Red Hat Certificate System 10

Enterprise Security Client を使用したスマートカードの管理

Red Hat Certificate System 10.1 向けに更新

Last Updated: 2023-05-14

Red Hat Certificate System 10 Enterprise Security Client を使用したスマートカードの管理

Red Hat Certificate System 10.1 向けに更新

Florian Delehaye
Red Hat Customer Content Services
fdelehay@redhat.com

Marc Muehlfeld
Red Hat Customer Content Services

Petr Bokoč
Red Hat Customer Content Services

Marc Muehlfeld
Red Hat Customer Content Services

Filip Hanzelka
Red Hat Customer Content Services

Ella Deon Ballard
Red Hat Customer Content Services

Tomáš Čapek
Red Hat Customer Content Services

法律上の通知

概要

本ガイドは、Certificate System サブシステムの通常のユーザーを対象としています。また、スマートカードのフォーマットおよび管理用のシンプルなインターフェイスである Enterprise Security Client を使用して、個人証明書および鍵を管理する方法を説明します。

目次

第1章 ENTERPRISE SECURITY CLIENT の概要

Enterprise Security Client は、スマートカードの管理を簡素化する Red Hat Certificate System のツールです。エンドユーザーは、セキュリティートークン (スマートカード) を使用して、シングルサインオン (SSO) アクセスやクライアント認証などのアプリケーションのユーザー証明書を保存できます。エンドユーザーには、署名、暗号化、およびその他の暗号化機能に必要な証明書および鍵が含まれるトークンが発行されます。

Enterprise Security Client は、Certificate System の完全なトークン管理システムの 3 番目の部分です。2 つのサブシステム (Token Key Service (TKS) および Token Processing System (TPS)) は、トークン関連の操作を処理するために使用されます。Enterprise Security Client は、スマートカードとユーザーがトークン管理システムにアクセスできるようにするインターフェイスです。

トークンの登録後、Mozilla Firefox や Thunderbird などのアプリケーションは、トークンを認識して、クライアント認証や S/MIME メールなどのセキュリティー操作に使用するように設定できます。Enterprise Security Client は、以下の機能を提供します。

- Gemalto 64K V2 や Safenet 300J Java スマートカードなどの Global Platform 準拠のスマートカードに対応します。
- セキュリティートークンを登録して、TPS で認識されるようにします。
- TPS でトークンを再登録するなど、セキュリティートークンを維持します。
- 管理対象トークンの現在のステータスに関する情報を提供します。
- トークンが失われた場合に別のトークンで鍵をアーカイブおよび復元できるように、TPS および DRM サブシステムによるサーバー側の鍵生成をサポートします。

1.1. RED HAT ENTERPRISE LINUX、シングルサインオン、および認証

ネットワークユーザーは、使用する各種サービスに複数のパスワードを送信する必要があります。たとえば、電子メール、Web 閲覧、組織のサーバー、およびネットワーク上のサーバーなどです。複数のパスワードを維持して、常にパスワードの入力を求められると、ユーザーおよび管理者にとっては面倒です。**シングルサインオン** は、管理者が単一のパスワードストアを作成してユーザーが一度ログインし、単一のパスワードを使用してすべてのネットワークリソースに認証できるようにするための設定です。

Red Hat Enterprise Linux は、ワークステーションへのログイン、スクリーンセーバーのロック解除、Mozilla Firefox を使用して暗号化された Web ページへのアクセス、Mozilla Thunderbird を使用した暗号化された電子メールの送信など、複数のリソースのシングルサインオンをサポートします。

シングルサインオンは、ユーザーにとって便利であると同時に、サーバーおよびネットワークのセキュリティーにおけるもう 1 つの層でもあります。シングルサインオンは、セキュアで効果的な認証をベースにしており、Enterprise Security Client は Red Hat Certificate System が実装する公開鍵インフラストラクチャーに関連付けられます。

セキュアなネットワーク環境を確立するための基盤の 1 つは、ネットワークへのアクセス権限を持つユーザーにアクセスが制限されるようにすることです。アクセスが許可されると、ユーザーはシステムに対して **認証** できます。つまり、ユーザーはアイデンティティーを検証できます。このような方法の 1 つとして **証明書** (証明書が存在するエンティティーを特定する電子ドキュメント) を表示することが挙げられます。

これらの証明書はスマートカードに保存できます。ユーザーがスマートカードを挿入すると、スマートカードは証明書をシステムに提示し、ユーザーを識別して認証できるようにします。Red Hat Enterprise Linux のシングルサインオンに対する 2 つの認証方法の 1 つはスマートカード認証です。もう 1 つは Kerberos ベースの認証です。

スマートカードを使用したシングルサインオンには、以下の 3 つの手順があります。

1. ユーザーがスマートカードをカードリーダーに挿入します。これは、Red Hat Enterprise Linux のプラグ可能な認証モジュール (PAM) により検出されます。

2. システムは、証明書をユーザーエントリーにマッピングし、スマートカードで提示された証明書をユーザーエントリーに保存されている証明書と比較します。

3. 証明書がキー配布センター (KDC) に対する検証に成功すると、ユーザーはログインを許可されます。

Enterprise Security Client は、シングルサインオンの管理に含まれるスマートカードを管理します。

1.2. RED HAT CERTIFICATE SYSTEM および ENTERPRISE SECURITY CLIENT

Red Hat Certificate System は、証明書および鍵の作成、管理、更新、取り消しを行います。Certificate System には、スマートカードを管理するために、キーの生成、証明書リクエストの作成、および証明書受け取りを行うトークン管理システムがあります。

2 つのサブシステム (Token Key Service (TKS) および Token Processing System (TPS)) は、トークン関連の操作を処理するために使用されます。Enterprise Security Client は、スマートカードとユーザーがトークン管理システムにアクセスできるようにするインターフェイスです。

合計 4 つの Certificate System サブシステムは、トークンの管理を行います。2 つはトークンの管理 (TKS および TPS) に、もう 2 つは公開鍵インフラストラクチャー (CA および DRM) 内の鍵と証明書の管理に使用します。

