HPKIカードを用いた電子署名のサンプル

解説書（Crypto API版）

2020年11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、Crypto APIのインターフェースの一部を用いた証明書の取得、署名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。

Crypto APIインターフェースを利用する際は、以下のプロバイダ名を使用します。

　電子署名用：HPKI Crypto Service Provider for Non Repudiation

　電子認証用：HPKI Crypto Service Provider for Authentication

ソフトウェア的にはどちらのPKI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

　　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（Crypto API）

プロジェクト名：HPKISignSampleCrypto

実行パラメータ：コンソールコマンド

HPKISignSampleCrypto <CSP\_Type> <実行処理> <PIN>

　　　CSP\_Type：署名用CSP：”sign”、 認証用CSP：” auth”

　　　実行処理：証明書取得：” getcert”、 署名：”sign”

　　　PIN：HPKIカードのPIN

利用者証明書取得処理の主な流れ

1. 暗号プロバイダとコンテナを指定して、プロバイダハンドルを取得
2. コンテナの保持するRSA鍵ペアのハンドルを取得
3. 鍵ハンドルに付随する利用者証明書データのデータ長を取得
4. 鍵ハンドルに付随する利用者証明書データのデータを取得

署名処理の主な流れ

1. 暗号プロバイダとコンテナを指定して、プロバイダハンドルを取得
2. コンテナの保持するRSA鍵ペアのハンドルを取得
3. 鍵ハンドルに付随する利用者証明書データのデータ長を取得
4. 鍵ハンドルに付随する利用者証明書データのデータを取得
5. ハッシュオブジェクトの生成
6. 署名対象データのハッシュ値を生成（ダミーデータ）
7. ハッシュオブジェクトのパラメータを設定
8. ハッシュ値に署名を行った結果のデータ長を取得
9. 署名用鍵のPINを設定
10. ハッシュ値に署名を行った結果を取得

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。