JNSA電子署名WG秋祭り
JNSA電子署名WG/スキルアップTF

J-LIS公開のAPIを読み解くなど

2017年11月1日

セイコーソリューションズ株式会社
DXソリューション部
DXソリューション課
村尾　進一

TIME
未来という「時」に、もっと笑顔を。

自己紹介

職歴：

2003年　セイコーインスツルメンツ(株)入社　クロノトラスト事業に配属

2008年　長期署名システム「NiXAdES」の開発を担当
・省庁、医療、国税e文書における長期署名システムの提供

2011年　長期署名クラウドサービス「eviDaemon」をリリース

2013年　セイコーソリューションズ(株)に（クロノトラスト事業ごと）異動

2014年　NSF 2014「タイムスタンプ活用の動向」について発表

2015年　PKI Day 2015「トラストリストと信頼のグローバル化」について発表

2016年　JNSA電子署名WG五月祭「電子署名入門」について発表

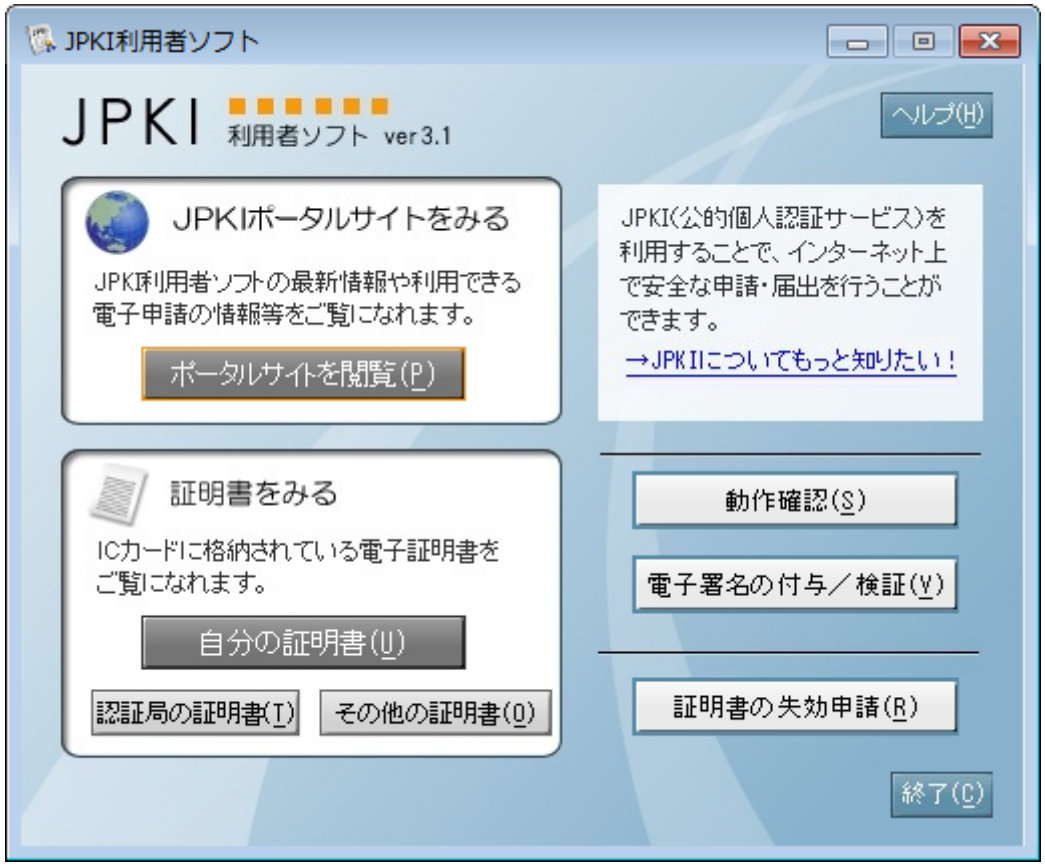
2017年　弊社クラウド署名サービスをクラウド署名コンソーシアム（CSC）規格に対応
10月26日　アドビ システムズ社様のAdobe Signとの連携を発表

アジェンダ

- 公的個人認証サービス・利用者クライアントソフトについて
- Androidインテント機能について
- まとめ

公的個人認証サービス・利用者クライアントソフト

利用者クライアントソフトの機能について（GUI画面機能）



公的個人認証サービス・利用者クライアントソフト

利用者クライアントソフトの機能について

GUI画面機能	ライブラリ機能	OS		
		Windows	MacOS	Android
ポータルサイトを閲覧		GUI	GUI	GUI
自分の証明書 認証局の証明書 その他の証明書	証明書表示機能 証明書取得機能 自己の電子証明書の 有効性確認機能 基本4情報取得機能 官職証明書検証機能	GUI/ライブラリ	GUI/ライブラリ	GUI/ライブラリ
電子署名の付与／検証	電子署名生成機能 電子署名検証機能	GUI/ライブラリ	GUI/ライブラリ	ライブラリ
動作確認	ICカード種別取得機能	GUI/ライブラリ	GUI/ライブラリ	GUI/ライブラリ
PC接続		—	—	GUI
証明書の失効申請		GUI	GUI	GUI
パスワード変更		GUI	GUI	GUI
更新通知		GUI	GUI	GUI