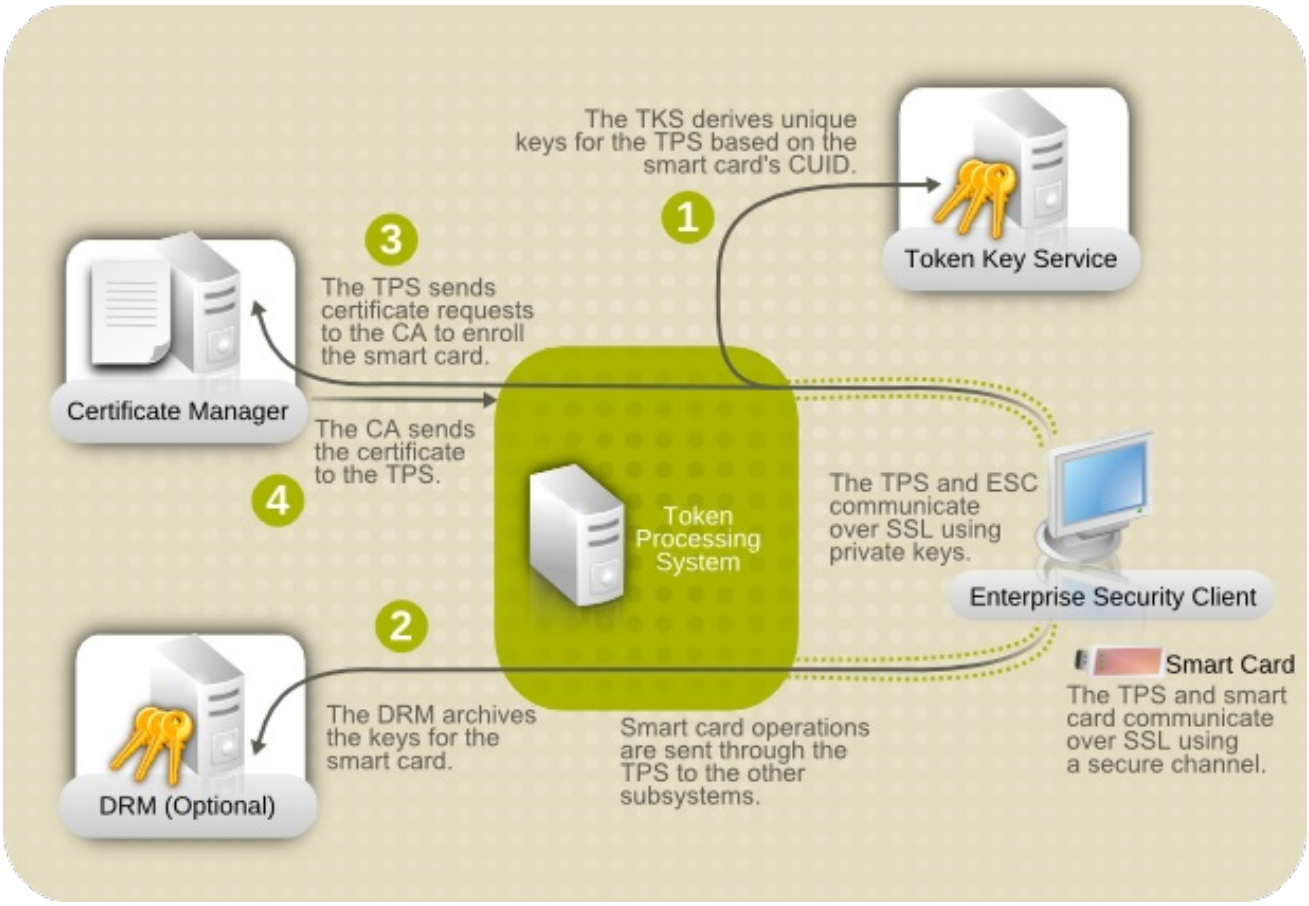
- Token Processing System (TPS) はスマートカードと対話し、ユーザーやデバイスなどの特定のエンティティーのキーと証明書を生成および保存できるようにします。スマートカード操作は TPS を経由して、証明書を生成する認証局やデータリカバリーマネージャーなどのアクションに適したサブシステムに転送され、キーをアーカイブおよび回復します。

- Token Key Service (TKS) は、TPS とスマートカード間の通信に使用される対称鍵を生成または取得します。TKS によって生成された鍵のセットは、カードの一意 ID を基にしているため固有のものとなっています。鍵は、スマートカード上でフォーマットされ、この鍵を使用してスマートカードと TPS との間で通信を暗号化するか、または認証を行います。

- 認証局 (CA) は、スマートカードに保存されているユーザー証明書を作成して破棄します。

- 必要に応じて、Data Recovery Manager (DRM) は、スマートカードのキーをアーカイブおよび復元します。

図1.1 Certificate System のスマートカードの管理方法



TPS は、図1.1「Certificate System のスマートカードの管理方法」 に示すように、Red Hat Certificate System トークン管理システムの中心となるハブです。トークンは TPS と直接通信します。その後、TPS は TKS と通信して、TPS のトークン通信 (1) に使用できる一意の鍵のセットを取得します。スマートカードが登録されると、トークンに新しい秘密鍵が作成されます。キーのアーカイブを設定する場合は、これらのキーを DRM(2) でアーカイブできます。CA は証明書要求 (3) を処理し、トークンに保存する証明書を発行します。TPS は、これらの証明書を Enterprise Security Client (4) に戻します。これらはトークンに保存されます。

Enterprise Security Client は、TPS が安全な HTTP チャンネル (HTTPS) で各トークンと通信し、Certificate System とともに TPS を介して通信するパイプになります。

トークンを使用するには、Token Processing System がトークンを認識して通信できるようにする必要があります。必要な鍵と証明書でトークンを設定し、Certificate System にトークンを追加するために、トークンを最初に **登録** する必要があります。Enterprise Security Client は、トークンを登録するエンドエンティティーのユーザーインターフェイスを提供します。

第2章 ENTERPRISE SECURITY CLIENT のインストール

2.1. クライアントでサポートされるプラットフォーム

Enterprise Security Client インターフェイスは、Red Hat Enterprise Linux 7.3 以降のプラットフォームでサポートされています。

また、Red Hat Enterprise Linux 5 および 6 の最新バージョンでもサポートされます。これらのプラットフォームは Red Hat Certificate System 10 をサポートしませんが、このクライアントは Red Hat Certificate System 10 の TMS システムで使用できます。

2.2. 対応するスマートカード

詳細は、Red Hat Certificate System 10 リリースノート で該当するセクションを参照してください。

2.3. RED HAT ENTERPRISE LINUX での ENTERPRISE SECURITY CLIENT のインストールおよびアンインストール

2.3.1. ESC クライアントのインストール

Enterprise Security Client のインストールの最初の手順は、必要なパッケージをダウンロードすることです。パッケージを取得する方法は 2 つあります。

- カスタマーポータルから ISO イメージをダウンロードする。
- Red Hat **yum** ユーティリティーを使用する。

RPM を取得する方法として、以下のように **yum** コマンドラインユーティリティーを使用することが推奨されます。

```
# yum install esc
```

yum コマンドが正常に完了すると、必要な Enterprise Security Client RPM と依存関係がすべてインストールされ、使用できる状態になります。

注記

yum ユーティリティーを使用して Enterprise Security Client をインストールした場合は、クライアントがすでにインストールされているので他にインストールする必要はありません。以下の手順では、CD イメージからインストールします。

1. **root** ユーザーとして、Enterprise Security Client パッケージをインストールします。

```
# yum install esc
```

Enterprise Security Client は、Red Hat Enterprise Linux 32 ビットシステムの **/usr/lib/esc-1.1.0** と、Red Hat Enterprise Linux 64 ビットシステムの **/usr/lib64/esc-1.1.0** にあります。**esc** シェルスクリプトが **/usr/bin/esc** にインストールされている。**esc** コマンドを実行すると、Enterprise Security Client を起動できます。

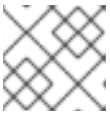
Enterprise Security Client for Linux は、スマートカードの挿入を待機する警告なしで実行されるデーモ

