eSecu FIDO Manager
取扱説明書
(V2.4)

Excelsecu Data Technology Co., Ltd.

ACOT Electronics Inc.

株式会社エクセルセクデータテクノロジーの機密情報

本マニュアル、いかなる性質の保証を行うものではありません。すべての製品および関連文書に開示されている資料は、正式に締結されたプログラム製品のライセンスまたは機器の購入またはリースに関する契約の条件に従ってのみ提供されます。

このマニュアルに記載されている製品に関して、ExcelsecuTechnology が行う唯一の保証は、あるとすれば、当該ライセンス、または契約書に記載されている物のみです。

Excelsecu テクノロジーは、お客様が本情報またはソフトウェアを使用した結果として生じる直接的、間接的、特別または結果的な損害を含む金銭的またはその他の責任を受け入れることができません。

この情報および/またはソフトウェア資料の使用が、使用されている管轄区の規則および規制に準拠していることを確認するように注意してください。無断転載を禁じます。

1. 概要

eSecu FIDOManager は、eSecu FIDO2/FIDO・U2F セキュリティキーや FIDO2 セキュリティキーを対象として、FIDO2、OTP、および指紋機能を構成するために使用されます。Windows オペレーティングシステムのセキュリティキー。現在、このツールは次のセキュリティキーを対象に次のシステム上で動作します。

1.1. サポートされているセキュリティキー：

- eSecu FIDO2/FIDO・U2F キー(FD200)、eSecu FIDO2/FIDO・U2F キー NFC (FD202)、eSecu FIDO2/FIDO・U2F キー Pro(FD203)
- eSecu FIDO2 指紋キー(FD210)、eSecu FIDO2 Pro +(FD213)

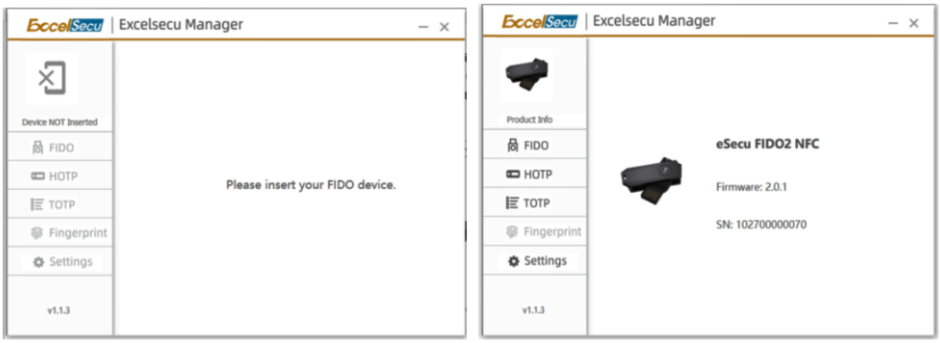
1.2. サポートされているシステム：

- windows7 から windows10、windows server 2016/2019

2. PC デバイス

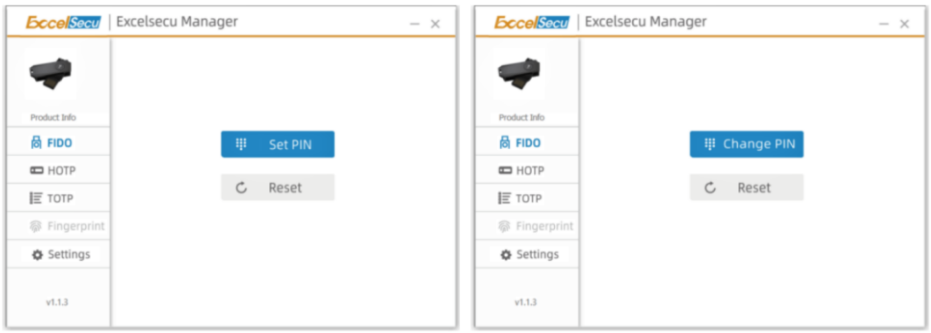
2.1. 製品情報

PC で FIDOManager.exe を開きます。 eSecu FIDO2 セキュリティキーを PC の USB ポートに挿入します。製品情報が自動的に表示されます。左側のメニューは、FIDO、HOTP、TOTP、fingerprint、settings(設定)です。製品の中には機能がすべてない場合がありますが、機能のないメニューは明るくなりません。

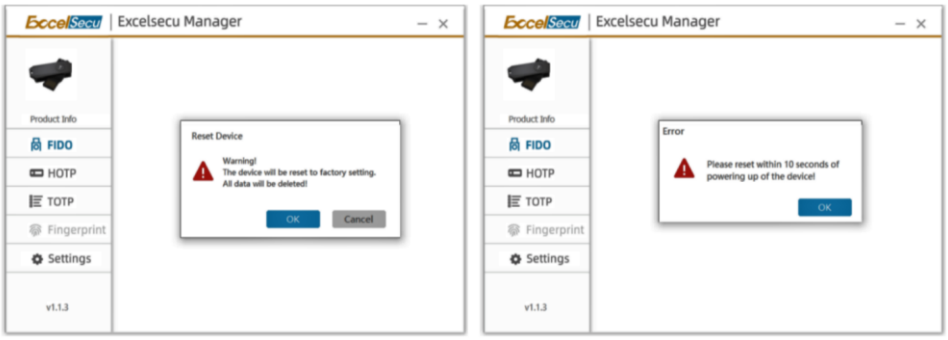


2.2. FIDO

FIDO ページでは、[change PIN]をクリックすると、セキュリティキーの暗証番号 PIN を設定するか、以前に PIN を設定したことがある場合は暗唱番号 PIN を変更できます。



