



PKI Day 2016

エストニアIDカード PKIマニアック解析

宮地 直人 (miyachi@langedge.jp)
電子署名WGサブリーダー/スキルアップTFリーダー
(有限会社ラング・エッジ)

2016年 4 月 22 日

- ラング・エッジのプログラマ！

長期署名/PKIライブラリの開発 (PAdES/XAdES)
PKI系受託開発 (OpenSSL/BC等オープン系)
ドキュメント系受託開発 (PDF/OOXML等)

- **JNSA**電子署名WGサブリーダー

スキルアップTFリーダー (勉強会の企画運営等)
標準化活動 (ISO 14533-3 / JTC1 SC34 等)
電子署名サーバ公開中 <http://eswg.jnsa.org/>

- e-Estoniaの**e-Residency**です！

e-Residency（電子居住）とは？

詳細 <https://e-estonia.com/e-residents/about/>



- エストニア共和国が提供するデジタル・アイデンティティ
- 登録者は電子居住者（e-Residents）と呼ばれる
- エストニア国民が持つものと同じスマートIDカードを提供
- エストニアに企業設立や、e-バンキングの利用が可能
- エストニアのポータルサイトを利用できる（制限あり）
- IDカードで署名や暗号化も可能（ソフトウェアも提供）

e-Residency で何が出来る？



○ できること (・o・)ウグッ!

ポータルサイトの企業向けサービスが利用可能。

エストニアに1日で企業設立が可能。

エストニアの銀行でe-バンキングや送金が可能。

デジタル署名にてオンライン契約が可能。

文書の暗号化と復号が可能。

オンラインでのエストニア税支払いが可能。

× できないこと (´・ω・`)ショボーン

国籍（市民権や住所）が貰えるわけではない。

IDカードは身分証明書に使えない（写真無し）。

電子申請 <https://apply.e-estonia.com/>

用意するもの：

1. 手数料支払い用クレジットカード

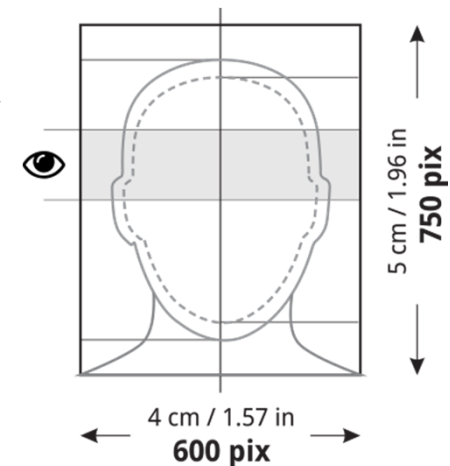
50.99 EUR : 50€+0.99€ (カード手数料)

2. パスポート等のIDスキャン画像

3. 証明写真画像 (カードには使われない)

4. 申請する理由 (英語で)

数行程度だけど事前準備が吉。



※ Pick-up location (受取場所) は **Japan, Tokyo** に

e-Residency 取得までの一例



Date	Mail / Action
2015/07/09	件名 : Your e-Residency application has been received 差出人 : e-Residency 電子申請の受け付け確認メール (電子申請後すぐに来る)
2015/07/15	件名 : E-Residency Digi-ID - application received 差出人 : Politsei-ja Piirivalveamet (警察・国境警備隊) 審査開始のメール (10ビジネス日かかると記載)
2015/07/29	件名 : E-Residency Digi-ID - e-Residency granted 差出人 : Politsei-ja Piirivalveamet (警察・国境警備隊) 審査完了のメール (ちょうど10ビジネス日 後でした!)
2015/08/12	件名 : e-Residency digital ID card at the Embassy 差出人 : Consul IS (返信は日本の大使館書記官のアドレス宛にする) 大使館に 受け取りに行く日程 を決める [※ 返信が必要!]
2015/08/13	駐日エストニア共和国大使館 (渋谷区神宮前2丁目) でカード受け取り パスポート持参、大使館で指紋採取、受け取りのサイン
2015/08/14	件名 : E-Residency Digi-ID - certificates activated 差出人 : Politsei-ja Piirivalveamet (警察・国境警備隊) 電子証明書のアクティベート通知 (この後利用可能になる)

スターターキットをGET!

内容物：

- スマートIDカード
- カードリーダー
- ピン通知封書
- 説明資料



スマートIDカードとカードリーダー



ドキュメント番号は8桁
Nxxxxxxx
シリアル番号??

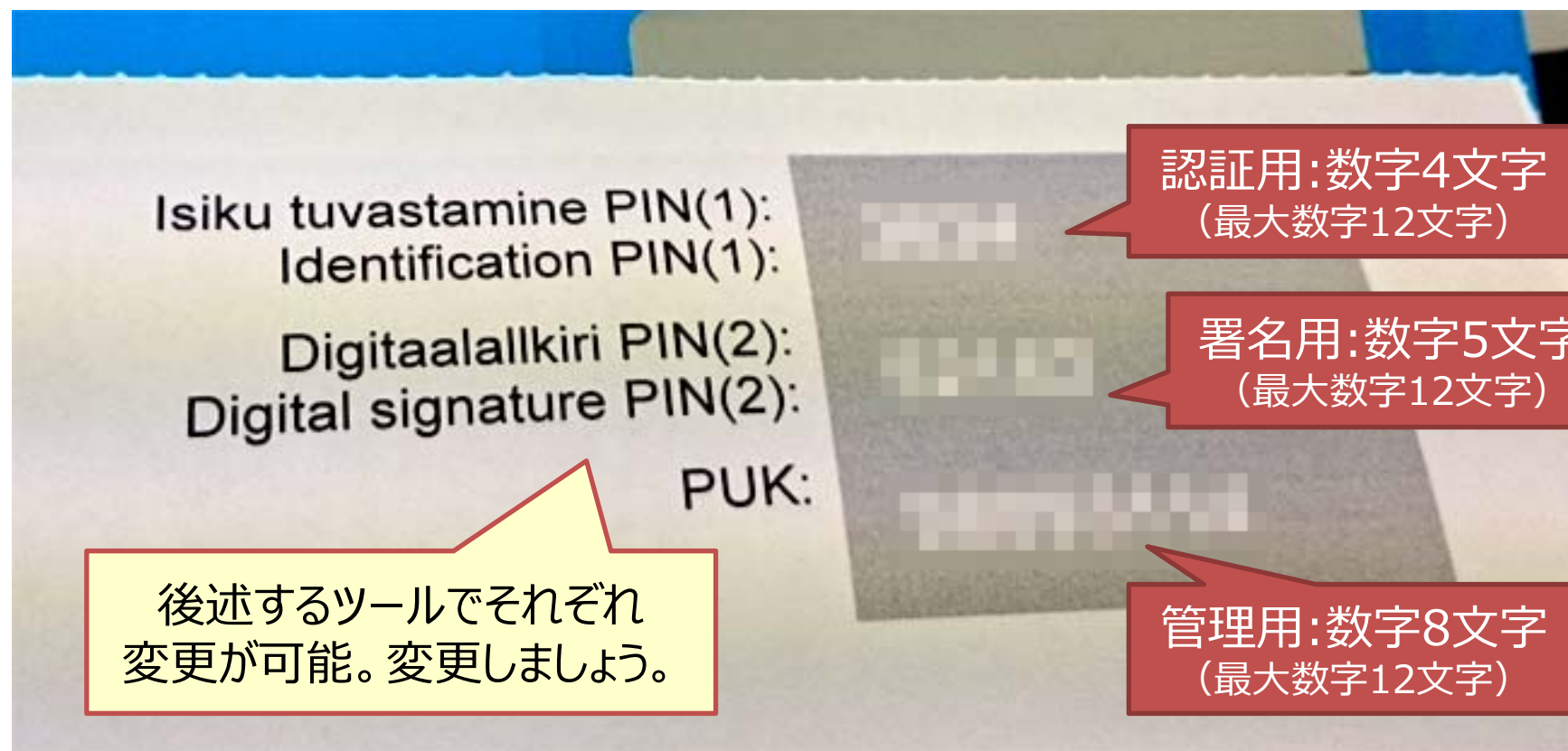
パーソナルコードは11桁
3YYMMDDSSSS
最初の3は種別??
YYMMDDは生年月日
SSSSはシリアルか?