ン (**escd**) を実装します。登録されていないスマートカードが挿入されると、デーモンは自動的にクライアント UI を起動し、Enterprise Security Client ガイドに従って登録プロセスを進めます。また、**System Settings** を選択して **Smart Card Manager** を設定して、**System** メニューからクライアントを手動で起動することもできます。

2.3.2. ESC クライアントのアンインストール

1. すべての USB トークンを取り外します。
2. Enterprise Security Client を停止します。
3. **root** ユーザーとしてログインし、**rpm -ev** を使用して Enterprise Security Client RPM を削除します。

```
# yum remove esc
```



注記

お使いのバージョンに一致する RPM ファイルのバージョン番号を更新します。

4. インストールディレクトリーの残りのファイルを削除します。

第3章 ENTERPRISE SECURITY CLIENT の使用

以下のセクションでは、Enterprise Security Client を使用したトークンの登録、フォーマット、およびパスワードのリセットの操作に関する基本的な手順を説明します。

3.1. ENTERPRISE SECURITY CLIENT のトレイアイコン

多くのプログラムは、トレイまたは通知エリアにアイコンがあり、このようなアイコンを使用してプログラムの動作を制御できます。通常は、アイコンを右クリックしてコンテキストメニューに移動します。Enterprise Security Client は、スマートカードの挿入や削除などのエラーやアクションのツールチップなど、トレイアイコンを提供します。

図3.1 トークントレイアイコンおよびツールチップの例

デフォルト設定では、Enterprise Security Client が起動して、自動的にトレイ部分に最小化されます。Red Hat Enterprise Linux では、Gnome の通知領域が有効になっている場合に限り、トレイアイコンが表示されます。

3.2. ENTERPRISE SECURITY CLIENT の起動

Enterprise Security Client の起動には、以下の 2 つの概念があります。Enterprise Security Client プロセスを開始して、挿入されたスマートカードまたはトークンを検出できるよう、通知なく実行される必要があります。スマートカードが挿入されたり、または手動で開くことができると、Enterprise Security Client のユーザーインターフェイスが自動的に開きます。

3.2.1. Red Hat Enterprise Linux での Enterprise Security Client の表示

コマンドラインから Enterprise Security Client デーモン (**escd**) を開始します。

```
esc
```

このデーモンはスマートカードを暗黙的にリッスンし、スマートカードが挿入されるとすぐに GUI を開きます。

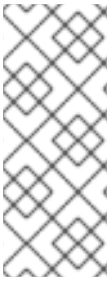
Enterprise Security Client GUI を手動で開くには、**Applications**、**System Settings**、**Smart Card Manager** の順にクリックします。

3.3. PHONE HOME の設定

Enterprise Security Client の **Phone Home** 機能は、各スマートカード内の情報を、固有の TPS サーバーおよび Enterprise Security Client UI ページを示す情報に関連付けます。Enterprise Security Client が新しいスマートカードにアクセスするたびに、TPS インスタンスに接続して、Phone Home 情報を取得できます。

Phone Home はこの情報を取得してキャッシュします。この情報はローカルでキャッシュされているため、フォーマットされたスマートカードが挿入されるたびに TPS サブシステムと通信する必要はありません。

この情報はキーまたはトークンごとに異なる場合があります。つまり、異なる TPS サーバーおよび登録 URL を企業やカスタマーグループごとに設定できます。Phone Home を使用すると、Enterprise Security Client を手動で設定して正しいサーバーと URL を特定することなく、発行者や会社単位で異なる TPS サーバーを設定できます。



注記

TPS サブシステムが Phone Home 機能を使用できるようにするには、以下のように TPS 設定ファイルで Phone Home を有効にする必要があります。

```
op.format.userKey.issuerinfo.enable=true
op.format.userKey.issuerinfo.value=http://server.example.com
```

3.3.1. Phone Home プロファイルについて

Enterprise Security Client は Gnome に基づいています。Enterprise Security Client が各トークンの情報をキャッシュすると、情報はユーザーの設定ファイルに保存されます。次回の Enterprise Security Client の起動時に、サーバーを再び接続する代わりに、設定ファイルから情報を取得します。

スマートカードが挿入され、Phone Home がトリガーされると、Enterprise Security Client は最初にトークンで **Phone Home URL** を確認します。これは、Enterprise Security Client が TPS への接続を試行するために使用するデフォルト URL です。

トークンに Phone Home 情報がない場合、Enterprise Security Client UI の **Phone Home** ボタンをクリックして、Phone Home URL 値を手動で指定できます。「Phone Home URL の設定」 を参照してください。その他の情報は、トークンのフォーマット時に提供され、保存されます。この場合、会社はユーザーに特定の Phone Home URL を提供します。ユーザーが URL を送信すると、フォーマットプロセスにより、残りの情報が Phone Home プロファイルに追加されます。フォーマットのプロセスは、ユーザーとは異なるものではありません。

