# ePass3003 ユーザマニュアル
# （Mac 版）

# V1.0

EnterSafe will do their best to keep the content of this document as accurate as possible. But EnterSafe will not take the responsibilities for any direct or indirect loss that may be caused by this document. The content of this document will be amended along with the updating of the product without notification.

Revision History:

| Date | Version | Description |
|---|---|---|
| 2010/05/20 | 1.0 | 1st Edition |

# CE Attestation of Conformity

The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.
This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in
Test report No. 70407310011
Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

# FCC certificate of approval

This Device is conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment.

# USB

This equipment is USB based.

# WEEE

Dispose in separate collection.

# EnterSafe

# Developer's Agreement

All Products of EnterSafe[*1] including, but not limited to, evaluation copies, diskettes, CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If developers do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse developers the cost of the Product, less freight and reasonable handling charges.

1. **Allowable Use** - Developers may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. Developers may make archival copies of the Software.

2. **Prohibited Use** - The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. Developers may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. Developers may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or an EnterSafe provided enhancement or upgrade to the Product.

3. **Warranty** - EnterSafe warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to developers.

4. **Breach of Warranty** - In the event of breach of this warranty, EnterSafe's sole obligation is to replace or repair, at the discretion of EnterSafe, any Product free of charge. Any replaced Product becomes the property of EnterSafe.

   Warranty claims must be made in writing to EnterSafe during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by EnterSafe. Any Products that developers return to EnterSafe, or an EnterSafe authorized distributor, must be sent with freight and insurance prepaid.

   EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. **Limitation of EnterSafe's Liability** - EnterSafe's entire liability to developers or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price developers paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall EnterSafe be liable for any damages caused by developer's failure to meet developer's obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if EnterSafe has been advised of the possibility of damages, or for any claim by developers based on any third-party claim.

6. **Termination** - This Agreement shall terminate if developers fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

*1:EnterSafe is a software subsidiary of Feitian Technologies Co.,Ltd.

# - 目次 -

# 第1章
# ePass3003 Mac 対応版概要

本マニュアルは ePass3003 Mac 対応版の使用方法について説明します。
ePass3003 Mac 対応版（EnterSafe_Shuttle-1.0.0.090820.dmg）は Mac OS X 環境にて利用するため、ランタイムパッケージや管理ツールを提供しております。

## 1.1 ePass3003 Mac 対応版の構成

ePass3003 Mac 対応版「EnterSafe_Shuttle-1.0.0.090820.dmg」は下記ファイルで構成されます：

- ReadMe.rtf：ReadMe ファイル（英語版）
- EnterSafe Shuttle 1.0.0：ePass3003 ミドルウェアとエンドユーザー用管理ツールのインストール・ランタイムパッケージ
- EnterSafeAdminMgr ：管理者用管理ツール
- instpk.html：Mozilla Firefox ブラウザ対応する PKCS#11 モジュールのインストール/アンインストール用ウェブページ
- license_en.rtf：ライセンスファイル（英語版）

## 1.2 サポートするプラットフォーム

ePass3003 Mac 対応版「EnterSafe_Shuttle-1.0.0.090820.dmg」は下記プラットフォームをサポートします：

- Mac OS X 10.3.X 以上

## 1.3 システム要件

- 前述の OS を使用していること
- Firefox 2.0 以上
- USB ポート（USB1.1/USB2.0）

※ ePass3003 の PKCS#11 モジュールは Mac 環境の Firefox のみ対応しています。ほかのブラウザ（Safali など）対応しておりませんので、ご注意ください。