同梱カードリーダーが
小さくて素晴らしい!
Advanced Card Systems Ltd.
<http://www.acs-japan.jp/>
カードリーダーも同梱して
いるのですぐ使える!



ピンピンピン (PIN1 / PIN2 / PUK)

スターターキットに初期設定のPIN3つが封入されて入っている。



※ 証明書が有効になるのは **activated** のメールが来てから。

認証パス (認証局SKと証明書)



Estonian Certification Centre Root CA (RSA2048-SHA1)

Issuer/ Subject:	E = pki@sk.ee, CN = EE Certification Centre Root CA, O = AS Sertifitseerimiskeskus, C = EE	https://www.sk.ee/en
---------------------	---	---

CA certificate (RSA2048-SHA1) 中間CA証明書

Subject:	E = pki@sk.ee, CN = ESTEID-SK 2011, O = AS Sertifitseerimiskeskus, C = EE	ESTEID-SK 2015 は RSA2048- SHA384
CRLDP	http://www.sk.ee/repository/crls/eccrca.crl (943bytes)	

EE Auth certificate (適格証明書 : RSA2048-SHA256) 認証用

Subject:	SERIALNUMBER = 3YYMMDDSSSS, G = NAOTO, SN = MIYACHI, CN = MIYACHI,NAOTO,3YYMMDDSSSS, OU = authentication, O = ESTEID (DIGI-ID E-RESIDENT), C = EE
CRLDP	http://www.sk.ee/repository/crls/esteid2011.crl (23.9MBytes)
拡張使用	クライアント認証 / 電子メールの保護

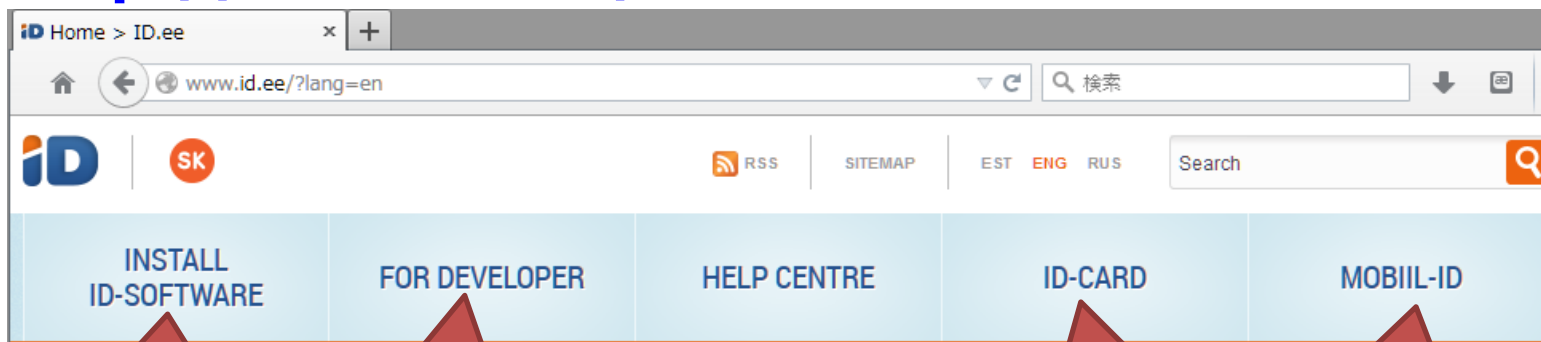
EE Sign certificate (適格証明書 : RSA2048-SHA256) 署名用

Subject:	SERIALNUMBER = 3YYMMDDSSSS, G = NAOTO, SN = MIYACHI, CN = MIYACHI,NAOTO,3YYMMDDSSSS, OU = digital signature, O = ESTEID (DIGI-ID E-RESIDENT), C = EE
CRLDP	http://www.sk.ee/repository/crls/esteid2011.crl (23.9MBytes)

IDカード用のサポートサイト



<http://www.id.ee/>



インストーラの
ダウンロード
installer.id.ee


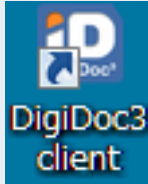

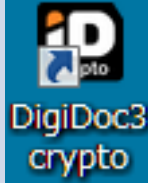
開発者向けの
情報

証明書の説明
や利用・更新

モバイルによる
証明書の利用

Windows		7 以降 (x86, x64)
MacOS-X		10.9 (Mavericks) 以降
Linux		Ubuntu 14.04 以降

標準ソフトウェア概要

	<p>ID-card utility</p>	<p>IDカード利用の為の管理ツール ※ JPKIの利用者クライアントソフトに相当</p> <ul style="list-style-type: none"> ➤ 認証/署名用の証明書の確認管理（検証とPINの変更） ➤ Mobile-IDの操作 ➤ eメール設定の確認 ➤ PUKコードによるリセット ➤ 動作環境の確認（Diagnostic） 	
	<p>DigiDoc3 client</p>	<p>電子署名/検証ソフト</p> <ul style="list-style-type: none"> ➤ ファイルへの署名と検証 	 <p>エストニアのIDカードと Mobile-IDおよび、リトアニアのMobile-IDへ対応したオープンソフトウェア digidoc.sk.ee</p>
	<p>DigiDoc3 crypto</p>	<p>暗号化/復号ソフト</p> <ul style="list-style-type: none"> ➤ ファイルの暗号化と復号 	
<p>NO ICON</p>	<p>Drivers & Plugins</p>	<ul style="list-style-type: none"> ➤ ICカード・カードリーダーのドライバ（OpenSC/CSP/CDSA） ➤ ブラウザ用のプラグイン（認証用/PKCS#11） 	