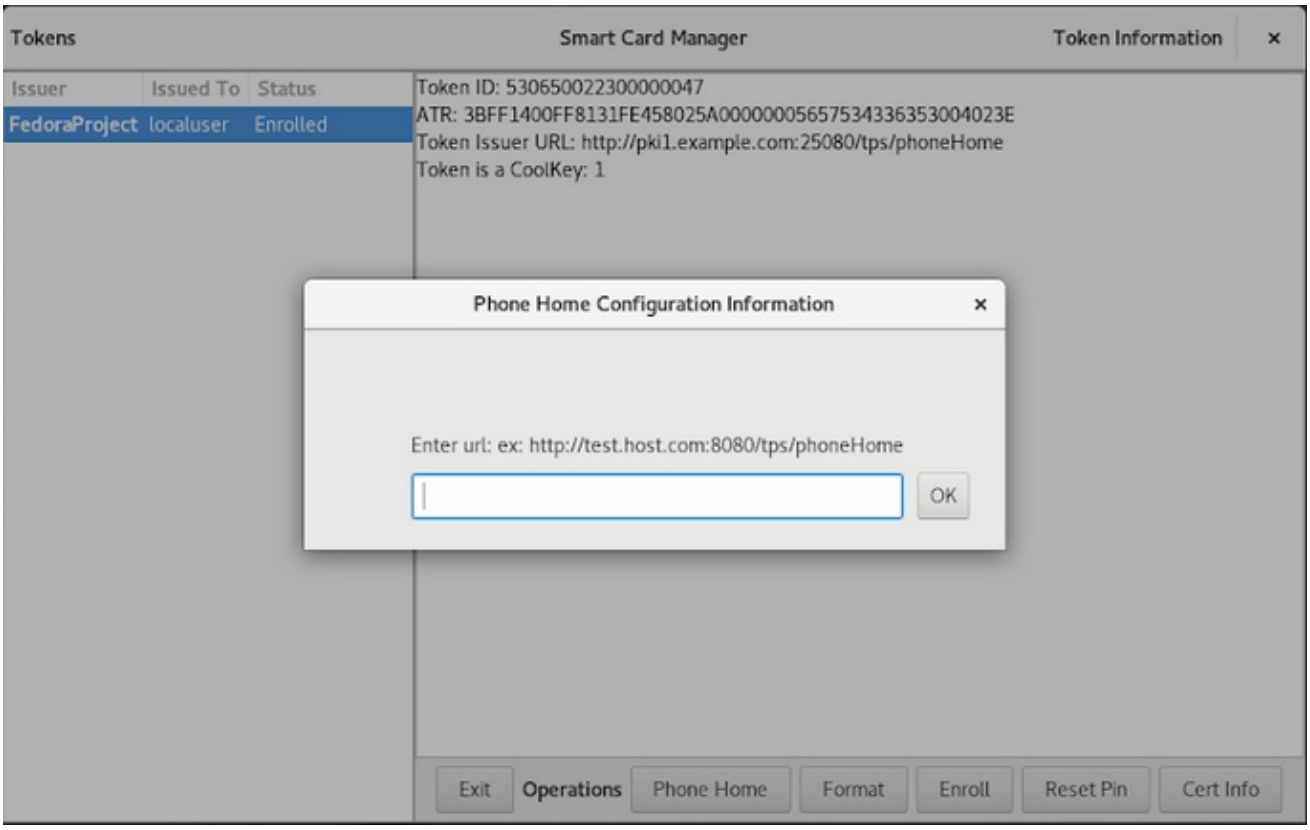
3.3.2. Phone Home URL の設定

Enterprise Security Client は、TPS と通信するように設定する必要があります。これは、**Phone Home URL** 経由で行われます。フォーマットされたトークン (製造元または IT 部門によりフォーマット可能) には、すでにこの URL が設定されている必要があります。トークンがフォーマットされていない場合、Enterprise Security Client は Phone Home URL を検出できません。このような空のトークンでは、URL を手動で定義する必要があります。

Phone Home ボタンを使用すると、ユーザーは Phone Home URL を指定できます。

1. 空のトークンが挿入されたら、Enterprise Security Client UI の **Phone Home** ボタンをクリックして、設定ダイアログを開きます。
2. **TPS Config URI** フィールドに、新しい TPS URL を入力します。
3. **OK** をクリックして保存します。新規の Phone Home URL が正しく設定されると、残りの情報が取得され、Phone Home プロファイルに追加されます。

図3.2 Phone Home URL の設定



3.3.3. Phone Home を使用する TPS の設定

Phone Home 機能と、Phone Home 機能が使用するさまざまなタイプの情報は、TPS が Phone Home を使用するように適切に設定されている場合に限り機能します。そうでない場合、TPS はこの機能を無視します。Phone Home は、**/var/lib/pki/pki-tomcat/tps/conf/** ディレクトリーの **phoneHome.xml** で設定されます。これにより、Phone Home 情報が XML に出力されます。

例3.1「TPS Phone Home 設定ファイル」 は、Phone Home 機能を設定する TPS サブシステムによって使用される XML ファイルの例を示しています。

例3.1 TPS Phone Home 設定ファイル

```
<ServiceInfo><IssuerName>Example Corp</IssuerName>
   <Services>
      <Operation>http://server.example.com:7888/nk_service ## TPS server URL
      </Operation>
      <UI>http://server.example.com:7888/cgi_bin/esc.cgi   ## Optional
Enrollment UI
      </UI>
      <EnrolledTokenBrowserURL>http://www.test.url.com   ## Optional
enrolled token url
      </EnrolledTokenBrowserURL>
   </Services>
</ServiceInfo>
```

TPS 設定 URI は TPS サーバーの URL で、残りの Phone Home 情報を Enterprise Security Client に返します。この URL の例は **http://localhost:8443/tps/phoneHome** です。この URL は、必要に応じて、マシン名、完全修飾ドメイン名、IPv4 アドレスまたは IPv6 アドレスを参照できます。TPS 設定 URI にアクセスすると、TPS サーバーは、すべてのホームディレクトリー情報を Enterprise Security Client に返すように求められます。

Smart Card サーバーの URL をテストするには、**TPS Config URI** フィールドにアドレスを入力し、**Test URL** をクリックします。

サーバーに正常に接続すると、成功を示すメッセージボックスが表示されます。テスト接続に失敗すると、エラーダイアログが表示されます。

3.4. 登録するユーザーの設定

Token Processing System がインストールされると、設定の 1 つに、トークンの登録が許可されるユーザーが含まれる LDAP ディレクトリーがあります。この認証ディレクトリーに保存されているユーザーのみが、トークンの登録、フォーマット、または所有を許可されています。トークンまたはスマートカードの登録を試みる前に、操作を要求するのユーザーが LDAP ディレクトリーにエントリーがあることを確認してください。

TPS は、LDAP ディレクトリーの特定ベース DN を確認するように設定されています。これは、TPS の **CS.cfg** で設定されます。

```
auth.instance.0.baseDN=dc=example,dc=com
auth.instance.0.hostport=server.example.com:389
```

ユーザーがトークンの登録を許可するには、ユーザーはベース DN の背後にある必要があります。

ユーザーにエントリーがない場合は、特定のベース DN 内に指定した LDAP ディレクトリーに、ユーザーを追加してからでないと、トークンをそのユーザーに登録できません。

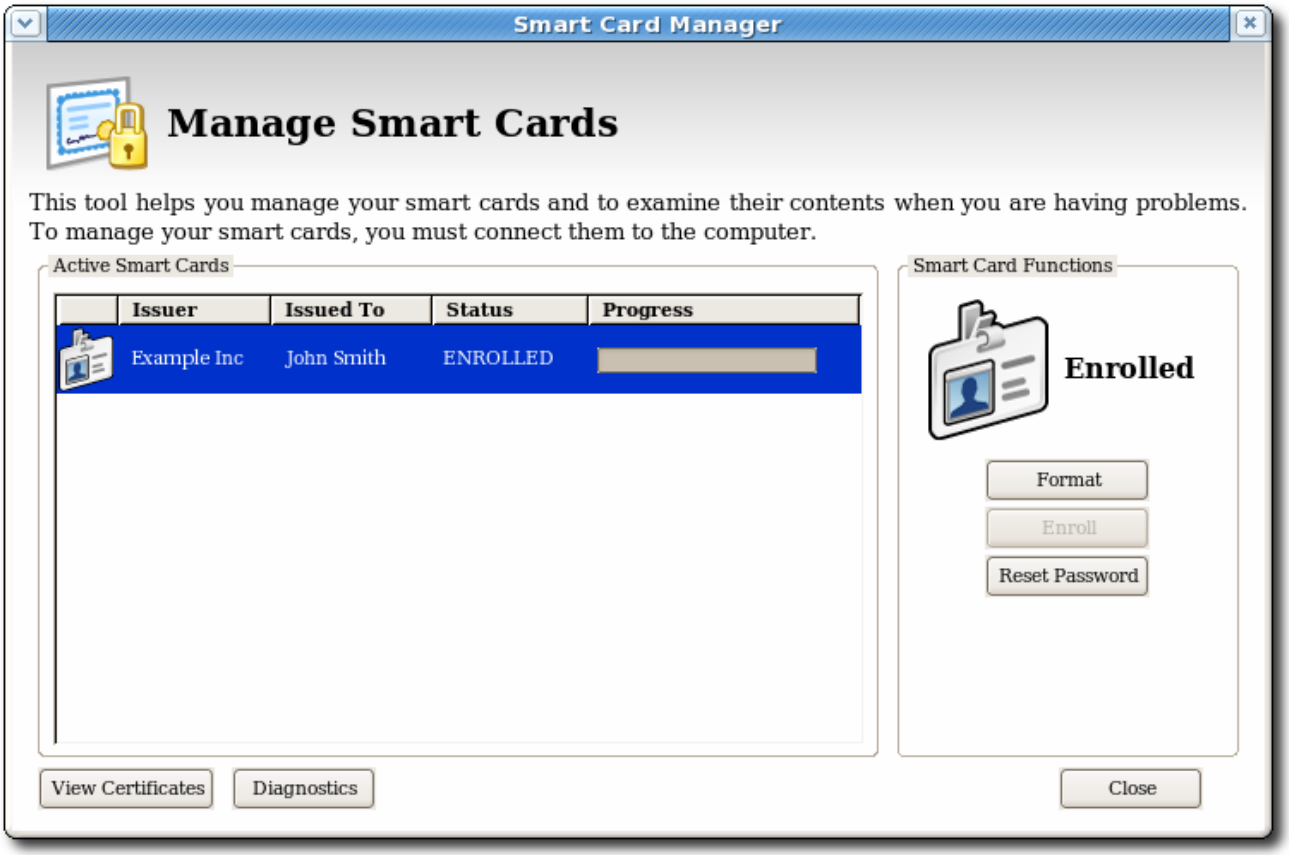
```
/usr/bin/ldapmodify -a -D "cn=Directory Manager" -w secret -p 389 -h server.example.com

dn: uid=jsmith,ou=People, dc=example,dc=com
objectclass: person
objectclass: inetorgperson
objectclass: top
uid: jsmith
cn: John Smith
email: jsmith@example.com
userPassword: secret
```