公的個人認証サービス・利用者クライアントソフト

利用者クライアントソフトのライブラリとしての機能について

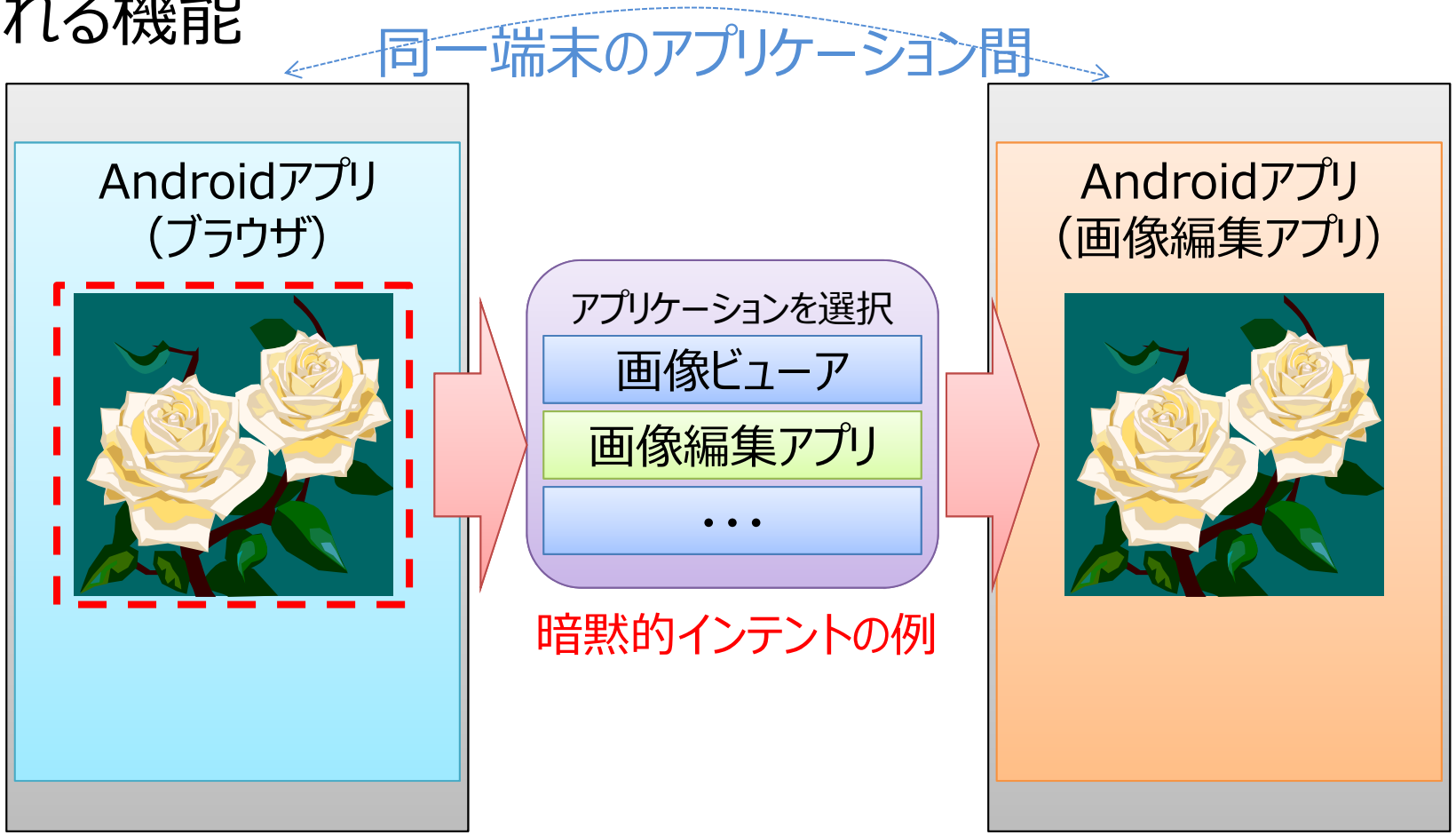
種別	機能	言語/IF	OS		
			Windows	MacOS	Android
カード APライブラリ	・証明書取得機能 ・電子署名生成機能 ・電子署名検証機能	CryptoAPI	○		
		PKCS#11	○	○	
		Java言語（JNI）	○	○	
		C言語		○	
		Android インテント			○
個人認証サービス APライブラリ	・証明書表示機能 ・基本4情報取得機能 ・官職証明書検証機能 ・自己の電子証明書の有効性確認機能 ・ICカード種別取得機能	C言語	○	○	
		Java言語	○	○	
		Android インテント			○