- 標準ソフト/ドライバは**オープンソース**の方針
https://svn.eesti.ee/projektid/idkaart_public/
<https://github.com/open-eid/> (ミラー?)
 - IDカードドライバは **OpenSC** 等を利用
 - **PKCS#11**と**CSP** (Win) と**CDSA** (Mac) を提供
 - **DigiDoc**ライブラリ (署名等) も上記で公開
 - ソフトウェアのアーキテクチャ説明サイトも公開
<http://open-eid.github.io/>
- ※ **オープンなソフト開発環境を提供している!**

公開 svn ルート下のフォルダ名



ライセンスは **LGPL v2.1**

cmake

digidocservice

digidocservice-testkit

esteid-browser-plugin

esteid-csp

esteid-pkcs11

esteid-plugin-loader

esteid-vaadin-component

externals

id-updater

jdigidoc

libdigidoc

OpenSCは標準の
サポートなので
OpenSC公式サイト
から入手が可能

libdigidocpp

libltdl

minidriver

misc

oldInsecureActiveX

packages

pdf-signer

qdigidoc

qesteidutil

smartcardpp

SmartCardRemoval

wiki

ドキュメント類

ID-card utility 証明書画面



リセット(PUK)

3年間有効

認証用証明書(PIN1)

署名用証明書(PIN2)

@eesti.ee e-mail

The screenshot shows the 'ID-kaardi' web interface. The user's information is as follows:

- Given Names: Naoto
- Surname: Miyachi
- Personal Code: [blurred]
- Birth: [blurred], Jaapan / Jpn
- E-mail: naoto.miyachi@eesti.ee

Navigation menu: Diagnostics | Settings | Help | About | English

Buttons on the left: Certificates, @eesti.ee e-mail, Mobiil-ID, PUK code, @eesti.ee e-mail

Card information: Card in reader N0108739, You're using Digital identity card, Card is valid till 27 July 2018.

Email forwarding list (highlighted in red):

- [blurred]@eesti.ee - miyachi@langedge.jp (active)
- naoto.miyachi@eesti.ee - miyachi@langedge.jp (active)

Additional text: For more detailed official email address forwarding, please visit eesti.ee

転送設定のみ可能

パーソナルコード@eesti.ee
一般利用不可：連絡用

氏名@eesti.ee 一般利用可能

Mobile-ID

The screenshot shows the 'ID-kaardi HALDUSVAHEND' utility page. It features a navigation menu with 'Certificates', '@eesti.ee e-mail', 'Mobiil-ID', and 'PUK code'. The 'Mobiil-ID' section is highlighted. Below the menu, there is a description: 'Mobiil-ID is possibility to use mobile phone instead of ID-card for identification and digital signing. More info from mobiil.id.ee'. The text 'To use Mobiil-ID...' is partially visible at the bottom.

初期費用として政府に**10ユーロ**が必要
毎月プロバイダに約**1ユーロ**が必要



利用可能なサービスは現在3つ
SIMを購入してアクティベートする
Police and Border Guard Board's website.
<https://www.politsei.ee/en/>

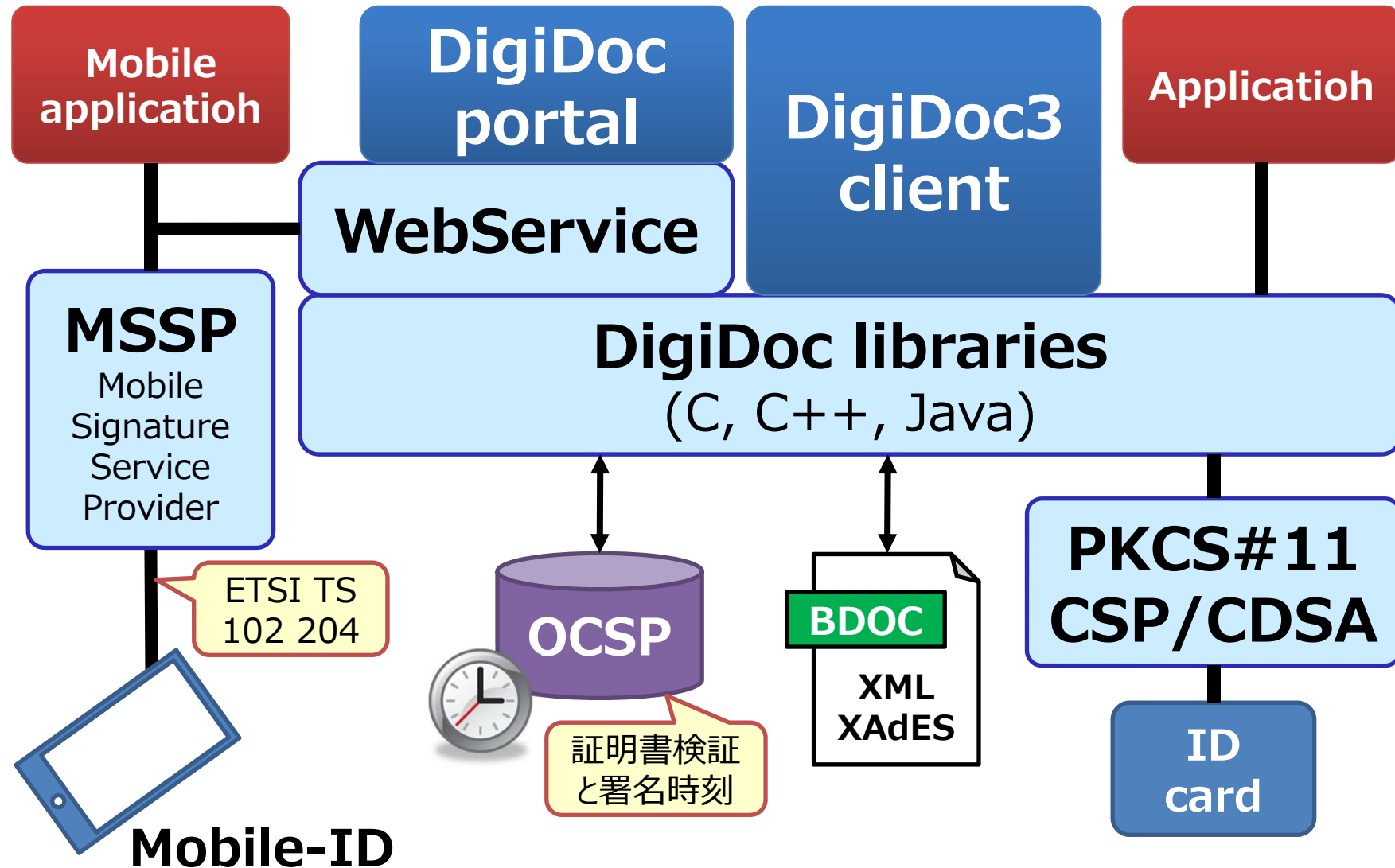
Mobile-ID用の PIN1/PIN2/PUK を設定
IDカード同様に認証や署名が使えるようになる