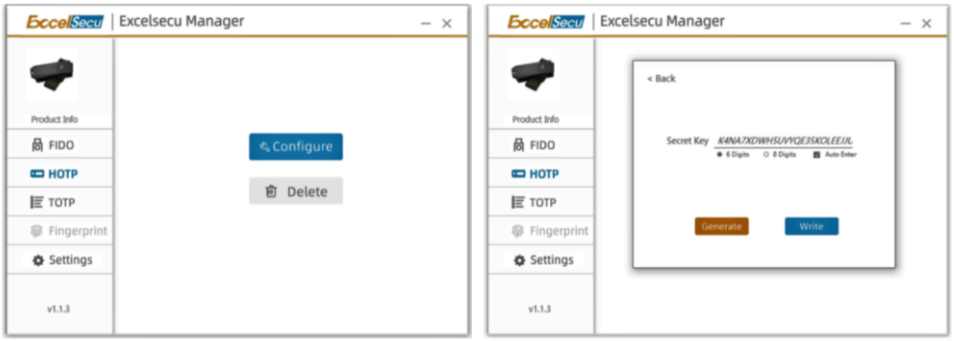
[リセット]をクリックすると、[OK]と[cancel]ボタンの画面が表示されます。 [OK]をクリックすると、キー上のボタンまたは指紋センサーを押すと、リセット操作を終了できます。FIDO および指紋機能のデータのみが工場出荷時の設定にリセットされます。他の機能のデータは削除されません。



プラグを差し込んだ後にキーをリセットしたくてもコンピュータに 10 秒間経つと、警告メッセージが表示されます。10 秒以内にリセットしてください。キーを抜いてもう一度 PC に接続し、10 分以内にリセットしてください。

3. HOTP

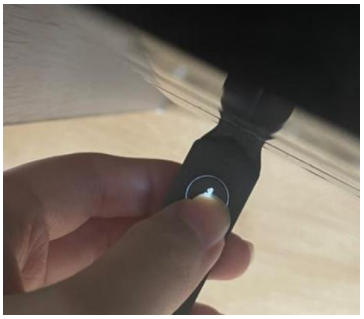
HOTP ページには、[configure(構成)]ボタン(数字キーパッドの選択)と [Delete(削除)]ボタンが表示されます。[configure(構成)]ボタンをクリックすると、 HOTP 値設定画面がホップアップします。

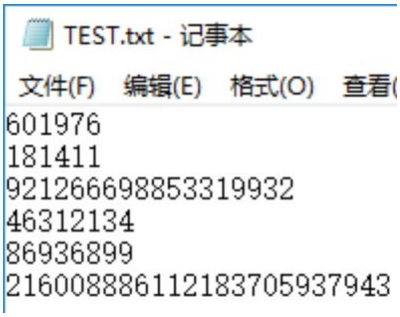


Base32 記数法でエンコードされた秘密鍵を手動入力するか、自動入力するか選択します。自動入力には、[Generate(生成)]ボタンをクリックしてランダムな秘密鍵を生成します。秘密鍵が生成して表示されたら、[Write(書き込み)]ボタンをクリックして表示の秘密鍵をセキュリティキーに書き込みます。次に、セキュリティキーのボタン/指紋センサーを 1 回押すと、キー内部で秘密鍵から HOTP 値が生成されます。次々にボタン/指紋センサーを押すと、その度に HOTP 値が次々と生成されます。

このとき、生成される HOTP 値を 10 進 6 桁か 8 桁にするかが選択できます。また、、Auto Enter(自動改行)を選択できます。選択すると、ボタンを押す度に連続的に生成される HOTP 値の間に”改行コードが自動的に挿入されます。選択しないと、”改行コード”は挿入されません。

HOTP 値が生成されると同時に、セキュリティコードから HOTP 値がテキスト出力されます。別のテキストファイルを開いてキー入力可能状態にすると、HOTP 値がファイルに入力されて表示されます。下の図は、テキストファイルを開いた状態で、6桁+”Auto Enter”で、ボタンを2回続けて押したときの、601976と181411、6桁+”Auto Enter なし”で、ボタンを3回続けて押したときの921266・698853・331932を示しています。その後の HOTP 値は、8桁に変更したときの同様な結果を示しています。

