資料3

エストニアの
電子証明書等について

令和3年1月29日

総務省　情報流通行政局　デジタル企業行動室

0. はじめに

◆ エストニアにおける電子識別手段にて利用可能な行政サービス、Mobile-ID/Smart-IDで利用可能な機種、発行・利用フロー等を整理した。

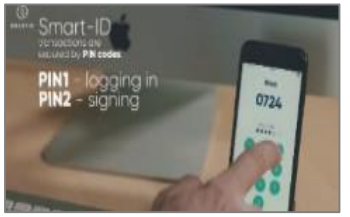
目次

<目次>

1.オンライン行政サービスに利用する3つの電子識別手段

◆ エストニア国内でオンライン行政サービスを利用するに当たり、エストニア国民が利用する電子識別手段は3つ
◆ eIDカードが日本におけるマイナンバーカードに相当

3つの電子識別手段



名称	• **eIDカード*** （ICカード）	• **Mobile-ID** （SIMカード）	• **Smart-ID** （アプリ）
開始年	• 2002年	• 2007年	• 2016年
概要	• 写真・ICチップ付きの**物理的なカード** ➢ 基本的に全国民に配布 ➢ **日本におけるマイナンバーカード**	• モバイル端末で利用する**SIMカード** ➢ **SIMカードを格納媒体**として利用 ➢ 希望者に発行	• モバイル端末で利用する**アプリ** ➢ **モバイルアプリとサーバを格納媒体**として利用
格納情報**	• 認証用の電子証明書/秘密鍵 ➢電子証明書にeID番号含む • 署名用の電子証明書/秘密鍵 ➢電子証明書にeID番号含む	• 認証用の電子証明書/秘密鍵 ➢電子証明書にeID番号含む • 署名用の電子証明書/秘密鍵 ➢電子証明書にeID番号含む	• 認証用の電子証明書/秘密鍵 ➢電子証明書にeID番号含む • 署名用の電子証明書/秘密鍵 ➢電子証明書にeID番号含む

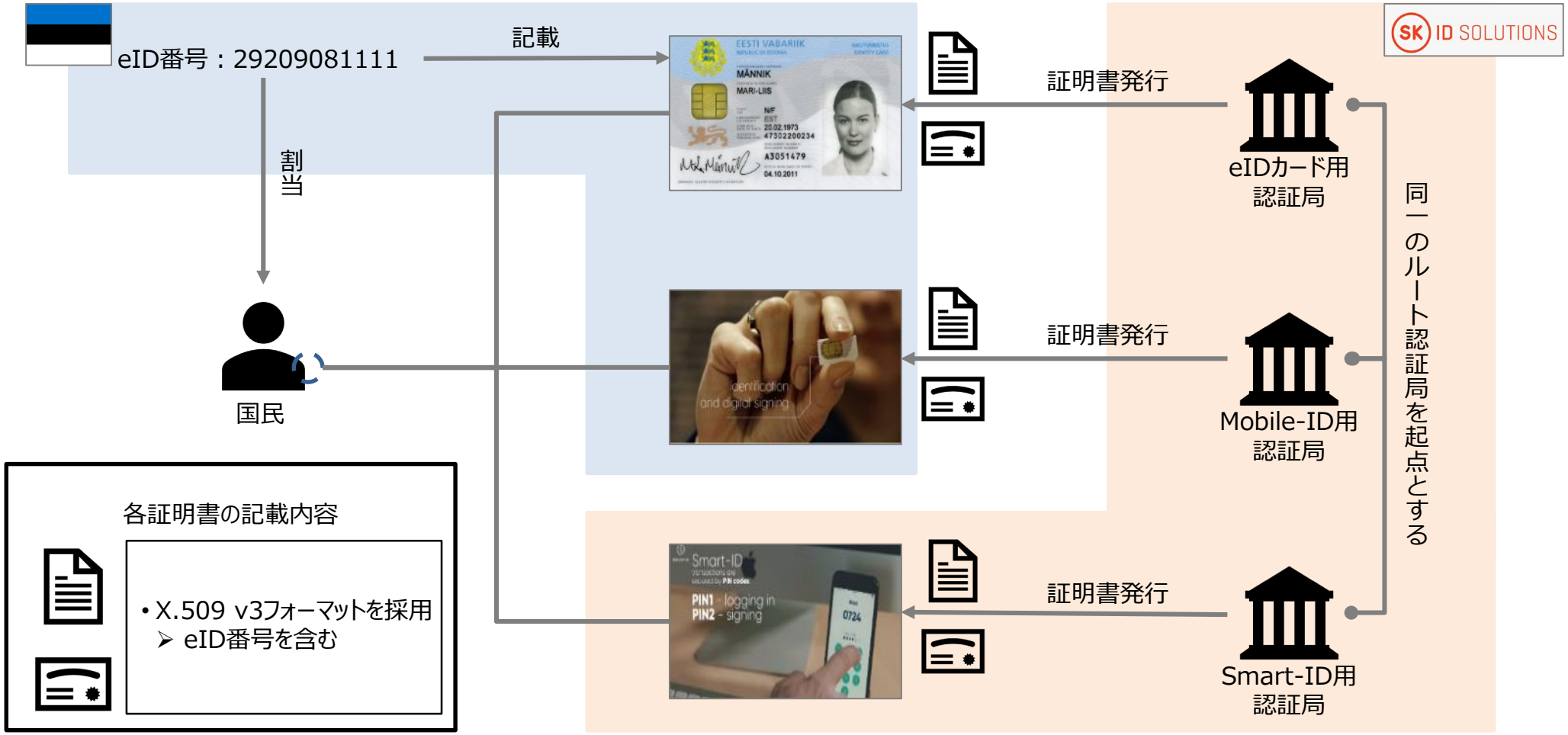
*eIDカードに記載されているIDは11桁で、1-6の数字（性別と生誕年（19世紀、20世紀、21世紀）の組み合わせ）の1桁、生年月日6桁、識別番号4桁で構成
**各手段に格納された認証用/署名用証明書は記載されている情報が異なる

1.オンライン行政サービスに利用する3つの電子識別手段

◆ エストニアの3つの電子識別手段に格納された証明書はすべて、エストニアの民間企業「SK ID Solutions」が発行
◆ 各証明書にはeID番号が含まれている

eID番号と電子識別手段に格納された電子証明書の簡易関係図

：認証用電子証明書　：署名用電子証明書



1.オンライン行政サービスに利用する3つの電子識別手段

◆ eIDカードは身分証明書法で本人確認手段として定められている物理的なカード
◆ 電子認証・電子署名ともにeIDASにおける最高保証レベルを取得しており、ほぼすべてのオンライン行政サービスが可能

eIDカードの概要

概要
- 写真・ICチップ付きの**物理的なカード**で基本的に全国民に配布

開始
- 2002年

普及率
- ほぼ100%

根拠法*
- **eIDAS**
  - 保証レベル、電子署名の効力
- **身分証明書法**
  - 発行対象者と身分証明書の定義
- **信頼サービス****
  - 電子署名の効力（eIDAS準拠）

対応機種
- -

eIDカードで利用可能な行政サービスと非対面における保証レベル

利用可能な行政サービス

対面
- **全ての行政サービス**
- IDカード所持・提示（券面またはICチップ）が次の証明書の代替にもなる
  - EU内パスポート/公的身分証明書/運転免許証/健康保険証/公共交通機関チケット
- 身分証明書法にて身分証明書として定義されている
  - 各行政サービスで使用可能な身分証明書について規定する公開文献は見受けられない

非対面
- **ほぼすべての行政サービス（結婚・離婚・不動産売買以外）**
  - Eesti.ee***：住民登録申請、出生届、年金・各種手当の申請等
  - Eesti.ee以外の各種サイト
    - ✓ 国民向けサービス：政府情報照会、確定申告・納税、電子投票等
    - ✓ 行政内部向けサービス：官報・公示掲載、住民登録、事業者登録等
- 身分証明書法にて身分証明書として定義されている
  - 各行政サービスで使用可能な身分証明書について規定する公開文献は見受けられない