Mobile-ID用アプリケーション

The image displays two screenshots of the DigiDoc application. The left screenshot shows the iTunes preview page for 'DigiDoc' by Finestmedia, with a red callout bubble stating 'iOS用' (iOS use). The right screenshot shows the Google Play store page for 'DigiDoc' by Finestmedia, with a red callout bubble stating 'Android用' (Android use). Below this, another Google Play screenshot shows 'DigiDoc 3 ANDROID' by Innovaatik Grupp, with a red callout bubble stating 'Android用 (複数ある)' (Android use (multiple exist)). A yellow callout bubble at the bottom left contains the text: 'これらのアプリにて BDOC署名が可能。認証は標準のブラウザで対応しているようだ。' (With these apps, BDOC signing is possible. Authentication seems to be supported by standard browsers.)

DigiDoc フレームワーク



- CRL (12h毎更新) は**24MB**あり巨大! (非実用的)
 - Low securityアプリの利用のみで他は非推奨
 - OCSPのアドレスは証明書には未記載
 - SK (認証局) サイトに証明書検証サービスの記載
<https://www.sk.ee/en/services/validity-confirmation-services/>
 - 試験環境は公開 (<http://demo.sk.ee/ocsp>)
 - 本番環境は有料 (<http://ocsp.sk.ee/>)
0.048€/約6円 (400回) ~ 0.007€/約1円 (750,000回)
 - ・ SKと契約してIPアドレスを登録する必要がある。
 - ・ 署名付きOCSP要求なら自分の証明書の検証は可能 (無償?) 。
- ※ **DigiDoc3 Client** は**月10回**まで**署名**検証可能。

- 2015年9月25日に以下で情報公開
<https://cybersec.ee/2015/09/25/hundred-thousand-id-card-certificates-issued-with-invalid-public-key-encoding/>
- エストニアIDカードの公開鍵のASN.1 DERエンコーディングに問題があった!
- 公開鍵モジュラス値は正の整数なのにASN.1 INTEGERで負の場合がある!
 - 負値になる場合は先頭にx00追加必要
駄目な確率は1/2。IDカード中に2つ証明書あるので3/4が該当か?

余談:私の証明書はどうか？

署名用 (現状)

```
<SEQUENCE>  
<INTEGER>97e7f3ac...</INTEGER>  
<INTEGER>010001</INTEGER>  
</SEQUENCE>
```

両方アウトの可能性は
1/4なのに...

どちらもアウト!

認証用 (現状)

```
<SEQUENCE>  
<INTEGER>9a40dc40...</INTEGER>  
<INTEGER>010001</INTEGER>  
</SEQUENCE>
```

署名用 (正解: あるべき値)

```
<SEQUENCE>  
<INTEGER>0097e7f3ac...</INTEGER>  
<INTEGER>010001</INTEGER>  
</SEQUENCE>
```

まあ標準署名/暗号ソフトの
DigiDocでは使えてるし...

正解はこちら

認証用 (正解: あるべき値)

```
<SEQUENCE>  
<INTEGER>009a40dc40...</INTEGER>  
<INTEGER>010001</INTEGER>  
</SEQUENCE>
```

エストニアIDカード バージョン



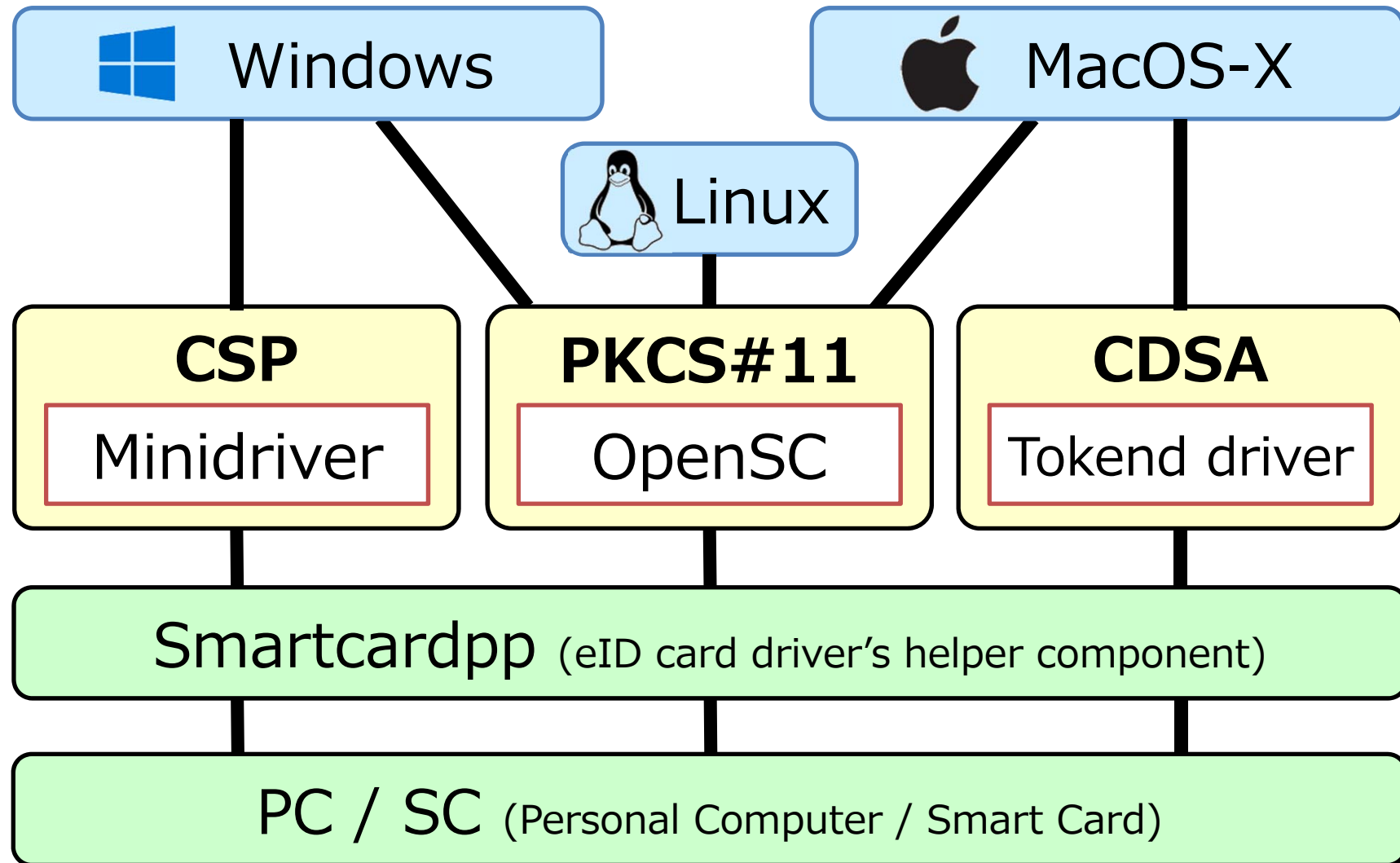
	V1.0	V1.1	V3.0	V3.4/5
Platform	MICARDO	Multos	Java Card	
RSA (bits)	1024		2048	1024~2048
HASH	SHA-1, SHA-224	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		
ECC (bits)	(Not Supported)		160~256 ※1 (RSAで1024~3072bits相当)	

