HPKIカードを用いた電子署名のサンプル

（Pkcs#11　検証版）

解説書

2021年3月

1. はじめに

掲載した署名サンプルは、JAHIS HPKI対応ICカードガイドラインVer.3.0に記載されている、Pkcs#11のインターフェースの一部を用いた証明書の取得、署名および署名検証のサンプルソースです。

1. 概要

HPKIカードには電子署名用アプリケーションと電子認証用アプリケーションが含まれています。今回利用するHPKIカードドライバにも、電子署名用と電子認証用を使い分けるための別々のドライバで構成されているので使い分けが必要です。

Pkcs#11インターフェースを利用する際は以下のDLLを使い分けます。

　電子署名用DLL：HpkiSigP11\_MPKCS11H.dll

　電子認証用DLL：HpkiAuthP11\_MPKCS11H.dll

ソフトウェア的にはどちらのHPKIも利用可能ですが、利用目的に合わせて電子署名に於いては電子署名用アプリケーションを使用してください。

HPKIカードは、接触型または非接触型（TypeB）のICカードリーダライタが利用可能です。

1. サンプルの開発環境

サンプルソースはC言語となります。

OS：Windows 10 Enterprise 1909

　　統合開発環境（IDE）：Microsoft Visual Studio 2017 Professional

　　ライブラリ：OpenSSL（Win64OpenSSL-1\_1\_1h.exe使用）

　　インストールドライバ：HPKIカードドライバ（Ver1.5）

　　　　　　　　　　　　　ICカードRWドライバ

1. 参考文献

18-001\_JAHIS HPKI対応ICカードガイドラインVer.3.0

1. 注意事項

HPKIカードのPINは規定回以上の誤りで閉塞します。

閉塞すると利用不可能となり、発行元に対応問合せとなります。

1. サンプルソースの内容（PKCS#11）

プロジェクト名：HPKISignVerifySampleP11

実行パラメータ：コンソールコマンド

HPKISignVerifySampleP11 <PKCS#11 Library\_Type> <PIN>

　　　　PKCS#11 Library\_Type： 署名用：” sign”、認証用：” auth”

PIN：HPKIカードのPIN

処理の主な流れ

1. HPKI P11ライブラリのロード
2. HPKI P11ライブラリの初期化
3. スロットIDの取得
4. セッションのオープン(スロットは先頭の1つに限定)
5. 証明書の検索
6. 証明書の取得（複数個存在する場合でも常に先頭の1つのみ取得）
7. 利用者証明書の取得処理
8. 暗号トークンへのログイン
9. 暗号トークン中の署名生成用秘密鍵の検索
10. 署名対象メッセージの生成（ダミーの固定メッセージ）
11. 署名対象メッセージのハッシュ生成（SHA256）
12. メッセージダイジェストをDigestInfo形式に編集
13. 署名メカニズムの設定（CKM\_RSA\_PKCS）
14. 署名処理の初期化
15. 署名の実行
16. 署名検証用公開鍵の取得
17. 署名の検証

結果表示

実行結果、エラーコードはコンソールに表示します。

OpenSSLライブラリの利用

1. ハッシュ計算
2. DigestInfoの生成
3. 署名検証処理

＜OpenSSLのインストール＞

* 1. インストーラーダウンロード

https://slproweb.com/products/Win32OpenSSL.html

「Win64OpenSSL-1\_1\_1h.exe」

* 1. インストール

「Win64OpenSSL-1\_1\_1h.exe」を実行

インストール先：C:\Program Files\OpenSSL-Win64

「Select Additional Tasks」-「The OpenSSL binaries(/bim) directory」を選択。

* 1. VisualStudioの設定

　　C/C++

　　・追加のインクルードディレクトリ

インストールしたフォルダの「include」フォルダ

例)C:\Program Files\OpenSSL-Win64\include;

　　リンカー

　　・全般 - 追加のライブラリディレクトリ

インストールしたフォルダの「lib」フォルダ

例)C:\Program Files\OpenSSL-Win64\lib;

　　・入力 - 追加の依存ファイル

「libcrypto.lib;」

* 1. Windows環境変数Pathにインストール先binを追加

　　例)C:\Program Files\OpenSSL-Win64\bin