非対面における保証レベル

eIDAS
- 電子認証手段の保証レベルを規定：**High（高）**を取得
- 電子署名の保証レベルを規定：**QES（適格電子署名）**を取得

身分
- 特に記載は見受けられない

信頼
- eIDASに準拠することで、電子署名に法的効力を付与

*日本・エストニア EUデジタルソサエティ推進協議会にインタビューした結果を反映
**正式名称は「電子取引法のための電子識別および信頼サービス」 ***エストニア国電子サービスポータル

1.オンライン行政サービスに利用する3つの電子識別手段

◆ Mobile-IDは身分証明書法で本人確認手段として定められているモバイル端末を利用するSIMカード
◆ 電子認証・電子署名ともにeIDASにおける最高保証レベルを取得しており、ほぼすべてのオンライン行政サービスが可能

Mobile-IDの概要

概要
- モバイル端末で利用する**SIMカード**

開始
- 2007年

普及率
- 約19%

根拠法*
- **eIDAS**
  - 保証レベル、電子署名の効力
- **身分証明書法**
  - 発行対象者と身分証明書の定義
- **信頼サービス**
  - 電子署名の効力（eIDAS準拠）

対応機種
- エストニア国内で販売されている
  スマホであれば、どの機種でも利用可能

Mobile-IDで利用可能な行政サービスと非対面における保証レベル

利用可能な行政サービス

対面
- 個人識別情報（写真生体認証画像など）が格納されていないため、利用不可

非対面
- **ほぼすべての行政サービス（結婚・離婚・不動産売買以外）**
  - Eesti.ee　：住民登録申請、出生届、年金・各種手当の申請等
  - Eesti.ee以外の各種サイト
    - ✓ 国民向けサービス　：政府情報照会、確定申告・納税、電子投票等
    - ✓ 行政内部向けサービス　：官報・公示掲載、住民登録、事業者登録等
- 身分証明書法にて身分証明書として定義されている
  - 各行政サービスで使用可能な身分証明書について規定する公開文献は見受けられない

非対面における保証レベル

eIDAS
- 電子認証手段の保証レベルを規定　：**High（高）**を取得
- 電子署名の保証レベルを規定　：**QES（適格電子署名）**を取得

身分
- 特に記載は見受けられない

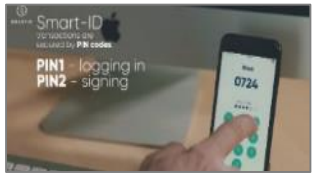
信頼
- eIDASに準拠することで、電子署名に法的効力を付与

*日本・エストニア EUデジタルソサエティ推進協議会にインタビューした結果を反映

1.オンライン行政サービスに利用する3つの電子識別手段

◆ Smart-IDはモバイル端末で利用するアプリ
◆ 電子認証・電子署名ともにeIDASにおける最高保証レベルを取得しており、一部のオンライン行政サービスが可能

Smart-IDの概要



概要	• モバイル端末で利用する**アプリ**で**モバイルアプリとサーバを格納媒体**に利用
開始	• 2016年
普及率	• 約42%
根拠法*	• **eIDAS** ➢ 保証レベル、電子署名の効力 • **信頼サービス** ➢ 電子署名の効力（eIDAS準拠）
対応機種	• 以下4点で要件が存在 ➢ OS/Disc容量/画面/HW

Smart-IDで利用可能な行政サービスと非対面における保証レベル

利用可能な行政サービス	対面	• 個人識別情報（写真生体認証画像など）が格納されていないため、利用不可
	非対面	• **一部の行政サービス** ➢ Eesti.ee　：住民登録申請、出生届、年金・各種手当の申請等 ➢ Eesti.ee以外の各種サイト ✓ 国民向けサービス　：政府情報照会、確定申告・納税・還付等 ✓ 行政内部向けサービス　：- • 身分証明書として定義されている公開文献は見受けられない ➢ 各行政サービスで使用可能な身分証明書について規定する公開文献は見受けられない
非対面における保証レベル	eIDAS	• 電子認証手段の保証レベルを規定　：**High（高）**を取得 • 電子署名の保証レベルを規定　：**QES（適格電子署名）**を取得
	身分	• 特に記載は見受けられない
	信頼	• eIDASに準拠することで、電子署名に法的効力を付与

*日本・エストニア EUデジタルソサエティ推進協議会、SK ID Solutions にインタビューした結果を反映

2.各電子識別手段ごとに利用可能な行政サービス

◆ eIDカードはほぼすべて、Mobile-IDは非対面のほぼすべて、Smart-IDは一部のオンライン行政サービスが利用可能

各電子識別手段で利用可能な行政サービス

eIDカード	対面	・**全ての行政サービス** ・IDカード所持・提示（券面またはICチップ）が次の証明書の代替にもなる ➢ EU内パスポート/公的身分証明書/運転免許証/健康保険証/公共交通機関チケット
	非対面	・**ほぼすべての行政サービス（結婚・離婚・不動産売買以外）** ➢ Eesti.ee　：住民登録申請、出生届、年金・各種手当の申請、国民健康保険の手続き、自動車の登録手続き等 ➢ Eesti.ee以外の各種サイト ✓ 国民向けサービス　：政府情報照会、確定申告・納税・還付、医療記録照会・電子処方箋、電子投票等 ✓ 行政内部向けサービス　：官報・公示掲載、住民登録、事業者登録、不動産登記、閣議管理、訴訟管理等
Mobile ID	対面	・個人識別情報（写真生体認証画像など）が格納されていないため、利用不可
	非対面	・**ほぼすべての行政サービス（結婚・離婚・不動産売買以外）** ➢ Eesti.ee　：　（同上） ➢ Eesti.ee以外の各種サイト ✓ 国民向けサービス　：　（同上） ✓ 行政内部向けサービス　：　（同上）
Smart ID	対面	・個人識別情報（写真生体認証画像など）が格納されていないため、利用不可
	非対面	・**一部の行政サービス** ➢ Eesti.ee　：（同上） ➢ Eesti.ee以外の各種サイト ✓ 国民向けサービス　：政府情報照会、確定申告・納税・還付、医療記録照会・電子処方箋等 ✓ 行政内部向けサービス　：-

3.Mobile-ID/Smart-IDで利用可能なスマホ機種

◆ Mobile-IDにOS等の要件はなく、エストニア国内で販売されているスマホであれば、すべての機種で利用が可能
◆ Smart-IDはOS等4つの要件が定められている

		OS	Disc容量	画面	ブラウザ	HW
Mobile ID*		• エストニア国内で販売されているスマホであれば、どの機種でも利用可能 ➢ 中古スマホや海外で発売されているスマホでも、SIMカード挿入後にSMSが動作するのであれば使用可能				
	Android	• -	• -	• -	• -	• -
	iPhone	• -	• -	• -	• -	• -
	その他機種（Windows Phone等）	• -	• -	• -	• -	• -
Smart ID		• 下記要件を満たしたAndroid/iPhone端末であれば利用可能				
	Android	• Android5以降	• Android5.x** ➢ 36MB以上	• 480ピクセル以上 • 3.5インチ以上	• -	• -
	iPhone	• iOS11以降	• OSによる違いは無し ➢ 28MB以上	• 480ピクセル以上 • 3.5インチ以上	• -	• iPhone7以降
	その他機種（Windows Phone等）	• サポート対象外	• サポート対象外	• サポート対象外	• サポート対象外	• サポート対象外

*Telia、elisa、tele2の3社へインタビューした結果より作成
**Android9以降は24MB以上の空き容量が必要

4.Mobile-ID/Smart-IDの発行・利用フロー

◆ Mobile-IDはMobile-ID SIM（M-SIM）をM-SIM提供会社で受取、ユーザー側でアクティベートを行い利用可能
◆ eIDカードやパスポートを用いて対面で1回、eIDカードを用いてオンラインで1回の最低2回、本人確認を実施する