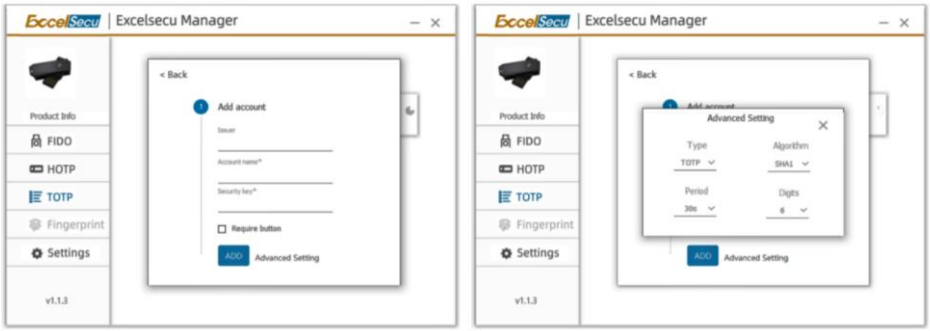




[Delete(削除)]ボタンをクリックして、eSecu セキュリティキーから秘密キーを削除します。

4. TOTP

+ボタンをクリックしてアカウントを追加し、ページにパラメータを入力します。



イシュア(発行会社):これはオプションです。空白のままにするか、TOTP を提供する Web サービスの名前を入力できます。

アカウント名:これがどのアカウントであるかを思い出させるために、何でも入力できます。

セキュリティキー:Base32 記数法の OTP 秘密鍵、TOTP を提供する Web サービスからコピーされたキーを入力します。

要求ボタン: このオプションが選択されている場合は、 OTP コードを表示するために、セキュリティキー上のボタン/指紋センサーを押す必要があります。

高度設定:TOTP 検証を提供する Web サービスの OTP パラメーターを設定します。

タイプ:TOTP、HOTP
アルゴリズム:SHA1、SHA256
時間間隔:30 秒、60 秒
桁:6、8

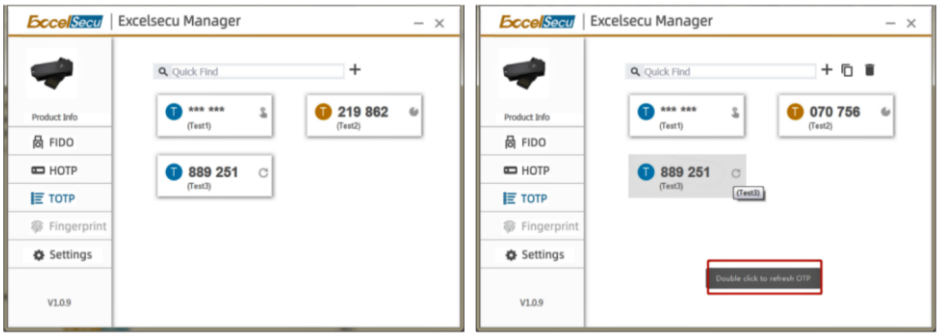
アカウントを正常に追加されると、ソフトウェアに動的コードが表示されます。

Test1 アカウントの動的コードは非表示になっています。つまり、アカウントに対してオプションの[Reguire(要求)]ボタンが選択されたことを意味しています。アカウントをダブル左クリックし、セキュリティキーのボタン/指紋センサーを押すだけで、

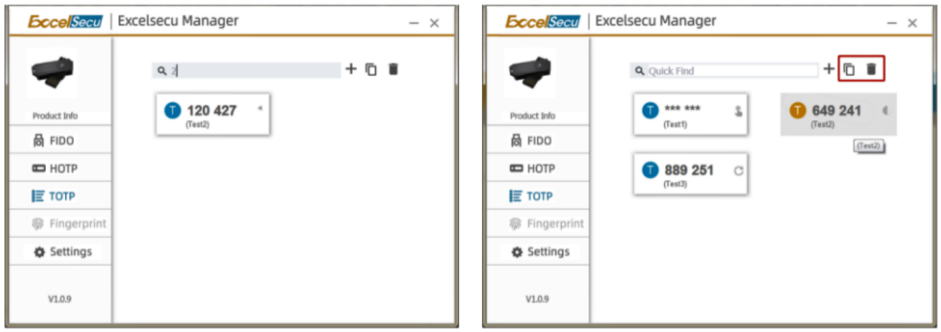
動的コードが現れます。OTP が次のタイムステップに入ると、コードは再び非表示になります。

Test2 アカウントの動的コードは常に表示され、自動的に更新されます。

Test3 は HOTP アカウントであり、TOTP アカウントとは異なる更新アイコンであり、ダブルクリックして HOTP コードを更新します。

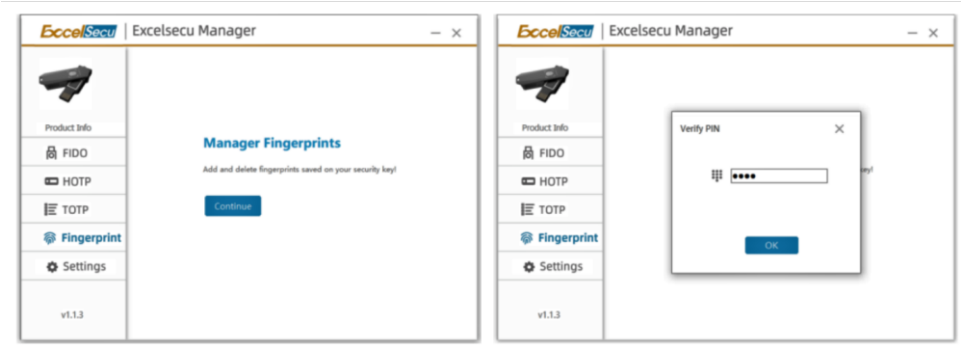


検索バーを使用して、必要なアカウントをすばやく見つけることができます。左クリックして 1 つのアカウントを選択します（背景色が灰色に変わります）。それから、上部の2つのボタンをクリックして、コードをコピーするか、アカウントを削除できます。