3.5. スマートカードの管理

Manage Smart Cards ページを使用すると、トークンに保存されている暗号鍵のいずれかに適用できる多くの操作を実行できます。

このページを使用して、トークンのフォーマット、カードのパスワードの設定とリセット、およびカード情報の表示を行うことができます。その他の 2 つの操作 (トークンの登録および診断ログの表示) は、**Manage Smart Cards** ページからもアクセスできます。これらの操作は他のセクションで扱われます。

図3.3 スマートカードページの管理



3.5.1. スマートカードのフォーマット

スマートカードをフォーマットすると、初期化されていない状態にリセットされます。これにより、以前に生成されたユーザーのキーペアがすべて削除され、登録時にスマートカードに設定されたパスワードが消去されます。

スマートカードをフォーマットするには、以下を行います。

1. 対応しているスマートカードをコンピューターに挿入します。カードが **Active Smart Cards** テーブルに表示されることを確認します。

2. **Manage Smart Cards** 画面の **Smart Card Functions** セクションで、**Format** をクリックします。

3. TPS がユーザー認証用に設定されている場合は、認証ダイアログにユーザー認証情報を入力して、**Submit** をクリックします。

4. フォーマットプロセス中に、カードのステータスが BUSY に変更され、進捗バーが表示されます。フォーマットプロセスが完了すると、成功メッセージが表示されます。**OK** をクリックしてメッセージボックスを閉じます。

5. フォーマットプロセスが完了すると、**Active Smart Cards** の表に、UNINITIALIZED というカードステータスが表示されます。

3.5.2. スマートカードパスワードのリセット

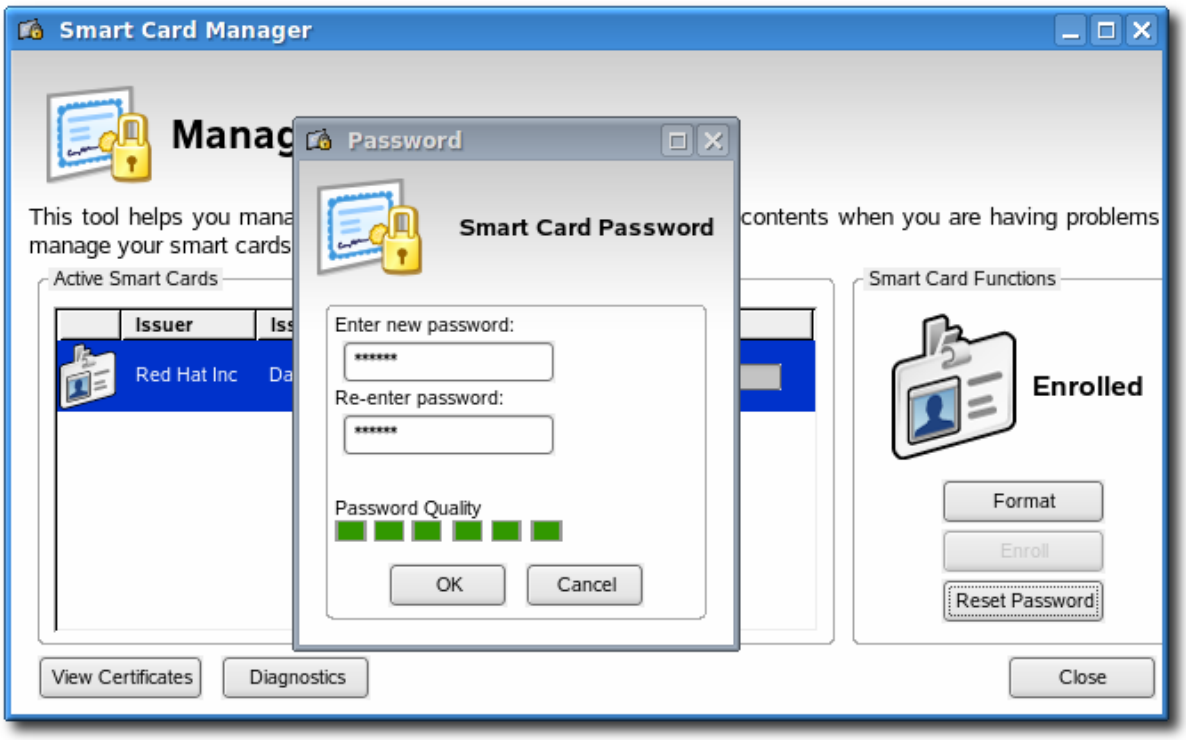
カードを登録した後にユーザーがスマートカードのパスワードを忘れた場合は、パスワードをリセットできます。スマートカードのパスワードをリセットするには、次のコマンドを実行します。