# 第2章
# ePass3003 ﾗﾝﾀｲﾑﾊﾟｯｹｰｼﾞのｲﾝｽﾄｰﾙとｱﾝｲﾝｽﾄｰﾙ

ePass3003 を使用する前にランタイムパッケージをインストール必要があります。

## 2.1 ePass3003 ランタイムパッケージのインストール

1、 インストールプログラム（EnterSafe Shuttle 1.0.0）を実行すると、下記画面が表示されます、「続ける」をクリックしてください。

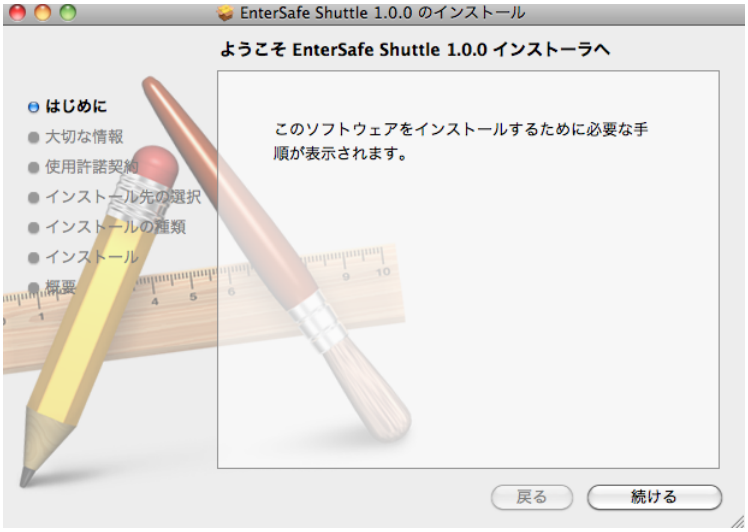


図 2-1

2、 Readme ファイルが表示されます、「続ける」をクリックしてください。

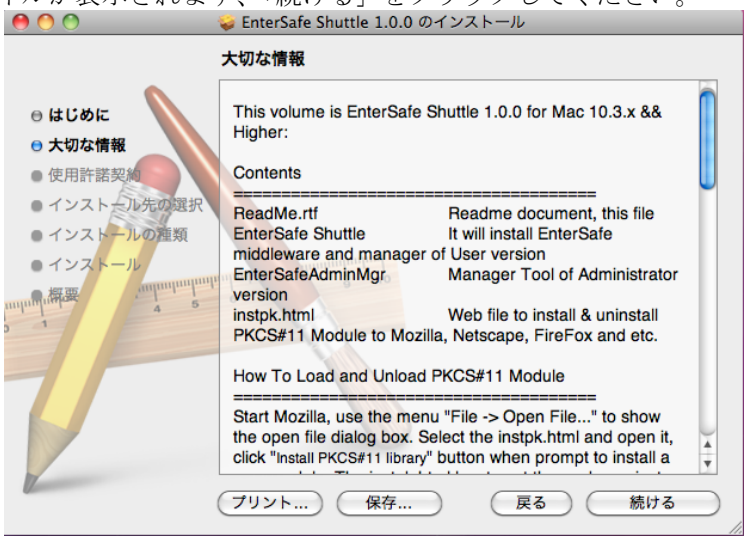


図 2-2

3、 使用許諾契約画面が表示されます、「続ける」をクリックしてください。

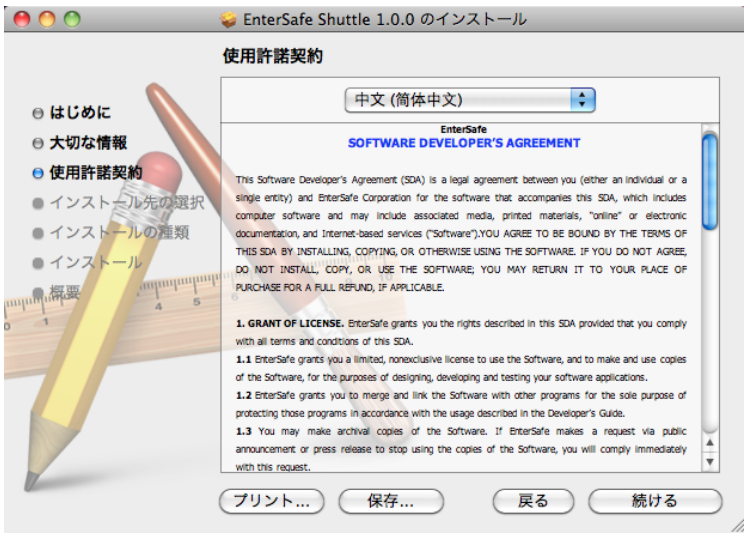


図 2-3

4、 同意可否メッセージ画面が表示されます、同意する場合、「同意する」をクリックして、インストールが続きます。同意しない場合、「同意しない」をクリックします、インストールを終了します。


図 2-4

5、 インストール画面が表示されます。デフォルトでは“Macintosh HD”にインストールされます。デフォルトでインストールする場合、「インストール」をクリックしてください。


図 2-5

インストール先を変更したい場合、上記画面（図 2-5）の「インストール先を変更」をクリックしてください。変更しましたら、「続ける」をクリックしてください。


図 2-6

インストールコンポーネントを選択したい場合、上記画面（図 2-5）の「カスタマイズ」をクリックしてください。インストール項目を選択して、「インストール」をクリックしてください。

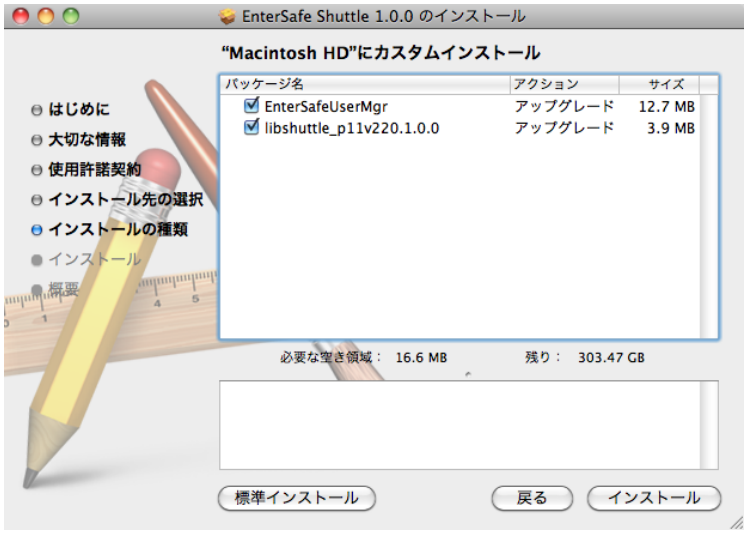


図 2-7

6、 インストールするのは管理者の認証が必要となります。下記認証画面が表示されましたら、管理者名とパスワードを入力し、「OK」をクリックして、インストールを行います。


図 2-8

7、 ePass3003 ランタイムパッケージのインストールが完了すると、以下の画面が表示されるので「閉じる」をクリックしてください。


図 2-9

## 2.2 ePass3003 ランタイムパッケージのアンインストール

ePass3003 ランタイムパッケージを手動アンインストール方法は下記の通りです：

1、 「アプリケーション」下の「EnterSfeUserMgr」をごみ箱に入れて、削除する。

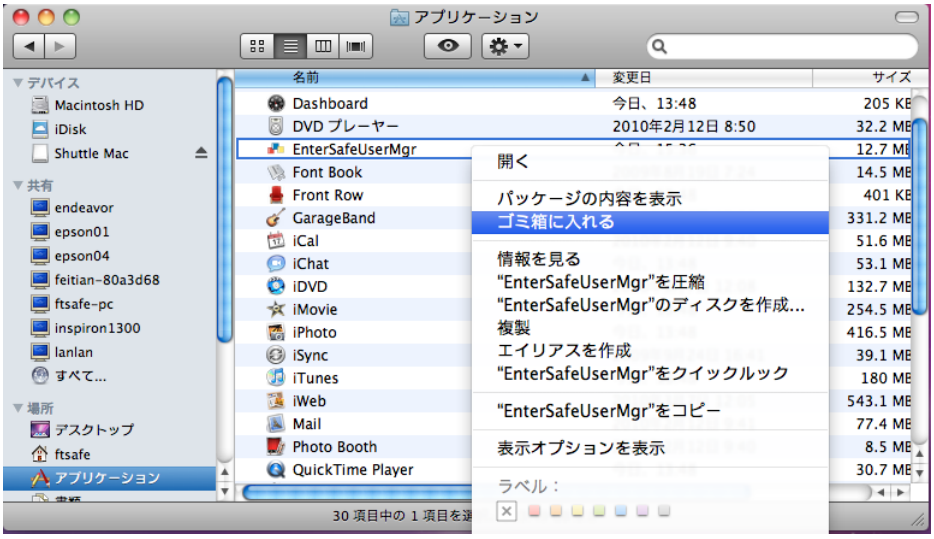


図 2-10

変更を許可するため、管理者のパスワードが必要となります、下記画面が表示されますので、管理者パスワードを入力してください。


図 2-11

2、 「アプリケーション」→「ユーティリティ」→「ターミナル」を起動して、下記コマンドを実行し、関連するファイルを削除してください：

```
$ rm /usr/lib/libshuttle_p11v220.1.0.0.dylib
$ rm -r /Library/Receipts/entersafeusermgr.pkg/
$ rm -r /Library/Receipts/libshuttlep11v220100.pkg/
```

※ 上記コマンドを実行する前に、root アカウントを有効する必要があります。Root アカウントが無効の場合、下記方法で root アカウントを有効することはできます：

① 管理者アカウントでログインします。

② 「アプリケーション」→「ユーティリティ」→「ターミナル」を選択し、ターミナルを開きます。

③ % sudo passwd root　を入力して、Enter を入力してください。パスワードを設定してください。

# 第3章
# ePass3003 PKCS#11 モジュールの追加と削除

ePass3003 ランタイムパッケージのインストール後に Firefox ブラウザを利用する場合は、PKCS#11 の必要コンポーネントをブラウザの設定に追加する必要があります。

PKCS#11 モジュールの追加/削除するには自動と手動の２つの方法があります。具体的な操作は以下の手順に従ってください。なお、下例では Firefox 3.6 での設定方法を明記していますが、各ブラウザのバージョンによって設定方法が若干異なる場合があります。

※ ePass3003 の PKCS#11 モジュールは Mac 環境の Firefox ブラウザのみ対応しています。ほかのブラウザ（Safali など）対応しておりませんので、ご注意ください。

## 3.1 PKCS#11 モジュールの自動追加方法

1、 EnterSafe_Shuttle-1.0.0.090820.dmg に含まれている「instpk.html」を Firefox で開いて、下記画面が表示されます。