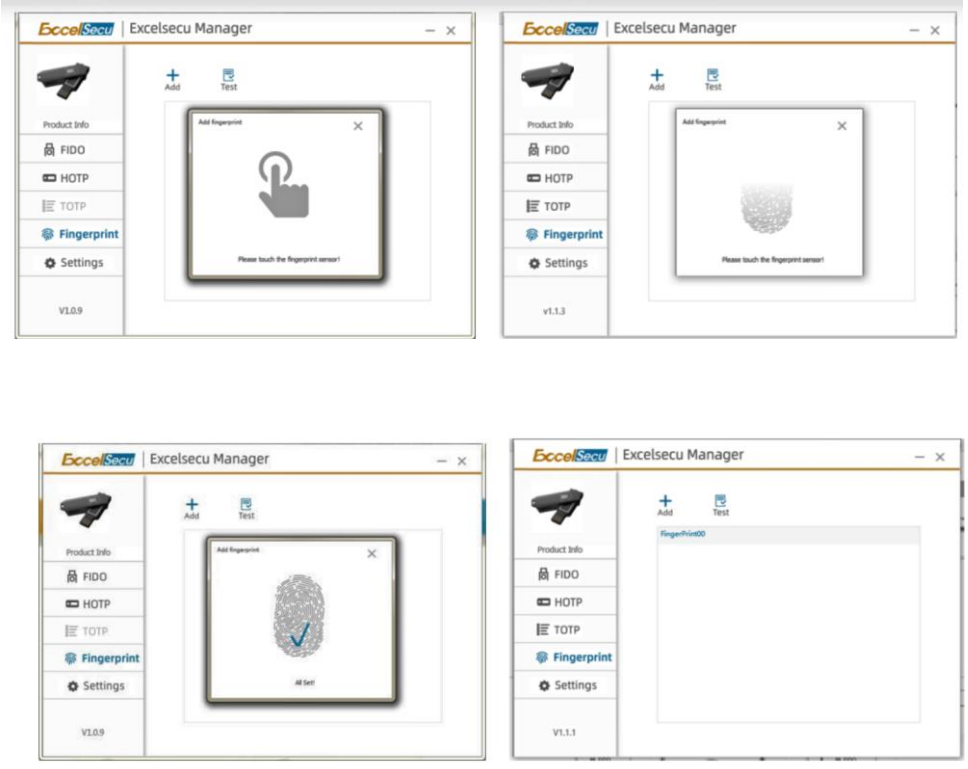


5. Fingerprint(指紋)

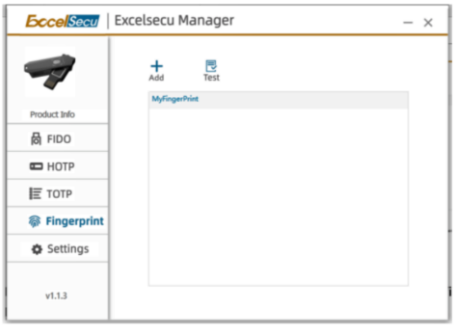
セキュリティキーに暗証番号 PIN を設定されている場合、指紋の管理を選択するときは、最初に暗証番号 PIN の確認を要求されます。



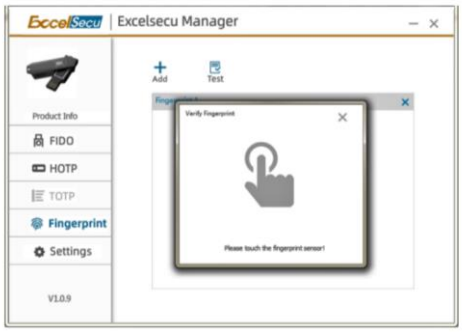
これまでに暗証番号 PIN が設定していなければ、[add(追加)]ボタンをクリックして指紋を追加できます。それには指紋登録を完了させる命令プロプトに従って、指紋を指紋センサーにタッチする必要があります。指紋は正常に登録できると、テキストボックスに表示されます。



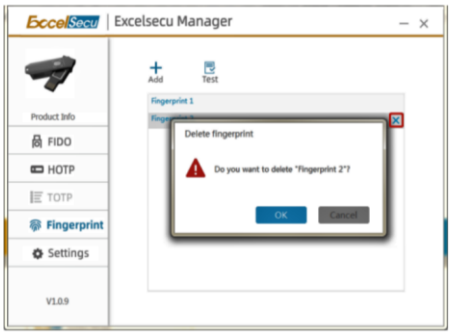
登録した指紋名をダブルクリックすると、変更できます。

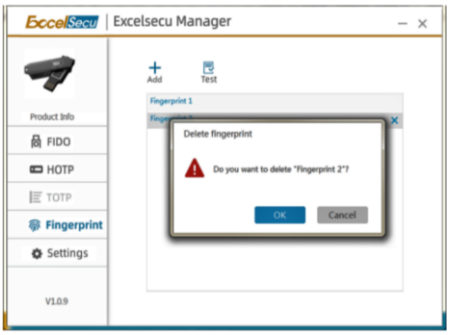


[テスト]ボタンをクリックすると、セキュリティキーが緑色に点滅します。指紋の認証が要求されます。セキュリティのための懸念事項として、ユーザーが指紋の確認に続けて 15 回失敗すると、キーがブロックされます(1 回の再試行につき 3 回 x5 回の再試行)。ブロックされると、ユーザーはリセットを介してのみロックを解除できます(保存されているすべてのデータが失われます)。

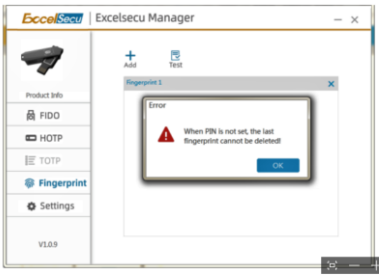


削除したい指紋を削除するには、X ボタンをクリックします。



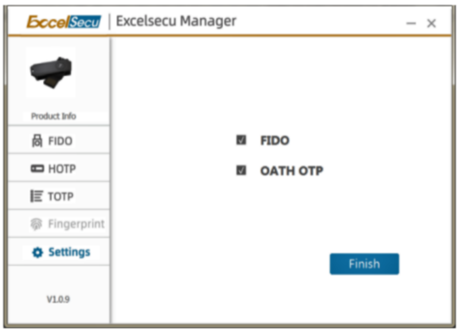


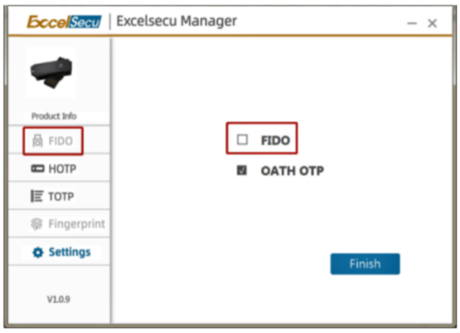
暗証番号 PIN が設定されていない場合、最後の指紋を削除することはできません。