※1 ECCの機能はあるがエストニアIDカードでは未使用。

詳しくは以下にスペックシートがある

<http://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3.4.pdf>

エストニアIDカード Drivers



\$ pkcs15-tool -D

PKCS#15 Card [NAOTO MIYACHI...]:

PIN [PIN1]

PIN [PIN2]

PIN [PUK]

エストニアIDカードのPKCS#15は
エミュレートで実装されている
OpenSC : pkcs15-esteid.c

Private RSA Key [Isikutuvastus]

認証用

Private RSA Key [Allkirjastamine]

署名用

X.509 Certificate [Isikutuvastus]

X.509 Certificate [Allkirjastamine]

エストニアIDカード PKCS#11



Windows (Windows/sys*)

onopin-opensc-pkcs11.dll	認証用 (FireFox)
※ 署名用モジュールは無い? CSPがあるから?	署名用

MacOS-X (/Library/EstonianIDCard/lib)

esteid-pkcs11-onopin.so esteid-pkcs11.so	認証用
esteid-pkcs11.so	署名用

```
$ pkcs11-tool --module esteid-pkcs11.so -L
```

Available slots:

```
Slot 0 (0x0): ACS ACR 38U-CCID 00 00  
token label      : NAOTO MIYACHI (PIN1, Auth)  
Slot 1 (0x1): ACS ACR 38U-CCID 00 00  
token label      : NAOTO MIYACHI (PIN2, Sign)
```

認証用

署名用

PKCS#11 CK_MECHANISM **JNSA**

PKCS#11サポートメカニズム	JPKI	種類	補足
CKM_SHA_1	○	HASH	エストニアIDカードのPKCS#11では、標準のSHA-1/2はもちろん、欧州のRIPEMD-160や、旧ソ連・ロシア系のGOST標準規格のR3411もサポート
CKM_SHA256	○		
CKM_SHA384	—		
CKM_SHA512	—		
CKM_MD5	—		
CKM_RIPEMD160	—		
CKM_GOSTR3411	—		
CKM_RSA_X_509	—	SIGN/VERIFY/ ENCRYPT/ DECRYPT	RSA_PKCS が最も重要なRSA暗号
CKM_RSA_PKCS	○		
CKM_SHA1_RSA_PKCS	—	SIGN/VERIFY	RSA_PKCSとOpenSSLで可能
CKM_SHA256_RSA_PKCS	—		

参考:JPKI PKCS#11モジュール **JNSA**

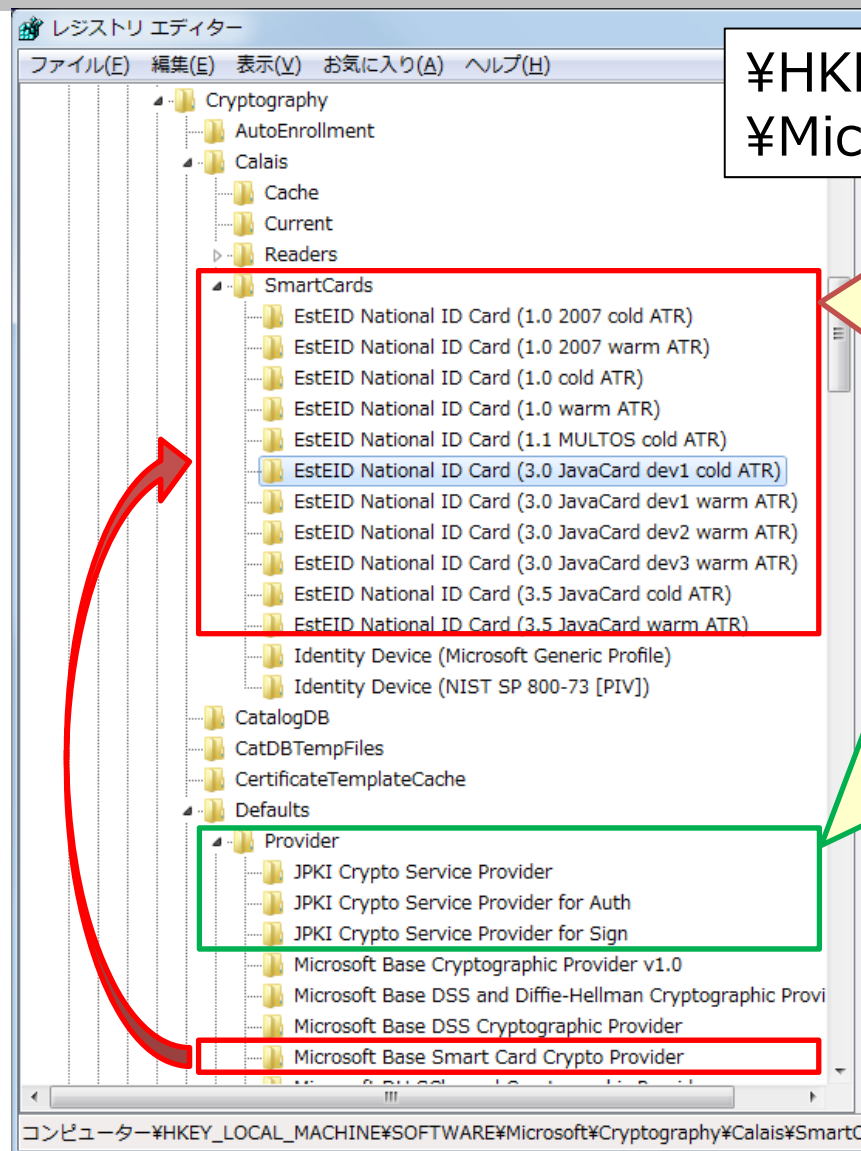
Windows (C:¥Program Files¥JPKI フォルダ下)

JPKIPKCS11.dll (JPKIPKCS1164.dll)	住基カード用
JPKIPKCS11Auth.dll (JPKIPKCS11Auth64.dll)	個人番号カード認証用
JPKIPKCS11Sign.dll (JPKIPKCS11Sign64.dll)	個人番号カード署名用

残念ながら **Firefox/Thunderbird/Acrobat** 等では利用できない！
PKCS#11の実装が一般的ではない箇所があることを解析して確認。

個人番号カードのPKCS#11の利用方法はまだ未公開。
以下にある情報は住基カード用のみ。ただしPKCS#11としては同じか？
<https://www.j-lis.go.jp/data/open/cnt/3/855/1/02PKCS11.pdf>

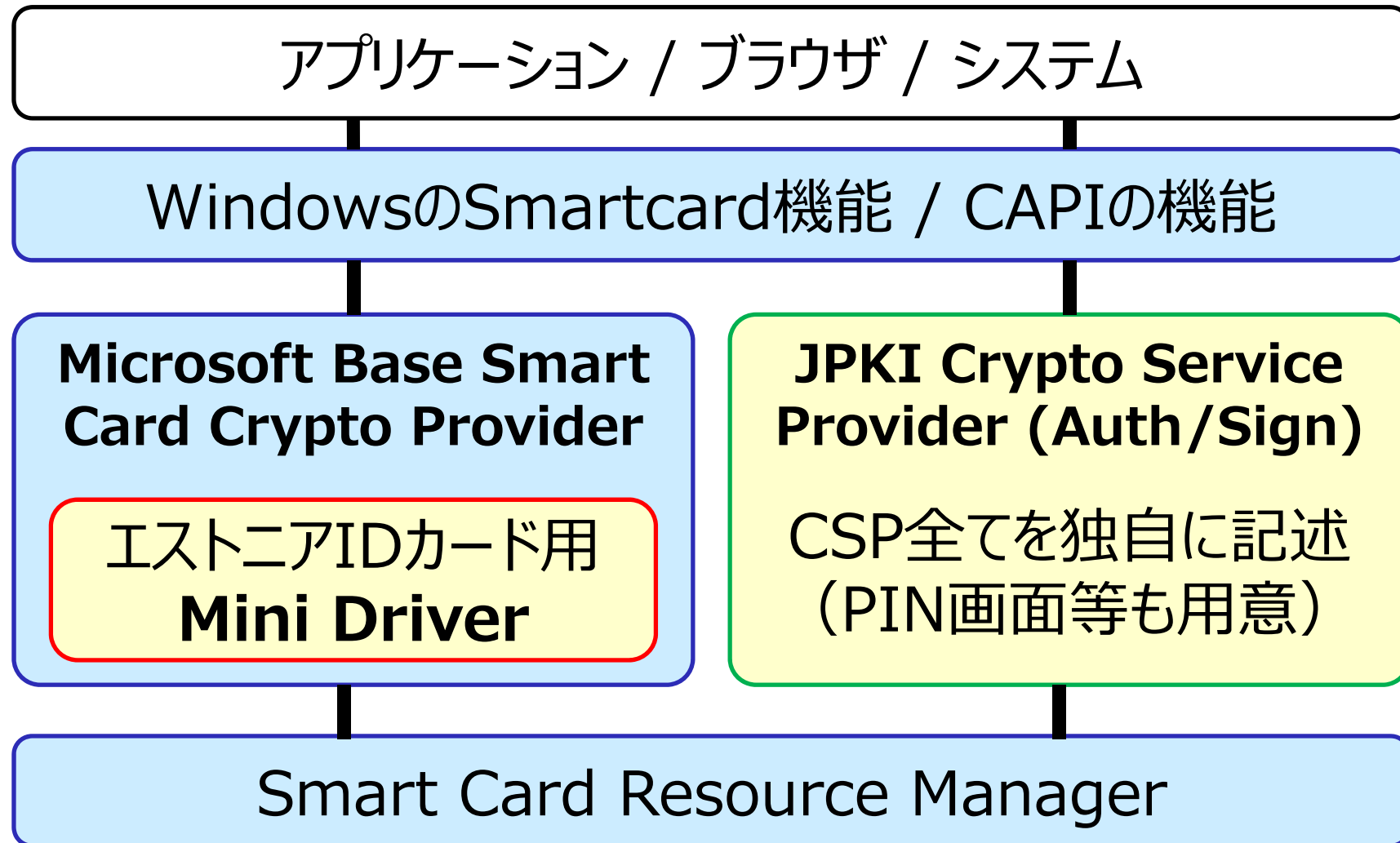
Windows CSPをレジストリから確認 **JNSA**



¥HKEY_LOCAL_MACHINE¥SOFTWARE
¥Microsoft¥Cryptography¥

Calais¥SmartCards の下に
Estonia IDカードの情報がある。
CSPは「**Microsoft Base Smart
Card Crypto Provider**」を使った
Mini Driverの形式になっている。

JPKIは**CSPを直接提供**する形式。
「**JPKI Crypto Service Provider**」
は住基カード用。これは公開されている。
「**JPKI Crypto Service Provider
for Auth**」が個人番号カードの認証用で、
「**JPKI Crypto Service Provider
for Sign**」は個人番号カードの署名用の
CSPだと予想される。これは現在非公開。
<https://www.j-lis.go.jp/data/open/cnt/3/855/1/01CAPI.pdf>



CSP利用例

Signature MIYACHI,
NAOTO
発行者: ESTEID-SK 2011
有効期間: 2015/07/29 から
2018/07/28

Authentication MIYACHI,
NAOTO
発行者: ESTEID-SK 2011
有効期間: 2015/07/29 から
2018/07/28

証明書選択時

Windows セキュリティ

証明書の確認
[OK] をクリックして、この証明書を確認します。この証明書が正しくない場合、[キャンセル] をクリックしてください。

Authentication MIYACHI,
NAOTO
発行者: ESTEID-SK 2011
有効期間: 2015/07/29 から
2018/07/28

証明書のプロパティを表示します

OK キャンセル

認証時

Windows セキュリティ

スマート カード
スマート カード デバイスの選択

EstEID National ID Card
(3.5 JavaCard cold ATR)
ACS CCID USB Reader 0
スマート カードは使用できる状態です。

OK キャンセル

JavaCard cold ATR と認識

Windows セキュリティ

スマート カード
認証の暗証番号 (PIN) を入力してください。

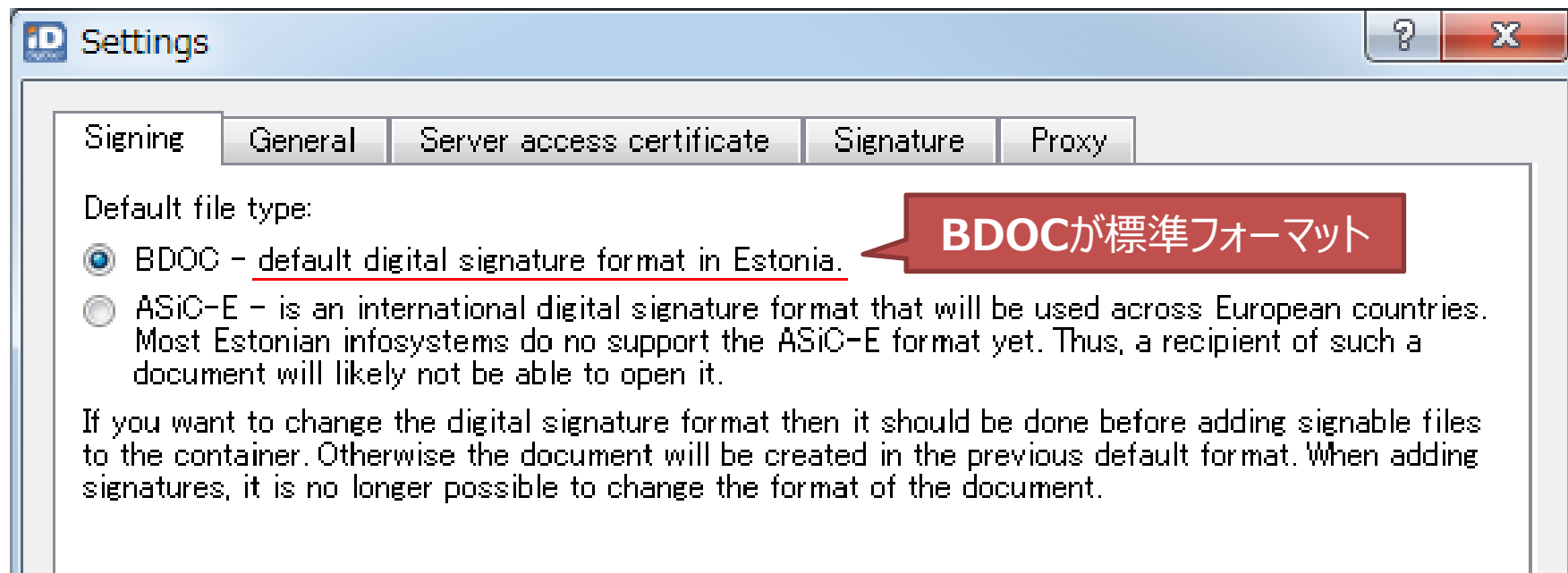
暗証番号 (PIN)
暗証番号 (PIN)

詳細についてはここをクリックしてください

OK キャンセル

Mini Driverなので標準PIN入力画面

2種類の署名フォーマット (DigiDoc3 client) **JNSA**



➤ **BDOC** : エストニア独自の署名フォーマット

<http://www.id.ee/public/bdoc-spec212-eng.pdf>

➤ **ASiC-E** : EU共通の署名フォーマット (EN仕様)

※ **ZIP+XAdES** なのは同じ、署名時刻の扱いが異なる

BDOC署名の詳細画面

Attribute	Value
Signer's Certificate issuer	ESTEID-SK 2011
Signer's Certificate	MIYACHI,NAOTO,
Signature method	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Container format	application/vnd.etsi.asic-e+zip
Signature format	EPES/time-mark
Signature policy	2.1.0
Signed file count	1
SPUri	https://www.sk.ee/repository/bdoc-spec21.pdf
OCSP Certificate issuer	EE Certification Centre Root CA
OCSP Certificate	SK OCSP RESPONDER 2011
Hash value of signature	30 31 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 0...
OCSP time	08.04.2016 10:18:48 +09:00
OCSP time (UTC)	08.04.2016 01:18:48 +00:00
Signer's computer time (UTC)	08.04.2016 01:17:54 +00:00

nonce : Nnumber used ONCE
通信等で用いられる
使い捨ての乱数値

time-mark って何？

Hash value of signature が
OCSP nonce 値

OCSP time を何故？

ASiC-E署名の詳細画面

Attribute	Value
Signer's Certificate issuer	ESTEID-SK 2011
Signer's Certificate	MIYACHI, NAOTO
Signature method	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Container format	application/vnd.etsi.asic-e+zip
Signature format	BES/time-stamp
Signed file count	1
Signature Timestamp	08.04.2016 18:43:46 +09:00
Signature Timestamp (UTC)	08.04.2016 09:43:46 +00:00
TS Certificate issuer	EE Certification Centre Root CA
TS Certificate	SK TIMESTAMPING AUTHORITY
OCSP Certificate issuer	EE Certification Centre Root CA
OCSP Certificate	SK OCSP RESPONDER 2011
Hash value of signature	30 31 30 0D 06 09 60 86 48 01 65 03 04 02 01 05...
OCSP time	08.04.2016 18:43:47 +09:00
OCSP time (UTC)	08.04.2016 09:43:47 +00:00
Signer's computer time (UTC)	08.04.2016 09:43:34 +00:00

Signature
Timestamp がある!

ここはBDOCと同じ

BDOCとASiC-Eの比較



	BDOC	ASiC-E
Container format	application/vnd.etsi.asic-e+zip	
Signature format	EPES/time-mark (XAdES-EPES)	BES/time-stamp (XAdES-BES)
Signature Timestamp	× 無し	○ 有り (RFC 3161)
TS Certificate	× 無し	SK TIMESTAMPING AUTHORITY
OCSP Certificate	SK OCSP RESPONDER 2011	
Hash value of signature	署名値<SignatureValue/>のハッシュ値/ハッシュ方式 (OCSP nonce にBER形式で埋め込まれている)	
OCSP time	○ 有り (BDOCでは署名時刻になる)	
Signer's computer time	○ 有り (署名PCのローカル時刻)	

BDOCとASiC-EのXAdES構造



BDOC (XAdES-EPES + time-mark)	ASiC-E (XAdES-BES + time-stamp)
<pre> <asic:XAdESSignatures> <ds:Signature> <ds:SignedInfo/> <ds:SignatureValue/> <ds:KeyInfo/> <ds:Object> <xades:QualifyingProperties> <xades:SignedProperties> <xades:SignedSignatureProperties> <xades:SigningTime/> <xades:SigningCertificate/> </pre>	<pre> <asic:XAdESSignatures> <ds:Signature> <ds:SignedInfo/> <ds:SignatureValue/> <ds:KeyInfo/> <ds:Object> <xades:QualifyingProperties> <xades:SignedProperties> <xades:SignedSignatureProperties> <xades:SigningTime/> <xades:SigningCertificate/> </pre>
<p>※ 署名タイムスタンプが無い</p>	<p>ETSI 標準</p>
<p>EPES</p>	<p>※ ポリシー定義が無いのでBES</p>
<pre> <xades:SignaturePolicyIdentifier/> <xades:SignedDataObjectProperties> <xades:DataObjectFormat> <xades:MimeType/> <xades:UnsignedProperties> <xades:UnsignedSignatureProperties> </pre>	<pre> <xades:SignedDataObjectProperties> <xades:DataObjectFormat> <xades:MimeType/> <xades:UnsignedProperties> <xades:UnsignedSignatureProperties> </pre>
<p>OCSP重要!(時刻)</p>	<p>署名時刻</p>

EESTi e-Estoniaポータルサイト



For visually impaired | Help

Eesti keel | **English** | Русский

Q Insert keyword

Search

Site map | Advanced search

My Data Services Topics Contacts

Naoto Miyachi Log out

Main page → Services

For a citizen

For an entrepreneur

For an official

Services A-Z

Services

Descriptions of e-services are available in English, all official documents are in Estonian.



For a citizen

- Prescriptions
- Application for needs-based study allowance
- Benefits for incapacity for work
- Entering the Admissions Information System (SAIS)

[View all](#)



For an entrepreneur

- Vacation pay and average wages compensation
- Submission of notices of economic activities and application for activity licences for the purpose of organising additional adult education
- Adding data on the certificate of temporary incapacity for work
- Traffic insurance history

[View all](#)



For an official

- Adding data on the certificate of temporary incapacity for work
- Economic Activities of Estonia (EMTAK)
- Query about identity documents
- Notarised documents

[View all](#)



Services A-Z

[View all](#)

事業主サービス
e-Residencyも
多くが利用可能

居住者サービス
e-Residencyは
ほとんど利用不可

公的サービス

Login

KAART Login with ID-card

MOBIL-ID Login with mobile-ID

* Personal code:

* Phone number:

Enter

Login via bank

SEB Swedbank Danske Bank

Nordea Krediidipank

Nordea pank Krediidipank

By entering this site you accept the Terms of use terms and conditions of the state portal Eesti.ee.

<https://www.eesti.ee/>

For a citizen

- ▶ Housing
- ▶ Company and activity licence search
- ▶ Education and Science
- ▶ Environment
- ▶ Culture and Leisure Time
- ▶ Traffic
- ▶ Family
- ▶ Money and Ownership
- ▶ Travelling
- ▶ National Defence
- ▶ The State and the Citizen
- ▶ Consumer Protection
- ▶ Health Care and Protection
- ▶ Benefits and Social Assistance
- ▶ Work and Employment Relations
- ▶ Legal Aid
- ▶ Official forms
- ▶ Electronic voter card
- ▶ Population Register

For an entrepreneur

- ▶ Official forms
- ▶ X-road
- ▶ Authorization
- ▶ Company and activity licence search
- ▶ Environment
- ▶ Local authorities
- ▶ Culture and Leisure Time
- ▶ Licences and registrations
- ▶ Taxes and customs
- ▶ National Defence
- ▶ Structural assistance information system
- ▶ Transport
- ▶ Labour environment
- ▶ Legal Aid
- ▶ Accounting and Reporting

For an official

- ▶ Official forms
- ▶ X-road
- ▶ Authorization
- ▶ Housing
- ▶ Education and Science
- ▶ Environment
- ▶ Local authorities
- ▶ Culture and Leisure Time
- ▶ Licences and registrations
- ▶ National Defence
- ▶ The State and the Citizen
- ▶ Structural assistance information system
- ▶ Health Care and Protection
- ▶ Benefits and Social Assistance
- ▶ Transport
- ▶ Work plan service
- ▶ Work and Employment Relations
- ▶ Legal Aid

多種多様なサービスが利用可能

IDカードを使い安全にドキュメントの送受信
12カ月間有効で50MBまで保管が可能

Main page → My Data → My documents → Personal documents

My calendar

My documents

▶ [Personal documents](#)

My services

E-mail

My links

Settings

Personal documents

Here you can safely send, receive, keep, manage, upload/download and share documents. The documents are stored for 12 months and their overall size must not exceed 50 MB.

▶ See your notarised documents [via respected e-service](#) and your personal IDs in [My Data](#).

To keep track of changes, access and signing in My documents, you can order [notifications](#).

[Personal documents settings](#)



User has been subscribed to service.

The name or party

All Documents

All periods

Search

Cancel

つまり...
電子私書箱
サービス

Add a new document Delete selected Send selected

Showing 1-1, Total 1

Results per page: 15

<input type="checkbox"/>	Title	Sender / recipient	Last Modified	Size
<input type="checkbox"/>	Welcome		18.09.2015	8 bytes
			Space used out of 50 MB:	8 bytes

Add a new document Delete selected Send selected

エストニアIDカードが普及した理由

1. カード/モバイル等のハードインフラ整備
 - ▶ 少ない国民数だから成立した可能性はある
2. ソフト開発オープンソース化のエコ環境
3. 署名フォーマット等標準化/ツール提供
4. ポータル機能充実によるオンライン化

※ マイナンバー/国民番号カードも参考に!

ご清聴ありがとうございました。

JNSA



電子署名WGへの参加者募集中です！
<https://www.facebook.com/eswg.jnsa.org>