Mobile-IDの発行フロー

本人確認：本人確認実施タイミング

利用者がMobile-ID SIMカードを契約（本人確認）

エストニア国内SIM提供企業（5社）

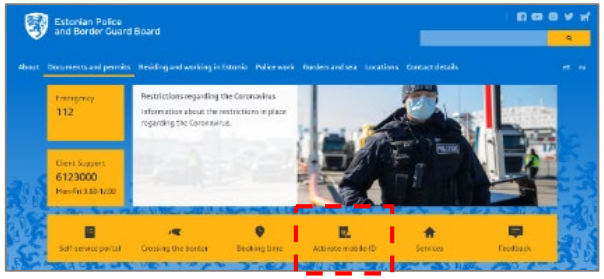
提供（3社）	未提供（2社）
Telia	top connect
elisa	GO-SIM
TELE2	

- 利用者はM-SIM提供会社（政府認定）にて本人確認を行い、**契約を締結**

M-SIM受取（本人確認）

- 契約日にM-SIM提供会社にて**M-SIMを受取、携帯電話に挿入**

警察サイトを訪問



- **PCから警察サイトを訪問し、M-SIMの証明書のアクティベート申請**を実施

M-SIM証明書アクティベーション（本人確認）

- eIDカードをカードリーダーに挿入し、本人確認を行うことで**アクティベート実施**

本人確認

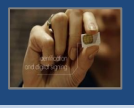
本人確認実施タイミング

- **本人確認は最低2回実施**
  - ➢ **Mobile-IDに係る契約時**（店舗でのみ契約可能）
  - ➢ 契約後、M-SIMの受取までに店舗を離れた場合は、M-SIMの受取時に再度、本人確認が必要
  - ➢ **M-SIM証明書アクティベーション時**
- 対面手続きが必須
  - ➢身分証明書法に規定

本人確認資料

- オンライン
  - ➢ M-SIM証明書アクティベーション時
    - ✓ eIDカード
- 店舗での契約時
  - ➢ 契約時/M-SIM受取時
    - ✓ eIDカード/パスポート e-residencyカード

4.Mobile-ID/Smart-IDの発行・利用フロー



◆ 通常のSIMからMobile-ID SIMへ交換することで、電話等の通常利用に加え、利用者はMobile-IDの認証が可能
◆ Mobile-IDの利用料金はイニシャルとランニングに分けることができ、通常料金と合算した形で利用者は料金を支払う

Mobile-IDの利用フロー

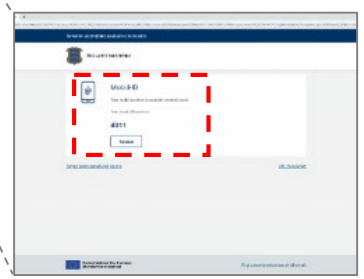
サイト訪問
- 利用者は利用したいサービスを提供しているサイトを訪問
- ログインボタンを押下

Eesti.ee（トップ画面）

ID等入力
- 認証方式でMobile-IDを選択
- eIDと電話番号を入力し、緑色のボタンを選択

ログイン画面

SMS認証
- 利用しているデバイスの画面に確認コードが表示され、利用者のスマホはSMSを受信
- SMSに同一の確認コードが記載されていることを確認し、同SMSに記載のURL先へ移動してPINを入力



SMS認証画面

ログイン完了
- PINが正しければ、利用しているデバイスが自動で利用者のマイページへ遷移
- 利用したいサービスを利用開始

価格表

イニシャル

州手数料 仲介 手数料	• Mobile-ID利用に係る州への手数料 • 携帯会社が負担しユーザーへ請求 • 0~10€
Mobile-ID SIMカード 交換料金	• SIMカードを交換する費用 • 3€

ランニング

Mobile-ID 月額料金	• Mobile-ID基本料金 • 0.99~1€
Mobile-ID 使用料金 （/1利用）	• Mobile-ID使用料金 • 現状ではどこの携帯会社でも無料 • 0€

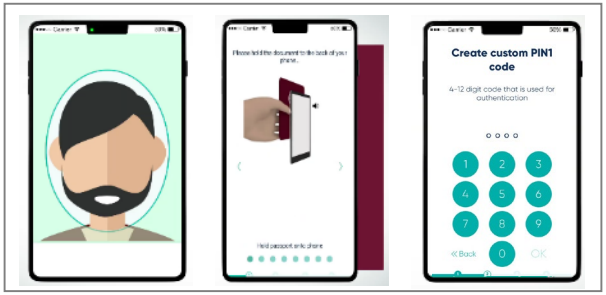
4.Mobile-ID/Smart-IDの発行・利用フロー

◆ Smart-IDは利用者がスマホにアプリをダウンロードすることで利用が可能
◆ PINコードを設定する時とSmart-IDポータルをログインする時の2回、本人確認を実施する

Smart-IDの発行フロー（eIDカード利用の場合の例）

本人確認：本人確認実施タイミング

利用者がアプリ上でPINコードを設定 【本人確認】

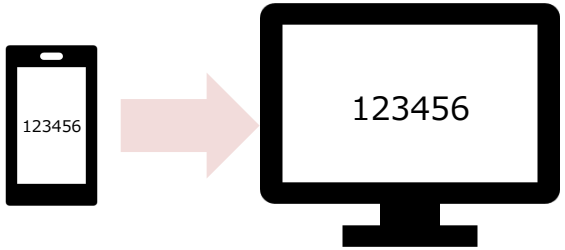


- 本人確認の際、**生体認証とNFCを利用可能***
- アプリ利用に必要な**PINを設定**

利用者はPCでアカウント登録を継続** 【本人確認】

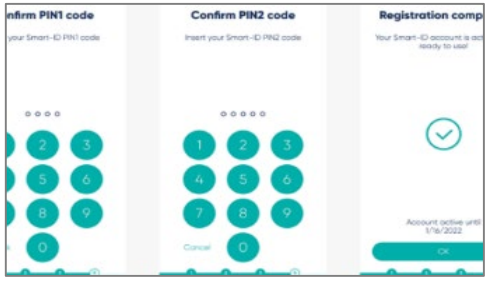
- 利用者はSmart-IDポータルを開き**eIDカードでログイン**

OTPコードの入力



- **アプリ上にOTPコードが表示**されるため、利用者はPCにOTPコードを入力

利用者の最終確認



- 利用者が設定した**PINを最終確認**し、利用登録は完了

本人確認

本人確認実施タイミング

- **本人確認は2回実施*****
  - ➢ PINコードを設定する時
    - ✓ オンラインor銀行窓口で本人確認
  - ➢ Smart-IDポータルにログインする時
    - ✓ オンラインで本人確認
- 対面手続きは必須ではない
  - ➢ eIDASにて、事前に対面での本人確認を行った認証手法であると規定
  - ➢ 対面の本人確認が必須であると規定された法律は見受けられない

本人確認資料

- **オンライン**
  - ➢ PINコードを設定する時
    - ✓ eIDカード/パスポート/Mobile-ID
  - ➢ Smart-IDポータルにログインする時
    - ✓ eIDカード
- **銀行窓口**
  - ➢ eIDカード/パスポート/e-residencyカード

*NFCで読み取った顔写真データと、撮影した顔写真を照合することで本人確認を実施。Mobile-IDを利用する場合は、生体認証での本人確認ではなく、Mobile-IDのPIN入力での本人確認。
Mobile-IDを利用する場合は、本人確認はPINコード設定時の1回であり、スマホのみで発行作業が可能 。*オフラインの場合、本人確認は1回（銀行窓口での本人確認のみ）

4.Mobile-ID/Smart-IDの発行・利用フロー

◆ 利用者は利用したいサイトへ訪問後、サイト上でeIDを入力すると画面に確認コードが表示される
◆ 画面に表示された確認コードがアプリ上でも表示されていることを確認し、アプリ上でPINを入力するだけでログイン完了