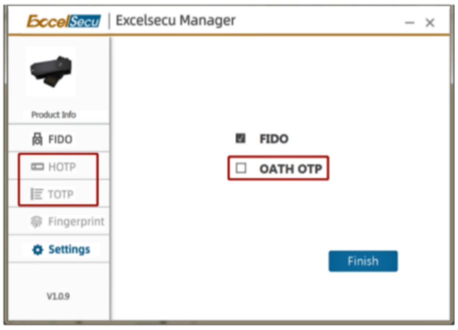


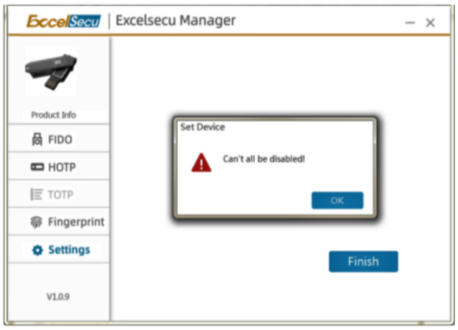
6. Settings(設定)

ここでは、FIDO または OATH 規格の OTP 機能を有効/無効にすることができます。しかし、同時に2つの機能を無効にできません。1 つを無効にすると、対応するメニューがグレーに表示されます。
注:プラットフォームが Windows 10 バージョン 1903(build 18298)以降の場合、OATH OTP が無効になっていると、管理者として Excelsecu FIDOManager ソフトウェアを実行する必要があります。



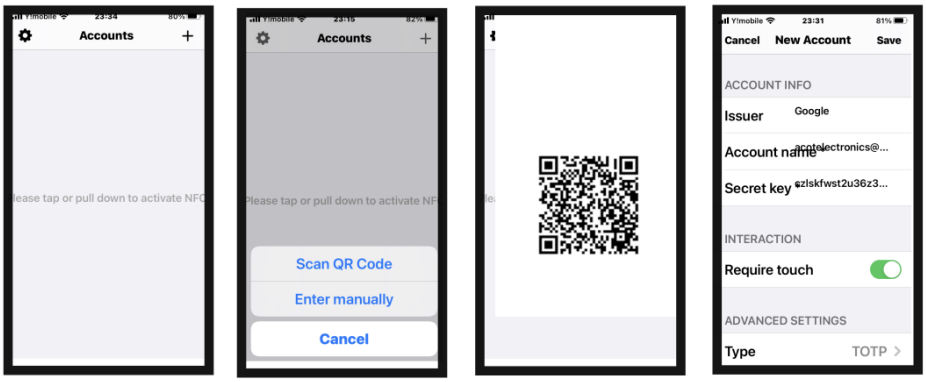






7. iPhone (iOS 13 以上)

1) IPhone に Authenticator アプリをインストールして開きます。アカウントが登録されていないときは、右上橋の”＋”ボタンをクリックすると、QR コードの読み込むか、手入力の選択ができます。この入力操作で、issuer(会社), アカウント名 TOTP 秘密鍵を入力して、保存(save)します。

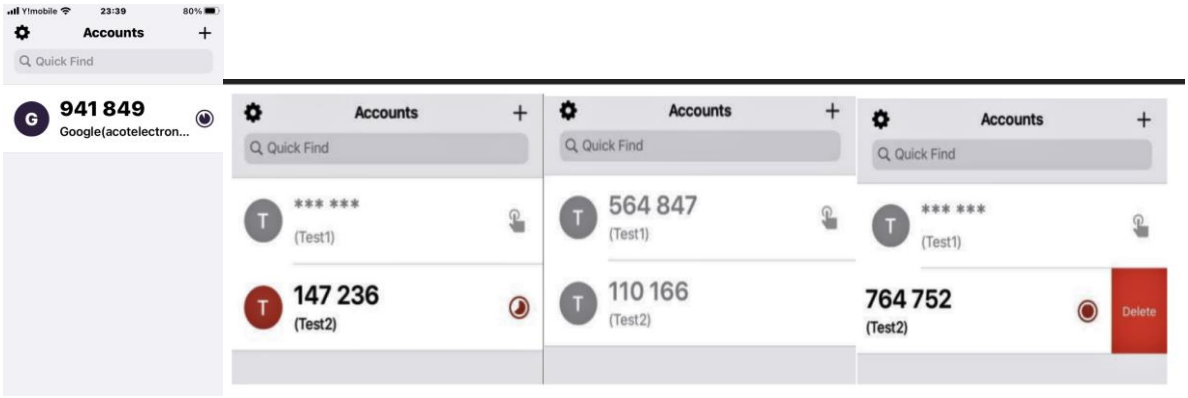


+ボタン　　入力選択　　QR コードう読込　　取得データ

2) TOTP の生成が必要な時、”Please tap or pull down to activate NFC”をクリックして、NFC をアクティブ(利用可能)にします。

3) セキュリティキーのカバーから回転させて USB コネクタを取出し、セキュリティキーを iPhone の本体上部にかざします。セキュリティキー内に既存のアカウントがある場合、アプリは既存のすべてのアカウントを表示します。アカウント、キーにアカウントがない場合、アプリはアカウントなしを表示します。 その場合は、＋ボタンを押してアカウントを追加します。その場合、PC ソフトウェアと同じようにすべてのパラメーターを手動で入力するか、TOTP 認証を提供する Web サービスから QR コードをスキャンします。

