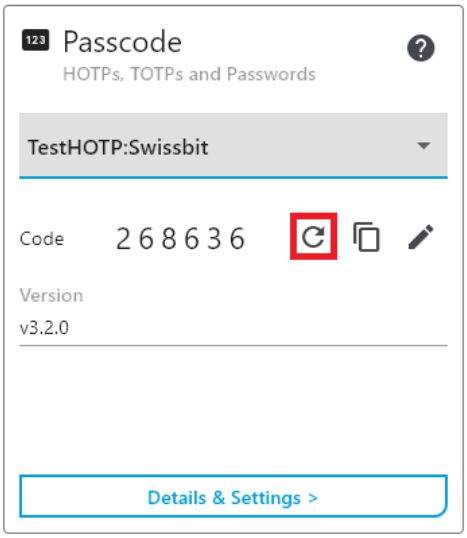
追加オプション：

• OTP コードをクリップボードにコピーして、他の場所で使用できるようにします。

- ゴミ箱アイコンをクリックしてスロットを削除します。

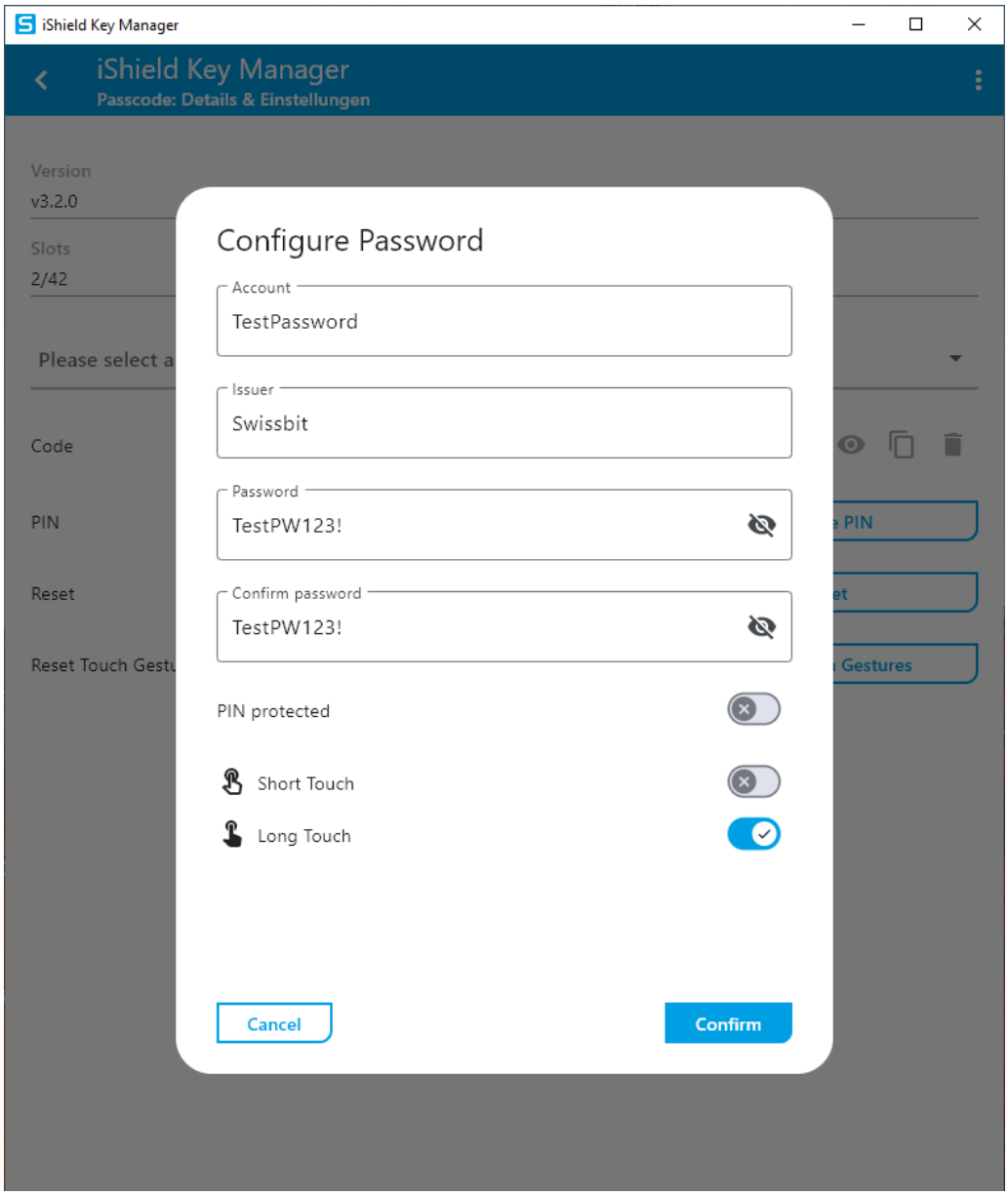


HOTP スロットの場合は、「更新」ボタンをクリックして手動で新しいコードを生成する必要があります。「鉛筆」アイコンをクリックするとダイアログが開き、スロットを削除したり、タッチジェスチャを割り当てたりできます。タッチジェスチャが割り当てられている場合は、iShield Key 2 の背面をタッチするだけで新しい HOTP コードを生成できます。タッチジェスチャの詳細については、「タッチ」ジェスチャのセクションを参照してください。



サービス プロバイダーによる HOTP ベースの 2 要素認証のために複数の iShield Key 2 デバイスを登録する必要がある場合は、「一括登録」セクションが役立つ場合があります。

パスワード



パスワードは、iShield Key 2 Pro で導入された新機能の 1 つです。デバイスにパスワードを保存できます。パスワードスロットにタッチジェスチャが割り当てられている場合は、iShield Key 2 Pro の背面をタッチするだけで、保存されているパスワードが接続されたホストに自動的に入力されます。タッチジェスチャの詳細については、「タッチ」ジェスチャのセクションを参照してください。

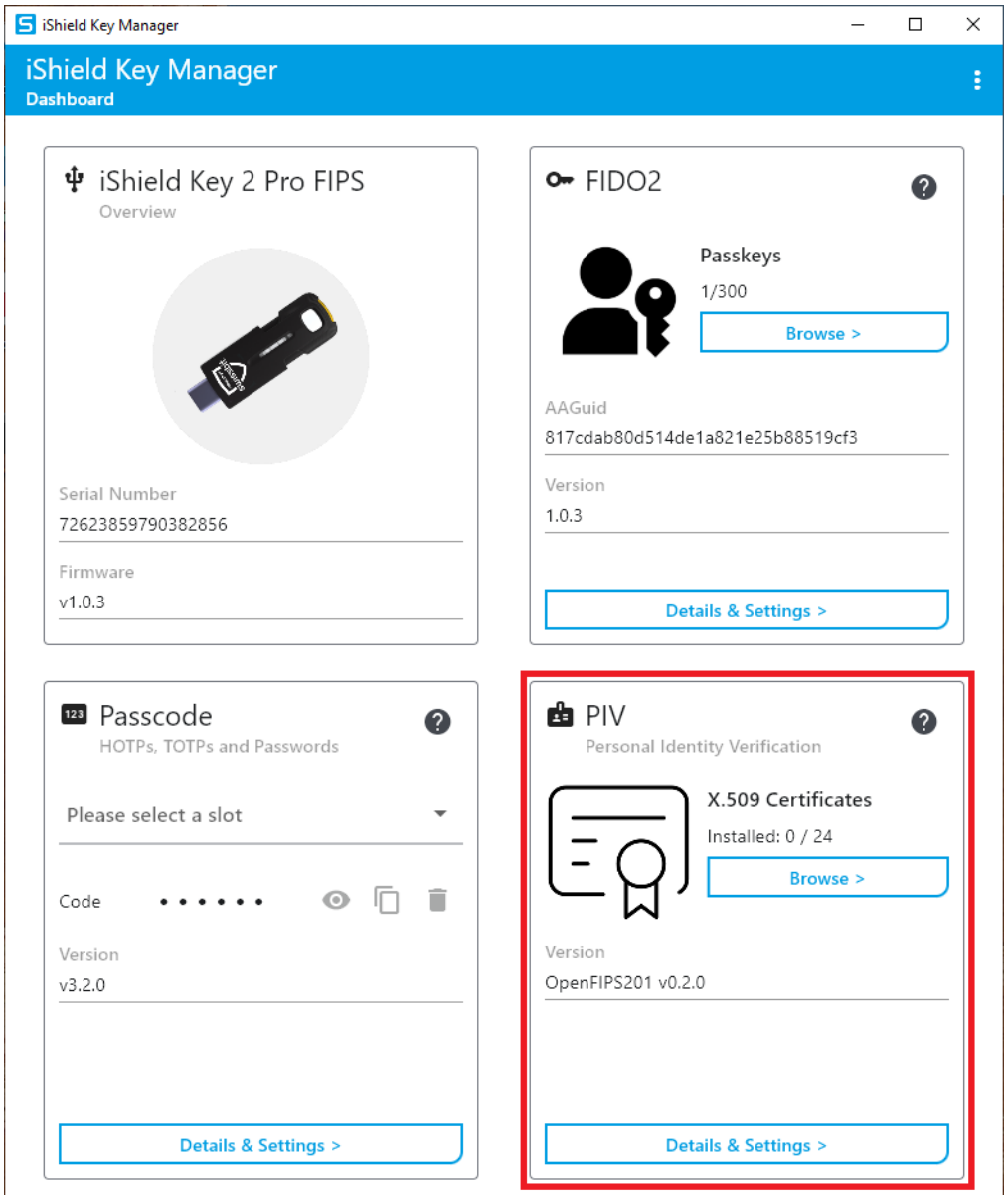
ドロップダウンメニューでは、すでに設定されているパスワードスロットを選択するか、新しいスロットを作成することができます。アカウント情報を入力し、それに応じてパスワードを指定します。オプションで、ユーザー PIN を使用してパスワードスロットを保護することもできます。このオプションを有効にすると、保存されているパスワードにアクセスするには、ユーザー PIN を入力する必要があります。

パスワードスロットでは、「表示」アイコンをクリックするとパスワードを表示できます。「鉛筆」アイコンをクリックすると、スロットを削除したり、タッチジェスチャを割り当てたりできるダイアログが開きます。タッチ ジェスチャが割り当てられている場合は、iShield Key 2 の背面をタッチするだけでパスワードを出力できます。タッチジェスチャの詳細については、「タッチ」ジェスチャのセクションを参照してください。