1. 対応しているスマートカードをコンピューターに挿入します。カードが **Active Smart Cards** テーブルに表示されることを確認します。

2. Manage Smart Cards 画面の **Smart Card Functions** セクションで、**Reset Password** をクリックして、**Password** ダイアログを表示します。

3. **Enter new password** フィールドに新しいスマートカードパスワードを入力します。

4. **Re-Enter password** フィールドで新しいスマートカードパスワードを確認して、**OK** をクリックします。



5. TPS がユーザー認証用に設定されている場合は、認証ダイアログにユーザー認証情報を入力して、**Submit** をクリックします。

6. パスワードのリセットが完了するのを待ちます。

3.5.3. 証明書の表示

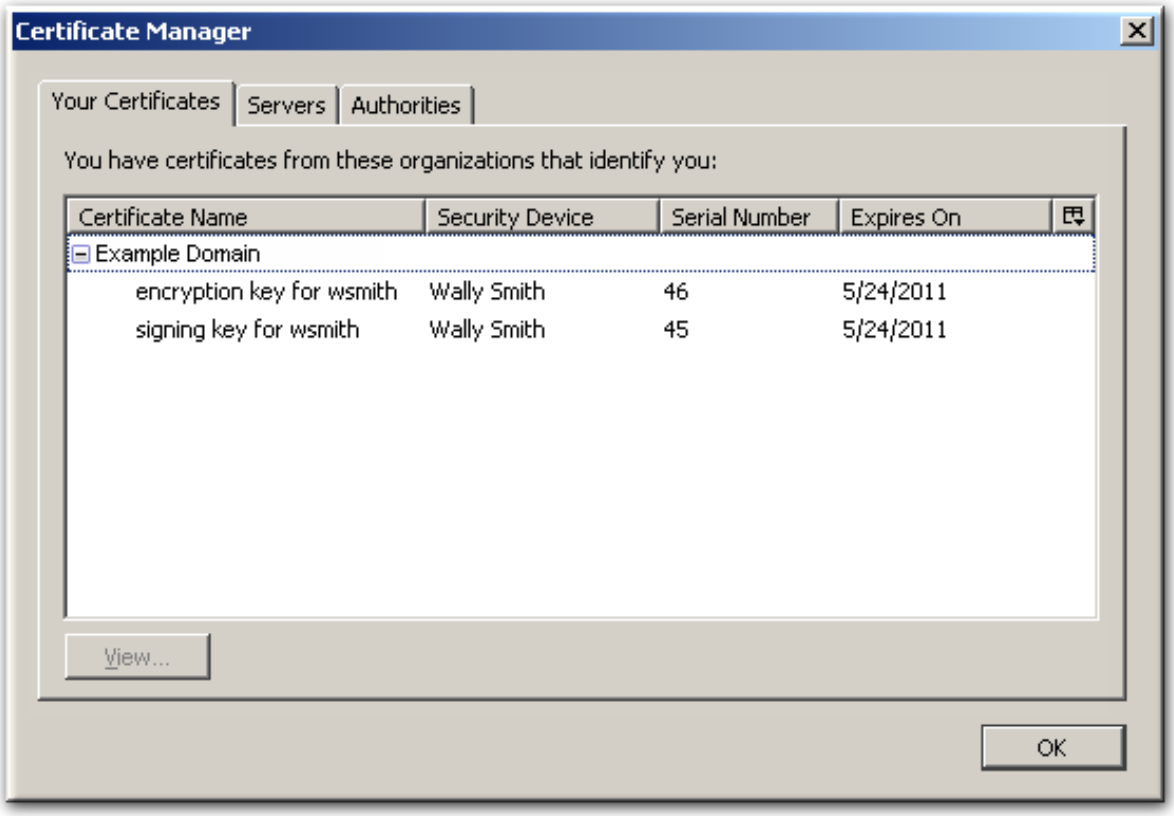
Smart Card Manager は、保存した鍵や証明書など、選択したスマートカードの基本情報を表示できます。証明書情報を表示するには、以下を行います。

1. 対応しているスマートカードをコンピューターに挿入します。カードが **Active Smart Cards** テーブルに表示されることを確認します。

2. 一覧からカードを選択し、**View Certificates** をクリックします。

これにより、シリアル番号、証明書のニックネーム、有効日など、カードに保存されている証明書の基本情報を表示します。

3. 証明書に関する詳細情報を表示するには、一覧から証明書を選択して **表示** をクリックします。



3.5.4. スマートカードの登録

ほとんどのスマートカードは、自動登録手順を使用して自動的に登録されます。**Manage Smart Cards** 機能を使用して、スマートカードを手動で登録することもできます。

ユーザーキーペアでトークンを登録する場合、トークンは SSL クライアント認証や S/MIME などの証明書ベースの操作に使用できます。

注記

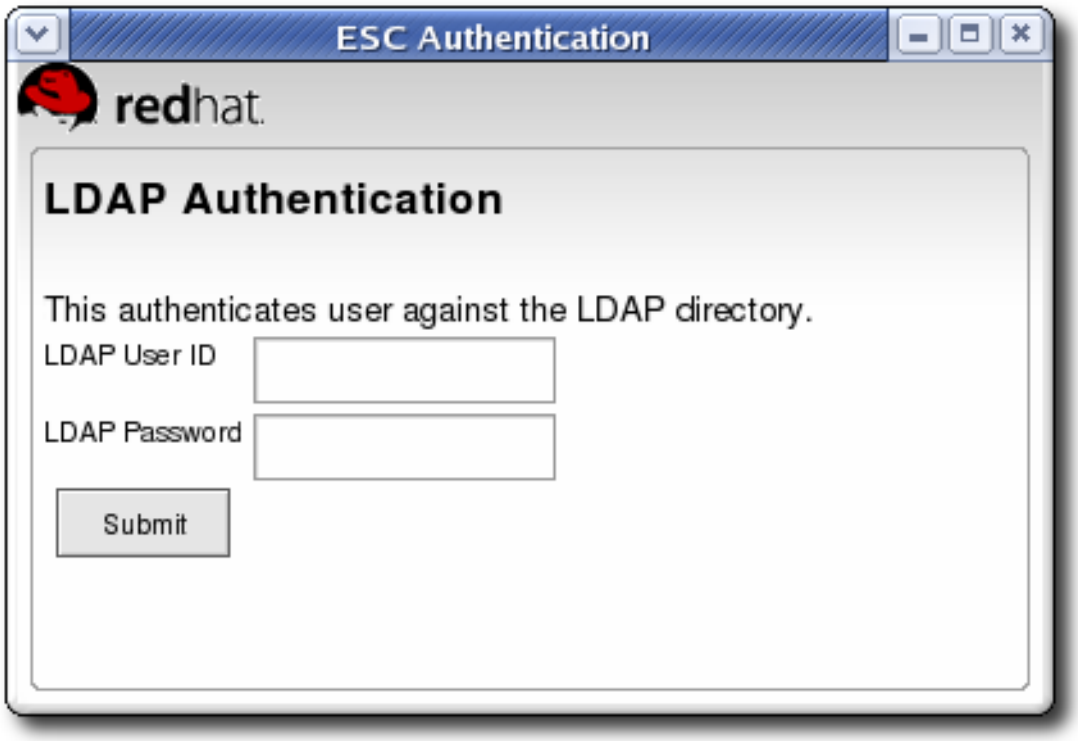
TPS サーバーは、トークンが失われた場合にリカバリーできるように、サーバー上でユーザーキーペアを生成し、DRM サブシステムでアーカイブするように設定できます。

スマートカードを手動で登録するには、以下を実行します。

1. 対応している未登録のスマートカードをコンピューターに挿入します。カードが **Active Smart Cards** テーブルに表示されることを確認します。
2. **Enroll** をクリックして、**Password** ダイアログを表示します。
3. **Enter a password** フィールドに新しいキーパスワードを入力します。