4) 数字が非表示の隠しコードを見たい場合は、それをクリックして、NFC 経由でセキュリティキーをもう一度スキャンします。セキュリティキーのボタンを押す必要はありません。アカウントが次のタイムステップに進むと、コードは灰色になって、自動的に更新されません。再び、ページをプルダウンしてセキュリティキーを NFC 経由でスキャンするる必要があります。アカウントを削除する場合は、アカウントを左にスライドすると、削除ができます。

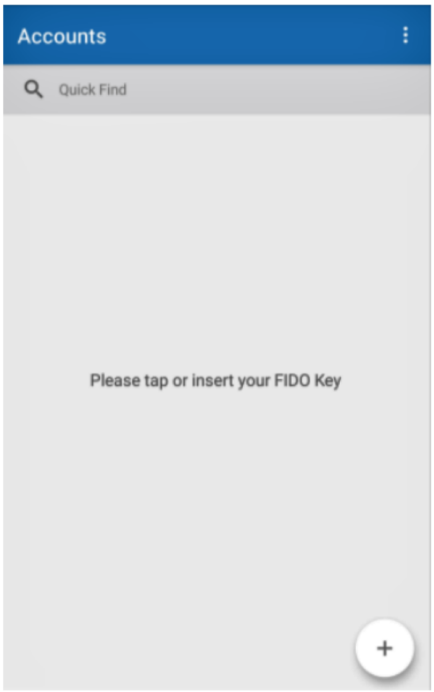


5) 上部の[設定]ボタンをクリックします。ここでいくつかの設定を行うことができます。

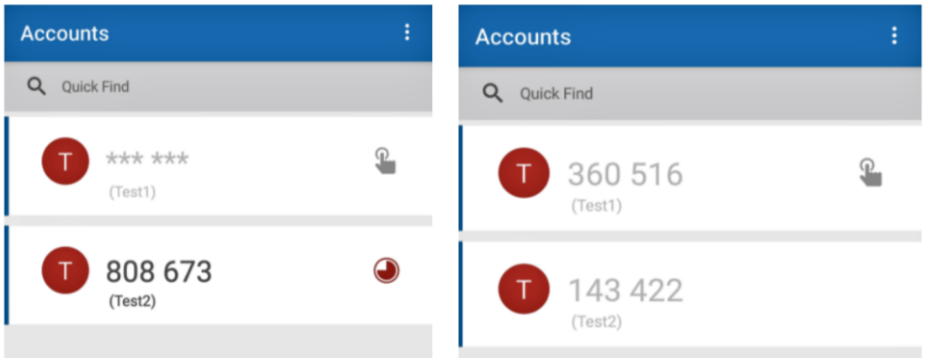
- NFC 警告:NFC が無効になっている場合、または電話にない場合、アプリは警告を発します。
- コード非表示： コードはアプリで非表示になっています。アカウントをクリックしてコードを表示します。てください。隠されます。アプリのホームページを離れた場合も同様に非表示になります。
- リセット:すべてのアカウントを削除します。

8. Android (4.3 以上)

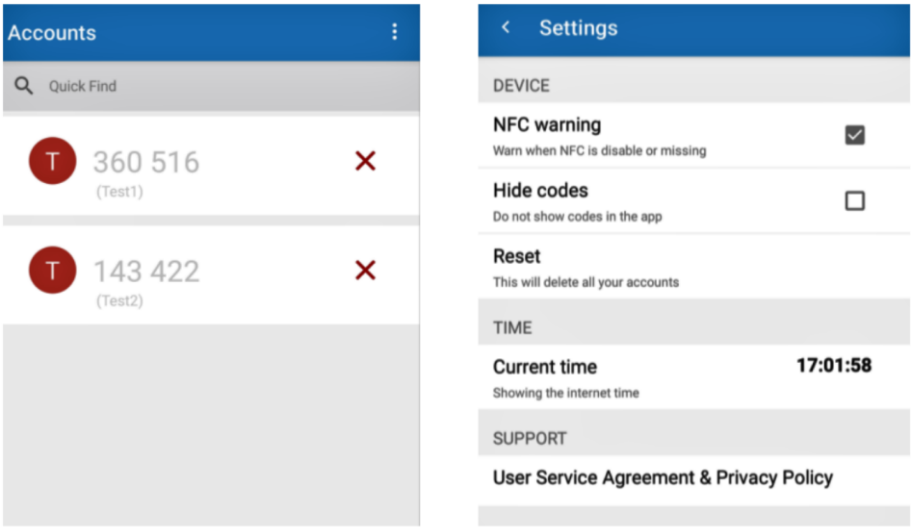
1) スマートフォンにアプリをインストールして開き、スマートフォンの NFC がオンになっていることを確認します。セキュリティキーのカバーから回転させて USB コネクタを取出し、セキュリティキーを電話機の背面に NFC 経由で持ちます。セキュリティキーに既存のアカウントがある場合、アプリは既存のすべてのアカウントを表示します。セキュリティキーにアカウントがない場合、アプリはアカウントなしを表示します。 ＋ボタンを押して追加します。PC ソフトウェアと同じようにすべてのパラメーターを手動で入力するか、TOTP 認証を提供する Web サービスからの QR コードをスキャンできます。



2) 非表示のコードを表示する場合は、アカウントの右側のアイコンをクリックして、セキュリティキーを電話機の背面に NFC 経由で持ちます。セ押したままにします
再び NFC 経由で電話の背面にあるので、キーのボタンを押す必要はありません。アカウントが次のタイムステップに進むと、コードはグレー表示になります。自動的に更新されません。次のことを行う必要があります。電話機の背面にセキュリティキーを持ったままにして、コードを更新します。