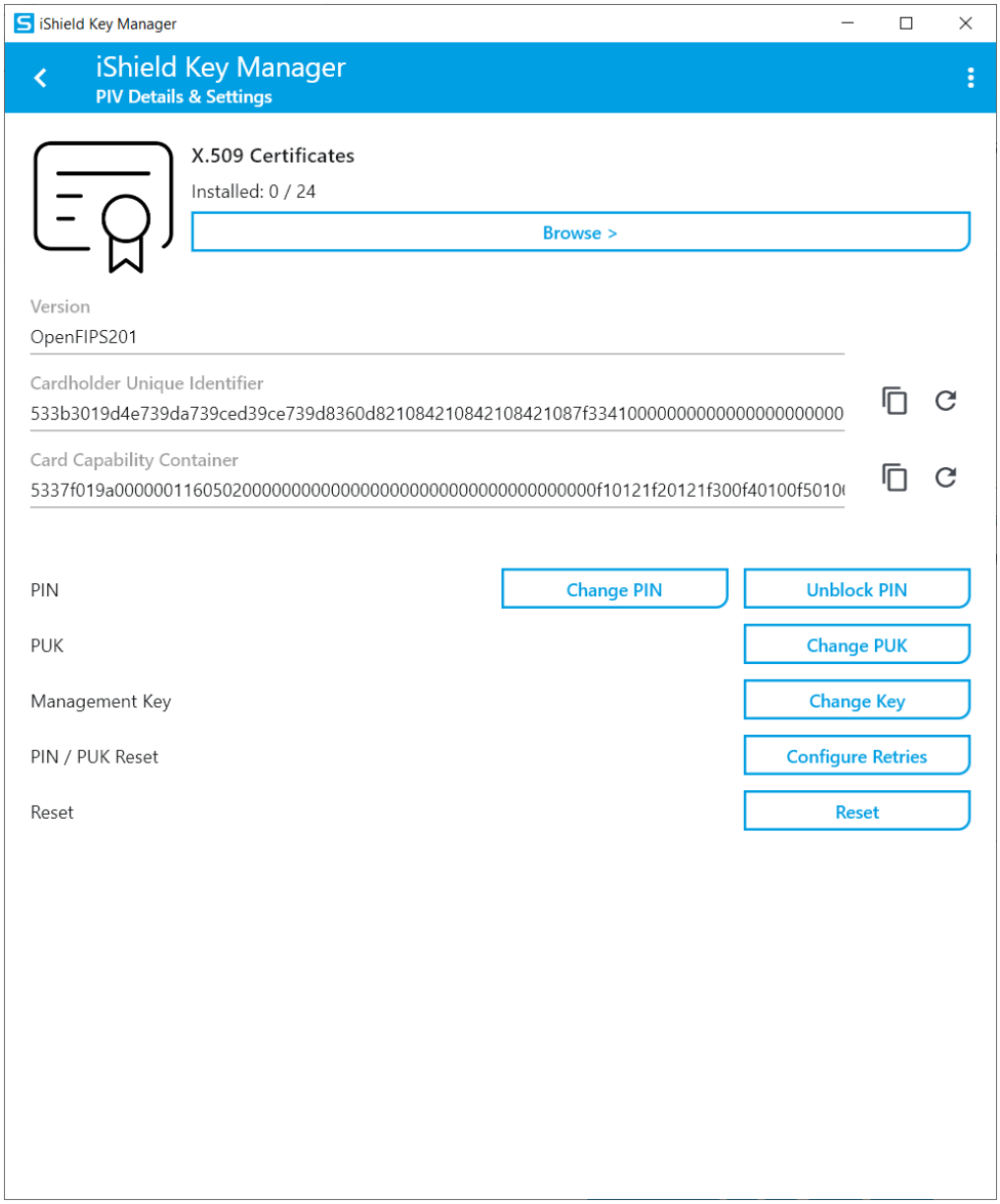
4.1.5 PIV ダッシュボードカード

iShield Key 2 Pro には PIV アプレットがインストールされています。ダッシュボードには PIV アプレットを管理するためのカードも付いています。このカードには、インストールされている PIV アプレットのバージョンと証明書の数が表示されます。

PIV（Personal Identity Verification）規格は、スマートカード技術とデジタル証明書（X.509）を使用することで、物理アクセスとコンピュータシステムの両方で強力な認証を実現します。



iShield Key 2 Pro を使用する前に、PIN、PUK、管理キーを変更することを強くお勧めします。変更するには、「Details & Settings」をクリックしてください。



このページでは、PIN、PUK、管理キーを変更できます。また、PUK を使用して PIN のブロックを解除したり、PIN と PUK の再試行を設定したり、PIN と PUK の両方がブロックされた場合に Factory Reset ですべての PIV を削除したりすることもできます。さらに、新しいカード所有者固有識別子（PIV）またはカード機能コンテナを生成することもできます。

PIN の工場出荷時のデフォルトは **123456**、デフォルトの PUK は **12345678**、管理キーは **010203040506070801020304050607080102030405060708**（AES 192）です。

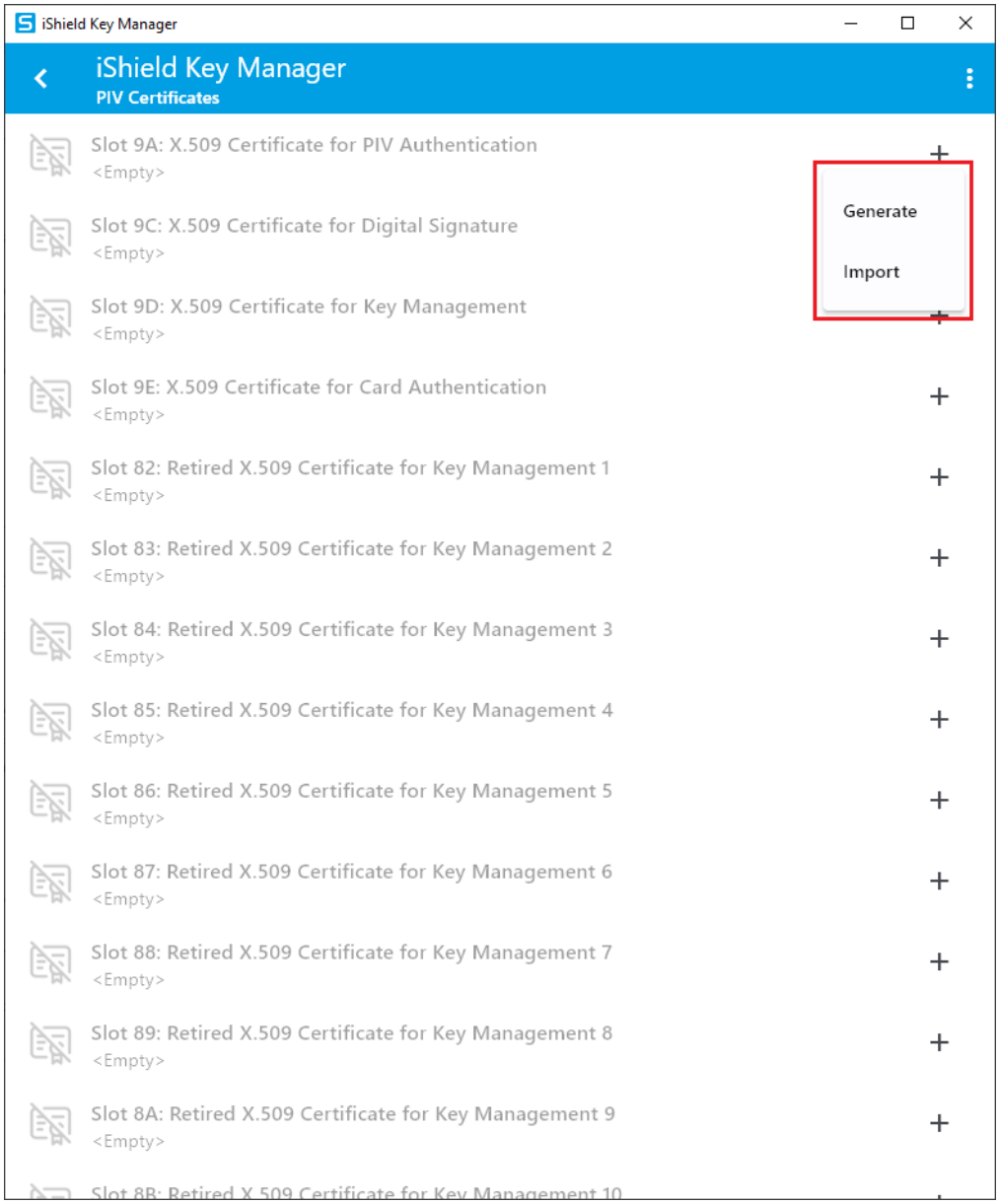
注： FIPS 準拠のため、iShield Key 2 Pro FIPS は **TDES** アルゴリズムをサポートしていません。

新しい PIV PIN と PUK は PIN ルールに準拠している必要があります。

PIV PIN には数字（0～9）のみを含めることができます。

PIV PUK は 8 文字でなければなりません。

「Browse」をクリックすると、インストールされている証明書を確認したり、新しい証明書を追加したりできます。PIV スロット用の証明書署名要求（CSR）を生成し、生成された証明書に CA による署名を付与して、iShield Key 2 Pro にインポートできます。



このビューでは、インストールされている証明書の詳細を確認したり、証明書をエクスポートまたは削除したりすることもできます。

4.2 *iShield Key Manager* コマンドラインツール

iShield Key Manager コマンドラインツール (iKMcli.exe) をパスに追加することをお勧めします。その後、OS のコマンドプロンプトから以下の操作を実行できます:

```
iKMcli <options> SUBCOMMAND
```

iKMcli のヘルプには、すべてのオプションとサブコマンドが一覧表示されます。ヘルプを表示するには、`iKMcli --help` または `iKMcli <options> --help` と入力してください。

このコマンドを実行すると、シリアル番号を含む iShield Key 2 の情報が表示されます。

```
iKMcli info --reader <reader>
```

利用可能なすべてのスマートカード リーダーと iShield Key 2 デバイスを一覧表示するには、次のコマンドを使用します:

```
iKMcli list
```

FIDO2 デバイスの検出には、管理者としてコマンドラインツールを実行する必要があります。

次の 3 つのセクションでは、FIDO2、パスコード（iShield Key 2 Pro のみ）、PIV（iShield Key 2 Pro のみ）でサポートされている操作について詳しく説明します。

4.2.1 FIDO2 コマンド

注: fido コマンドを実行するには、Windows の管理者権限が必要です。

fido オプションは FIDO2 アプレットを管理するためのものです。接続された iShield Key 2 に関する情報を出力するオプションを提供します:

```
iKMcli fido --info
```

`fido` コマンドは最初に検出された iShield Key 2 を使用しますが、iShield Key 2 デバイスを指定することもできます。特定のデバイスに対して操作を実行するには、オプション `--fido-path <path>`でそのパスを渡します。list コマンドを使用すると、接続されているすべての iShield Key 2 デバイスのパスを一覧表示できます。

PIN がまだ設定されていない場合は、以下のコマンドで新しい PIN を設定できます:

```
iKMcli fido --set-pin <new pin>
```

PIN を変更する

```
iKMcli fido --change-pin <new pin> --pin <pin>
```

注: FIPS 準拠のため、iShield Key 2 Pro FIPS の新しい FIDO2 PIN は PIN ルールに準拠する必要があります。

PIN を強制的に変更する

```
iKMcli fido --force-change-pin --pin <pin>
```

iShield Key 2 のパスキーを一覧表示する:

```
iKMcli fido --list-passkeys --pin <pin>
```

iShield Key 2 のパスキーを削除する:

```
iKMcli fido --delete-passkey --pin <pin> --passkey-id <passkey ID>
```

パスキーID は `--list-passkeys` オプションで取得できます。

すべての認証情報と PIN を消去するには、FIDO2 アプレットをリセットします:

```
ikmcli fido --reset
```

リセットするには、iShield Key 2 をタッチするよう求められます。タッチポイントはデバイスの端にあります。

4.2.2 パスコードコマンド

パスコードアプレットを管理するための `password` オプションは、接続された iShield Key 2 Pro のパスコードアプレットのバージョンと利用可能なスロットの数を印刷するオプションを提供します:

```
ikmcli password --info
```

`password` 操作では、最初に検出された iShield Key 2 Pro を使用するか、オプション `--reader <reader>` で使用されるスマートカードリーダーを指定します。`list` コマンドを使用すると、接続されているスマートカードリーダーを表示できます。

以下のコマンドで、ユーザーPIN が設定されているかどうかを確認し、最大試行回数と残り試行回数を取得できます。:

```
ikmcli password --pin-info
```

no User-PIN が設定されている場合, 新たにユーザー PIN を設定できます

```
ikmcli password --set-pin <new pin>
```

ユーザー PIN の変更もできます

```
ikmcli password --change-pin <new pin> --pin <pin>
```

`set-pin` コマンドおよび `change-pin` コマンドの場合、新しいユーザーPIN は PIN のルールに準拠し、最大 16 バイトの長さである必要があります。`--pin-format <ascii|hex>` オプションを使用して PIN の形式を指定できます。オプションが指定されていない場合は、ASCII 形式が想定されます。

ユーザーPIN を 10 回間違えて入力すると、永久にブロックされます！ブロックされると、ユーザーPIN で保護されたスロットからワンタイムパスワードを生成したり、パスワードを取得したりできなくなります。ユーザーPIN 機能へのアクセスを復元するには、**ユーザーPIN のリセット**を実行する必要があります。リセットにより、以下のことが行われます:

PIN で保護されたスロットに保存されているすべての認証情報が削除されます。

ユーザーPIN が削除されます。

新しいユーザーPIN を設定できるようになります。

ユーザーPIN のリセットを実行:

```
ikmcli password --reset-pin
```

注: これにより、PIN で保護されたすべてのパスコードスロットとユーザーPIN が削除されます。

iShield Key 2 のパスコードスロットの一覧を表示:

```
ikmcli password --list-slots
```

次のコマンドを実行すると、すべてのパスコード スロットおよびユーザー PIN を削除し、デフォルト設定を復元できます:

```
ikmcli password --reset
```

注: これにより、すべてのパスコードスロットが削除され、ユーザーPIN が削除されます。

新規パスコードスロットの設定

新しいパスコードスロットを設定

```
ikmcli password --conf-slot --key <key> --account <account>
[--type <TOTP|HOTP|STATIC>]
[--slot-index <index>]
[--key-format <base32|hex|raw>]
[--issuer <issuer>]
[--hmac <SHA1|SHA256|SHA512>]
[--otp-length <6|7|8|9>]
[--period <time period / interval>]
[--pin-protected]
[--touch-gesture <SHORTTAP|LONGPRESS>]
```

下記の指定が必要です:

`--key` HOTP および TOTP の秘密鍵、またはパスワード (最大 58 文字)。

`--account` アカウント名.