※個人番号を取得するAPIは無い！

参考URL：https://www.j-lis.go.jp/jpki/procedure/procedure1_2_3.html

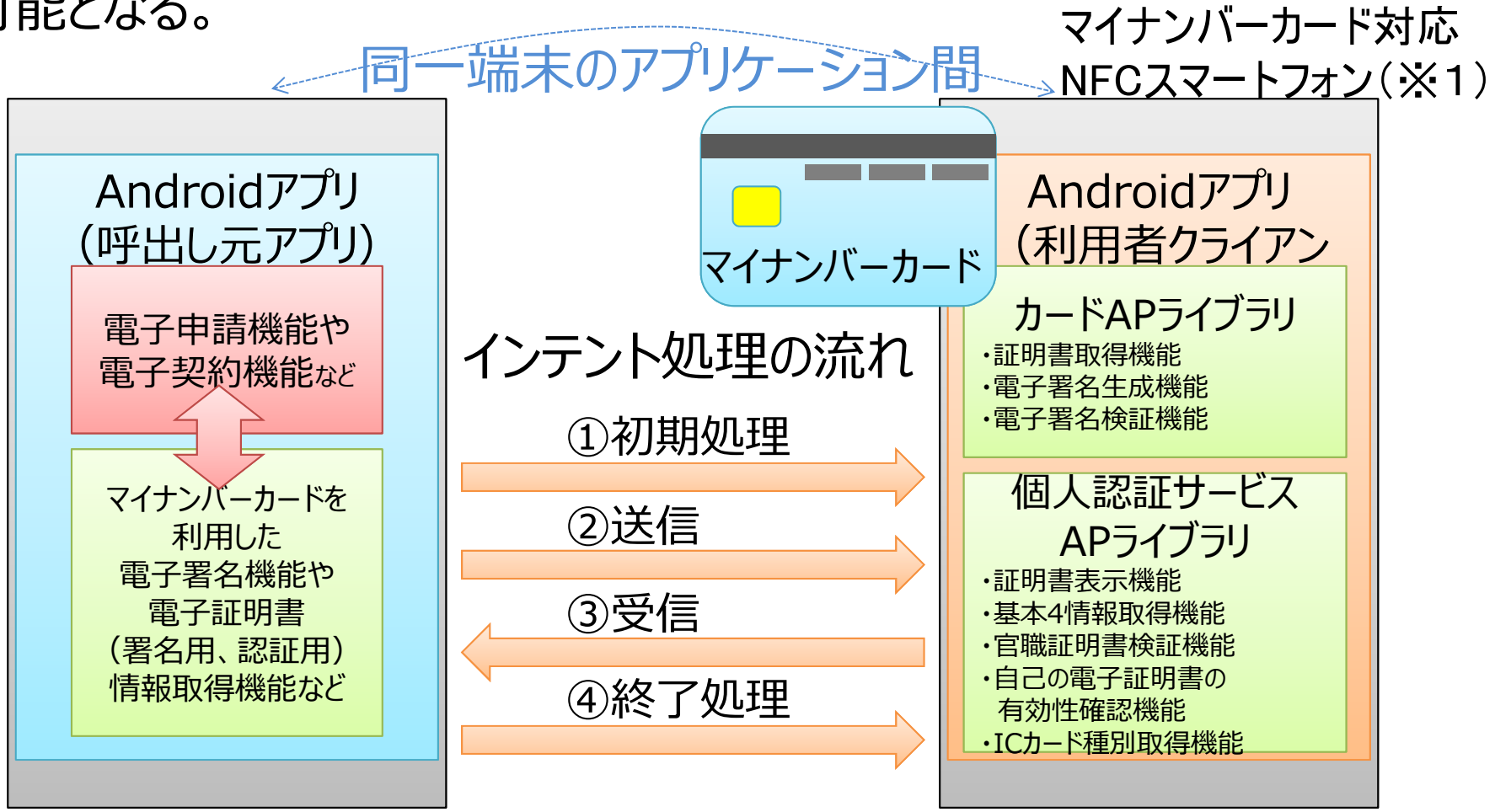
Androidのインテント機能について

インテント機能：アプリケーション間やソフト内の機能間をつなぎ合わせる仕組みでアプリケーション間の画面遷移などに利用される機能



利用者クライアントのAndroidの対応について

インテント機能を利用して、電子申請アプリや電子契約アプリなどから、利用者クライアントに対して、電子証明書取得要求や電子署名要求が可能となる。



※1　https://www.jpki.go.jp/prepare/pdf/nfclist.pdf

利用者クライアントのAndroidの対応について

例）カードAPライブラリ：署名用電子証明書取得処理

処理	送信データ		受信データ	
	キー（型）	値	キー（型）	値
初期化処理	コマンドタイプ command_type(int)	0x01004001	コマンドタイプ command_type(int)	0x01004001
			結果 result(boolean)	成功：true 失敗：false
			エラーコード※２ err_code(int)	（4桁）
			エラー詳細コード※２ detail_code(int)	（8桁）
送信処理	コマンドタイプ command_type(int)	0x01002002	コマンドタイプ command_type(int)	0x01002002
			電子証明書 p_cert(byte[])	―
終了処理	コマンドタイプ command_type(int)	0x01004002	コマンドタイプ command_type(int)	0x01004002

※2　エラーコードとエラー詳細コードはコマンド共通のため省略

利用者クライアントのAndroidの対応について

例）カードAPライブラリ：署名生成処理（署名対象データを渡す場合）

処理	送信データ		受信データ	
	キー（型）	値	キー（型）	値
初期化処理	コマンドタイプ command_type(int)	0x01004001	コマンドタイプ command_type(int)	0x01004001
			結果 result(boolean)	
送信処理	コマンドタイプ command_type(int)	0x01002003	コマンドタイプ command_type(int)	0x01002003
	署名対象データ message(byte[])	―	署名値 signature(byte[])	―（※３）
	ハッシュアルゴリズム alg_id(int)	SHA1:0 SHA256:1		
終了処理	コマンドタイプ command_type(int)	0x01004002	コマンドタイプ command_type(int)	0x01004002

※３　内部処理として署名対象データに対するハッシュ値に
ハッシュアルゴリズムのOIDを付与している

利用者クライアントのAndroidの対応について