Smart-IDの利用フロー

サイト訪問
- 利用者は利用したいサービスを提供しているサイトを訪問
- ログインボタンを押下

Eesti.ee（トップ画面）

eID入力
- 認証方式でSmart-IDを選択
- eIDを入力し、緑色のボタンを選択

ログイン画面

確認コードによるチェック
- 利用しているデバイスの画面（ブラウザ）に確認コードが表示される
- アプリへ移動し、同一の確認コードが表示されていることを確認し、アプリ上でPINを入力

確認コードのチェック画面

ログイン完了
- PINが正しければ、利用しているデバイス（ブラウザ）が自動で利用者のマイページへ遷移
- 利用したいサービスを利用開始

価格表

イニシャル
- 利用料金の負担はなく、利用が可能

ランニング
- 利用料金の負担はなく、利用が可能

5.Mobile-ID/Smart-IDまとめ

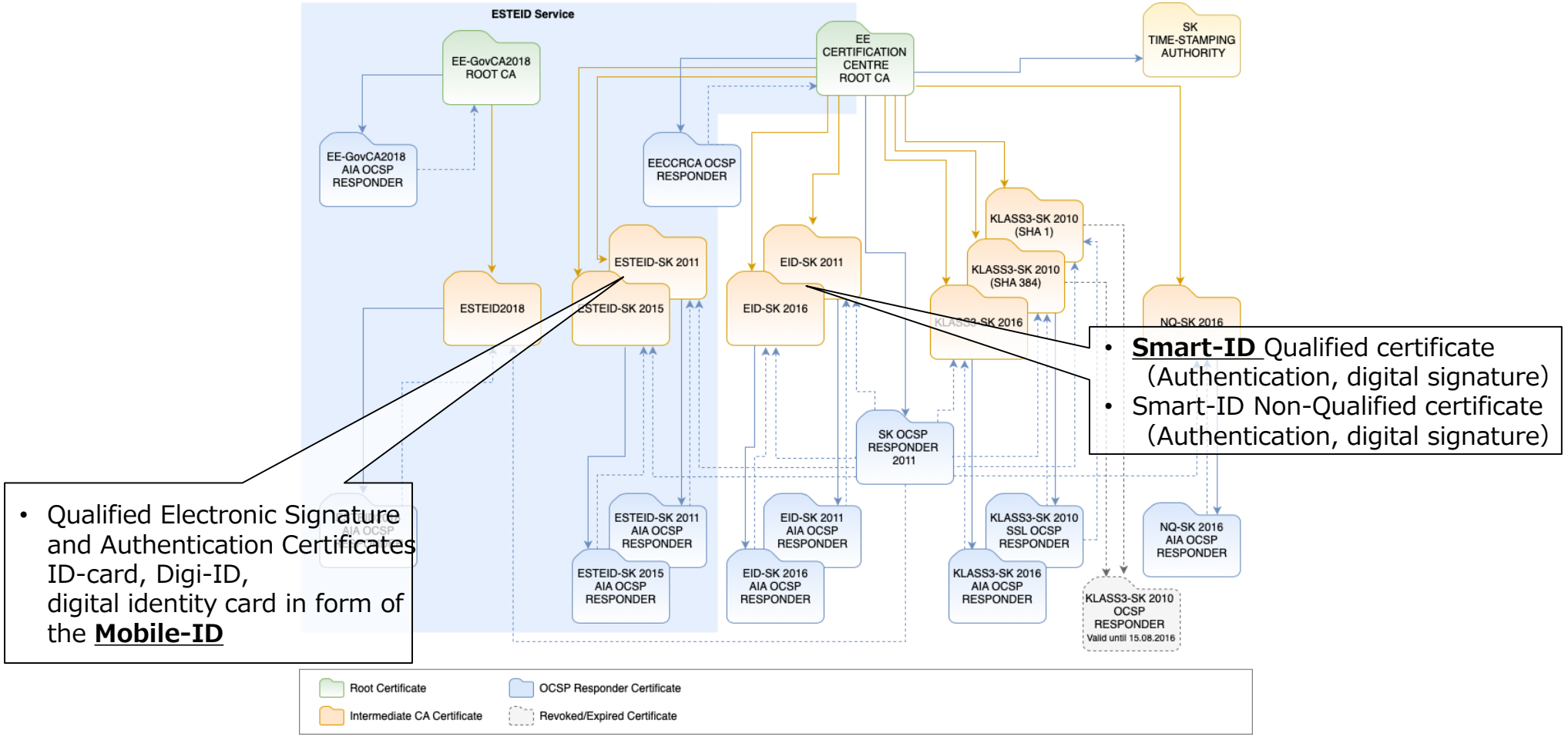
◆ Mobile-IDおよびSmart-IDの調査結果は以下の通り

		Mobile-ID	Smart-ID
利用者のコスト		• イニシャルコスト：有料 • ランニングコスト：有料	• イニシャルコスト：無料 • ランニングコスト：無料
求められる要件		• エストニア国内で販売されているスマホであればどの機種でも利用可能	• 以下4点で要件が存在 ➢ OS/Disc容量/画面/HW
セキュリティ	法/制度	• eIDAS、身分証明書法、電子取引法のための電子識別および信頼サービスに準拠	• eIDAS、電子取引法のための電子識別および信頼サービスに準拠
	第三者評価	• eIDASに定められた適格性評価を実施	• eIDASに定められた適格性評価を実施
	本人確認	• SIM契約時とM-SIM証明書アクティベーション時に本人確認 ➢対面での本人確認が必須	• PINコード設定時とSmart-IDポータルログイン時に本人確認 ➢事前に対面での本人確認を行った資料でのオンライン本人確認
行政サービス		• ほぼすべてのオンライン行政サービスを利用可能	• 一部のオンライン行政サービスで利用可能
UI/UX		• Mobile-IDを発行後、PCによるアクティベーションを実施 • スマホのみでMobile-IDを利用可能	• スマホのみでSmart-IDを発行することも可能 • スマホのみでSmart-IDを利用可能

参考資料

◆ ３つの電子識別手段の電子証明書は、共通のルート認証局を基点としている
◆ 各電子識別手段毎に、署名用の電子証明書と認証用の電子証明書は同一の中間認証局から発行されている

各電子識別手段における認証局の体系図



- **Smart-ID** Qualified certificate (Authentication, digital signature)
- Smart-ID Non-Qualified certificate (Authentication, digital signature)

- Qualified Electronic Signature and Authentication Certificates ID-card, Digi-ID, digital identity card in form of the **Mobile-ID**

参考資料

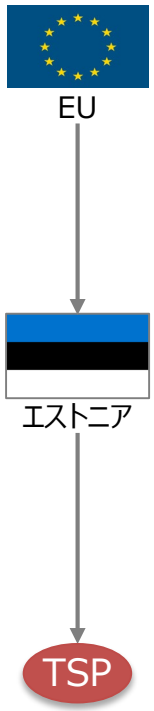
◆ エストニアのeIDはeIDASに準拠
◆ eIDカードとMobile-IDはエストニア政府が身分証明書法内で本人確認手段として定めている

eIDに関係する法律

電子署名法：日本における電子署名法相当の法律

	法律名（施行年）	概要	eIDに関する規制内容
EU	電子署名法 ・eIDAS（2016）	・EU加盟国に直接効力を持つRegulationとして制定 ・トラストサービスを定義（電子署名/eシール/e-derivary/タイムスタンプ/webサイト認証）	・**「第三者評価機関の選定」**と**「自国内のTSPが第三者評価を受けること*」**を加盟国へ義務化 ・デジタル署名へ手書き署名または印鑑と**同じ法的効力**を付与
エストニア	・身分証明書法（2000）	・エストニアの市民および居住者への**身分証明書の管理・運用について規定**	・**以下の身分証明書に関して、定義・発行・利用（対面・非対面）を規定** ➢ eIDカード/ Mobile-ID/ e-residencyカード**
	電子署名法 ・電子取引法のための電子識別および信頼サービス（2016）	・eIDASの発効に伴い、国内法「デジタル署名法」を本法律へ引き継ぐ	・**eIDASを遵守**することを規定

eIDカードの法律に係る関係図



・eIDASをはじめとした**Regulationで EU加盟国を規制**
➢ 第三者評価機関の選定

・身分証明書法をはじめとした**国内法でTSPを規制**
➢ 第三者評価の実施

・EUのRegulation並びにエストニア国内法の**両法に準拠**
➢ 第三者評価の申請

*公的なオンラインサービスにおける電子認証手段の保証レベルは「Substantial」以上を推奨（eIDAS一般条項）
**居住権を持たない外国人に対して発行されるデジタルIDカード