オプションとして、下記の指定ができます:

`--type` 設定するパスコードスロットの種類（デフォルトは **TOTP**）。**HOTP または パスワード**スロットを設定する場合は指定する必要があります。

`--slot-index` 指定されたパスワードスロットのインデックス（指定されていない場合は、デフォルトで最初の空きスロットになります）

注: 指定されたスロットがすでに構成されている場合は、警告なしに新しい値で上書きされます。

`--key-format` キー値の形式。パスワードが設定されている場合は、raw を指定する必要があります。

`--issuer` アカウントにリンクされているプロバイダーまたはサービス名。最大 60 文字。

`--hmac` HMAC ハッシュアルゴリズム。デフォルトは SHA1（HOTP スロットでは常に SHA1 を使用）。

`--otp-length` TOTP または HOTP スロット用に生成される OTP の長さ。デフォルトは 6。

`--period` TOTP アルゴリズムの期間/間隔（秒）。デフォルトは 30。

`--pin-protected` パスコードスロットに PIN 保護フラグを設定する。

`--touch-gesture` HOTP またはパスワードスロットにタッチジェスチャーを割り当てる。

例:

アカウント「testTOTP」と発行者「SBDE」のインデックス「2」で TOTP スロットを設定します:

```
ikmcli password --conf-slot --key I65VU7K5ZQL7WB4E --account testTOTP --issuer SBDE --slot-index 2
```

アカウント「testHOTP」、OTP の長さ「8」、インデックス「3」、タッチジェスチャ「ショートタッチ」の HOTP スロットを設定します:

```
ikmcli password --conf-slot --key I65VU7K5ZQL7WB4E --account testHOTP --type HOTP --slot-index 3 --otp-length 8 --touch-gesture SHORTTAP
```

PIN で保護されたインデックス「4」のアカウント「testPassword」のパスワードスロットを設定します:

```
iKMcli password --conf-slot --key TestPW123! --account testPassword --type STATIC --slot-index
4 --key-format raw --pin-protected
```

タッチ ジェスチャを使用して構成済みのスロットを割り当てることができます:

```
iKMcli password --conf-default-slot
--slot-index <index> --touch-gesture <SHORTTAP|LONGPRESS>
```

注: TOTP スロットおよび PIN で保護されたスロットは、タッチ ジェスチャでは割り当てられません。

設定されたスロットに割り当てられたタッチ ジェスチャをリセット:

```
iKMcli password --reset-default-slots
```

新しい OTP を生成、またはパスワードを取得する

特定のスロットおよび現在のホスト時間の TOTP を生成:

```
iKMcli password --gen-totp --slot-index <index> [--pin <pin>]
```

特定のスロットの HOTP を生成:

```
iKMcli password --gen-hotp --slot-index <index> [--pin <pin>]
```

特定のスロットから保存されたパスワードを取得:

```
iKMcli password --get-password --slot-index <index> [--pin <pin>]
```

1 つのスロットをクリア

```
iKMcli password --clear-slot --slot-index <index>
```

4.2.3 PIV コマンド

piv コマンドには、iShield Key 2 Pro にインストールされている PIV アプレットのバージョンとキーのシリアル番号を表示するオプションもあります:

```
iKMcli piv --info
```

piv 操作では、最初に検出された iShield Key 2 Pro を使用するか、オプション --reader <reader> を使用して使用するスマートカードリーダーを指定します。list コマンドを使用すると、接続されているスマートカードリーダーを表示できます。

iKMcli を使用すると、PIV 操作の認証に使用する PIN、PUK、管理キーを変更できます。PIN の工場出荷時のデフォルトは **123456**、デフォルトの PUK は **12345678**、管理キーは AES 192 で **010203040506070801020304050607080** です。以下のコマンドを使用して、PIN を変更したり、PUK による PIN のブロックを解除したりできます:

```
iKMcli piv --change-pin <new pin> --pin <pin>
iKMcli piv --unblock-pin <new pin> --puk <puk>
```

PUK を変更:

```
iKMcli piv --change-puk <new puk> --puk <puk>
```

PIN と PUK の再試行:

```
iKMcli piv --configure-retries --pin-retries <new pin retries> --puk-retries <new puk
retries> --management-key <key> --pin <pin>
```

このコマンドは、PIN と PUK を工場出荷時のデフォルトパスワードにリセットします。

新しい管理キーを設定:

```
iKMcli piv --set-management-key <new key> --management-key <key>
[--new-management-key-algorithm <TDES|AES128|AES192|AES256>]
```

キーは 16 進数でエンコードされた文字列で指定する必要があります。

オプションとして指定:

--new-management-key-algorithm the algorithm of the Management key is AES192 by default.

注: FIPS 準拠のため、iShield Key 2 Pro FIPS は **TDES** アルゴリズムをサポートしていません。

新しい PIV PIN と PUK は PIN のルールに準拠する必要があります。

PIV PIN には数字（0～9）のみを使用できます。

PIV PUK は 8 文字である必要があります。

以下のコマンドを使用して、スマートカード内のすべての証明書を一覧表示したり、スロット内の証明書を印刷したりできます:

```
iKMcli piv --list-certificates
iKMcli piv --read-certificate <slot> [--output <output file>]
```

スロットに新しいキーペアを生成:

```
iKMcli piv --generate-key-pair <slot> --management-key <key> [--output <output file>]
```

公開鍵は出力ファイルまたはコマンドラインに出力されます。その後、公開鍵を使用して証明書署名要求を作成できます:

```
ikmcli piv --request-certificate <slot> --pin <pin> --input <input file> [--output
<output file>]
```

入力ファイルで公開鍵を渡し、対応する秘密鍵でスロットの証明書を要求する必要があります。PIN は、秘密鍵による証明書署名要求の署名を認証するために必要です。

その後、生成された証明書署名要求を CA に送信して署名を依頼し、次のコマンドで署名済みの証明書をインポートできます:

```
ikmcli piv --import-certificate <slot> --management-key <key> --input <input file>
```

秘密鍵をインポート

```
ikmcli piv --import-key <slot> --management-key <key> --input <input file>
```

必ず正しいスロットを指定してください。スロット内の秘密鍵は公開鍵と証明書に紐付けられます。

スロット番号で証明書を削除

```
ikmcli piv --delete-certificate <slot> --management-key <key>
```

PIN と PUK の両方がブロックされている場合は、PIV アプレットをリセットできます。これにより、すべての PIV データが消去され、デフォルト設定が復元されます。

```
ikmcli piv --reset
```

カード所有者の一意の識別子 (CHUID) とカード機能コンテナ (CCC) の新しい値は、次のコマンドで設定できます:

```
ikmcli piv --set-chuid --management-key <key>
ikmcli piv --set-ccc --management-key <key>
```

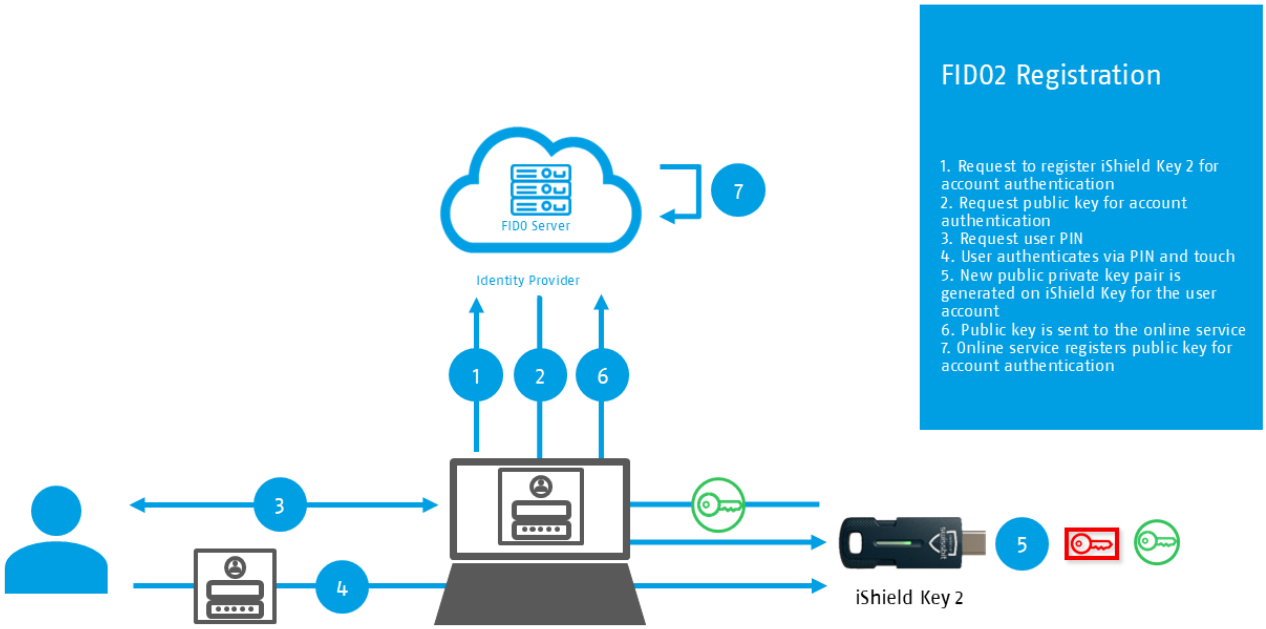
5 FIDO2 アプリケーション (スタンダード)

5.1 概要

Swissbit iShield Key 2 は、オンラインアカウントを保護するために FIDO2 および U2F 標準をサポートする FIDO 認定のプラグアンドプレイセキュリティ製品です。これらは、最も強力で信頼性の高いハードウェア認証を提供し、ユーザーが Google、Microsoft、Salesforce、Amazon Web Services などの Web サイト、アプリケーション、オンラインサービスに安全にアクセスできるようにし、企業ネットワークへのアクセスを保護できます。詳細については、FIDO Alliance の Web サイト（https://fidoalliance.org/fido2/）をご覧ください。テスト Web サイト（https://webauthn.io/）を使用して、ユーザーが Swissbit iShield Key 2 の機能をテストできるようにすることができます。

このセクションでは、FIDO2 の登録とログインについて説明します。すべての FIDO2 機能は、iShield Key 2 製品バリアントで同等です。セクション 5.2 では iShield Key 2 の使用を開始し、セクション 5.3 では、さまざまなサービスのより詳細な構成について Swissbit コミュニティポータルにアクセスする方法について説明します。

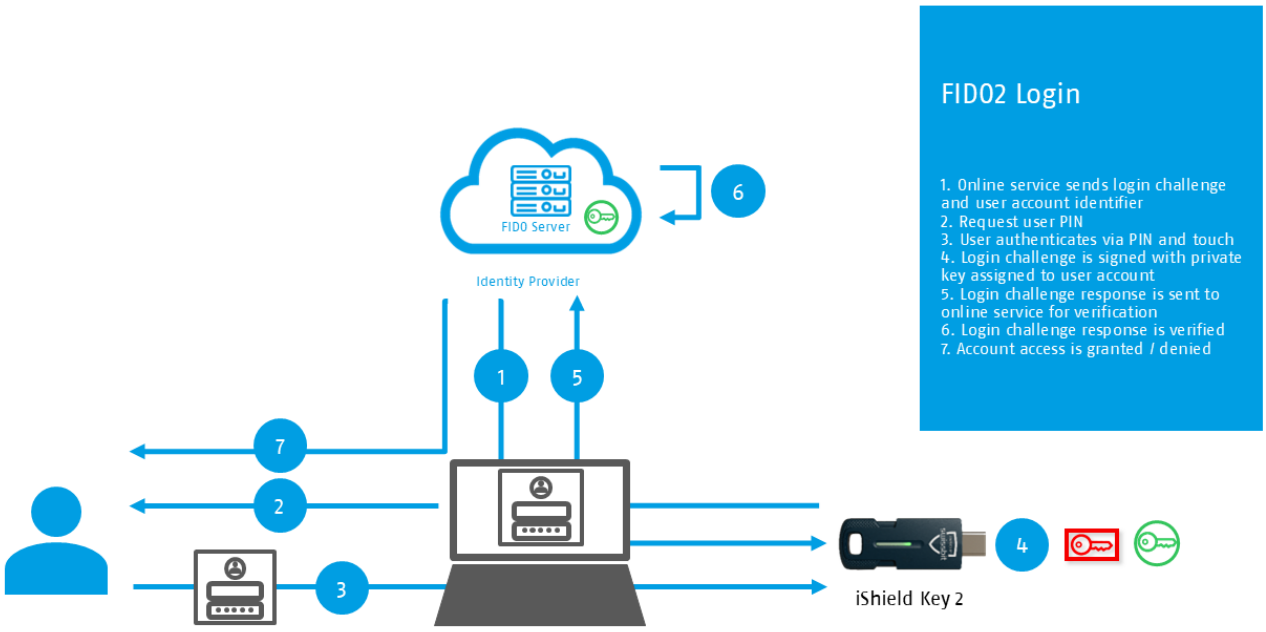
5.1.1 FIDO2 登録



FIDO2 をサポートするサービスへの登録時、サーバーはユーザーのアカウントに関連付ける公開鍵を要求します。ユーザーは対応する秘密鍵を所有していることを証明することで認証できます。

iShield Key 2 を使用して FIDO2 に登録すると、秘密鍵は安全に生成され、デバイス本体に保存されます。秘密鍵はハードウェア認証装置から外部に漏洩することがないため、強力な保護と FIDO2 セキュリティ標準への準拠が確保されます。

5.1.2 FIDO2 ログイン



FIDO2 登録が成功すると、オンラインサービスはユーザーアカウントの公開鍵を取得し、対応する秘密鍵は iShield Key 2 に安全に保存されます。オンラインサービスは、ユーザーに秘密鍵による署名を求めます。オンラインサーバーが公開鍵を使用して署名を検証できた場合、認証は成功し、ユーザーはアカウントへのアクセスを許可されます。

5.2 FIDO2 アプリケーションを開始する

5.2.1 前提条件

Swissbit iShield Key 2 の FIDO 機能は、以下のプラットフォームでご利用いただけます。

- OS:
  - Windows 10 & 11
  - MacOS
  - Linux
  - Chrome OS
  - Android
  - iOS

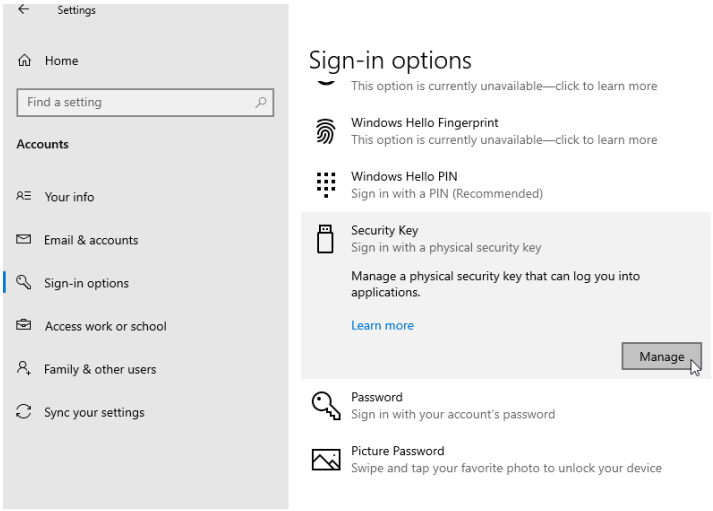
- ブラウザ:
  - Firefox
  - MS Edge
  - Chrome
  - Apple Safari

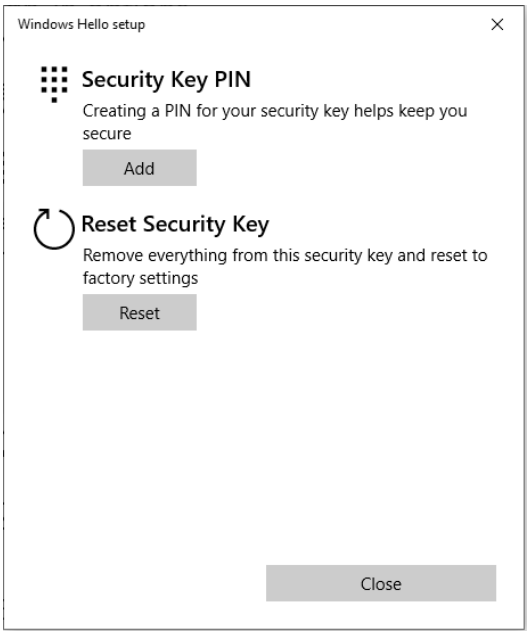
5.2.2 Swissbit iShield Key 2 の PIN を設定

注: Swissbit iShield Key 2 はすぐに使用できます。FIDO2 PIN が不要な場合は、セクション 5.2.3 に進んでください。

FIPS 準拠のため、iShield Key 2 Pro FIPS の新しい FIDO2 PIN は PIN のルールに準拠する必要があります。

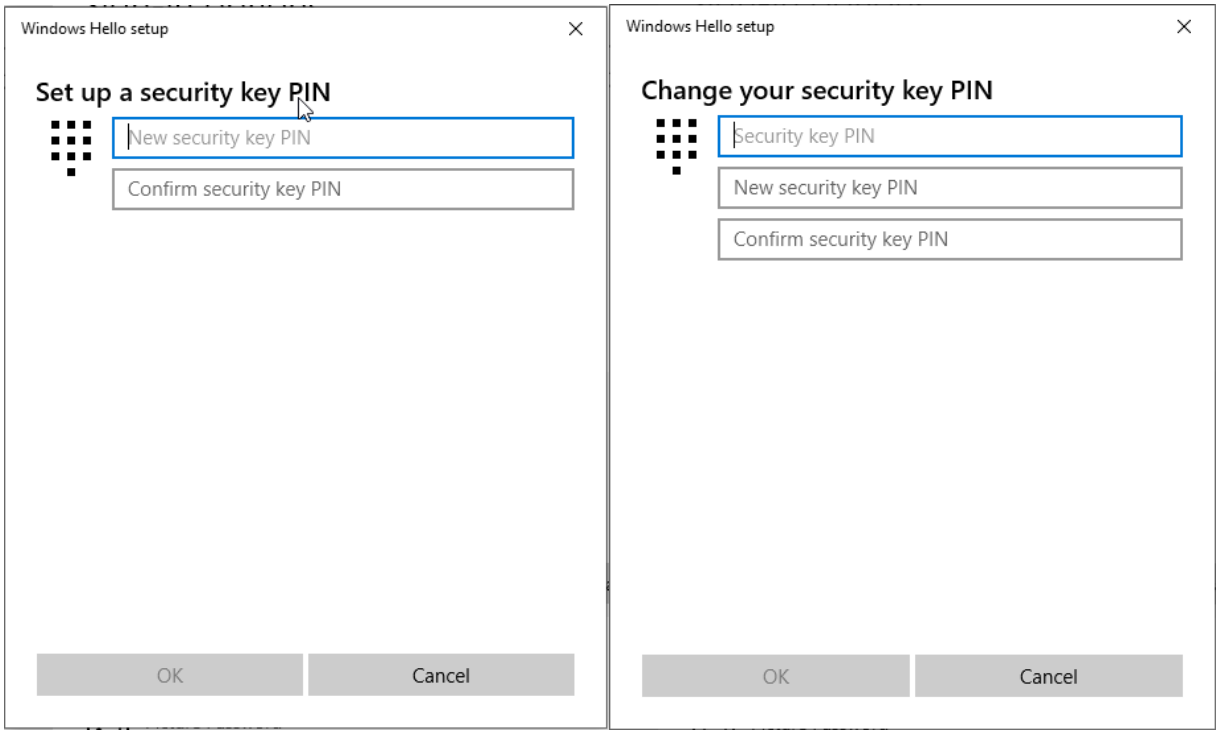
Swissbit iShield Key 2 の FIDO2 アプレットをリセットしたり、FIDO2 PIN を設定/変更したりするには、Windows 10/11 に組み込まれているセキュリティキー管理機能を使用できます。セキュリティキー管理を起動するには、「Start ---> Settings ---> Accounts」の順に進み、「SecurityKey」オプションを選択して「Manage」ボタンをクリックしてください。



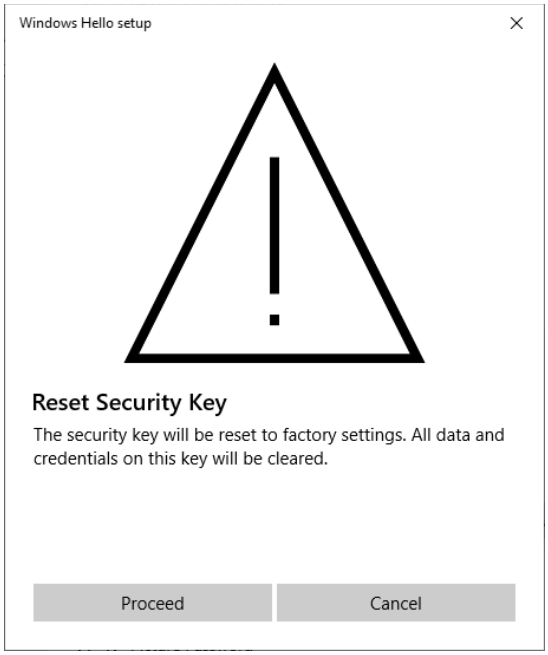


ポップアップウィンドウが表示され、セキュリティキーを USB ポートに挿入するよう求められます。Swissbit iShield Key 2 を挿入してください。

Swissbit iShield Key 2 が認識されると、Swissbit iShield Key 2 の FIDO2 PIN を作成するか変更するかを選択できます。PIN を紛失または忘れた場合は、Swissbit iShield Key 2 の FIDO2 アプレットをリセットできます。ただし、これにより FIDO2 PIN とすべての FIDO2 認証情報が削除されることに**ご注意ください**。



リセットすると、iShield Key 2 に保存されている資格情報が失われることに**注意してください**。


Windows Hello setup
Reset Security Key
The security key will be reset to factory settings. All data and credentials on this key will be cleared.
Proceed
Cancel

5.2.3 テスト登録

Swissbit iShield Key 2 をテストするには、WebAuthn をサポートするテストサイト https://webauthn.io にアクセスしてください。

ウェブサイトは以下のようなものです:

Swissbit iShield Key を登録するには、認証 ID に任意の名前を入力し、「Register」をクリックします。

セクション 5.2.2 に記載されているようにセキュリティ PIN が設定されている場合は、FIDO2 PIN が必要になります。

注: FIDO2 PIN を紛失した場合、または使用ケースで必要ない場合は、セクション 5.2.2 に進み、iShield Key 2 をリセットしてください。リセット後にキーを再度登録する必要があります。

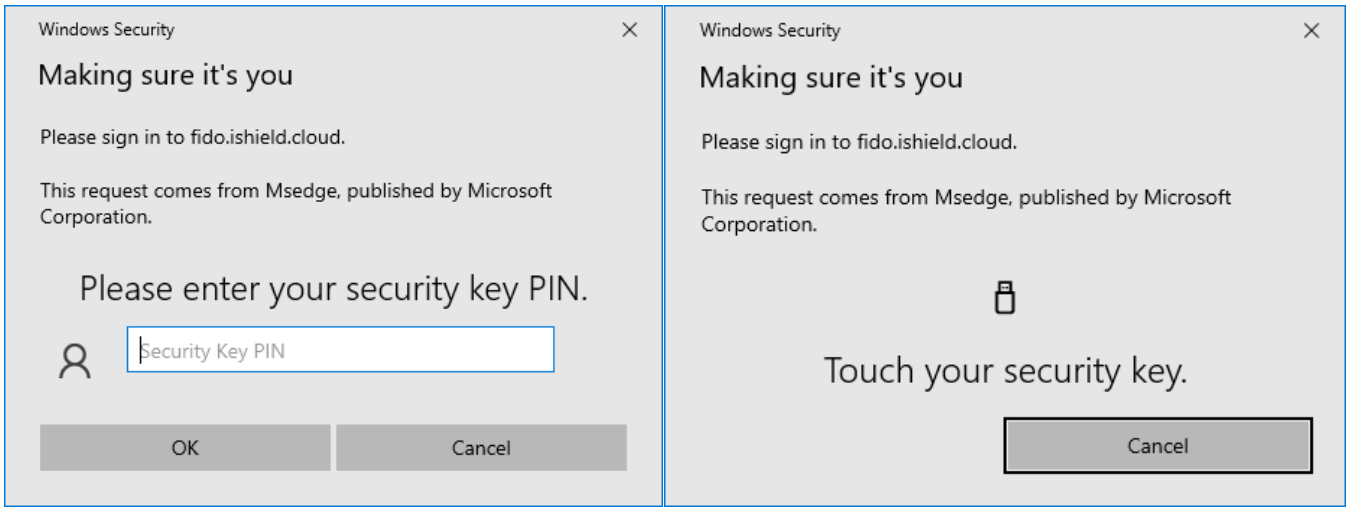
FIDO2 PIN が承認されたら、iShield Key 2 の端をタッチしてユーザーの存在を証明する必要があります。

これで登録が完了しました。iShield Key 2 はログインを求められる状態です。

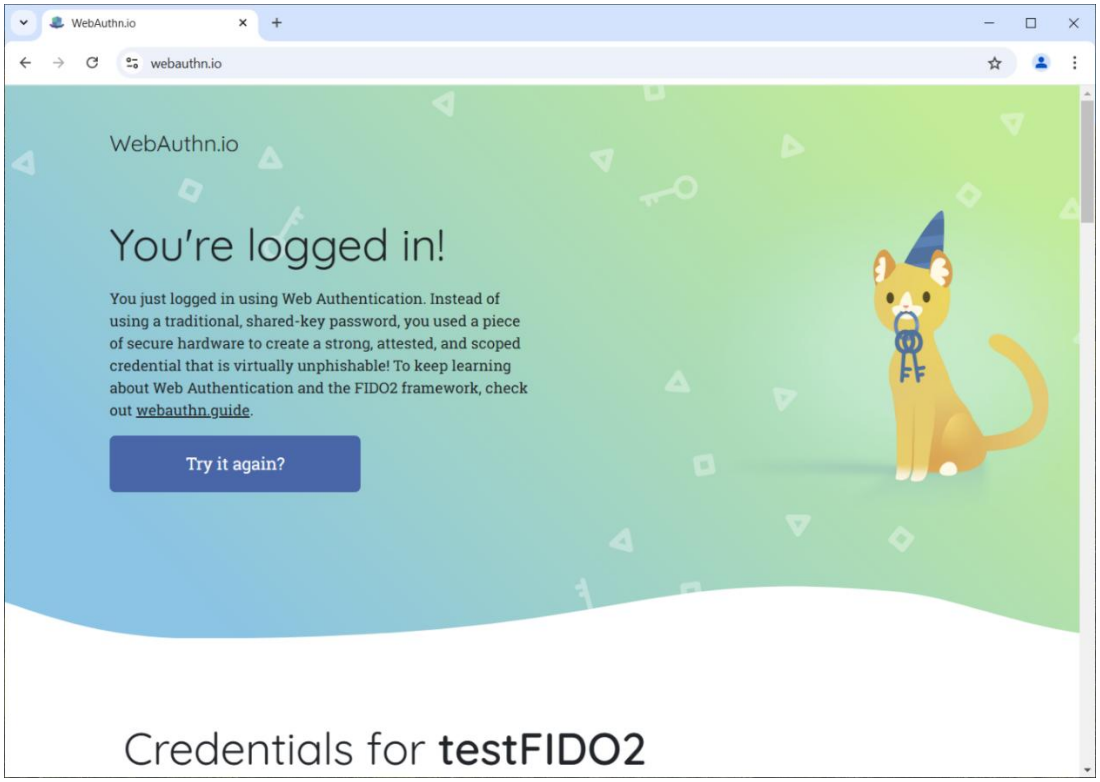
5.2.4 テストログイン

事前に登録したテスト ID を入力し、「ログイン」をクリックしてください。

FIDO2 PIN がセクション 5.2.2 に記載されている通りに設定されているかどうかに応じて、FIDO2 PIN が要求される場合があります。要求された場合は、iShield Key 2 の先端をタッチしてユーザーの存在を証明してください。



最後に、以下に示すような成功メッセージと、使用した Swissbit iShield Key の認証情報が表示されます。これは、Swissbit iShield Key が正常に動作していることを意味します。



5.3 Swissbit iShield Key 2 の様々なサービス

Swissbit iShield Key 2 をセキュリティキーとして登録し、様々なサービスで 2 要素認証を有効にすることにご興味をお持ちの場合は、コミュニティポータルをご覧ください。様々なオンラインサービスの設定詳細やビデオチュートリアル、よくある質問への包括的な回答、役立つガイドなどがご覧いただけます。

ポータルには、https://community.swissbit.com/c/ishield-key/ からアクセスできます。

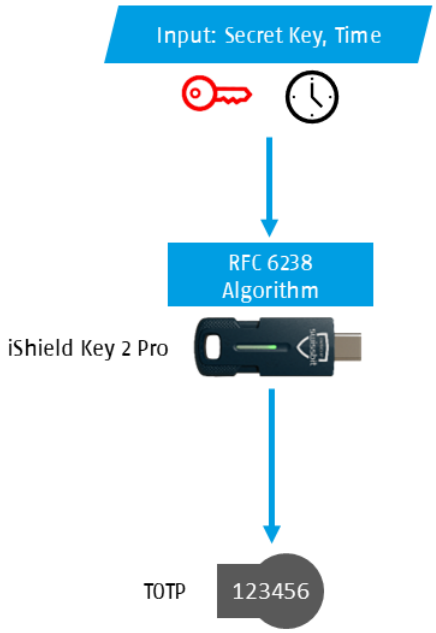
6 TOTP アプリケーション

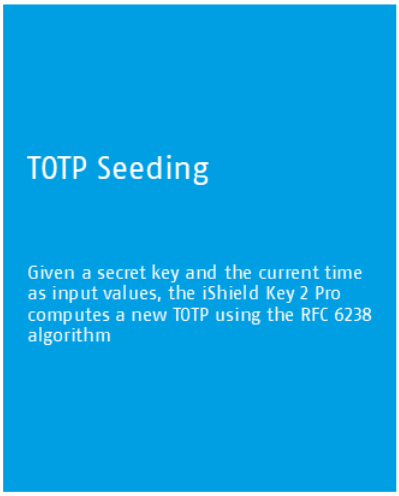
6.1 概要

iShield Key 2 Pro は、時間ベースのワンタイムパスワードの生成をサポートしています。iShield Key 2 Pro のパスコードアプレットの TOTP 機能を使用して、実装された TOTP アルゴリズムをサポートするサービスで二要素認証を行うことができます。iShield Key 2 は、IETF の RFC 6238 アルゴリズムを実装しています。TOTP 資格情報用に 42 個のスロットが用意されています。そのため、iShield Key 2 Pro を使用して、さまざまなサービスやアカウントで二要素認証を行うことができます。オプションで、特定のアカウントを PIN で保護するように TOTP 生成を構成することもできます。その場合、新しい OTP を生成するには PIN が必要になります。

セクション 6.1.1 では時間ベースの OTP のシードについて説明し、セクション 6.1.2 では TOTP によるパスコード生成と認証について説明します。

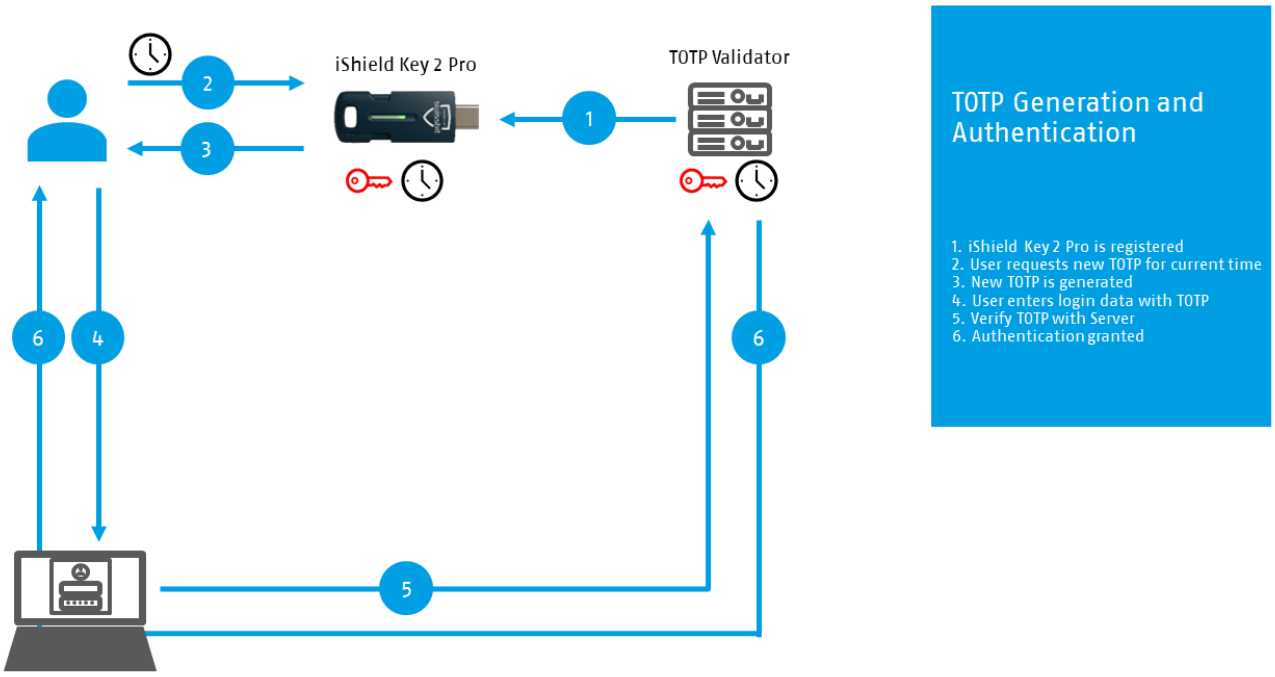
6.1.1 TOTP シーディング





iShield Key は、RFC 6238 アルゴリズムを用いて時間ベースの OTP（タイムスタンプ）を計算します。秘密鍵と現在時刻を入力値として、iShield Key は 6 桁から 9 桁のパスコードを計算します。このとき、時刻が変化要素となります。一定時間内（例：30 秒または 60 秒）であれば、TOTP の計算結果は同じになります。TOTP は通常、30 秒の有効期間で生成されます。

6.1.2 パスワードの生成と認証



iShield Key 2 Pro とサービスのペアリングが成功すると、セキュリティキーとサービスは設定されたスロットに対して同じ一連の OTP を計算します。iShield Key 2 Pro は、指定された現在時刻のリクエストに応じて新しい OTP を生成します。ユーザーがサービスにログインし、生成された OTP を送信すると、サービスも現在時刻の OTP を生成し、ユーザーが入力した OTP と比較します。両方の OTP が一致すると、アクセスが許可されます。ステップ 3 については、前のセクションで詳しく説明しています。

TOTP 検証サービスと iShield Key が正確に同じ時刻を使用しない場合、iShield Key によって生成された OTP が検証サービスで期待される OTP と異なる可能性があります。また、iShield Key で生成された OTP が OTP 検証サーバーに到着した時点で既に期限切れになっている可能性もあります。通常、検証サーバーサイトで時間オフセットを設定できるため、これは大きな問題にはなりません。検証サーバーは、これらのシナリオに対処できるように、いくつかの OTP を事前に計算します。例えば、検証には最初の期限切れ OTP + 予想される OTP + 次に予想される OTP が使用されます。つまり、検証サーバーは過去 30 秒と未来 30 秒の時間オフセットを受け入れることになります。これは、既に述べたように、OTP 検証サーバーで設定可能です。ただし、許容される時間差が大きいほど、システムのセキュリティは低下します。

iShield Key 2 Pro と検証サーバーには、TOTP 計算の入力として同じタイムスタンプが与えられないため、結果が異なる間隔になる場合があります。通常、サービスはパスワードを受信した時刻を検証の入力として使用します。そのため、有効期限が迫っているコードが送信された場合、または短い期間が設定されている場合、検証が失敗する可能性が高くなります。さらに、クライアント側とサーバー側の間のクロックドリフトによって不一致が発生する可能性があります。通常、TOTP 検証ツールは、許容範囲内で一定数の前方および後方の時間間隔で、複数のコードとパスワードを計算します。

6.2 Swissbit iShield Key の様々なサービス

多くのサービスが時間ベースのワンタイムパスワードアルゴリズム（TWA）方式をサポートしているため、iShield Key の TOTP 機能を様々なサービスの 2 要素認証としてご利用いただけます。iShield Key 2 Pro を様々なオンラインサービスに登録する方法の詳細については、Swissbit コミュニティポータル（https://community.swissbit.com/c/ishield-key/）をご覧ください。