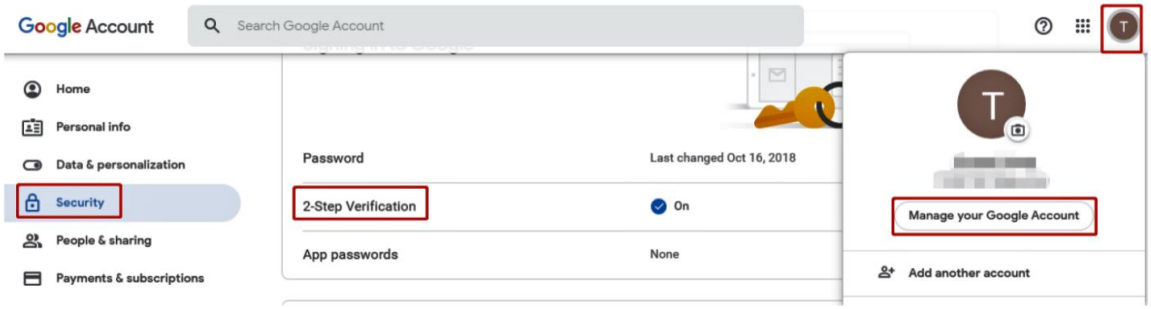
3) 右上隅にある 3 つのドットのアイコンをクリックし、[編集]をクリックすると、希望のアカウントを削除できます。[設定]をクリックすると、iPhone と同じ設定を行うことができます。

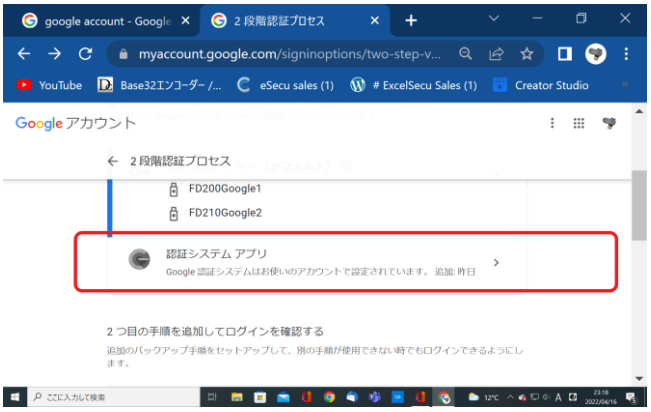


9. Google Authenticator

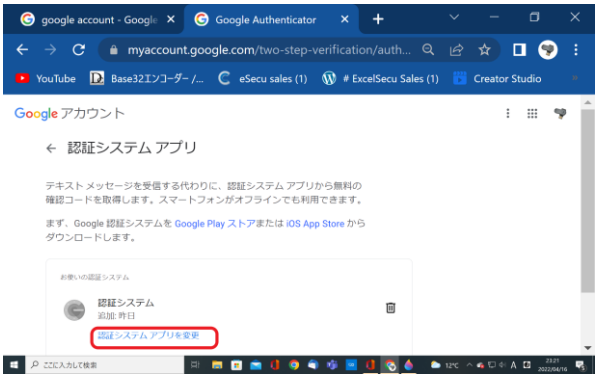
9.1 設定方法

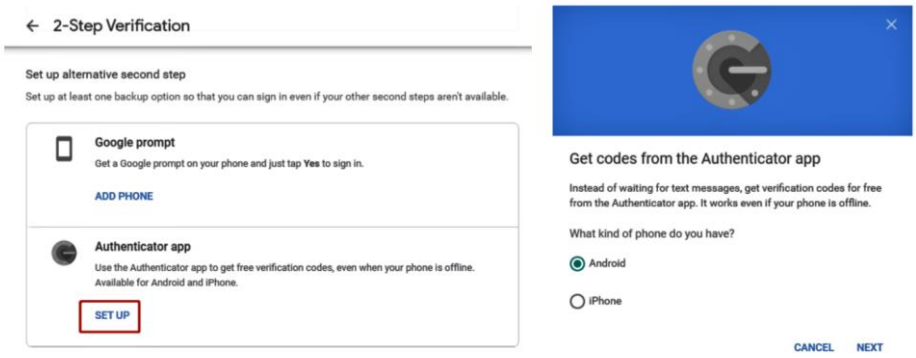
1) https://www.google.com にアクセスし、Google アカウントでサインインします。次に、[管理]に移動します。Google アカウント->セキュリティ-> 2 段階認証プロセス、オンになっていることを確認します。