   Re-Enter a password フィールドで新規パスワードを確認します。
4. **OK** をクリックして登録を開始します。
5. TPS がユーザー認証用に設定されている場合は、認証ダイアログにユーザー認証情報を入力して、**Submit** をクリックします。

   TPS がキーを DRM にアーカイブするように設定されている場合は、登録プロセスでキーの生成およびアーカイブが開始されます。



登録が完了すると、スマートカードのステータスが ENROLLED として表示されます。

3.6. 問題の診断

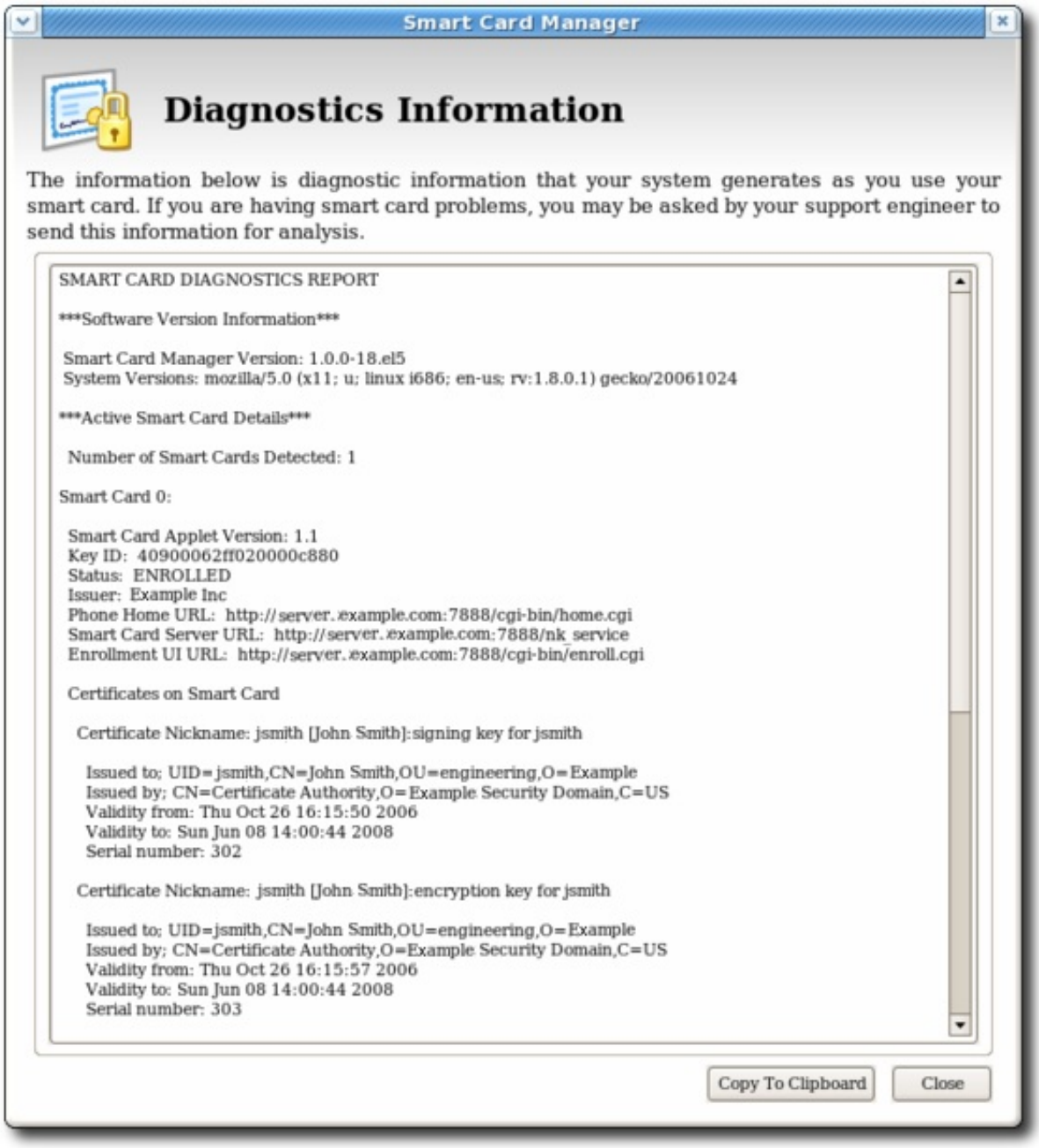
Enterprise Security Client には、基本的な診断ツールと、スマートカードの挿入や削除、カードのパスワードの変更など、エラーや一般的なイベントを記録する簡単なインターフェイスが含まれています。診断ツールは、Enterprise Security Client、スマートカード、および TPS 接続の問題について、ユーザーに特定して通知できます。

Diagnostics Information ウィンドウを開くには、次を実行します。

1. Enterprise Security Client を開きます。

2. 一覧から確認するスマートカードを選択します。
3. **Diagnostics** ボタンをクリックします。

4. これにより、選択したスマートカードの **Diagnostic Information** ウィンドウが開きます。



Diagnostics Information 画面には、以下の情報が表示されます。

- Enterprise Security Client のバージョン番号。
- Enterprise Security Client によって検出されたカードの数。

検出されたカードごとに、以下の情報が表示されます。

- スマートカードで実行しているアプレットのバージョン。
- スマートカードの英数字 ID。
- カードのステータス。以下の 3 つのいずれかになります。
  - **NO_APPLET**。キーが検出されませんでした。
  - **UNINITIALIZED**。キーが検出されても、証明書は登録されていません。
  - **ENROLLED**。検出されたカードが、証明書およびカード情報に登録されています。

- カードの Phone Home URL。これは、すべての Phone Home 情報を取得するための URL です。
- **Example Corp.** などのカード発行者名
- カードの ATR (answer-to-reset) 文字列。これは、スマートカードの異なるクラスの識別に使用できる一意の値です。たとえば、以下のようになります。

```
3BEC00FF8131FE45A00000005633333304A330600A1
```

- TPS Phone Home URL。
- TPS サーバーの URL。これは Phone Home 経由で取得されます。
- TPS 登録フォーム URL。これは Phone Home 経由で取得されます。
- カードに含まれる各証明書に関する詳細情報。
- 最新の Enterprise Security Client エラーと一般的なイベントの稼働中のログ。

Enterprise Security Client は、2 種類の診断情報を記録します。これは、スマートカードによって返された **エラー** を記録し、Enterprise Security Client 経由で発生した **イベント** を記録します。また、スマートカード設定の基本情報を返します。

3.6.1. エラー

- Enterprise Security Client はカードを認識しません。
- 証明書の登録、パスワードのリセット、フォーマット操作など、スマートカードの操作中に問題が発生します。
- Enterprise Security Client は、スマートカードへの接続を失います。これは、**PCSC** デーモンとの通信で問題が発生すると発生する可能性があります。
- Enterprise Security Client と TPS 間の接続が失われます。

スマートカードは、TPS に特定のエラーコードを報告できます。これは、メッセージの原因に応じて TPS の **tps-debug.log** ファイルまたは **tps-error.log** ファイルに記録されます。