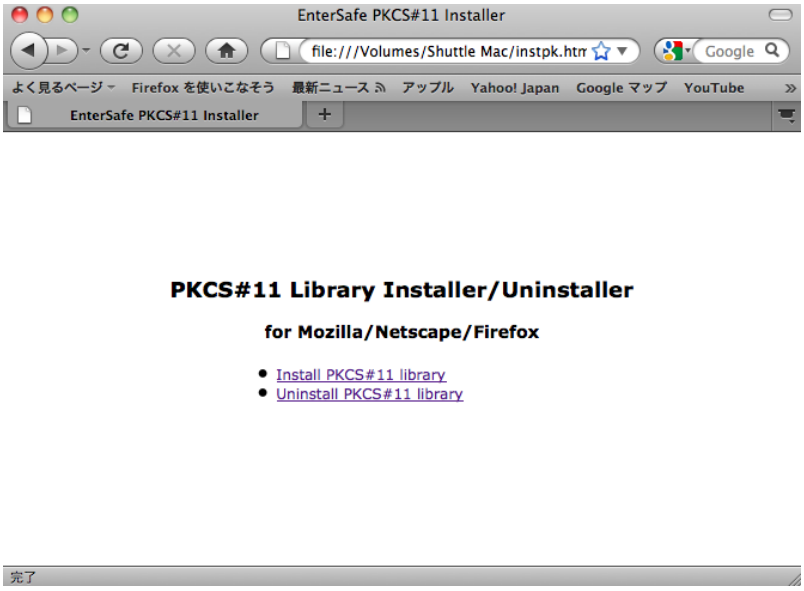


図 3-1

2、 「Install PKCS#11 library」を選択し、インターネットセキュリティ画面が表示されます、「許可」をクリックしてください。

※ Firefox のバージョンよる、表示される画面が異なる場合があります。
※ 確認画面が起動されていない、インストールできない場合、下記「3.2 PKCS#11 モジュールの手動追加方法」をご利用ください。

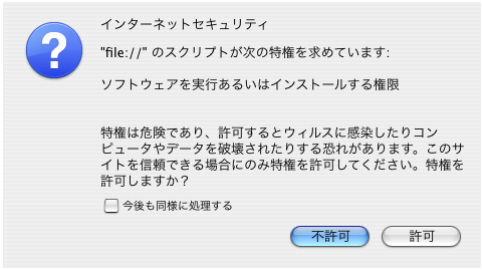


図 3-2

3、 PKCS#11 モジュールがインストールされると、「The PKCS#11 library installed successfully.」メッセージが表示されます。

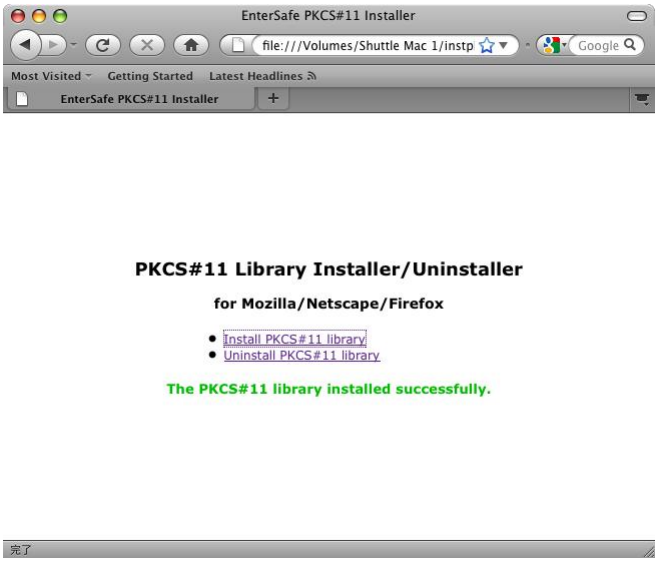


図 3-3

## 3.2 PKCS#11 モジュールの手動追加方法

1、 Firefox を開いて、Firefox→「環境設定」を選択し、下記設定画面が表示されます。

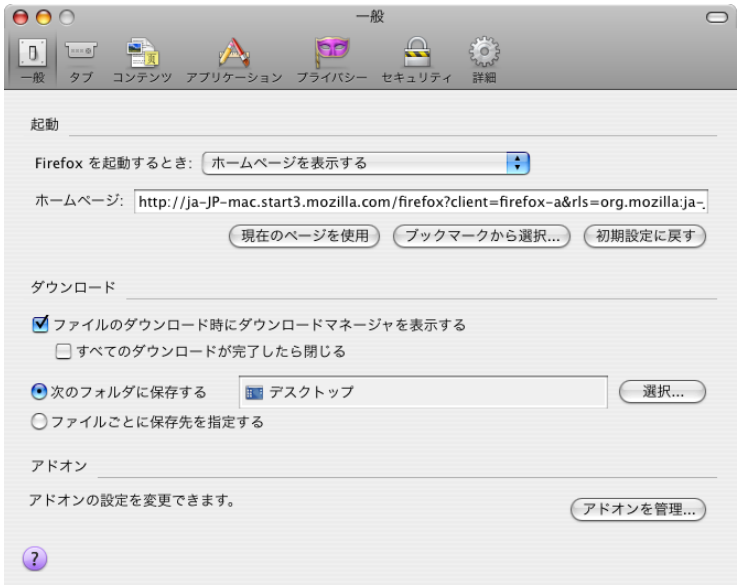


図 3-4

2、 メニュー欄から「詳細」を選択し、「暗号化」タブを選択してください。下記画面が表示されます。

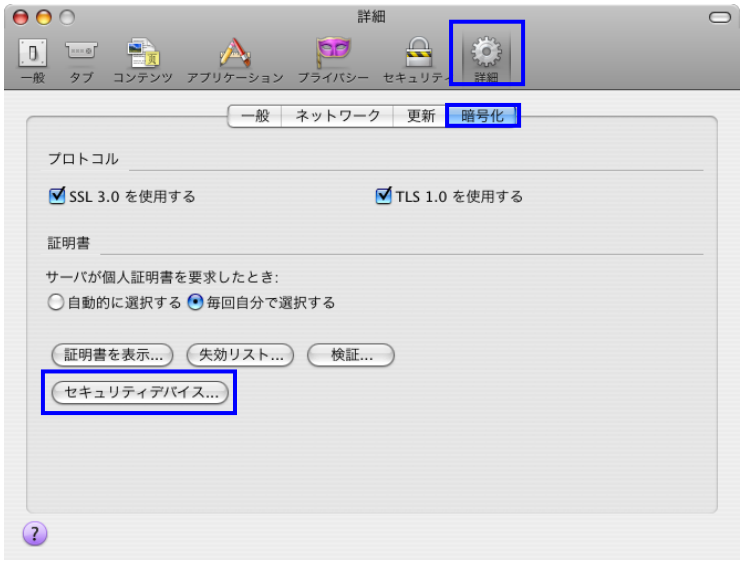


図 3-5

3、 上記画面（図 3-5）の「セキュリティデバイス」ボタンをクリックし、デバイスマネージャ画面が表示されます。

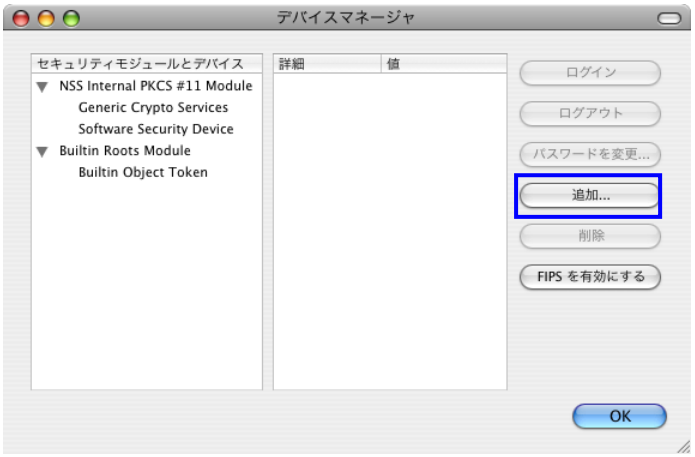


図 3-6

4、 「追加」ボタンをクリックし、PKCS#11 デバイスの追加画面に下記内容を入力してください。
「モジュール名」:「ePassToken PKCS#11 Module」
「ファイルパス」:「/usr/lib/libshuttle_p11v220.1.0.0.dylib」を手動入力してください。

※ 「ファイルパス」の右側が「選択」ボタンがありますが、Mac OS X には、システムファイルはダイナミックライブラリのように保護されますため、libshuttle_p11v220.1.0.0.dylib を選択できません。「ファイルパス」に手入力してください。


図 3-7

5、 「ePassToken PKCS#11 Library」モジュールをデバイスマネージャに追加されます。


図 3-8

## 3.3 PKCS#11 モジュールの自動削除方法

1、 EnterSafe_Shuttle-1.0.0.090820.dmg に含まれている「instpk.html」を Firefox で開いて、下記画面が表示されます。

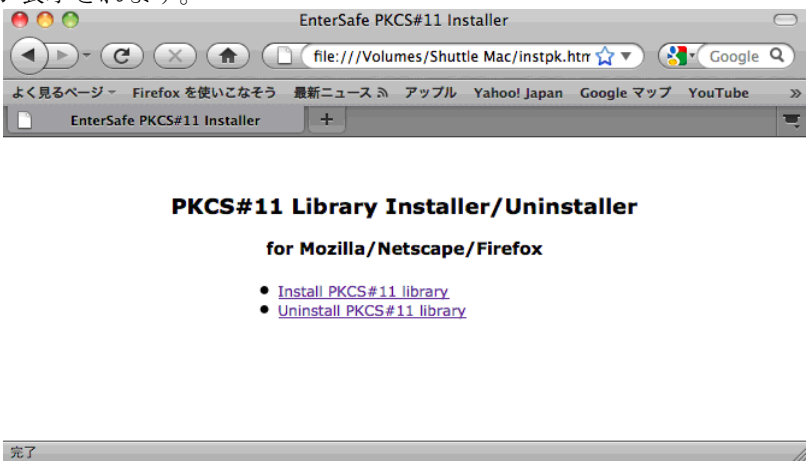


図 3-9

2、 「Uninstall PKCS#11 library」を選択し、インターネットセキュリティ画面が表示され、「許可」をクリックしてください。

※ Firefox のバージョンよる、表示される画面が異なる場合があります。
※ 確認画面が起動されていない、アンインストールできない場合、下記「3.4 PKCS#11 モジュールの手動削除方法」をご利用ください。

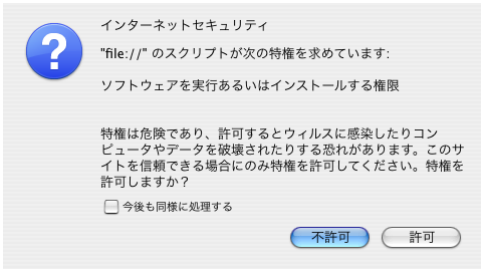


図 3-10

3、 PKCS#11 モジュールをアンインストールされると、「The PKCS#11 library uninstalled successfully.」メッセージが表示されます。

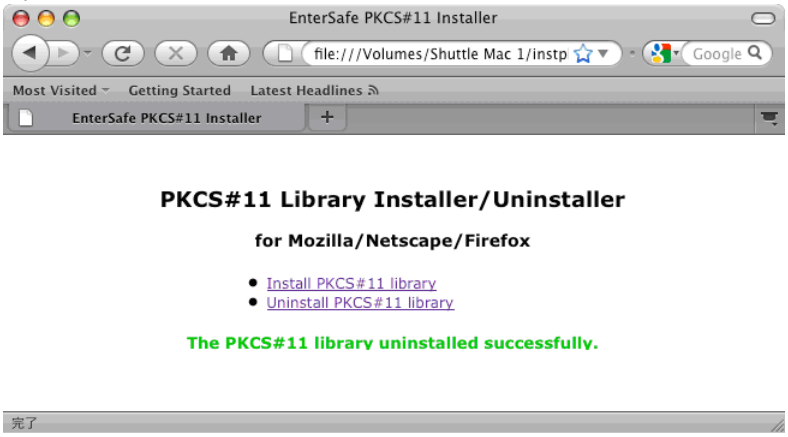


図 3-11

## 3.4 PKCS#11 モジュールの手動削除方法

1、 Firefox を開いて、Firefox→「環境設定」を選択し、設定画面が表示されます。
2、 「詳細」タブを選択し、画面真ん中の「暗号化」タブを選択します（図 3-5 を参照)。
3、 「セキュリティデバイス」ボタンを選択して、デバイスマネージャ画面が表示されます。

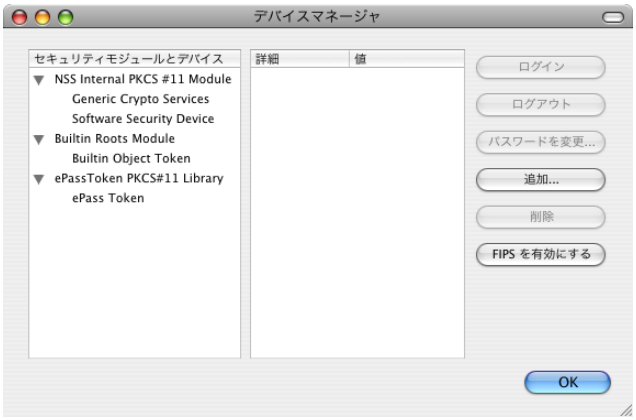


図 3-12

4、 画面左側の「ePassToken PKCS#11 Library」を選択し、「削除」ボタンが選択できるようになります。

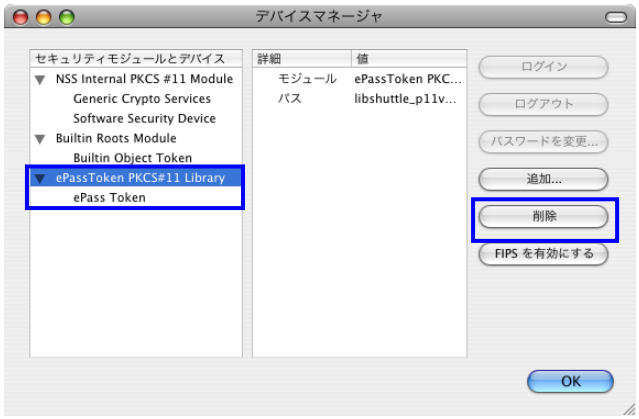


図 3-13

5、 「削除」ボタンをクリックし、下記確認画面が表示されます、「OK」をクリックして、PKCS#11 モジュールが削除されます。


図 3-14

※ Firefox にモジュールを一旦削除されましたら、すぐ追加できません。モジュールを追加する場合、Firefox を再起動してください。

# 第4章
# ePass3003 管理ツール

ePass3003 管理ツールでは ePass3003 の様々な設定変更が行えます、本章は ePass3003 管理ツールの使用方法について説明します。

## 4.1 ePass3003 管理ツール使用の前提条件

ePass3003 管理ツールを利用する前に、ePass3003 のランタイムパッケージをインストール必要があります（「2.1 ePass3003 ランタイムパッケージのインストール」を参照)。
また、ePass3003 トークンは使用前に、PKI 初期化する必要があります。(通常、工場から出荷する際には PKI 初期化されています)

## 4.2 概述

ePass3003 管理ツールには管理者用とエンドユーザー用二つバージョンがあります。エンドユーザー用管理ツールを再配布することは可能です。

- 管理者用管理ツール（EnterSafeAdminMgr)：「EnterSafe_Shuttle-1.0.0.090820.dmg」に含まれています。
- エンドユーザー用管理ツール（EnterSfeUserMgr)：ランタイムパッケージをインストールすると、自動的にアプリケーションにインストールされます。

二つ管理ツールは下記機能が含まれます：

- 「ログイン」(Login)
- 「ユーザ PIN の変更」(Change User PIN)
- 「トークン名の変更」(Change Token Name)
- 証明書の「インポート」(Import)、「エクスポート」(Export)、「削除」(Delete) 及び「証明書情報の表示」(View)

区別は、管理者用バージョンには下記機能が含まれますが、エンドユーザー用バージョンには含まれません。

- 「SO PIN 変更」(Change SO PIN)
- 「ユーザ PIN のブロック解除」(Unlock Token)
- 「初期化」(Initialize Token)

下記エンドユーザー用管理ツール（略称：管理ツール）と管理者用管理ツールについて、説明します。

### 4.2.1 ePass3003 エンドユーザー用管理ツールの起動

- 管理ツールの起動方法
  「アプリケーション」→「EnterSfeUserMgr」をダブルクリックして、管理ツールが起動できます。

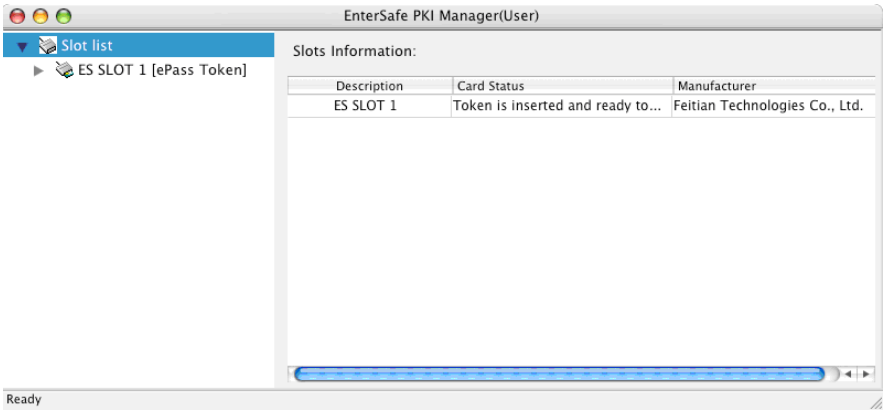


図 4-1

マネージャ画面の左側はトークン・スロット・リストで、右側はスロット情報です。トークンの接続状態は下表でご参照ください。

| トークンの状態 | スロットリスト | スロット情報のカード状態 |
|---|---|---|
| トークン未挿入 | カードが見つかりません | カードが見つかりません |
| PKI 初期化されてないトークンが挿入された | カードが認識されていません | トークンが接続されていますが、未だ利用できません。 |
| PKI 初期化されたトークンが挿入された | トークン名を表示する | トークンが接続され、使用可能になります。 |

画面左側のスロットリストから ePass3003 の名前をクリックすると、スロット詳細情報とトークン詳細情報、操作ボタンが画面の右側に表示されます。

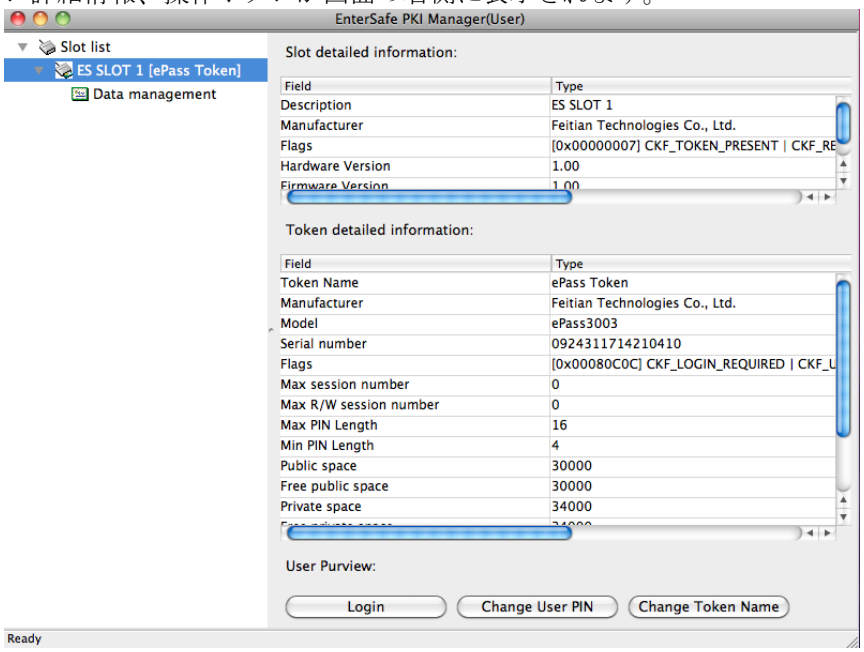


図 4-2

### 4.2.2 ePass3003 管理者用管理ツールの起動

- 管理者用管理ツールの起動方法
  「EnterSafe_Shuttle-1.0.0.090820.dmg」に含まれる EnterSafeAdminMgr を適当な場所へコピーして実行すれば管理者用管理ツール画面が表示されます。

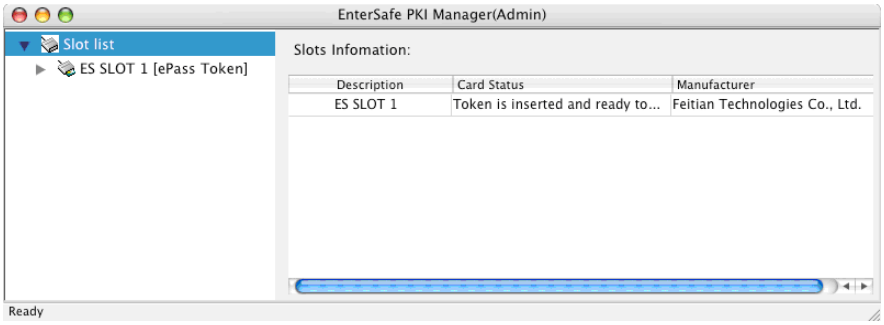


図 4-3

画面左側のスロットリストから ePass3003 の名前をクリックすると、スロット詳細情報とトークン詳細情報、操作ボタンが画面の右側に表示されます。
エンドユーザー用管理ツール画面の違いは、管理者用管理ツールの画面の右下、「Change SO PIN」ボタン、「Unlock Token」ボタン、「Initialize Token」ボタンが表示されます。

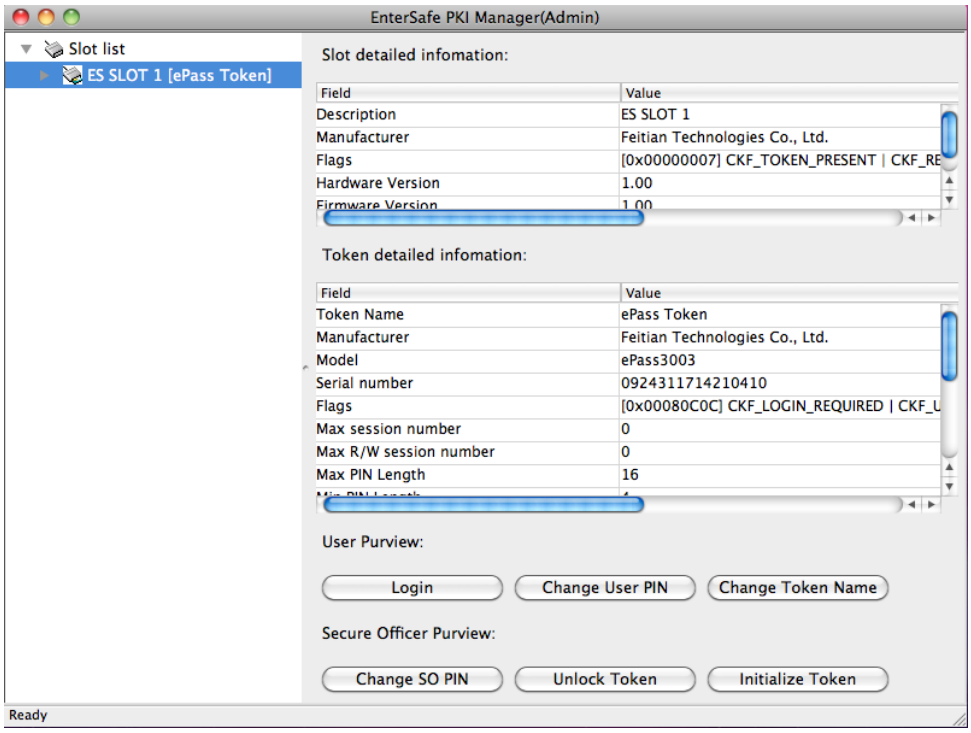


図 4-4

## 4.3 ログイン

管理ツールの左側の「トークン一覧」に表示されている ePass3003 トークンを選んで、「Login」ボタンをクリックすると、ユーザ PIN の入力画面が表示されます。

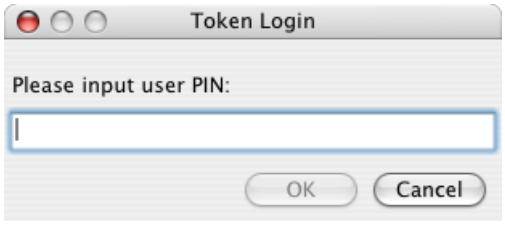


図 4-5

「Please input user PIN」に正しいユーザ PIN を入力します。

※工場出荷時のユーザ PIN は“1234”に設定されています。

「OK」ボタンをクリックすると、下記の証明書画面が表示されます。そのあと、証明書の操作ができます。証明書関連する各操作は「4.9 証明書管理」をご参照ください。

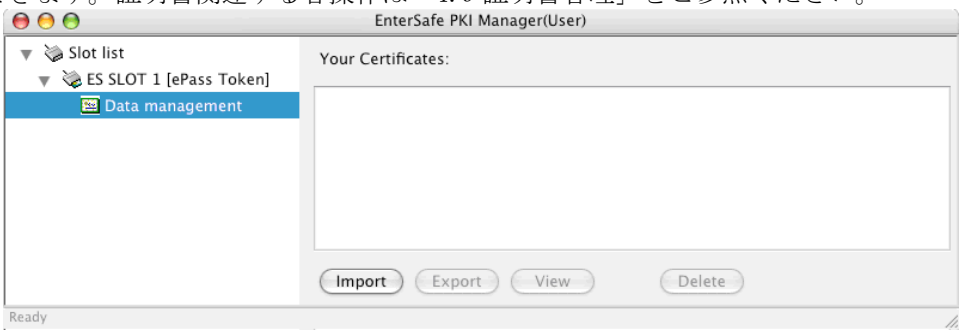


図 4-6

## 4.4 ユーザ PIN 変更

トークンのユーザ PIN を個別に変更することができます。ユーザ PIN 変更機能はすべての既存データを残し、ユーザ PIN のみ変更します。セキュリティ性を高めるため、弊社では User PIN を頻繁に変更する事を推奨しています。

ユーザ PIN を変更するには ePass3003 管理ツールの「Change User PIN」ボタンをクリックしてください。下記画面が表示されます。

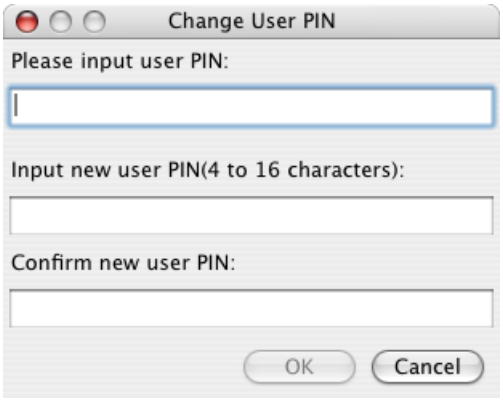


図 4-7

「Please input user PIN」に現在のユーザ PIN を入力し、「Input new user PIN」と「Confirm new user PIN」に新しいユーザ PIN（半角英数字 4～16 文字）を入力して、「OK」ボタンをクリックして変更を行います。PIN の変更に成功すると「Change User PIN successfully!」メッセージが表示されます。

※ 工場出荷時のユーザ PIN は”1234”です。現在のユーザ PIN の入力が間違うと、エラーメッセージが表示されます。もし連続で 6 回入力を誤ると、ユーザ PIN がブロック（一時的にトークンが使用不可能となる）されます。ブロックされたトークンは管理者用管理ツールでしか解除できません。

## 4.5 トークン名の変更

トークンの内部にはシリアル番号で区別されます、シリアル番号が長くて、覚えにくいから、一般的にトークン名で標示します。管理ツールでトークン名の変更ができます。
管理ツール画面の「Change Token Name」をクリックして、下記の画面が表示されます。

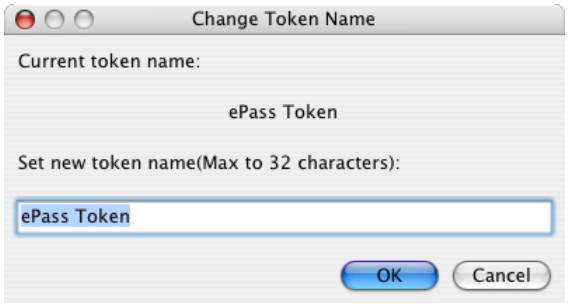


図 4-8

新しいトークン名を入力し（最大 32 桁設定できます)、「OK」ボタンをクリックするとトークン名を変更することができます。変更に成功すると、「Change token name successfully!」メッセージが表示されます。

## 4.6　SOPIN の変更（管理者用管理ツールのみ）

SO PIN は ePass3003 の最も高いレベルのアクセスコードで、通常、管理者などの ePass3003 に全てのコントロール権限を持つ方が利用するので、SO PIN は厳重に保管するようにしてください。

管理者用管理ツールの「Change SO PIN」ボタンをクリックすると、SOPIN 変更画面が表示されます。

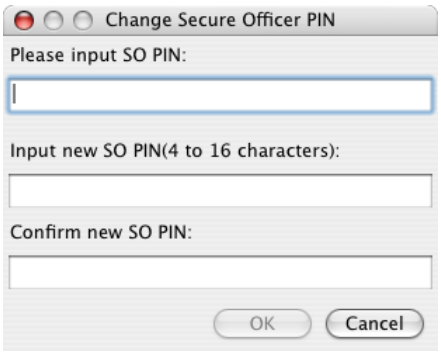


図 4-9

「Please input SO PIN」にトークンの SO PIN を入力し、「Input new SO PIN」と「Confirm new SO PIN」に新しい SO PIN（半角英数字 4～16 文字）を入力して、「OK」ボタンを押下すると、新しい SO PIN に変更されます。変更に成功すると、「Change SO PIN successfully!」メッセージが表示されます。

※工場出荷時の SO PIN は“rockey”です。
SO PIN を変更するには、現在の SO PIN を正しく入力しなければいけません。もし連続で 6 回 SO PIN 入力を誤ると、トークンは以後、使用不能となりますので、十分注意して入力してください。

## 4.7　PIN ブロックの解除（管理者用管理ツールのみ）

ePass3003 に格納したデータは User PIN により保護されており User PIN の再入力回数はハードウェアにより制御されています。ePass3003 では、設定された回数以上 User PIN の入力を誤ると、自動的にブロックされます。User PIN コードがブロックされると、正しいユーザ PIN を入力しても利用することはできません。

User PIN のブロックを解除するには、管理ツールの「Unlock Token」をクリックしてください。トークンブロック解除の画面が表示されます。なお、ブロックの解除には SO PIN が必要です。

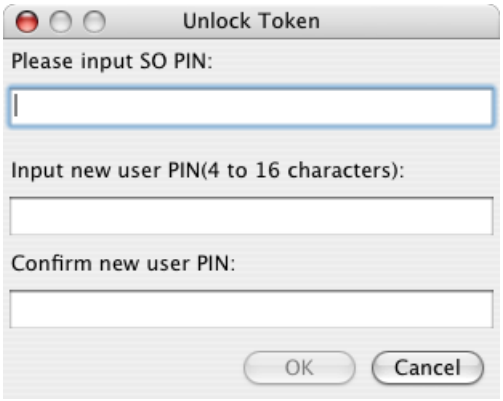


図 4-10

「Please input SO PIN」に SOPIN を入力して、「Input new user PIN」と「Confirm new user PIN」に新しいユーザ PIN(4～16 桁文字)を設定してください。

※　工場出荷時の SOPIN は“rockey”です。ユーザ PIN ブロック解除するには現在の SOPIN を正しく入力しなければいけません。もし 6 回連続して SOPIN 入力を誤ると、トークンは以後、使用不能となりますので、十分注意して入力ください。

「OK」ボタンをクリックするとユーザ PIN がリセットされます。変更に成功すると「Unlock token successfully!」メッセージが表示されます。

※　トークンのユーザ PIN がブロック状態になっていなくても、ユーザがユーザ PIN を忘れてしまった場合、この「トークンブロックの解除」機能から管理者が新しいユーザ PIN を設定できます。

## 4.8　初期化（管理者用のみ）

ePass3003 は利用前に初期する必要があります。初期化は ePass3003 の管理者用管理ツールでのみ行うことができます。初期化時には SOPIN、ユーザ PIN、トークン名を設定する事が出来ます。

※ 初期化により ePass3003 に格納されているデータがすべて削除されます。一旦初期化されたデータは回復することができませんのでご注意下さい。

ePass3003 を初期化するには、管理者用管理ツールの「Initialize Token」ボタンをクリックしてください、下記画面が表示されます。

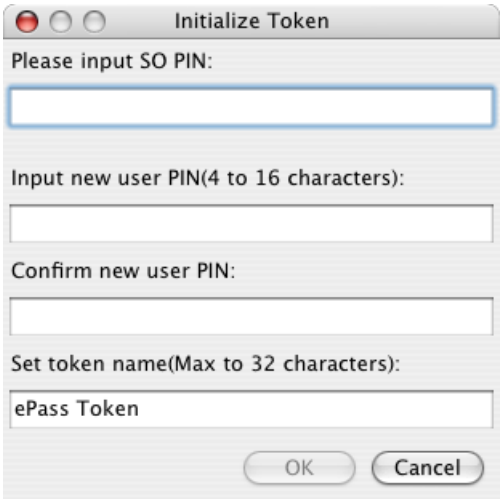


図 4-11

- 「Please input SO PIN」に現在の SO PIN を入力します。(工場出荷時の SO PIN は“rockey”です)
- 「Input new user PIN」と「Confirm new user PIN」に新しいユーザ PIN(4～16 桁文字)を入力します。
- 「Set token name」では ePass3003 のトークン名（最大 32 桁）を設定する事ができます。既定値としては現在のトークン名を表示されています。

「OK」ボタンを押下すると初期化を開始します、初期化に成功すると「Initialize token successfully!」メッセージが表示されます。

## 4.9　証明書管理

ePass3003 マネージャを利用して、証明書のインポート、エクスポート、表示、削除が行えます。証明書を管理する前に、トークンへログインする必要があります。ログイン方法は「4.3 ログイン」をご参照ください。

### 4.9.1 証明書ファイルのインポート

証明書画面の「インポート」ボタンをクリックすると、証明書のインポート画面が表示されます。


図 4-12

「Certificate path」(証明書パス)右側の「…」ボタンをクリックし、“Select your certificate file”画面から証明書ファイルの種類と証明書ファイルを選択します。

※ 現在 ePass3003 は P12、PFX、P7B、CRT と CER の 5 種類の証明書ファイルをサポートします。

「Certificate password」(証明書パスワード) に証明書ファイルのパスワードを入力します。

※ パスワード設定されてない場合は空白のままで構いません。

「OK」ボタンをクリックして、インポートできます。
正しくインポートされると、証明書が画面に反映されます。

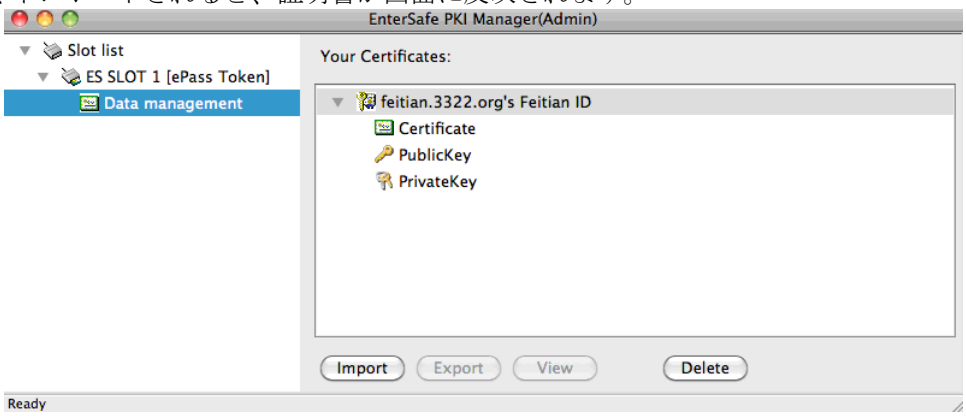


図 4-13

## 4.9.2 証明書ファイルのエクスポート

ePass3003 管理ツールの証明書エクスポート機能を利用して、トークンに保存された証明書をエクスポートして、証明書ファイルに保存できます。
ePass3003 管理の証明書を一つ選択して、「エクスポート」ボタンをクリックすると、証明書保存場所のダイアログボックスが表示されます。

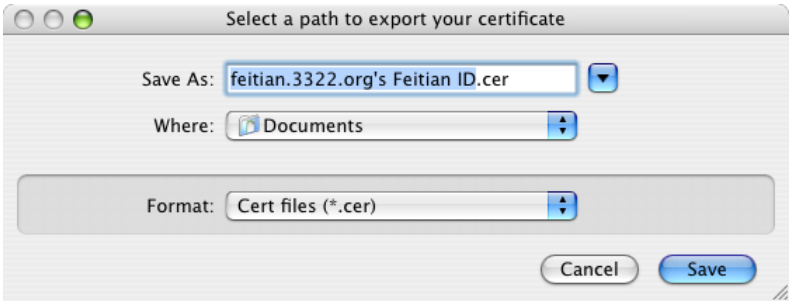


図 4-14

ファイル名とファイルの類型を入力し、「Save」ボタンをクリックして、正常に保存されたら、「Export certificate successfully!」メッセージが表示されます。

※ 管理ツールで証明書をエクスポートできますが、証明書の公開鍵と秘密鍵の鍵ペアはエクスポートできません。

### 4.9.3 証明書情報の表示

証明書画面に「証明書」(Certificate)、「公開鍵」(PublicKey)、「秘密鍵」(PrivateKey)のいずれか選択して、「View」ボタンをクリックすると、トークン内保存されたデータの詳細画面が表示されます。

トークンに保存された「Certificate」を選択して、「View」ボタンをクリックすると、下記の画面が表示されます。

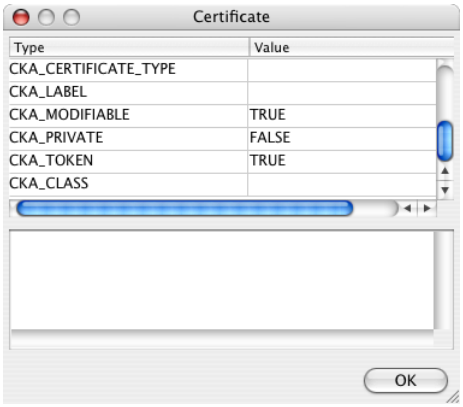


図 4-15

トークンに保存された「PublicKey」を選択して、「View」ボタンをクリックすると、下記の画面が表示されます。

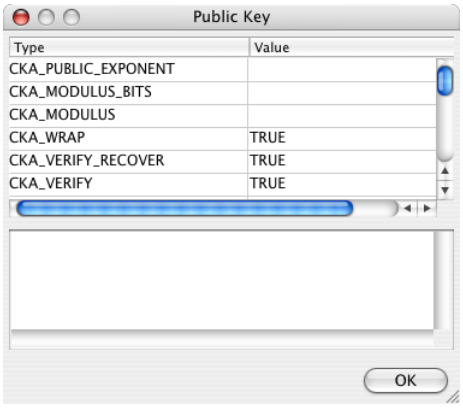


図 4-16

トークンに保存された「PrivateKey」を選択して、「View」ボタンをクリックすると、下記の画面が表示されます。

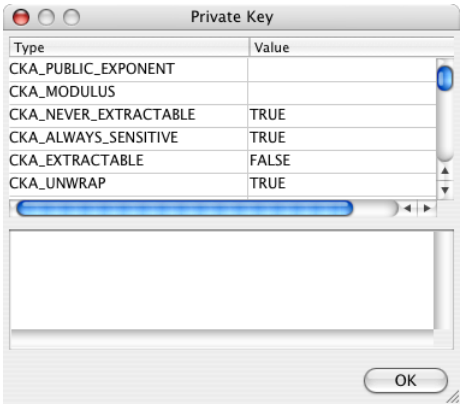


図 4-17

### 4.9.4 証明書の削除

管理ツールで不要な証明書を削除する事ができます。削除するには証明書画面から削除したい証明書を選択し、「Delete」ボタンをクリックすると、下記メッセージ画面が表示されます。


図 4-18

「Yes」ボタンをクリックして、証明書が削除され、占有されているメモリ領域も開放されます。
同じ方法で、ePass3003 内の秘密鍵と証明書コンテナをクリックして、「Delete」ボタンをクリックすると、ePass3003 内の秘密鍵と証明書コンテナを削除できます。もし ePass3003 のトークン一覧を選択して、「Delete」ボタンをクリックすると、ePass3003 内にすべてのコンテナ、証明書、秘密鍵を削除できます。

# 付録
# 用語と略称

| 用語、略称 | 説明 |
|---|---|
| ePass3003 | Feitian Technologies 社が開発、販売する携帯性、利便性とコストパフォーマンスにも優れたセキュリティデバイスです。 |
| Token | コンピュータサービスの利用権限のある利用者に、認証の助けとなるよう与えられる物理デバイスのことです。 |
| USB Token | USB インターフェイスを持つトークンのことです。ePass3003 はその１種です。<br>携帯に便利で操作が簡単であるため、証明書などの認証情報の格納に利用されています。 |
| PKCS#11 インターフェイス | PKCS#11 は、RSA Security 社が策定した、ハードウェアに依存しない、暗号化アクセラレータやスマートカードなどの暗号化トークンに対するプログラミングインタフェースです。 |