

オープンソースな個人番号 カードドライバ



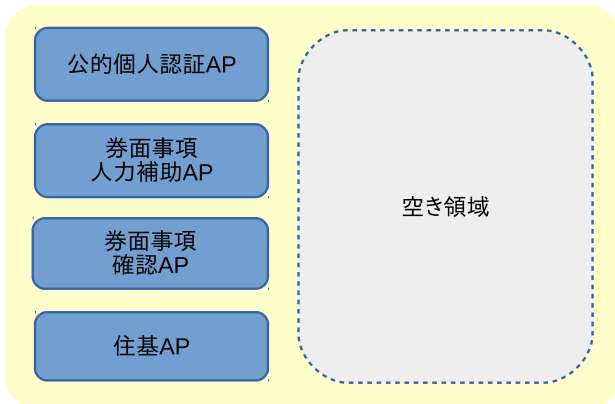
OSSTech

Open Source Solution Technology Corporation

HAMANO Tsukasa <hamano@osstech.co.jp>

OSS コンソーシアム

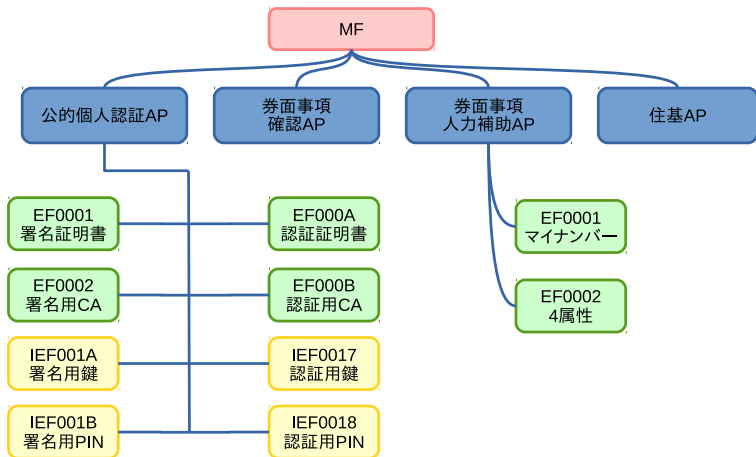
個人番号カード(マイナンバーカード)



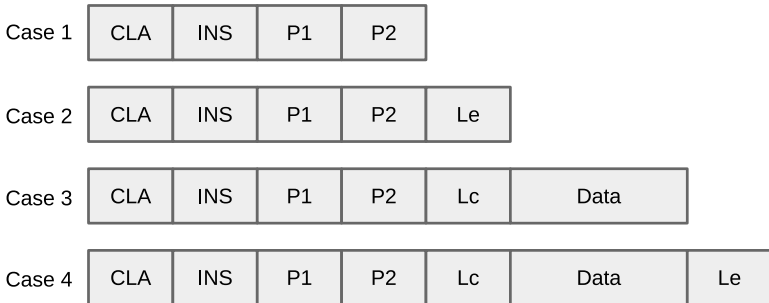
2種類の証明書

- 署名用証明書
 - 身分証明
 - 電子申請
- 利用者認証用証明書
 - 行政・民間サイトでの認証用

データモデル



APDU(ISO 7816-4)



APDU 通信例

```

> 00 A4 02 0C 02 00 01 # SELECT FILEコマンド
> 90 00
< 00 B0 00 00 10 # READ BINARYコマンド
> FF 10 0C XX XX XX XX XX XX XX XX XX XX XX FF

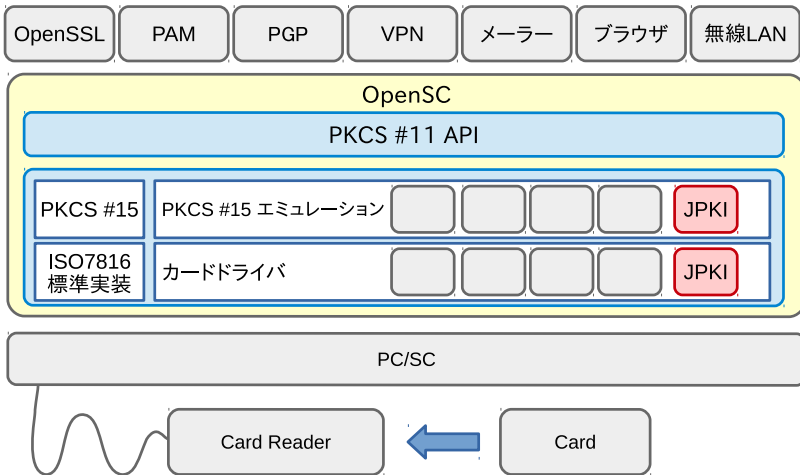
> 00 A4 02 0C 02 00 02 # SELECT FILEコマンド
< 00 B0 00 00 FF # READ BINARYコマンド
> FF 20 82 00 83 DF 21 08 00 10 00 1F 00 79 00 84
> DF 22 0C E6 BF B1 E9 87 8E E3 80 80 E5 8F B8 DF
> 23 57 E6 9D B1 E4 BA AC E9 83 BD E5 A4 A7 E7 94
> B0 E5 8C BA XX XX XX XX XX XX XX XX XX XX XX
> XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
> XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
> XX XX XX XX XX XX XX XX XX XX DF 24 08 YY YY YY YY
> MM MM DD DD DF 25 01 31 FF FF FF FF FF FF FF FF