例）カードAPライブラリ：署名生成処理（ダイジェスト【ハッシュ値】を渡す場合）

処理	送信データ		受信データ	
	キー（型）	値	キー（型）	値
初期化処理	コマンドタイプ command_type(int)	0x01004001	コマンドタイプ command_type(int)	0x01004001
			結果 result(boolean)	
送信処理	コマンドタイプ command_type(int)	0x01002004	コマンドタイプ command_type(int)	0x01002004
	ダイジェスト hash(byte[])	—	署名値 signature(byte[])	—（※４）
	ハッシュアルゴリズム alg_id(int)	SHA1:0 SHA256:1		
終了処理	コマンドタイプ command_type(int)	0x01004002	コマンドタイプ command_type(int)	0x01004002

※４　内部処理としてダイジェスト【ハッシュ値】にハッシュアルゴリズムのOIDを付与していない

利用者クライアントのAndroidの対応について

署名生成処理（ダイジェスト【ハッシュ値】を渡す場合）

・ハッシュアルゴリズムがSHA1の場合（データサイズは35Byte）

DigestInfo (ASN.1構造：DERエンコード)

sequence 長さ33	sequence 長さ9	object identifier 長さ5	SHA1 OID(1.3.14.3.2.26)
0x30, 0x21	0x30, 0x09	0x06, 0x05	0x2b, 0x0e, 0x03, 0x02, 0x1a
NULL	octet string 長さ20		
0x05, 0x00	0x04, 0x14	SHA1ハッシュ値(20Byte)	

・ハッシュアルゴリズムがSHA256の場合（データサイズは51Byte）

DigestInfo (ASN.1構造：DERエンコード)

sequence 長さ49	sequence 長さ13	object identifier 長さ9	SHA256 OID(2.16.840.1.101.3.4.2.1)
0x30, 0x31	0x30, 0x0d	0x06, 0x09	0x60, 0x86, 0x48, 0x01, 0x65
0x03, 0x04, 0x02, 0x01		NULL 0x05, 0x00	
octet string 長さ32			
0x04, 0x20	SHA256ハッシュ値(32Byte)		

```
DigestInfo ::= SEQUENCE {
    digestAlgorithm AlgorithmIdentifier,
    digest OCTET STRING
}
```

参考URL：http://blog.livedoor.jp/k_urushima/archives/979220.html

まとめ

Android対応の利用者クライアントの

インテントインターフェース機能により、

スマホ・モバイル端末によるマイナンバーカードの

利活用シーン（電子申請・電子契約など）の

拡大が期待できる！

ご清聴ありがとうございました。