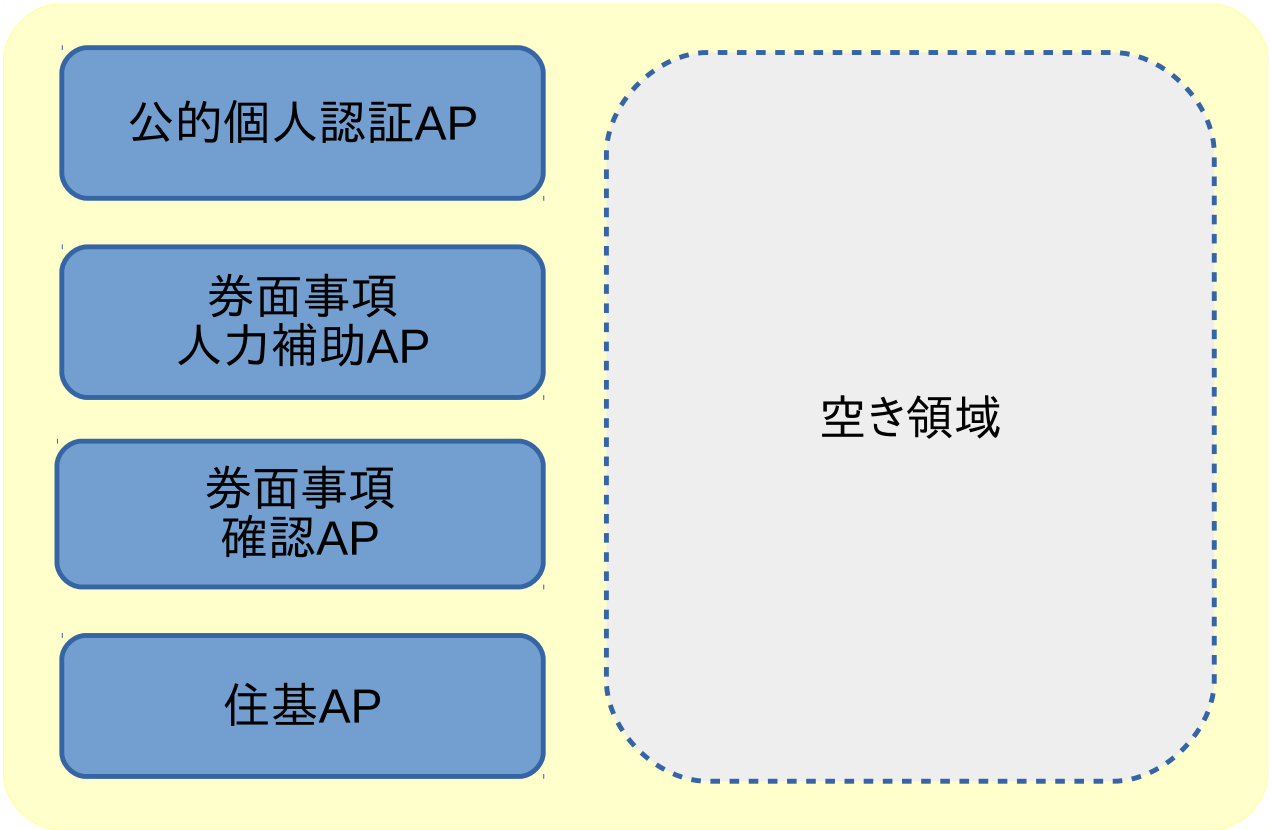
オープンソースな個人番号カードドライバ

Open Source Solution Technology Corporation
HAMANO Tsukasa <hamano@osstech.co.jp>
OSS コンソーシアム

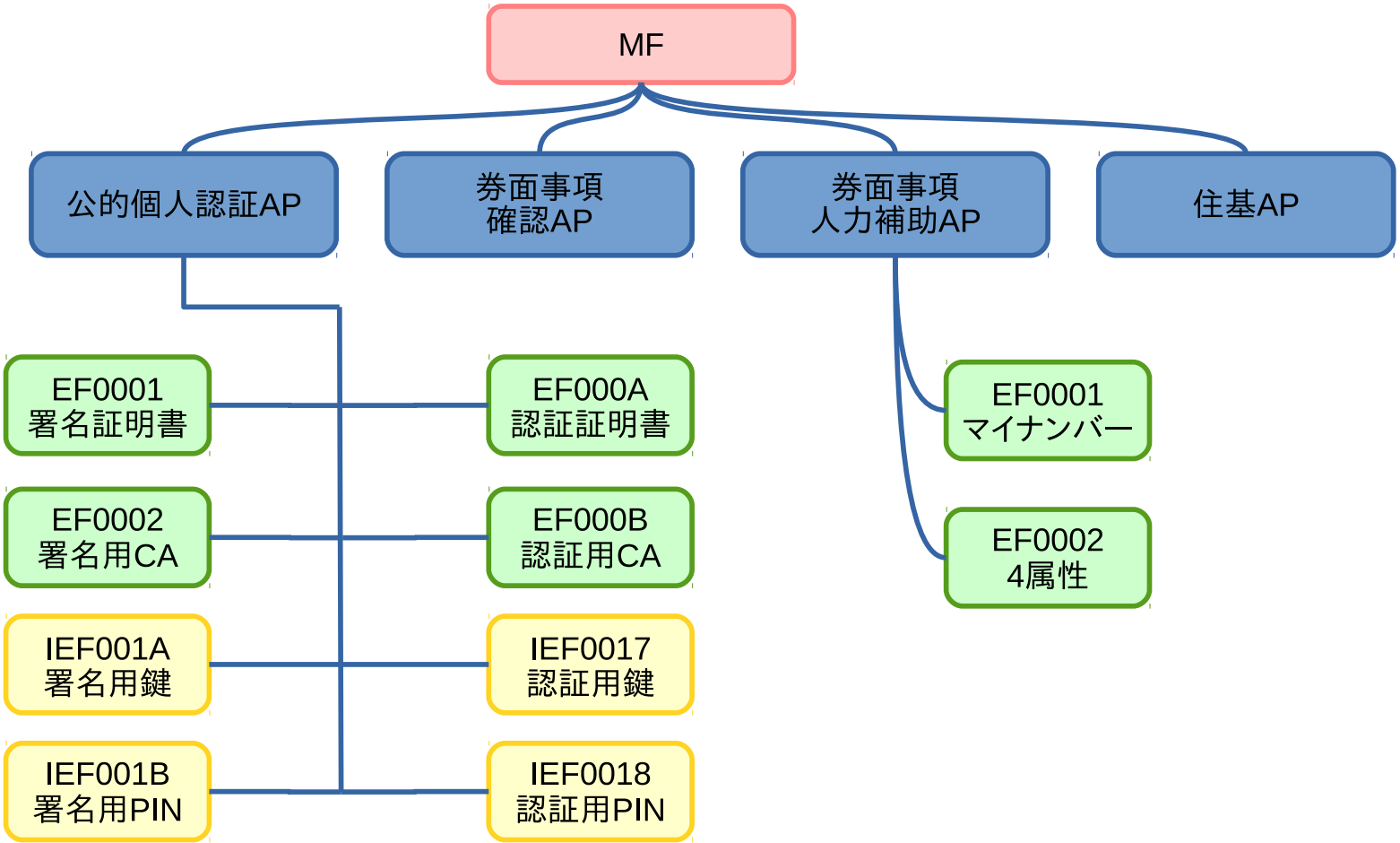
個人番号カード(マイナンバーカード)



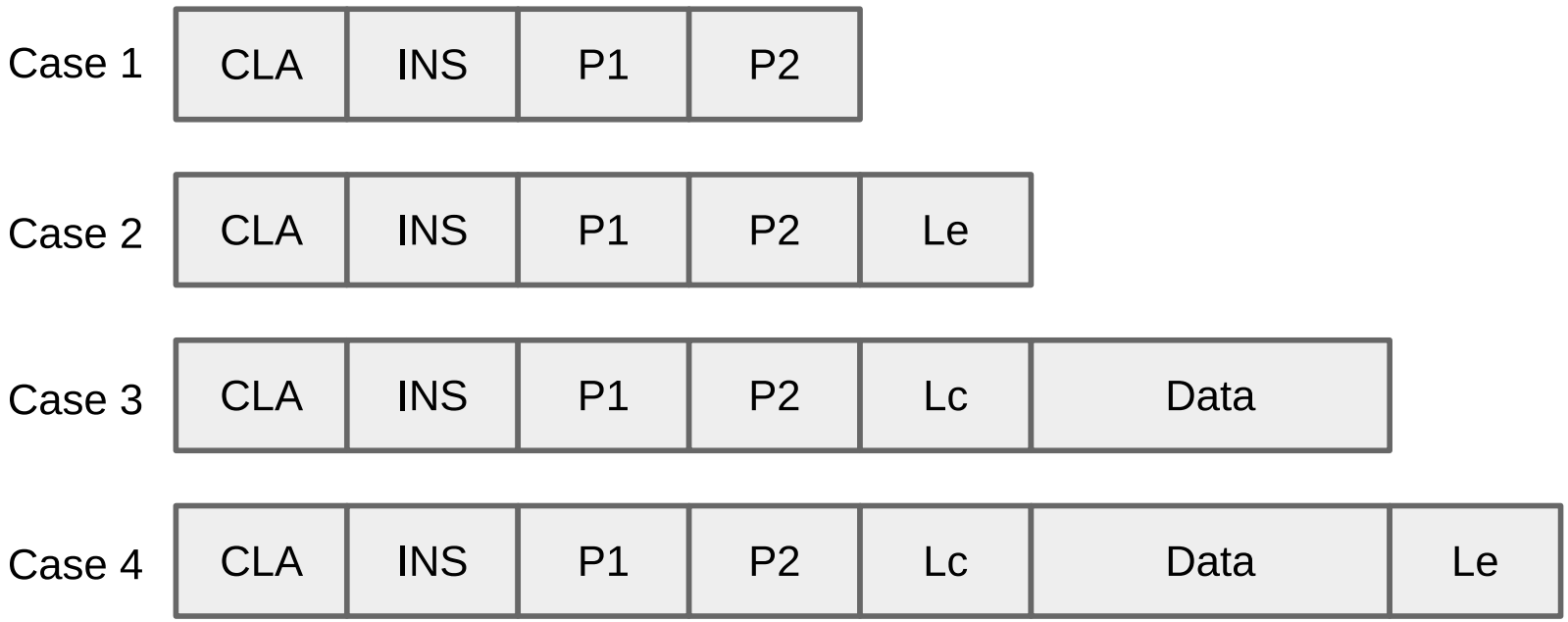
2種類の証明書

- 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


MF
公的個人認証AP
券面事項
確認AP
券面事項
人力補助AP
住基AP
EF0001
署名証明書
EF0002
署名用CA
IEF001A
署名用鍵
IEF001B
署名用PIN
EF000A
認証証明書
EF000B
認証用CA