```

ロードマップ

- プロトコル仕様の解析
- OpenSC カードドライバ開発
- オープンな PKCS#11 実装
- PKCS#15 カードエミュレーション
- 公的個人認証の普及

OpenSC スタック



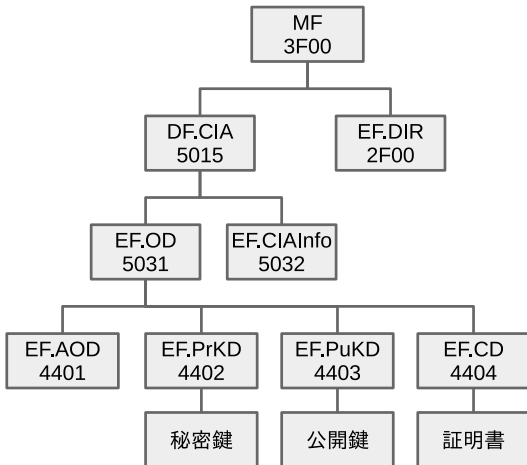
OpenSCカードドライバ

- esteid(エストニア)
- Belpic(ベルギー)
- DNle(スペイン)
- CNS(イタリア)
- pteID(ポルトガル)
- PIV(米国)

PKCS#11 APIs

- C_Initialize()
- C_Finalize()
- C_GetInfo()
- C_Sign()
- C_Verify()
- C_Encrypt()
- C_Decrypt()

PKCS#15 エミュレーション



マイナンバーカードでSSH

<https://www.osstech.co.jp/~hamano/posts/jpki-ssh/>



仕様を隠さないで

- 安全性の為に
- 普及の為に

目指すべき社会

- 電子先進国 (エストニア・ベルギー)
 - オープン・スタンダード
 - オープン・ソース
 - OS・ブラウザ非依存
 - 普及率・利用率が高い
- 電子後進国 (日本)
 - 仕様が非公開
 - クローズドソース
 - Java Applet(笑)

課題


- 運用に対する不安
 - マイナンバーに対する不信
 - 鍵生成の仕組み
 - 仕様公開されないと安心できない
- 失効情報の検証
 - 総務大臣の認可
- 名寄せの問題
 - 信頼できる ID Provider が必要
 - 複数の鍵管理

github.com/open-eid

The screenshot shows the GitHub repository page for 'Open Electronic Identity'. At the top, there is a search bar with 'This organization' and a search input field. To the right are links for 'Pull requests', 'Issues', and 'Gist', along with notification and user icons. The repository name 'Open Electronic Identity' is displayed with a logo and a description: 'Estonian Electronic Identity Software'. Below this, location and contact information are provided: 'Tallinn, Estonia', a website link 'https://www.ria.ee/public...', and an email 'martin.paljak@ria.ee'. The main content area is divided into 'Repositories' and 'People'. The 'Repositories' section has a search bar and a list of repositories with their names, languages, star counts, and fork counts. The 'People' section shows a profile for 'martinpaljak' (Martin Paljak).

This organization Search

Pull requests Issues Gist

 **Open Electronic Identity** ⓘ

Estonian Electronic Identity Software

Tallinn, Estonia <https://www.ria.ee/public...> martin.paljak@ria.ee

Repositories People 1

Filters Find a repository...

SiVa Java ★ 6 🍴 1

Signature Verification Service

Updated 4 hours ago


digidoc4j Java ★ 23 🍴 8

DigiDoc for Java. Javadoc:

Updated 4 hours ago

firefox-pkcs11-loader CMake ★ 2 🍴 0


People 1 >

 **martinpaljak**
Martin Paljak

github.com/JPKI

The screenshot shows the GitHub organization page for JPKI. At the top, there is a navigation bar with "This organization" and a search box, and links for "Pull requests", "Issues", and "Gist". The organization's profile includes a logo of a white rabbit holding a red number 1, the name "JPKI", and the description "Software for Japanese Individual Number Card" with a location tag for "Japan". Below the profile are tabs for "Repositories", "People", "Teams", and "Settings". The "Repositories" section features a search bar, a "New repository" button, and a list of repositories. Two repositories are visible: "jinc" (forked from hamano/jinc, 0 stars, 1 fork) and "OpenSC" (forked from OpenSC/OpenSC, 0 stars, 250 forks). A "People" sidebar on the right shows a member named "hamano" (HAMANO Tsukasa) with an "Invite someone" button.

This organization Pull requests Issues Gist

 **JPKI**
Software for Japanese Individual Number Card
Japan


Repositories **People** 1 Teams 1 Settings

Filters [New repository](#)

jinc Go ★ 0 🍴 1
🍴 forked from hamano/jinc
MyNumber Card Utility
Updated 11 hours ago

OpenSC C ★ 0 🍴 250
🍴 forked from OpenSC/OpenSC
Open source smart card tools and middleware. PKCS#11/MiniDriver/Tokened
Updated 11 hours ago

People 1 >

 **hamano**
HAMANO Tsukasa

[Invite someone](#)

jinc コマンド

<https://github.com/hamano/jinc>

```
$ jinc
```