◆ エストニアの3つの電子識別手段において、eIDASで定められている保証レベルについては以下の通り
◆ 全３種類のeIDにおいて、保証レベル『High』の電子認証、適格電子署名『QES』を提供

	電子認証手段の保証レベル	電子署名の保証レベル	電子署名生成装置*の種類
eID カード	・**High（高）** ➢ 対面での本人確認 ➢ 所有（ICカード）と知識（PIN）の２要素認証 ➢ 複製や改ざんに対する保護機能を有したICカードを利用	・**QES（適格電子署名）** ➢ PKIベースの電子署名 ➢ 適格TSPから発行された証明書 ➢ 認定された電子署名生成装置（Qualified Electronic Signature/ Secure Signature Creation Device）を利用	・**QSCD** ➢ **CC認証（EAL5+）**取得の仏IDEMIA製品**を採用
Mobile ID	・**High（高）** ➢ 対面での本人確認 ➢ 所有（SIMカード）と知識（PIN）の２要素認証と、SMSによる動的認証 ➢ 複製や改ざんに対する保護機能を有したSIMカードを利用	・**QES（適格電子署名）** ➢ 同上	・**QSCD** ➢ 公開文献は見受けられない
Smart ID	・**High（高）** ➢ eIDカードやMobile-IDでのオンライン本人確認あるいは対面での本人確認 ➢ 所有（スマホアプリ）と知識（PIN）の２要素認証に加え、OTPコードによる動的認証 ➢ 複製や改ざんに対する保護機能を有した、システム***を利用	・**QES（適格電子署名）** ➢ 同上	・**QSCD** ➢ ソフトウェア製品、モバイルクライアント、HSMの組み合わせ ➢ SK ID Solution の“Smart-ID SecureZone” が**CC認証（EAL4+）**取得

*EU所属機関ECのHPに掲載 **RIA構築のeIDサイトに掲載
***ソフトウェア製品、モバイルクライアント、HSMの組み合わせ

参考資料

◆ eIDASにおける電子識別手段の保証レベルは各種標準やガイドライン（SP800-63-3等）を参考に定義されている
◆ 電子署名の最高レベルQESは、SESやAESと異なり、適格認定を受けたデジタル証明書、電子署名装置を用いる

第８条に基づく電子認証手段の保証レベル

保証レベル*	概要*	例*	SP800-63-3**
Low（低）	本人確認書類での本人確認、**対面での本人確認**を実施 なりすまし、盗聴、リプレイ攻撃、改ざんに耐性を持つ認証方法を利用	各種サイトなどへログインするためのID/PW	IA Lv.1/AA Lv.1相当
Substantial（中）	上記の要件に加えて 真正であることが確認された本人確認書類により本人確認を実施 （但し、対面での本人確認は行わなくてもよい） 動的認証、2つ以上の要素（知識、所有物、生体情報）を利用した多要素認証を利用	運転免許証でeKYCを行いID/PWに加えて、OTPを利用	IA Lv.2/AA Lv.2相当
High（高）	上記の要件に加えて 有効な本人確認書類を用いた**対面での本人確認**が実施 （もしくは、**事前に対面での本人確認を行った認証手法による本人確認**を実施） 複製や改ざんに対する保護機能を有したデバイスを利用	国民IDカードのICチップに格納された電子証明書を利用	IA Lv.3/AA Lv.3相当