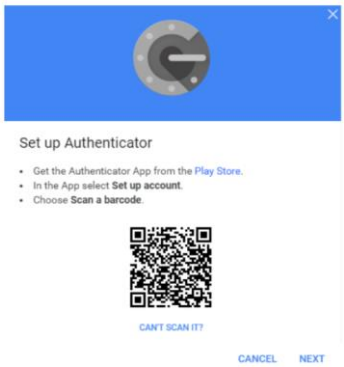


2) 次に、認証システムアプリに移動し、[設定]をクリックして、[Android]または[iPhone]を選択し、[次へ]に移動します。

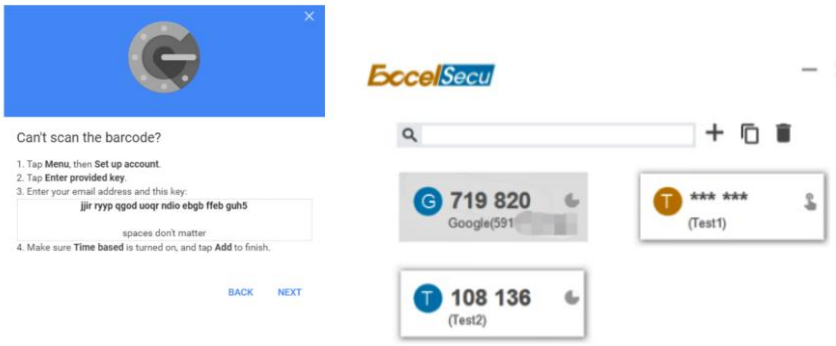




3) [Excelsecu Authenticator] 次に、iPhone または Android フォンで Excelsecu Authenticator を使用して QR コードをスキャンします。 QR コードの下にある[スキャンできません]をクリックし、QR コードの代わりに現れる TOTP 秘密鍵などをコピペして Excelsecu Authenticator に手入力します。Google が出力する秘密鍵データは、Base64形式ですので、パソコンアプリ等で Base32形式に変換してからコピーします。 [次へ]に進みます。



[eSecu FIDO Manager] 同様に QR コードまたは表示データを利用して issuerer (会社名), account (アカウント名), Secret code (TOTP 秘密鍵)を設定します。
Google が出力する秘密鍵データは、Base64形式ですので、パソコンアプリ等　　で Base32形式に変換してからコピーします。 [次へ]に進みます。



4) Excelsecu Authenticator または Excelsecu FIDO Manager からセキュリティコードを取得して、Google ページに入力して確認します。確認できれば完了です。

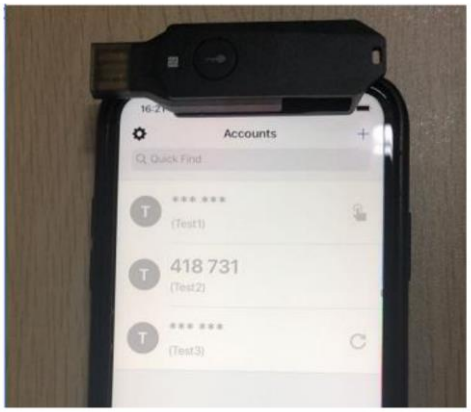
9.2 ２段階認証

Google２段階認証は、パスワードと他の認証方法の組み合わせです。他の認証の時に、セキュリティキーなど選択肢が現れます。ここで、Google 認証システムによる認証を選択すると、６桁のセキュリティコードが要求されますので、Excelsecu Authenticator か、Excelsecu FIDO Manager と、登録した FIDO キーを利用して、セキュリティコードを生成、表示させます。そのコードを Google のコード欄にコピーして２段階認証を行い、サインインできます。

10. FAQ

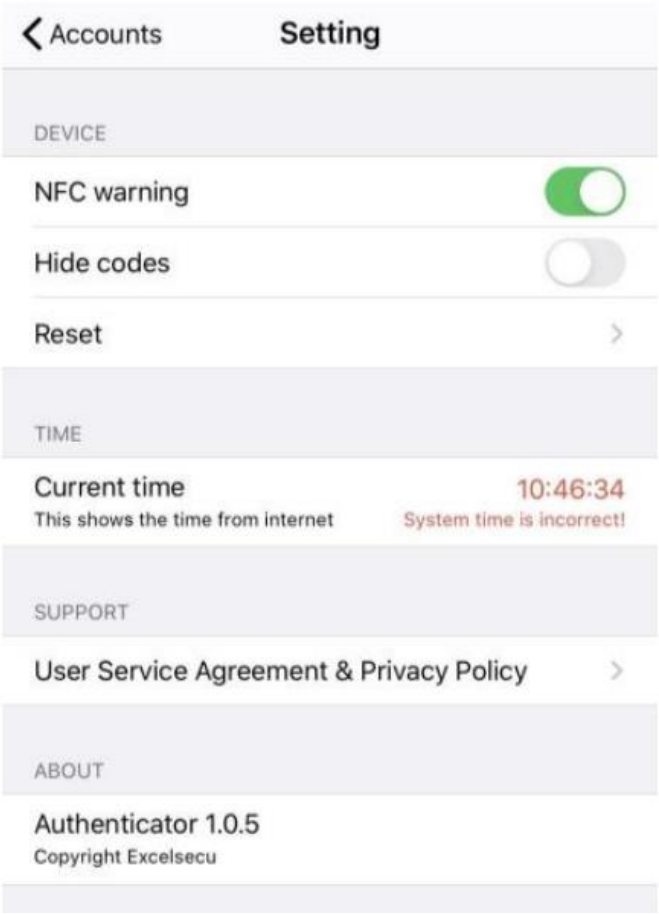
質問： iPhone の認証器アプリが eSecu セキュリティキーにある既存のアカウントをスキャンできないのはなぜですか？

回答： iPhone に iOS 13 以降がインストールされていること、およびセキュリティキーに NFC 機能があることを確認してください。次に、スキャンするときに iPhone の上部にセキュリティキーを置きます。次のようにキーを置くことをお勧めします。



質問: 認証システムアプリの設定で現在時刻はどのように設定しますか？

回答： Excelsecu Authenticator が生成するコードは、お使いの携帯電話の現在時刻に依存します。現在時間はインターネットの時間を示します。電話の時間が正しくない場合、てアプリから生成されたコードは動作しません。「システム時刻が正しくありません！」というエラーが表示された場合設定ページで確認してください。


Accounts
Setting
DEVICE
NFC warning
Hide codes
Reset
TIME
Current time
10:46:34
This shows the time from internet
System time is incorrect!
SUPPORT
User Service Agreement & Privacy Policy
ABOUT
Authenticator 1.0.5
Copyright Excelsecu