7 HOTP アプリケーション

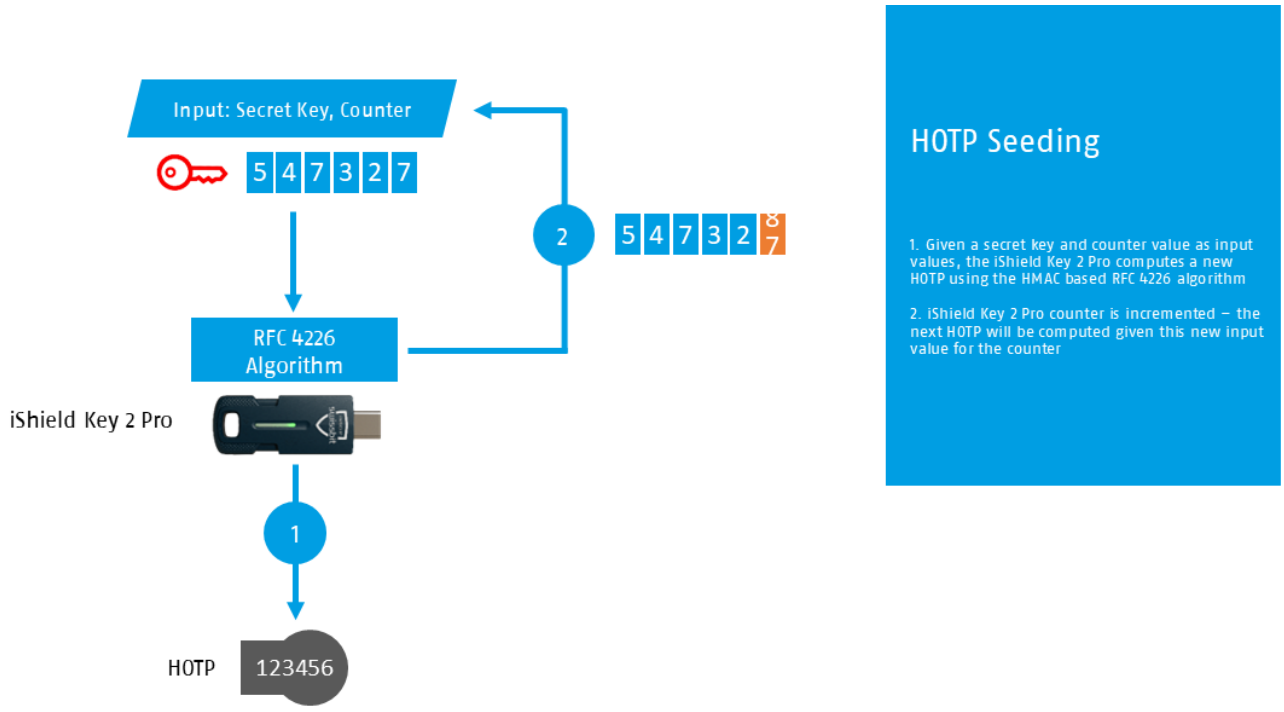
7.1 概要

iShield Key 2 Pro は、HMAC ベースのワンタイムパスワード（HOTP）の生成をサポートしています。WebAuthn 準拠の FIDO2 セキュリティキーをサポートしていないサービスでは、二要素認証に TOTP を使用することをお勧めします。iShield Key 2 Pro は、IETF の RFC 4226 アルゴリズムを用いた HOTP 生成を実装しています。VPN アクセスなどのネットワークアプリケーションでは、この標準アルゴリズムがよく使用されています。iShield Key 2 Pro の HOTP 機能は、インストールの手間なく使用できます。プラグアンドプレイのように簡単です。iShield Key 2 Pro には最大 42 個の HOTP スロットを適用できます。

セクション 7.1.1 では HOTP のシードについて詳しく説明し、セクション 7.1.2 ではパスワード生成と認証のプロセスについて説明し、セクション 7.1.3 ではハードウェア認証装置とサーバーの再同期について説明します。セクション 7.2 では、HOTP ユースケース「一括登録」について簡単に説明します。

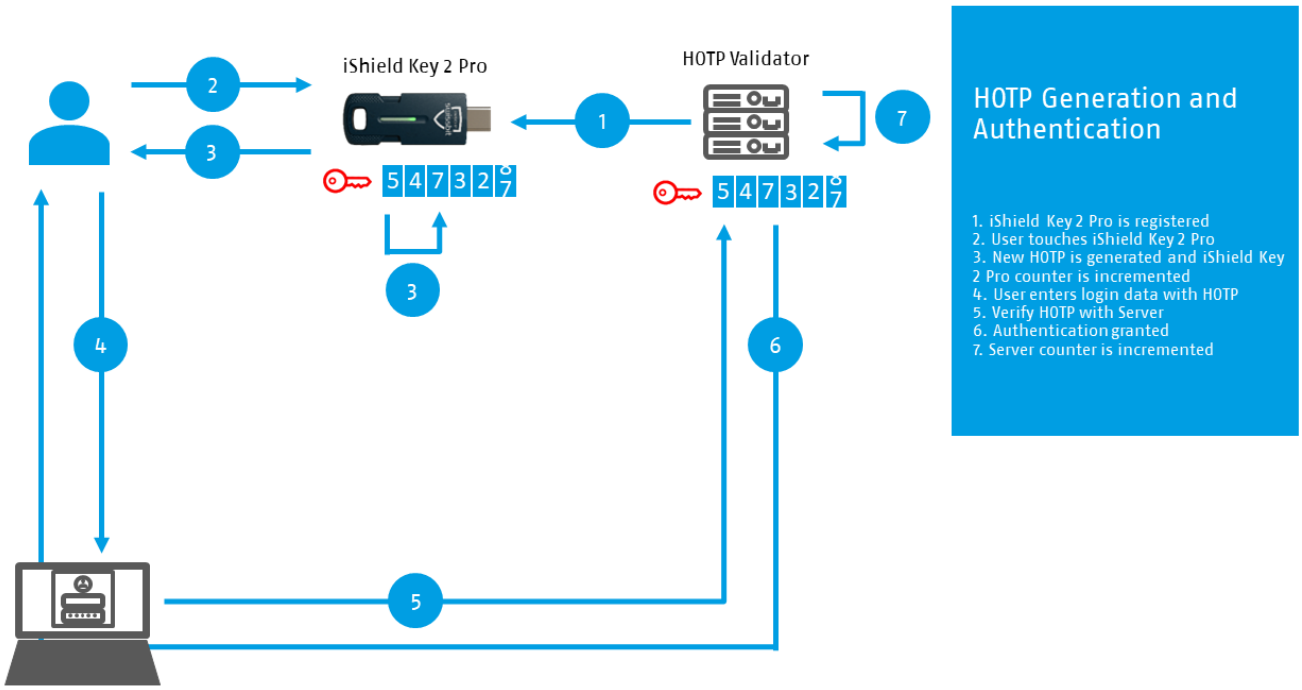
このセクションは、製品バリアント「iShield Key 2 FIDO2」には関係ありませんのでご注意ください。

7.1.1 HOTP シーディング



iShield Key 2 Pro は、HMAC ベースの RFC 4226 アルゴリズムを用いて、秘密鍵とカウンタに基づく HOTP 生成を実装しています。秘密鍵とカウンタ値を入力値として与えると、iShield Key 2 Pro は 6～9 桁の人間が判読可能な OTP を計算します。カウンタは変動係数です。HOTP が生成されるたびにカウンタがインクリメントされます。次の OTP は、この更新されたカウンタ値を使用して計算されます。そのため、各カウンタ値はワンタイムパスワードの生成において一度だけ使用されます。

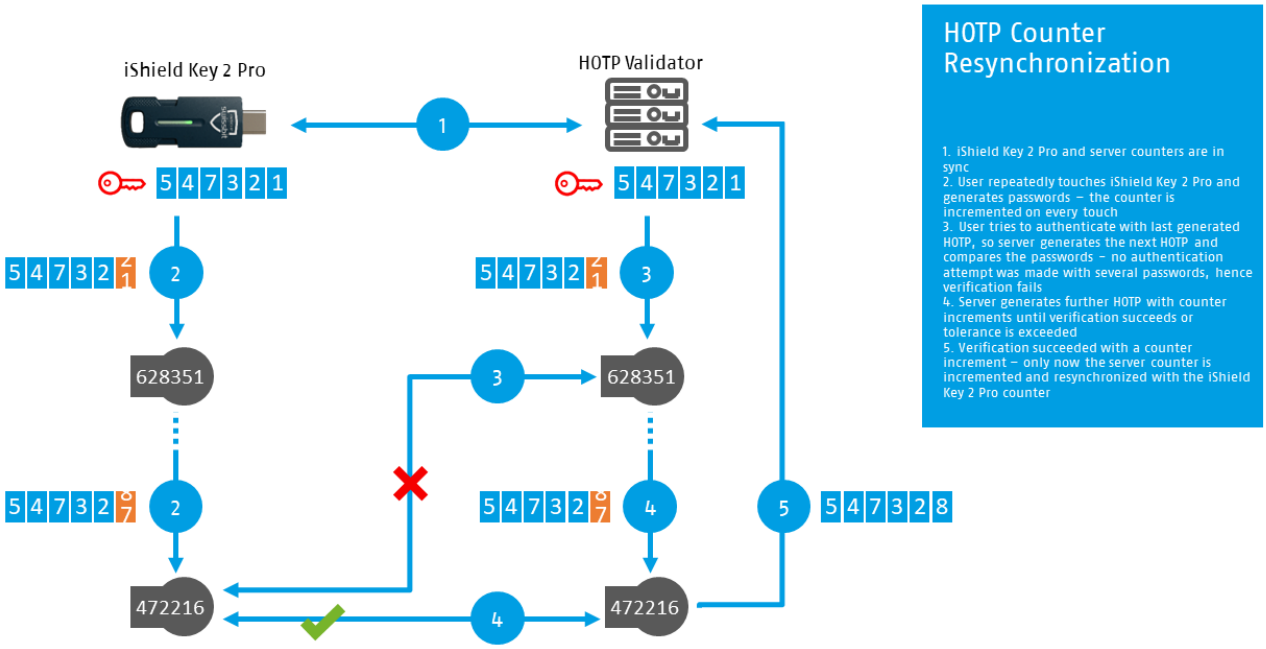
7.1.2 パスワードの生成と認証



iShield Key 2 Pro を HOTP を使用するサービスに登録すると、対応する一連のパスワードを生成するために接続は必要ありません。これは、HOTP アルゴリズムの決定論的な性質と、トークンとサーバー間の共有秘密鍵とカウンターによるものです。トークンは新しいパスワードを生成し、カウンターをインクリメントします。ユーザーがサービスに認証すると、そのパスワードはサーバーによって生成されたパスワードと比較されます。認証に成功すると、サーバーのカウンターがインクリメントされます。

HOTP 計算のステップ 3 については、前のセクションで詳しく説明しています。

7.1.3 カウンタの再同期



トークンとサーバーのカウンターの同期が失われる場合があります。例えば、ユーザーがトークンにアクセスし、新しいパスワードを生成したものの、それに関連付けられたサービスへの認証を行わなかった場合などです。認証の失敗を回避するには、サーバー側で先読みパラメータを設定します。このパラメータは、パスワードの比較においてカウンターの増分を何倍とするかを定義するため、ある程度の許容範囲が設けられています。認証が成功すると、生成器とサーバーのカウンターが再同期されます。ただし、許容範囲を大きくするほど、システムのセキュリティは低下します。

7.2 一括登録

一括登録とは、多数のデバイスを企業の IT 環境に登録するプロセスを指します。この方法により、組織は複数のデバイスを集中管理されたデバイス管理システムに効率的に登録できるため、デバイス管理が簡素化されます。バージョン 1.7.4 以降、iKMcli ツールは複数の iShield Key 2 Pro に HOTP スロットを展開できるようになりました。各 iShield Key 2 Pro の HOTP 機能は、固有のランダムシークレット/キーで初期化されます。この情報は、デバイスのシリアル番号、初期カウンター値、HOTP の長さとともに CSV ファイルに記録され、追跡と管理を効率化します。

iKMcli による一括登録の詳細については、セクション 4.2.2 を参照してください。

8 PIV アプリケーション

ガイドのこの部分では、Windows 上で Swissbit iShield Key 2 Pro を個人識別および検証 (PIV) デバイスとして使用する方法を説明します。PIV アプレットを備えた iShield Key 2 Pro キーは、さまざまなユースケース向けにさまざまな証明書を保存およびサポートするためのさまざまなスロットを提供します。このガイドでは、Swissbit iShield PIV モジュールで補完された OpenSC Minidriver を使用して、スマートカードにこれらの証明書をプロビジョニングします。次のセクションでは、これらを生成して使用する方法を説明します。

このセクションは iShield Key 2 FIDO2 には関係ありませんのでご注意ください。PIV ユースケース向けに iShield Key 2 Pro を設定および使用する方法に関するガイドをお探しの場合は、Swissbit コミュニティ ポータル (https://community.swissbit.com/c/ishield-key/) にアクセスしてください。

8.1 ユースケース

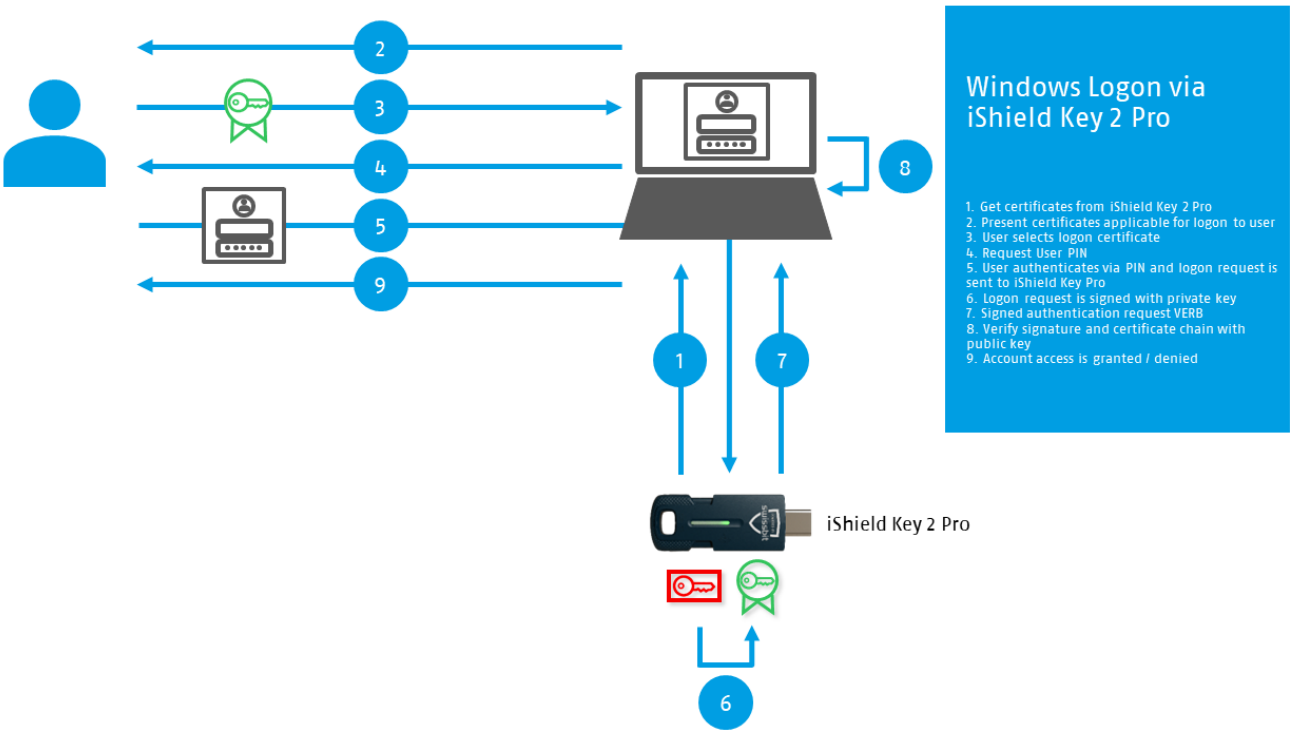
	ローカル Windows Account	**Active Directory ドメインアカウント**
Windows Logon	iShield Key 2 Pro を使用して、ローカル Windows ユーザー アカウントにログオンします。	iShield Key 2 Pro を使用すると、ドメイン構成内の任意のワークステーションにログオンできます。スマートカードの証明書にはアカウント情報が保存されています。ユーザーはスマートカードの PIN を PC に接続して入力するだけで済みます。
Bitlocker	自己署名証明書を使用してデータ ドライブを暗号化します。	ドメイン CA が発行した証明書を使用してデータ ドライブを暗号化します。

これらの PIV ユースケースでは、Windows 環境の 2 つの構成を区別する必要があります。

- **ローカルアカウント**: 1 つまたは複数のアカウントが 1 台の PC に存在します。これらのアカウントはドメインに属しておらず、中央組織によって管理されます。この構成は、主に家庭用 PC で見られます。
- **Active Directory ドメインアカウント**: 中央ドメインサーバーが、このドメインネットワーク内のマシン、ユーザー、プリンターなどを管理します。この構成は、企業などの大規模組織が従業員のアカウント/マシンを管理するのに役立ちます。

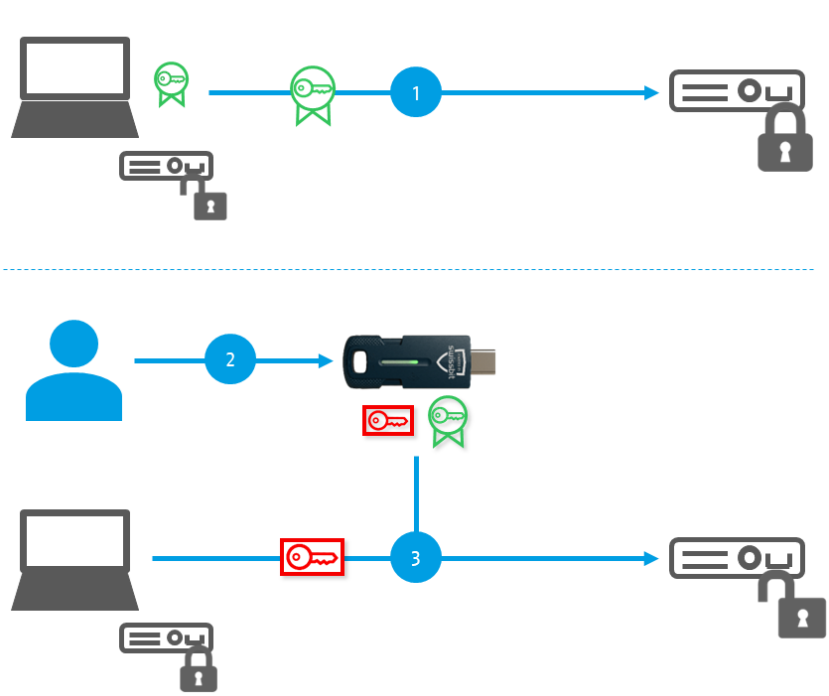
どちらの構成もすべての PIV ユースケースに対応できますが、設定と使用方法に違いがあります。このガイドでは、主にローカルアカウントのシナリオに焦点を当て、次に Active Directory のセットアップ手順について説明します。また、同じ PC にローカルアカウントと Active Directory ドメインアカウントの両方が存在することも可能ですが、異なるユースケース間で互換性の問題が発生する可能性があります。詳細については、このガイドのそれぞれの手順を参照してください。

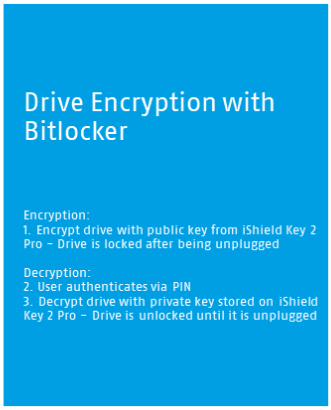
8.1.1 ログオン



iShield Key 2 Pro を使用すると、パスワードの代わりに PKI ハードウェアトークンに基づく、より安全なログインを実現できます。Windows ユーザーアカウントは、スマートカード上の証明書を信頼するように設定されます。さらに、iShield Key 2 Pro を接続して短い PIN を入力するだけで済むため、パスワードよりも安全であるだけでなく、利便性も向上します。このタイプのワークステーションログインは、Windows AD ドメインに参加しているマシンでサポートされていますが、スタンドアロンワークステーションでは追加のソフトウェアが必要です。

8.1.2 Bitlocker





BitLocker は、データドライブの暗号化と復号化に使用される Microsoft ツールです。PC に内蔵されているドライブ、または通常はさまざまなマシンに接続される外付けドライブが対象となります。ドライブにデータを保存すると、BitLocker は事前に定義された証明書を使用してデータを暗号化します。BitLocker セッションが終了すると（外付け USB ドライブの取り外しや PC の電源切断など）、データは暗号化され、読み取り不能になります。デバイスに再度アクセスするには、復号化情報（通常、ドライブの挿入時または PC の起動時に入力する PIN またはキーの形式）を入力する必要があります。

セキュリティをさらに強化するには、iShield Key 2 Pro を使用して必要な証明書と復号化情報を保存できます。ユーザーがドライブ上のデータにアクセスする際は、対応する暗号化証明書が保存されたスマートカードを挿入し、その PIN を入力する必要があります。これにより、データセキュリティが強化されます。データにアクセスするには、証明書を iShield Key 2 Pro に提示し、その PIN を入力する必要があります。

Windows OS (C:) パーティションはデータドライブとはみなされないことに注意してください。BitLocker はスマートカードを使用して暗号化を行いませんが、その他の限定的な構成はサポートしています。

8.1.3 Active Directory

Microsoft は、ドメイン インフラストラクチャである Active Directory (AD) 用のコンポーネントを提供しています。この PIV ガイドの以下のセクションでは、セットアップと互換性について説明します。Active Directory ドメイン構造は、複数のコンポーネントで構成されています:

- **ドメイン サーバー**: この構造内のすべてのコンポーネントを構成するために使用される管理ユーティリティ。これには、ユーザー、ワークステーション、サーバー コンポーネント、そして PIV にとって重要な証明書などが含まれます。
- **ワークステーション**: ユーザーがアカウントにログインできるクライアント PC。これらの構成はドメインサーバーから取得されます。

AD のユースケースについては、このガイドでは必要なコンポーネントが既にセットアップされていることを前提としています。

8.2 基礎的なコンポーネント

8.2.1 Windows でのトークンのプロビジョニングと使用

Windows Inbox スマートカードミニドライバーは PIV スマートカードをサポートしていますが、読み取りアクセスのみ可能です。ミニドライバーは iShield Key 2 Pro の PIV 機能を使用するには十分ですが、カード管理はサポートされていません。PIV カードがユースケースに合わせてプロビジョニングされると（つまり、必要なすべての証明書がスマートカード上に生成されると）、Windows PIV ドライバーを使用して iShield Key 2 Pro で署名または復号化を行うことができます。

カードのプロビジョニングに書き込みアクセスを有効にするには、Swissbit OpenSC ミニドライバーをインストールし、カード管理に Swissbit iShield PIV モジュールを使用するように設定する必要があります。

8.2.2 認証

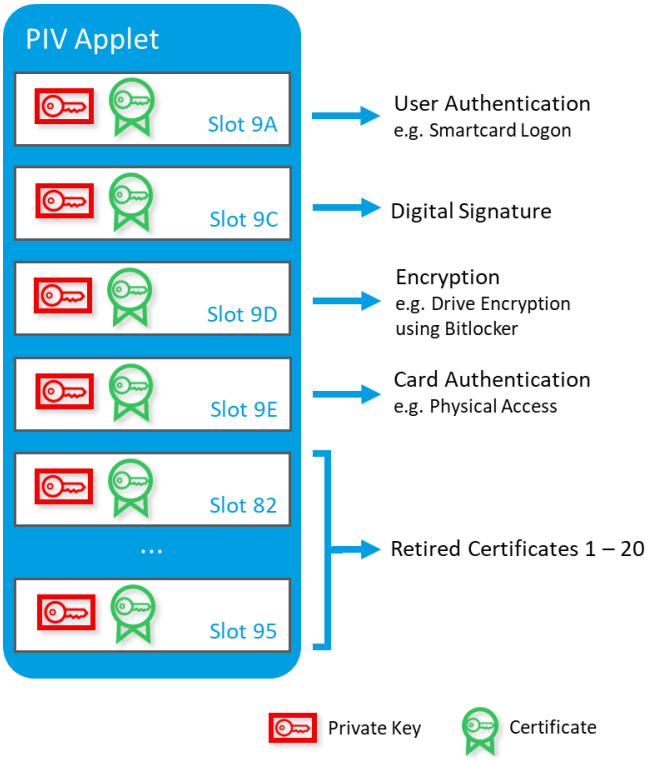
iShield Key 2 Pro は、管理操作と使用のために 3 つのパスワードが必要です。PIN は、署名や復号化などの秘密鍵操作を含む通常のトークン使用に不可欠です。また、PIN の変更や PIN の再試行設定にも必要です。PUK は PIN のロック解除に使用されます。管理キーは、管理操作時の認証に必要です。このような操作の例としては、キーのインポート、証明書の生成、削除、カードへの PIV データの書き込みなどがあります。