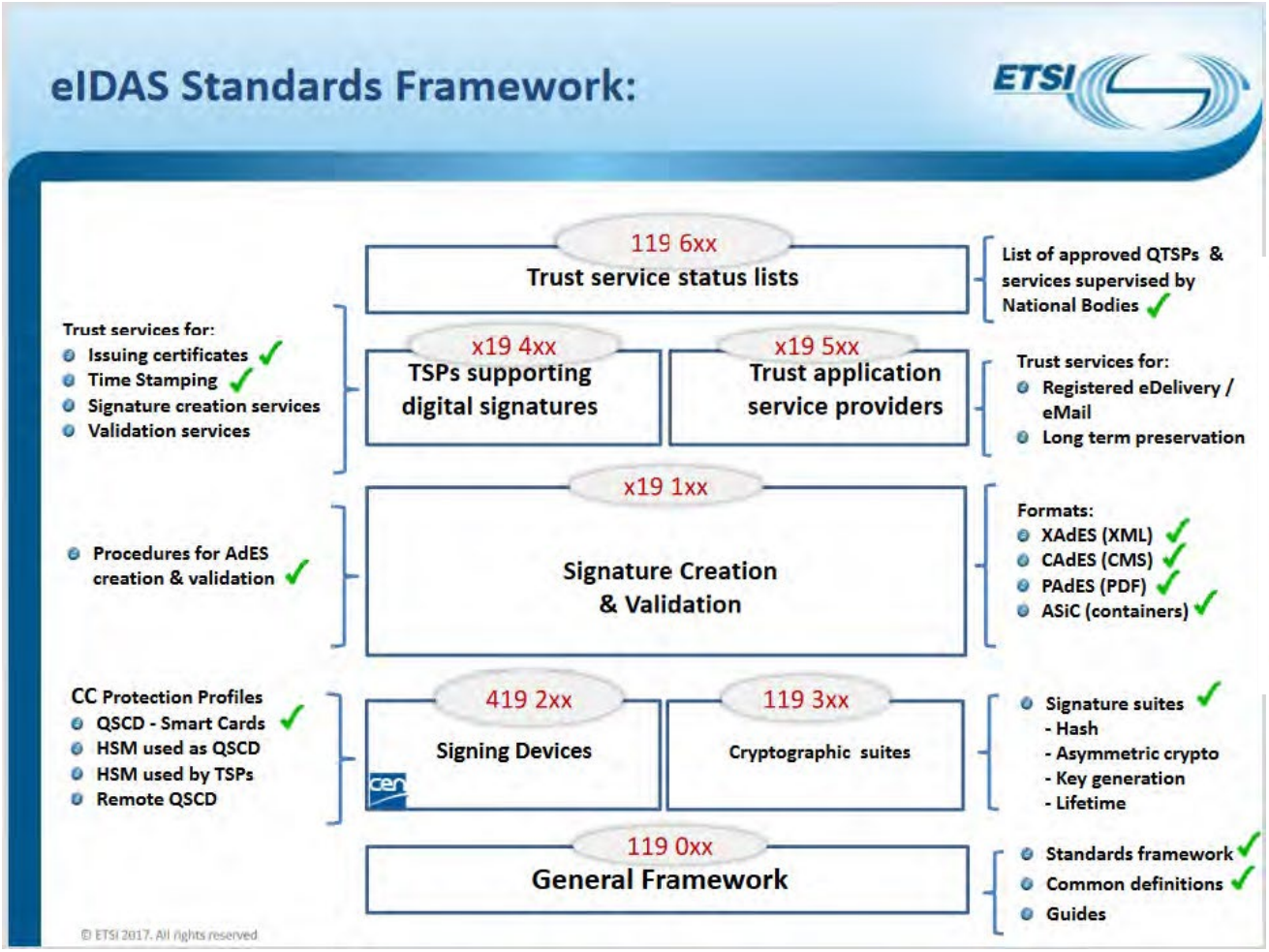
第4節に基づく電子署名の保証レベル

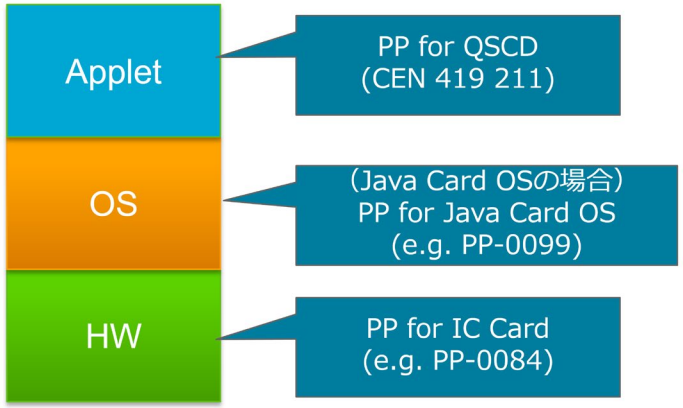
レベル	概要
Standard Electronic Signature（標準電子署名）	手書き署名の画像など、あらゆる電子形式の署名をカバー
Advanced Electronic Signature（高度電子署名）	**PKI**を使用して作成された署名 • 固有の署名者に関連し、デジタル証明書と署名者の同一性を確認できる • 署名者が独自に制御可能な署名生成装置を用いて生成する • 署名後の改ざんが検知可能
Qualified Electronic Signature（適格電子署名）	上記AESの特徴に加えて • EU加盟国において、**法的ステータス**を持つ署名 • **適格トラストサービスプロバイダー（TSP）**が発行するデジタル証明書を利用 • 電子署名は認定を受けた**適格電子署名生成装置（QSCD）**にて生成

*『海外事例から見るマイナポータルの活用』P.5から抜粋
**eIDAS規則と異なり、NIST SP800-63は、詳細な技術要件を規定しているため、単純比較はできない

参考資料

◆ QSCD（Qualified electronic Signature Creation Device）とは、eIDASに規定される要件を満たす装置
◆ ISO/IEC 15408（Common Criteria）とProtection Profile（EN 419 211シリーズ）に適合した製品を使用





- ISO/IEC 15408（Common Criteria）認証は、IT製品に搭載されるセキュリティー機能が、脅威に対して適切に設計され、正しく実装されているか評価する規格
- 日本政府のIT製品の調達において、ICカードに対するセキュリティ要件の多くが、EAL4以上を標準的に要求

表：評価保証レベル （Evaluation Assurance Level）

確認内容の深さ（≒セキュリティ強度）

EAL	概要	詳細
EAL1	機能テスト	セキュリティへの脅威が重大ではない場合に適用され、特定の機能の要件が対処されていることを確認する。 仕様に対する評価者のテスト、ガイダンスの調査など開発者の支援を受けずに最小の費用で評価を実施できる。 EAL1は、評価されていないITに比べ、保証の増加を提供する。
EAL2	構造テスト	古くから継承されたシステムの安全性を確保するなど完全な開発資料を提供できないような場合で、低レベルから中レベルの保証されたセキュリティを要する環境で適用できる。開発者からの設計情報と開発者テスト結果の提供レベルで評価を実施する。 また、開発環境における構成管理や製品の配付の手続きを評価する。 EAL2は、EAL1の保証に加え、開発者テスト、基本的攻撃能力を想定した脆弱性分析、さらに詳細なTOE仕様に基づく評価者のテストを要求する。
EAL3	方式テスト及びチェック	中レベルの保証されたセキュリティを必要とし、既存の適切な開発方法を大幅に変更することなく、TOEとその開発の完全な調査を要する状況に適用される。 EAL3は、EAL2の保証に加え、テストの網羅性や開発時のTOE改ざんを防止するメカニズムや手続きを要求する。
EAL4	方式設計、テスト及びレビュー	既存の商用製品の開発に対し、セキュリティに係るエンジニアリングコストの追加を受け入れられ、中レベルから高レベルの保証されたセキュリティを必要とする場合に適用される。 EAL4は、EAL3の保証に加え、より多くの設計記述、ソースコードなどのセキュリティ機能のすべての実装表現、開発時のTOE改ざんを防止する向上されたメカニズムや手続きを要求する。
EAL5	準形式的設計及びテスト	EAL5レベルの保証をはじめから達成する意図を持って開発され、高レベルのセキュリティを必要とし、専門的なセキュリティエンジニアリング技法の適用する適切なコストを負担する場合に適用される。 EAL5は、EAL4の保証に加え、準形式的な設計記述、構造化され分析可能なアーキテクチャ、TOE改ざんを防止する、さらに向上されたメカニズムや手続きを要求する。
EAL6	準形式検証済み設計及びテスト	保護する資産の価値が、高い保証のための追加的な開発コストを正当化するようなリスクの高い状況で使用する場合に適用される。 EAL6は、EAL5の保証に加え、さらに広範囲な分析、実装の構造化表現、さらなるアーキテクチャ構造、さらに広範囲な評価者の脆弱性評定、さらに向上された構成管理と開発環境の制御を要求する。
EAL7	形式的検証済み設計及びテスト	リスクが非常に高いか、高い資産価値により、さらに高い開発コストが正当化される場合に適用される。 EAL7は、EAL6の保証に加え、数学的検証を伴う形式的表現と対応、広範囲のテストを使用する包括的分析を要求する。

◆ アメリカでは、NISTが電子的認証に関するガイドラインを規定しており、3つの指標（IA/AA/FA）が存在
◆ 3つの指標それぞれに対し、3段階の認証レベルが規定されており、サービス内容ごとに準拠すべき認証レベルが異なる

NISTについて

機関名
- National Institute of Standards and Technology（アメリカ国立標準技術研究所）

概要
- 科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関

主なガイドライン
- **サイバーセキュリティに関する技術標準やベストプラクティス**をSpecial Publication（SP）シリーズとして発行
  - ➢ **SP 800シリーズ**
    - ✓ 米国政府機関がセキュリティ対策を実施する際に、利用することを前提としてまとめられたガイドライン
  - ➢ SP 1800シリーズ
    - ✓ サイバーセキュリティに関するプラクティスガイドを扱う
  - ➢ SP 500シリーズ
    - ✓ 基本的な情報システムの取扱方法を扱う

NIST-SP800-63-3（電子的認証に関するガイドライン）

指標		認証レベル Lv.1（低）	Lv.2	Lv.3（高）
IA Identity Assurance	• ユーザーが申請者として新規登録を行う際に、CSP*が実施する**本人確認の厳密さ、強度を示す**	• 本人確認不要 • 自己申告での登録で良い	• サービス内容により**識別に用いられる属性をリモート又は対面確認する必要あり**	• **識別に用いる属性を対面で確認**する必要があり、**確認書類の検証担当は有資格者**
AA Authenticator Assurance	• 登録済ユーザーが、**ログインする際の認証プロセスの強度を示す**	• 単要素認証で可	• **2要素認証が必要** • 2要素目の認証手段は**ソフトウェアを用いたもので可**	• **2要素認証が必要** かつ2要素目の認証手段は、**ハードウェアを用いたもの**
FA Federation Assurance	• SAML AssertionやIDトークンにおける**Assertionのフォーマットやデータのやり取りの方法についての強度を示す**	• **Assertion**（RPに送るIdPでの認証結果データ）**への署名**	• 署名に加え、**対象RPのみが複合可能な暗号化**	• Lv.2に加え、Holder-of-Key Assertionの利用

*クレデンシャル情報（ユーザーの認証に使う情報）を保護しセキュアな接続を実現するための認証技術を提供する事業者

◆ エストニアのMobile-IDの対応機種表を記載
◆ Mobile-IDは海外の特定地域で販売されているスマホ以外すべてのスマホで対応可能

	国内販売スマホ（他キャリア販売のスマホ含む）			海外販売スマホ		
	Android	iPhone	その他機種	Android	iPhone	その他機種
Telia	• 対応可能*	• 対応可能*	• 対応可能*	• 対応可能*	• 対応可能*	• 特定の地域で販売されているスマホに対応不可
elisa	• 対応可能*	• 対応可能*	• 対応可能*	• 対応可能*	• 対応可能*	• 特定の地域で販売されているスマホに対応不可
TELE2	• 対応可能*	• 対応可能*	• 対応可能*	• 対応可能*	• 対応可能*	• 特定の地域で販売されているスマホに対応不可