IEF0017
認証用鍵
IEF0018
認証用PIN
EF0001
マイナンバー
EF0002
4属性

APDU(ISO 7816-4)



APDU通信例

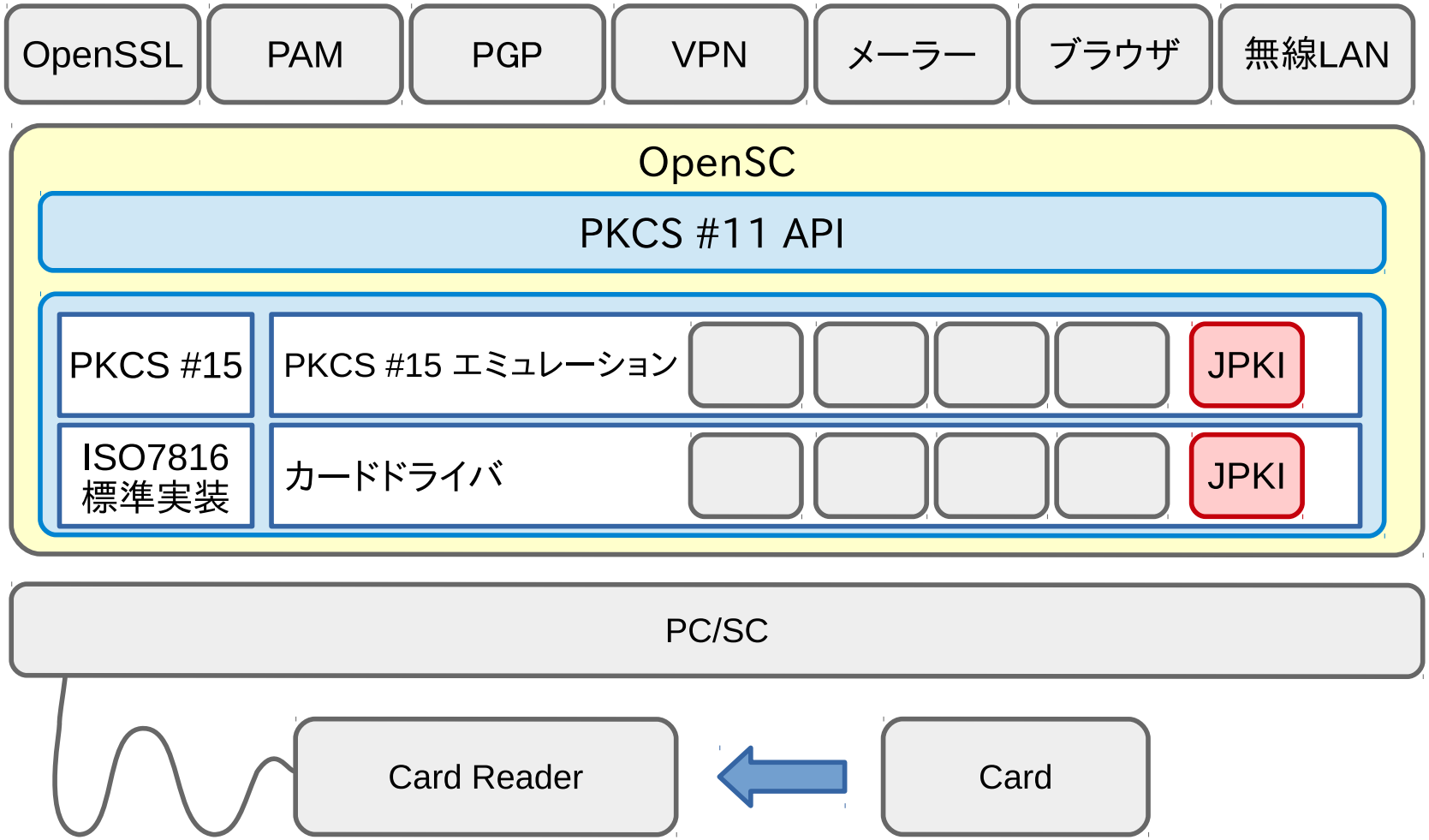
```
> 00 A4 02 0C 02 00 01 # SELECT FILEコマンド
> 90 00
< 00 B0 00 00 10       # READ BINARYコマンド
> FF 10 0C XX XX XX XX XX XX XX XX XX XX XX FF

> 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 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


OpenSSL
PAM
PGP
VPN
メーラー
ブラウザ
無線LAN
OpenSC
PKCS #11 API
PKCS #15
PKCS #15 エミュレーション
JPKI
ISO7816
標準実装
カードドライバ
JPKI
PC/SC
Card Reader
Card

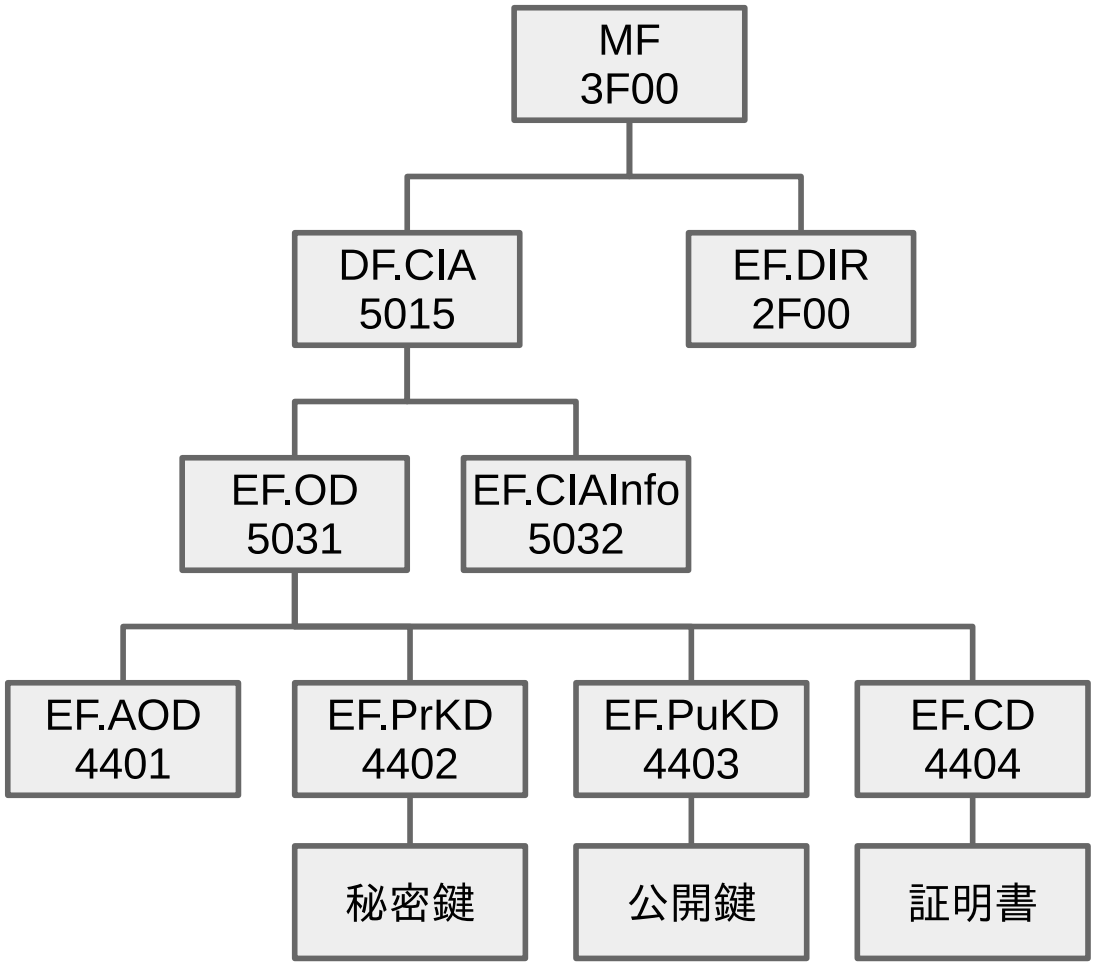
OpenSCカードドライバ

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

PKCS#11 APIs

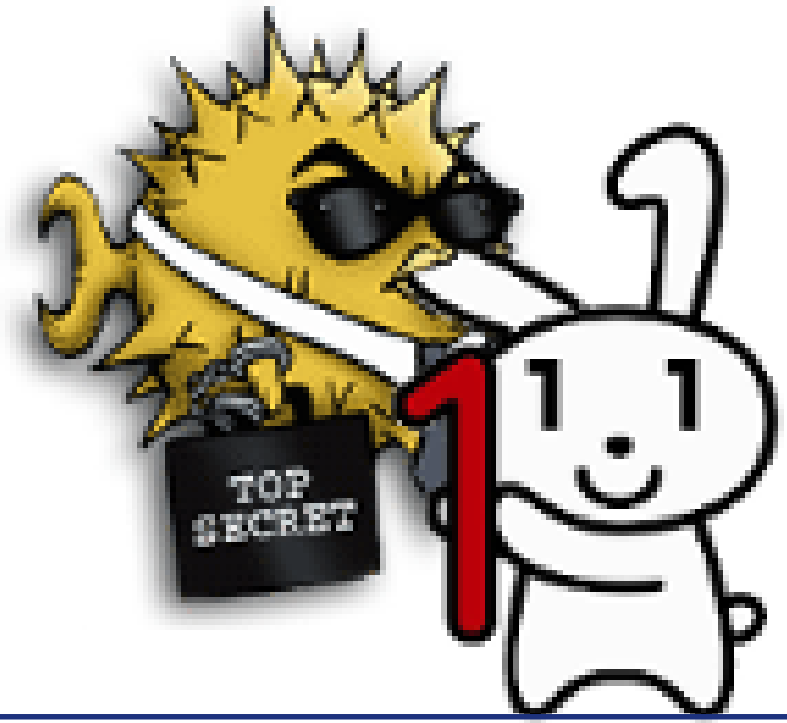
- C_Initialize()
- C_Finalize()
- C_GetInfo()
- C_Sign()
- C_Verify()
- C_Encrypt()
- C_Decrypt()

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

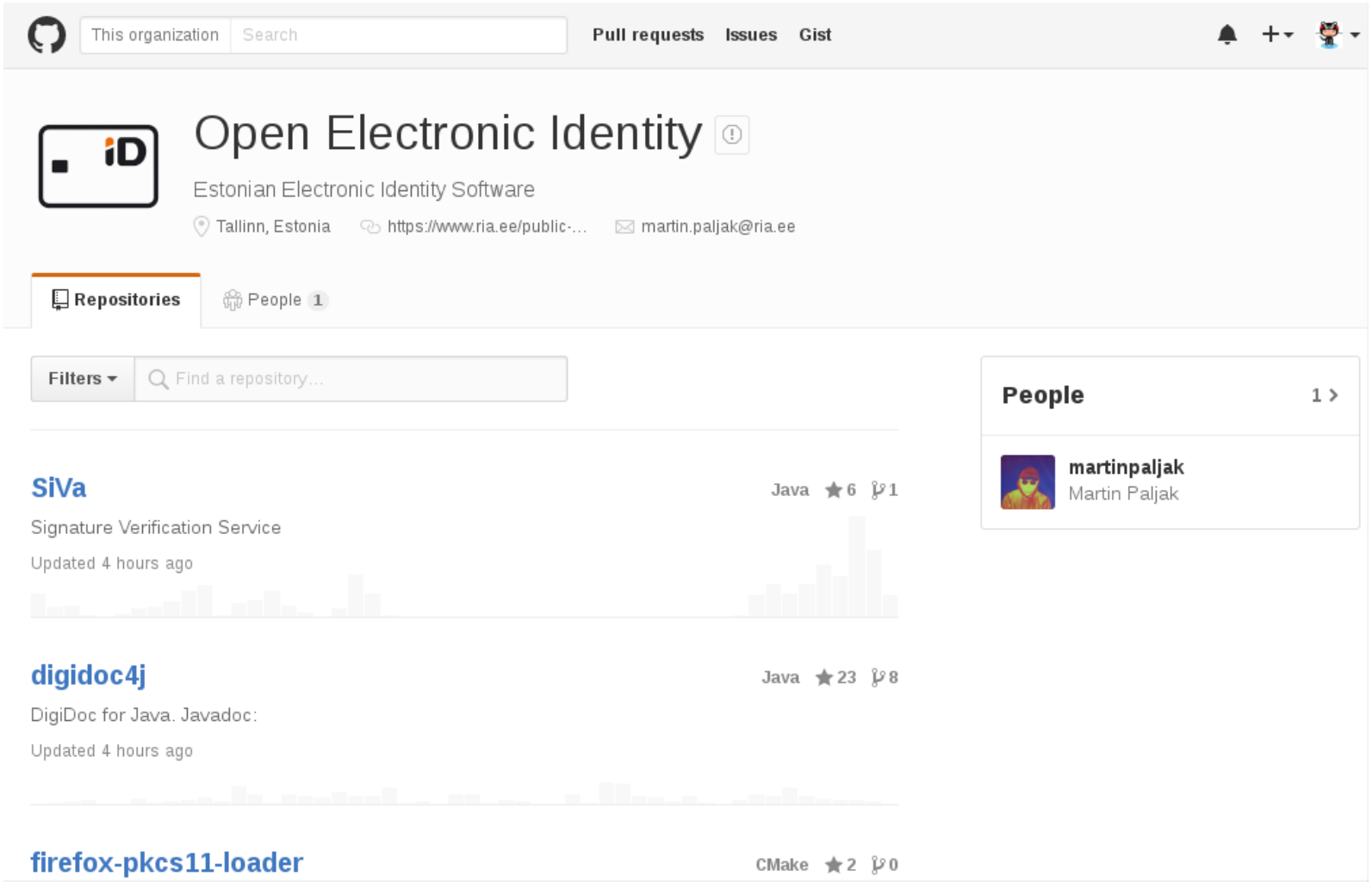
目指すべき社会

- 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)

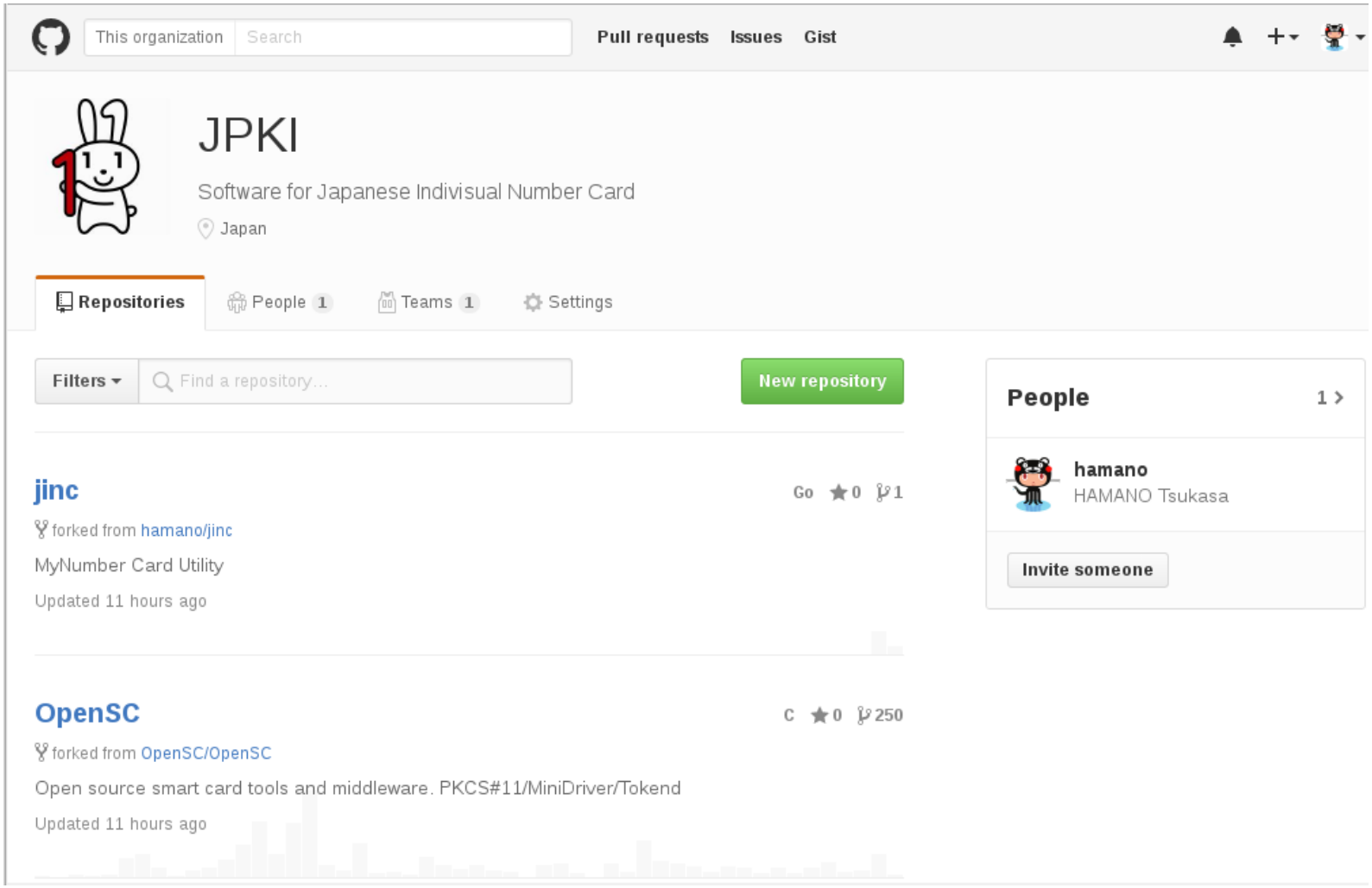
課題

- 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



github.com/JPKI



jincコマンド

https://github.com/hamano/jinc

```
$ jinc
```