表3.1 スマートカードのエラーコード

戻りコード	説明
一般的なエラーコード	
6400	特定の診断なし
6700	Lc の誤った長さ
6982	セキュリティーステータスが満たされない
6985	使用条件が満たされない

戻りコード	説明
6a86	間違った P1 P2
6d00	無効な命令
6e00	無効なクラス
インストール読み込みエラー	
6581	メモリー障害
6a80	データフィールドの誤ったパラメーター
6a84	不十分なメモリー容量
6a88	参照データが見つからない
削除エラー	
6200	アプリケーションを論理的に削除
6581	メモリー障害
6985	参照データを削除できない
6a88	参照データが見つからない
6a82	アプリケーションが見つからない
6a80	コマンドデータの値が正しくない
データ取得エラー	
6a88	参照データが見つからない
ステータス取得エラー	
6310	より多くのデータが利用可能
6a88	参照データが見つからない
6a80	コマンドデータの値が正しくない
読み込みエラー	
6581	メモリー障害

戻りコード	説明
6a84	不十分なメモリー容量
6a86	間違った P1/P2
6985	使用条件が満たされない

3.6.2. イベント

- カードの挿入および削除、正常に完了した操作、エラーの原因となるカード操作などの単純なイベント。
- TPS から Enterprise Security Client に報告されるエラー。
- 初期化された NSS 暗号ライブラリー。
- 検出されたその他の低レベルのスマートカードイベント。

第4章 WEB およびメールクライアントでのスマートカードの使用

スマートカードの登録後、スマートカードは SSL クライアント認証および S/MIME メールアプリケーションに使用できます。PKCS #11 モジュールの名前は異なり、オペレーティングシステムによって異なるディレクトリーに配置されます。

表4.1 PKCS #11 モジュールの場所

プラットフォーム	モジュール名	場所
Red Hat Enterprise Linux	onepin-opensc-pkcs11.so	/usr/lib64/

4.1. トークンに対して SSL をサポートするブラウザーの設定

トークンの SSL をサポートするように Firefox ブラウザーを設定するには、以下を実行します。

1. **Edit** メニューを開き、**Preferences** を選択します。

   Firefox にメニューバーが表示されない場合は、**Alt** キーを押して一時的に表示します。

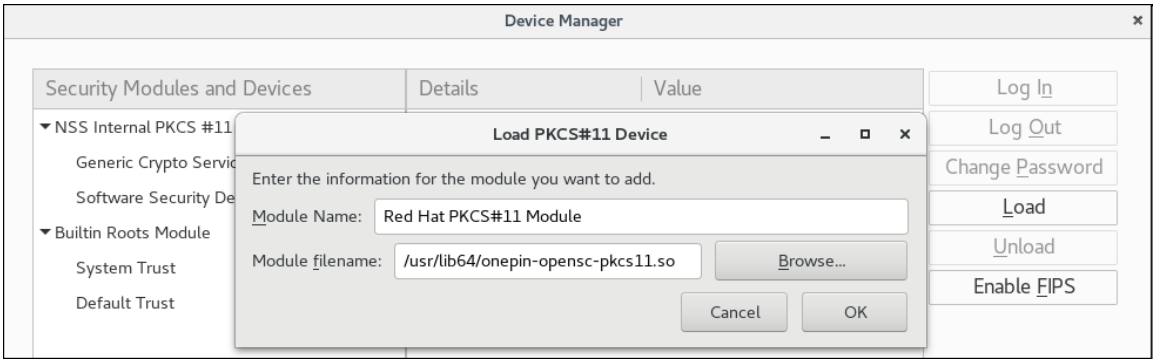
2. **Advanced** エントリーで **Certificates** タブを選択し、**Security Devices** ボタンをクリックします。

3. PKCS #11 ドライバーを追加します。

   a. **Load** ボタンをクリックします。

   b. モジュール名を入力します。

   c. **Browse** をクリックして、Enterprise Security Client PKCS #11 ドライバーライブラリーを選択し、**OK** をクリックします。



4. CA がまだ信頼されていない場合は、CA 証明書をダウンロードしてインポートします。

   1. CA で **SSL End Entity** ページを開きます。たとえば、以下のようになります。

      ```
      https://server.example.com:9444/ca/ee/ca/
      ```

   2. **Retrieval** タブをクリックし、**Import CA Certificate Chain** をクリックします。

   3. **Download the CA certificate chain in binary form** をクリックし、**Submit** をクリックします。

4. 証明書チェーンを保存する適切なディレクトリーを選択し、**OK** をクリックします。
5. **Edit > Preferences**をクリックして、**Advanced** タブを選択します。
6. **View Certificates** ボタンをクリックします。
7. **Authorities** をクリックし、CA 証明書をインポートします。

5. 証明書信頼関係を設定します。
   1. **Edit > Preferences**をクリックして、**Advanced** タブを選択します。
   2. **View Certificates** ボタンをクリックします。
   3. **Edit** をクリックして、Web サイトへの信頼を設定します。

証明書は SSL に使用できます。

第5章 ENTERPRISE SECURITY CLIENT の設定

注記

Enterprise Security Client は、追加の設定なしに起動できます。

5.1. トークン操作の LDAP 認証の無効化

デフォルトでは、トークン操作を要求する各ユーザーは LDAP ディレクトリーに対して認証されます。ユーザーにエントリーがある場合は、操作が許可されます。ユーザーにエントリーがない場合は、操作が拒否されます。

テスト目的や特定タイプのユーザーの場合は、LDAP 認証を無効にする方がより簡単で適切な方法になります。これは、Enterprise Security Client 設定では設定されませんが、トークン処理システム設定で設定されるため、TPS 管理者によって実行する必要があります。

1. TPS サブシステムを停止します。

```
# systemctl stop pki-tps
```

2. TPS 設定ファイルを開きます。

```
# vim /var/lib/pki-tps/conf/CS.cfg
```

3. 認証パラメーターを **false** に設定します。

```
op.operation_type.token_type.loginRequest.enable=false
op.operation_type.token_type.auth.enable=false
```

operation_type は、**enroll**、**format**、または **pinreset** などの LDAP 認証が無効になっているトークン操作です。ある操作タイプで認証を無効にしても、他の操作タイプでは無効になりません。

token_type はトークンプロファイルです。通常のユーザー、セキュリティー担当者、およびセキュリティー担当者が登録したユーザーには、デフォルトのプロファイルがあります。他の種類のユーザーや証明書のカスタムトークンタイプもあります。

たとえば、以下のようになります。

```
op.enroll.userKey.loginRequest.enable=false
op.enroll.userKey.pinReset.enable=false
```

4. TPS サブシステムを再起動します。

```
# systemctl restart pki-tomcatd@pki-tomcat.service
```

TPS 設定の編集については、『Red Hat Certificate System 10 管理ガイド』で説明しています。

付録A 改訂履歴

改訂番号は本ガイドに関するものであり、Red Hat Certificate System のバージョン番号とは関係ありません。

改訂 10.1-0 **Fri Nov 20 2020** **Florian Delehaye**

Red Hat Certificate System 10.1 のガイドを公開。