*デバイスでサポートしている周波数が3G,4Gのスマホに限る

M-SIM提供会社インタビュー結果

#	質問	Telia	Elisa	Tele2
1	利用可能な機種は	• キーボード付きのスマートフォンが利用不可（ただし、通話できなくなるだけ）	• Mobile-IDはエストニアのすべてのスマートフォンで使用可能	• すべての電話で使用可能
2	M-SIMは過去の機種で対応可能か	• 対応可能で、古いスマートフォンでも使用可能 • 3G,4G対応のスマホであれば対応可能	• 2G GSM規格が採用された後のスマホであれば対応可能	• デバイスでサポートしている周波数が以下であれば可能 ➢2G - GSM, 900 ja 1800mHz ➢3G / WCDMA / UMTS 900 and 2100 ➢4G LTE800, LTE1800 and LTE2100
3	海外から持ち込まれたスマホは対応可能か	• Mobile-IDはSMSで機能するため、SMSが機能していれば、利用可能 • 国固有の機種には対応不可	• SMSが動作するのであれば、お使いの携帯でMobile-IDを使用可能 • グローバルで標準化されているスマホであれば対応可	• SIMカードが通話、SMS、データ等の点で動作するのであれば、利用可能 • 特定の地域でしか取り扱っていないデバイスは使用不可
4	本人確認はどのタイミングで行うのか？	• 契約時の1回（店舗）	• 契約時に1回、身分証明書をもって実施 • 店舗で契約を行う	• 契約時の1回のみ本人確認を実施 • その際にTele2オフィスにて行う
5	SIMを受け取る際も本人確認は行うのか	• ショップから離れるのであれば、オフィスに戻るたびに本人確認が必要	• あまり想定できないが、外出をする場合は再度本人確認が必要	• 契約時のみなのでSIM受取時は不要 • SIMを間違った人に渡さないように本人確認をする場合もある
6	M-SIMを受け取る際の所要時間はどのくらいかかるのか	• それほど長くないが、15分程度かかる	• 混雑具合にもよるが、さほど時間はかからない想定	• 数分で可能

参考資料

◆「エストニア」のSmart-IDの仕組みについて、調査を実施
◆ Smart-IDはスマホで生成した秘密鍵を分割し、スマホとサーバの両方で保管する割符の仕組みを採用

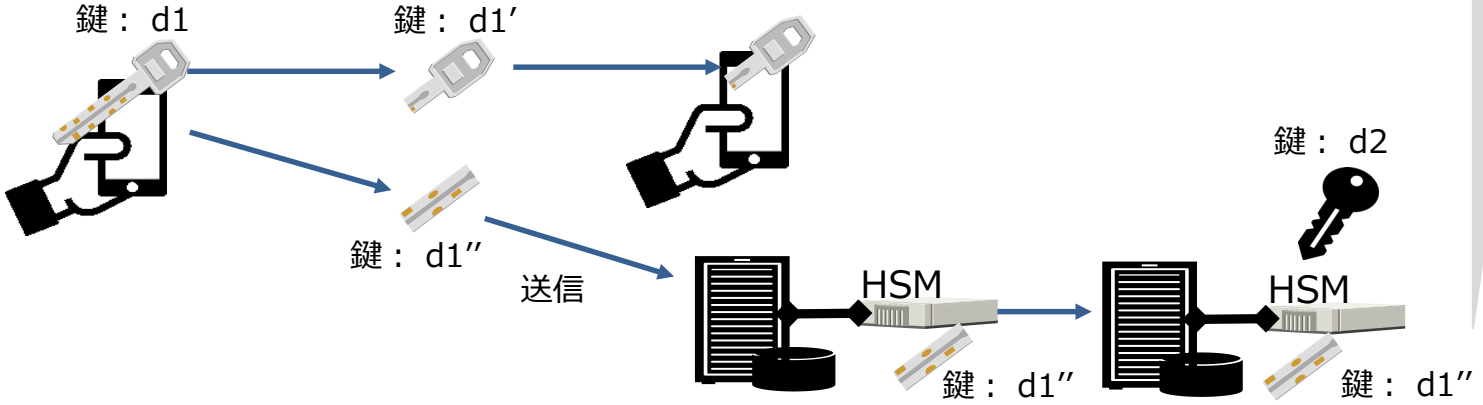
パターン

① スマホに電子証明書を格納する
② サーバに電子証明書を格納する
③ スマホとサーバに電子証明書を格納する → **Smart-ID方式**

■Smart-ID

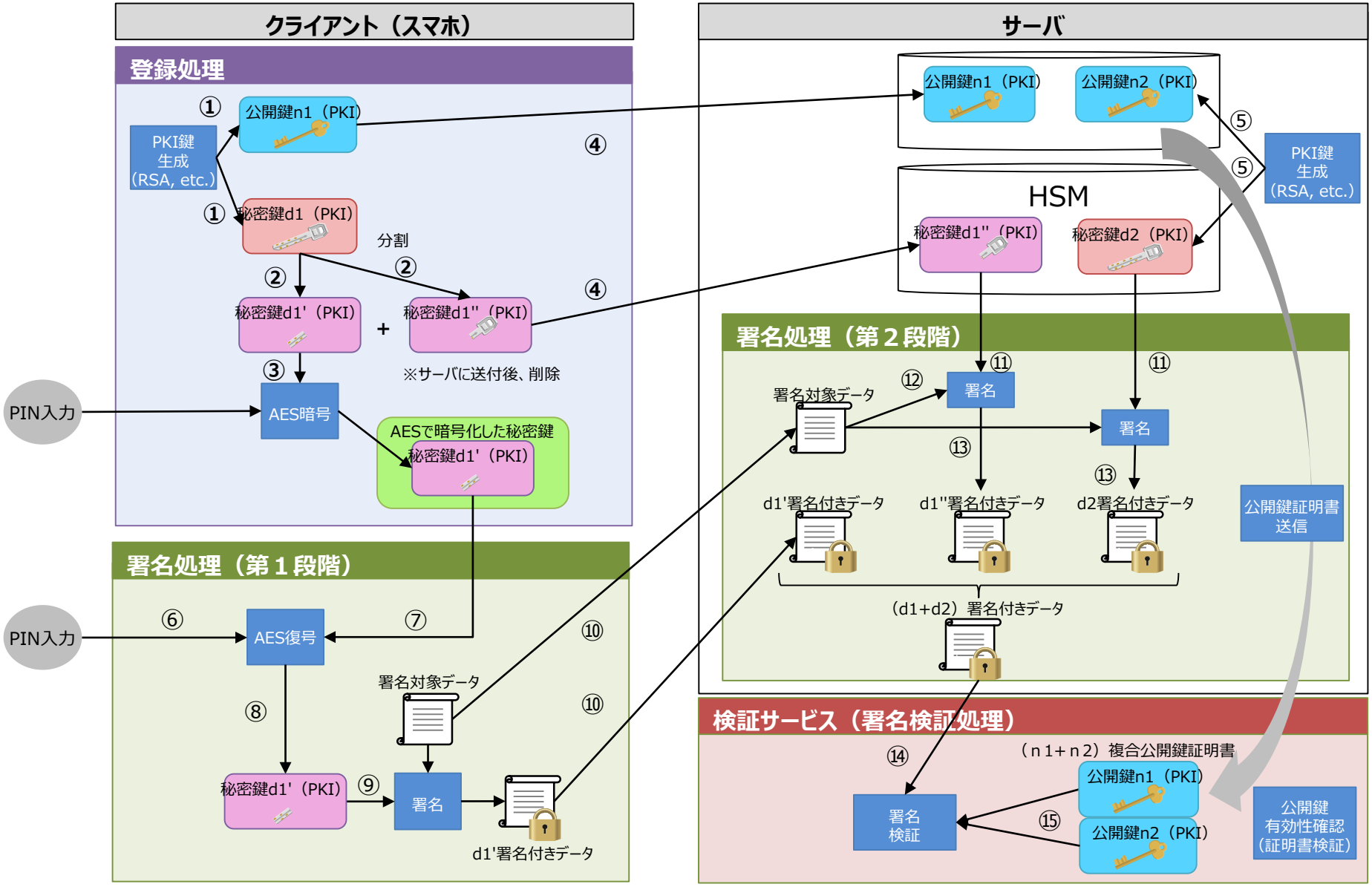
エストニアでは、下図のように国民の秘密鍵を分割し（以下、割符とよぶ）
スマホとサーバ（HSM：耐タンパ性のある専用装置）双方で持つ仕組みを導入しています