注：FIPS 準拠のため、iShield Key 2 Pro FIPS は **TDES** アルゴリズムをサポートしていません。PIN と PUK は PIN ルールに準拠する必要があります。

8.2.3 証明書スロット

PIV アプレットは、証明書とそれに対応する公開鍵と秘密鍵のペアをスロットに保存します。各スロットには 1 つの証明書が格納されます。iShield Key 2 Pro には、4 つの標準 PIV スロット (9A、9C、9D、9E) と 20 個の追加の廃止スロット (82 ～ 95) があります。各標準 PIV スロットには特定の目的があり、廃止スロットは通常、期限切れの証明書に使用されます。ただし、他のスロットの証明書と同様に、署名や復号化にも使用できます。

- スロット 9A の証明書は通常、ユーザー認証に使用されます。このスロットは、スマートカード ベースの Windows ログオン用の証明書に使用できます。
- スロット 9C の証明書は、電子メールの署名などのデジタル署名に使用されます。このスロットの秘密鍵は、標準に従って特別な PIN ポリシーを使用して生成されます。標準に従って、秘密鍵の操作ごとに PIN が必要です。
- スロット 9D の証明書は、機密性を確保するための暗号化に使用されます。このスロットの一般的な使用例は、BitLocker などのハードディスク暗号化です。
- スロット 9E には特別な PIN ポリシーがあります。秘密鍵操作には PIN は不要であるため、このスロットの証明書はカード認証に使用されます。一般的な使用例は建物へのアクセスです。



OpenSC ミニドライバーと PIV 管理用の iShield PIV モジュールを使用して iShield Key 2 Pro をプロビジョニングする場合、証明書は標準の PIN ポリシーを使用して次の空きスロットに生成されます。最初の証明書はスロット 9A に保存され、次の証明書はスロット 9D に保存され、その後、使用されていないスロットが順番に保存されます。

8.3 要件

Swissbit は現在、Swissbit iShield Key 2 Pro for PIV で以下のシステムとアプリケーションをテストしています。

- PC オペレーティングシステム：**Windows 10 Pro**; Home エディションは BitLocker またはドメインアカウントをサポートしていません。Windows 7/8/11 でも手順は同様です。
- サーバーインフラストラクチャ：**Windows Server 2019**; Active Directory とのセットアップ。他のサーバーバージョンではセットアップ手順が異なる場合があります。

8.4 *iShield Key 2 Pro* で *PIV* を開始する

Swissbit iShield Key ランディングページから iShield Key Manager インストールパッケージをダウンロードしてください。

8.4.1 PIV インストールパッケージ

インストールパッケージには、以下のツールが含まれています:

- ├── UserManual.pdf — This guide
- ├── iKM/ishield_key_manager.msix — iShield Key Manager installer
- ├── iKMcli/iKMcli.exe — iShield Key Manager command line tool
- ├── minidriver/windows64
- │ ├── openSC.msi — **PIV installer**
- │ ├── ishield-piv-module
- │ │ ├── PIV-II.profile — OpenSC PIV profile
- │ │ └── vcruntime140.dll, msvcp140.dll, etc. — Required system runtime libraries
- └── minidriver/windows32
- │ ├── openSC.msi — **PIV Installer**
- │ ├── ishield-piv-module
- │ │ ├── PIV-II.profile — OpenSC PIV profile
- │ │ └── vcruntime140.dll, msvcp140.dll, etc. — Required system runtime libraries
-

8.4.2 OpenSC Minidriver と iShield PIV Module のインストール

OpenSC ミニドライバーインストーラーとその他のすべての PIV 構成は、PIV インストーラーにバンドルされています。「OpenSC.msi」を実行し、インストーラーの指示に従って PIV のインストールを完了してください。必ず「完全」インストールを選択してください。

管理キーが既に変更されている場合は、キーファイル (C:\Program Files\OpenSC Project\OpenSC\management_key.txt) も更新する必要があります。

Microsoft の公式 Web ページから「Microsoft Visual C++ Redistributable for Visual Studio 2015」以降がインストールされていることを確認するか、インストールパッケージから必要なシステムランタイムライブラリをローカルに配置してください。

[3] https://visualstudio.microsoft.com/downloads/#microsoft-visual-c-redistributable-for-visual-studio-2022

8.4.3 iShield Key 2 Pro の準備

iShield Key 2 Pro を使用する前に、PIN、PUK、管理キーを変更することを強くお勧めします。変更には、iShield Key Manager（セクション 4.1.5 を参照）またはコマンドラインツール iKMcli をご利用ください。iShield Key 2 Pro を接続し、以下のコマンドを実行してください:

```
iKMcli piv --change-pin <new pin> --pin <pin>
iKMcli piv --change-puk <new puk> --puk <puk>
iKMcli piv --set-management-key <new key> --management-key <key>
[--new-management-key-algorithm <TDES|AES128|AES192|AES256>]
```

キーファイル（C:\Program Files\OpenSC Project\OpenSC\ management_key.txt）内の管理キーも必ず更新してください。

PIN の工場出荷時のデフォルトは **123456**、PUK のデフォルトは **12345678**、管理キーは **AES 192** で **010203040506070801020304050607080102030405060708** です。

注： FIPS 準拠のため、iShield Key 2 Pro FIPS は **TDES** アルゴリズムをサポートしていません。

新しい PIV PIN と PUK は PIN のルールに準拠する必要があります。

PIV PIN には数字（0～9）のみを含めることができます。

PIV PUK は 8 文字である必要があります。

新しいカード所有者の一意の識別子とカード機能コンテナを生成

```
iKMcli piv --set-chuid --management-key <key>
iKMcli piv --set-ccc --management-key <key>
```

8.4.4 iShield Key 2 Pro のリセット

iShield Key 2 Pro の PIV アプレットをリセットし、すべての PIV データを消去してデフォルト設定を復元する場合は、iShield Key Manager を使用するか、次の手順に従ってください。

無効な PIN または PUK を繰り返し入力して、PIN と PUK をブロックします。例:

```
iKMcli piv --change-pin 332211 --pin 112233
iKMcli piv --change-puk 44332211 --puk 11223344
```

PIN と PUK をブロックしたら、iShield Key 2 Pro をリセットすることができます。

```
iKMcli piv --reset
```

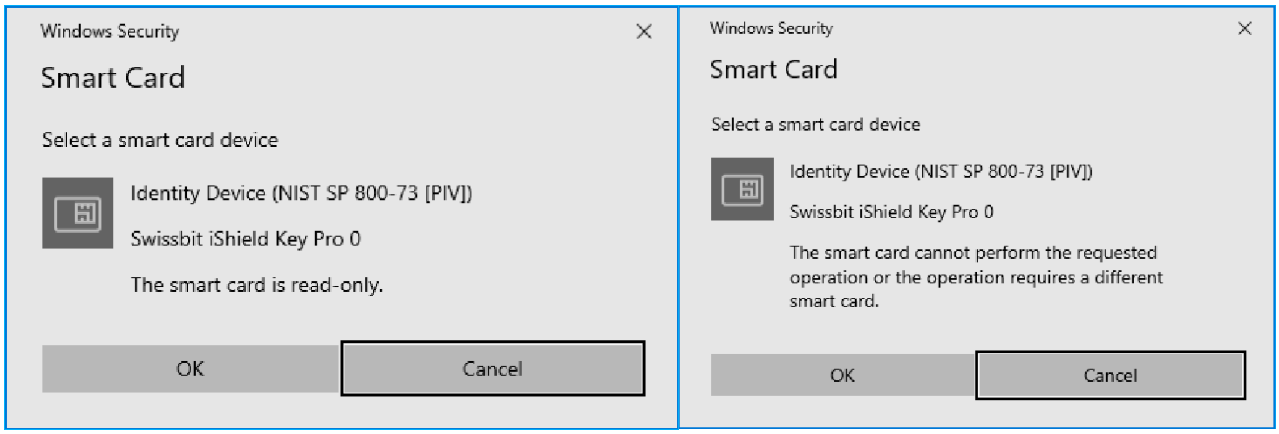
新しいカード所有者の固有識別子とカード機能コンテナを設定

```
iKMcli piv --set-chuid --management-key <key>
iKMcli piv --set-ccc --management-key <key>
```

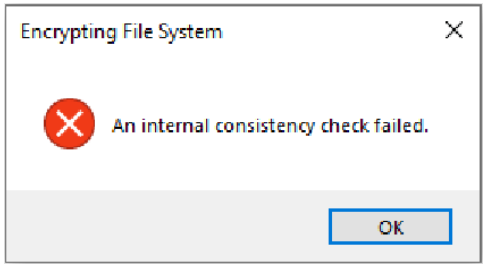
iShield Key 2 Pro を使用できるように準備し、セクション 8.4.3 に従って新しい PIN、PUK、管理キーを設定します。

8.5 トラブルシューティング

トラブルシューティング "The smart card is read-only / cannot perform the requested operation"
iShield Key 2 Pro が読み取り専用、または要求された操作をサポートしていないと表示される場合は、OpenSC ミニドライバーが正しくインストールされていません。キーのプロビジョニングには、OpenSC ミニドライバーを使用する必要があります。セクション 8.2.1 を参照してください。PIV インストーラーがインストールされていることを確認してください。



トラブルシューティング "An internal consistency check failed"
「An internal consistency check failed」というエラーは、OpenSC の設定ミスが原因で発生することがよくあります。セクション 8.4.2「管理キーファイルの検証」のすべての手順に従い、新しい管理キーが適用されているかどうかを確認してください。



9 Glossary

Abbreviation	Description
2FA	Two-Factor Authentication
AD	Active Directory
CA	Certificate Authority
CEP	Certificate Enrollment Policy Service
CES	Certificate Enrollment Service
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
DC	Domain Controller
EFS	Encrypting File System
FIDO	Fast Identity Online
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-Time Password
IETF	Internet Engineering Task Force
iKM	iShield Key Manager
MFA	Multi-Factor Authentication
NFC	Near Field Communication
OIDC	OpenID Connect
OTP	One-Time Password
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public-Key Cryptography Standard
PUK	Personal Unblocking Key
SHA	Secure Hash Algorithm
SSO	Single Sign-On
TOTP	Time-based One-Time Password
U2F	Universal 2nd Factor
VPN	Virtual Private Network

10 Document History

Version	Updated on	Updated by	Short description
1.0	February 24, 2025	Swissbit AG	Initial release
1.1	May 2, 2025 Jan 14, 2026	Swissbit AG Swissbit Japan Co., Ltd.	Revisions & formatting Translation in Japanese

免責事項:

Swissbit AG（以下「SWISSBIT」）の正式な代表者の書面による事前の同意なく、本書のいかなる部分も、いかなる形式または手段によっても複製、複写、または第三者に譲渡することはできません。本書の情報は予告なく変更される場合があります。SWISSBITは、本書に含まれる誤りや遺漏について一切の責任を負わず、本書に記載されている情報の使用から生じるいかなる結果についても責任を負いません。SWISSBITは、本書に含まれる情報を更新または最新の状態に維持する義務を負いません。本書に記載されている製品は、航空機制御システム、航空宇宙機器、海底ケーブル、原子炉制御システム、生命維持システムなどの用途（ただしこれらに限定されない）には適していません。さらに、SWISSBITは、生命維持装置またはシステム、または故障が傷害または死亡につながる可能性のある用途での製品の使用を推奨または承認していません。 SWISSBIT製品をSWISSBITが想定していない用途で使用することを希望される場合は、SWISSBITの正規代理店にご連絡の上、当該用途に対するSWISSBITのサポート可否をご確認ください。本書に記載されている情報は、SWISSBITが主張し保有する著作権、特許権、商標権、その他の知的財産権に基づくいかなるライセンスも付与するものではありません。本書に記載されている情報は、SWISSBITが所有する「専有財産」および「機密」財産とみなされます。

SWISSBITが販売するすべての製品は、SWISSBITの販売条件に記載されている条項（責任の制限、保証、および権利侵害に関する条項を含む）のみに適用されます。 SWISSBIT は、ここに記載されている情報に関して、または記載されている製品が知的財産権を侵害していないことに関して、明示的、法的、黙示的、またはその他のいかなる種類の保証も行いません。また、明示的、法的、黙示的を問わず、商品性または特定目的への適合性の保証を含め、そのような保証を明示的に否認します。

©2025 SWISSBIT AG All rights reserved.