1. 電子証明書/秘密鍵をスマホで生成
2. スマホ内で鍵を分割
3. 片方はスマホ内に、もう片方はサーバ（HSM）に
4. サーバ（HSM）で国民の秘密鍵（別鍵d2）を生成



つまり、国民が利用（署名する）際は、
「d1′」「d1″」「d2」の3種類の鍵が必要
どれか1つでも欠落すると電子署名できない

参考資料


クライアント（スマホ）
サーバ
登録処理
PKI鍵
生成
(RSA, etc.)
公開鍵n1（PKI）
秘密鍵d1（PKI）
分割
秘密鍵d1'（PKI）
秘密鍵d1''（PKI）
※サーバに送付後、削除
PIN入力
AES暗号
AESで暗号化した秘密鍵
秘密鍵d1'（PKI）
公開鍵n1（PKI）
公開鍵n2（PKI）
HSM
秘密鍵d1''（PKI）
秘密鍵d2（PKI）
署名処理（第２段階）
署名対象データ
署名
署名
d1'署名付きデータ
d1''署名付きデータ
d2署名付きデータ
公開鍵証明書
送信
（d1+d2）署名付きデータ
署名処理（第１段階）
PIN入力
AES復号
署名対象データ
秘密鍵d1'（PKI）
署名
d1'署名付きデータ
検証サービス（署名検証処理）
（ｎ1+ｎ2）複合公開鍵証明書
公開鍵n1（PKI）
公開鍵n2（PKI）
署名
検証
公開鍵
有効性確認
(証明書検証)

参考資料

◆ エストニアにおけるeIDの電子識別手段のPINについて調査
◆ eIDカード、Mobile-ID、Smart-IDの3方式いずれも数字のみの利用

		PIN設定における桁数	英字利用	大/小文字の区別
eIDカード	認証用PIN	• 4～12桁の数字	**利用無し**	**利用無し**
	署名用PIN	• 5～12桁の数字		
Mobile ID	認証用PIN	• 4～8桁の数字		
	署名用PIN	• 5～8桁の数字		
Smart ID	認証用PIN	• 4～12桁の数字		
	署名用PIN	• 5～12桁の数字		

出典一覧

国名	内容	URL
エストニア	Telia HP	https://www.telia.ee/ru/era/lisateenused/mobiil-id
エストニア	IDカードの利用状況	https://www.soumu.go.jp/main_sosiki/kenkyu/kojin_ninsho/pdf/070201_si4.pdf
エストニア	エストニアの市民ポータルはeesti	https://www.soumu.go.jp/main_content/000495567.pdf
エストニア	スマートIDを利用したサービス一覧	https://www.smart-id.com/services/
エストニア	Smart-ID登録/利用方法	https://www.smart-id.com/lt/apie-smart-id/
エストニア	オンラインバンキングの手続きデモ映像	https://www.smart-id.com/intro/#14
エストニア	スマートID利用動画	https://www.smart-id.com/help/faq/using-smart-id/how-to-switch-between-apps-when-using-smart-id
エストニア	Smart-ID発行時の本人確認等	https://www.smart-id.com/help/faq/registering/registration-methods-for-smart-id/
エストニア	生体認証の利用について	https://www.smart-id.com/help/faq/biometric-identification/biometric-identification-is-it-for-me
エストニア	Smart-ID要件	https://www.smart-id.com/download/
エストニア	Smart-ID登録/利用方法（動画）	https://www.smart-id.com/about-smart-id/
エストニア	電子取引法のための 電子識別および 信頼サービス	https://www.riigiteataja.ee/akt/125102016001
エストニア	身分証明書法	https://www.riigiteataja.ee/akt/113032019066
エストニア	日本・エストニア/EUデジタルソサエティ推進協議会	https://www.jeeadis.jp/jeeadis-blog/9108878
エストニア	Mobile-ID申請手順	https://www.id.ee/en/article/you-wish-to-start-using-mobile-id/
エストニア	モバイルIDの利用フロー	https://www.id.ee/en/article/using-mobile-id/

出典一覧

国名	内容	URL
エストニア	eIDカードPINの桁数	https://www.id.ee/en/article/pin-and-puk-codes-security-recommendations-4/
エストニア	新IDカードがCC認証（EAL5+）取得の仏IDEMIA製品採用	https://www.id.ee/en/article/new-id-card-and-its-changes/
エストニア	Mobile-IDのPINの桁数	https://www.id.ee/en/article/mobile-id-pin-codes/
エストニア	Elisa HP	https://www.elisa.ee/et/eraklient/apid-ja-lisateenused/lisateenused/mobiil-id
エストニア	リモート署名について	https://www.dekyo.or.jp/tbf/data/seminar/180305shiba.pdf
エストニア	Tele2 HP	https://tele2.ee/teenused/mugavusteenused/mobiil-id
エストニア	スマートID40%	https://pencil.schoo.jp/posts/darjQXW9
エストニア	e-estoniaについて	https://e-estonia.com/wp-content/uploads/2828-e-estonia-introduction-presentation-jap-estonian-design-team-19121622.pdf
エストニア	スマートIDについて	https://e-estonia.com/solutions/e-identity/smart-id/
エストニア	Mobile-IDの利用（e-identity）	https://e-estonia.com/solutions/e-identity/mobile-id/
エストニア	Mobile-IDの利用動画	https://courses.cs.ut.ee/2019/infsec/fall/Main/EstonianID-card
エストニア	デジタルIDのCertificate Policies（CP）	https://clicktime.symantec.com/3NHwbaDfvgLkfPgUuVeHnfM7Vc?u=https%3A%2F%2Fwww.skidsolutions.eu%2Fen%2Frepository%2FCP%2F
エストニア	eIDカードの普及率はほぼ100%	https://ascii.jp/elem/000/001/814/1814465/

出典一覧

国名	内容	URL
-	eIDAS電子署名レベル（日本トラストテクノロジー協議会資料）	https://www.soumu.go.jp/main_content/000600452.pdf
-	諸外国における国民 ID 制度の現状等に関する調査研究報告書	https://www.soumu.go.jp/johotsusintokei/linkdata/h24_04_houkoku.pdf
-	AAL判断根拠	https://www.nic.ad.jp/sc-sendai/program/iwsc-sendai-d2-6.pdf
-	電子政府セキュリティガイドライン	https://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf
-	電子認証の保証レベルの条件	https://www.jnsa.org/seminar/pki-day/2015/data/11_hamaguchi.pdf
-	海外事例から見るマイナポータルの活用	https://www.gov-online.go.jp/tokusyu/COVID-19/img/policy/pdf/mynaportal_iwate_06.pdf
-	ポルトガルなどの官民利用などを調査	https://www.government.nl/binaries/government/documents/reports/2015/05/13/international-comparison-eid-means/international-comparison-eid-means.pdf
-	eIDAS電子署名レベル	https://www.docusign.jp/blog/eidas-regulation-and-basic
-	トラストサービス日欧の違い	https://www.dekyo.or.jp/tbf/data/seminar/180305hama.pdf
-	EIDAS と比較した NIST デジタル ID モデルの概要	https://www.cryptomathic.com/news-events/blog/overview-of-the-nist-digital-identity-model-compared-to-eidas
-	EUのeIDAS規則から見えてくる電子契約のあり方	https://jp.globalsign.com/documentsigning/news_column/eidas_190507.html
-	eIDAS電子認証の保証レベル（High,substantial）一般規定（15）	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
-	EUのSSCD および QCD に関する加盟国通知	https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds