



eObčanka veřejná



WARNING

**VSTUP NA
VLASTNÍ
RIZIKO**



Agenda

- Vlastnosti eObčanky a jak se používá
- Architektura
- Java knihovna k eObčance
- Inspirace
- Otázky





Vlastnosti eObčanky

- Vzdálená identifikace
- Podepisování kvalifikovaným certifikátem
- Obsahuje strojově čitelné údaje
- Obsahuje privátní klíč, kterým lze při znalosti PINu podepisovat.
- Neobsahuje fotografii



Elektronické služby
finanční správy ČR



Portál eRecept -
elektronická preskripce



Portál národního bodu



ePortál ČSSZ



Portál občana

KLÍČ K ELEKTRONICKÝM SLUŽBÁMČesky

18. ledna 2019

Přihlášení občanským průkazem

Přihlašování prostřednictvím občanského průkazu smí využívat pouze osoby starší 15 let.

Přihlášení prostřednictvím nového občanského průkazu vydaného po 1. 7. 2018, který obsahuje čip a jeho elektronická funkcionality byla aktivována. Pro přihlášení tímto občanským průkazem je zapotřebí čtečka dokladů a nainstalovaný příslušný software. Pokud chcete pokračovat v přihlášení svým občanským průkazem, klikněte na tlačítko „Přihlásit“.

Více informací o přihlašování prostřednictvím občanského průkazu jsme pro Vás připravili na našich [informačních stránkách](#).



Přihlásit



Aplikace a PINy

Identifikační klient

Identifikace občanským průkazem

Datum a čas
26.10.2018 17:54:52

ID transakce
f0f9d3b6-4456-44de-9abc-315c632fb458

Zadáním hodnoty IOK udělujete souhlas s provedením identifikace

Zadejte identifikační osobní kód

Zadejte hodnotu IOK pomocí klávesnice počítače. Po zadání IOK stiskněte tlačítko OK

OK Zrušit

Správce karty

eObčanka - Správce karty

Soubor Zobrazení Nástroje nápověda

Gemplus USB Smart Card Reader

ČÍPOVÁ KARTA

Číslo karty:

Typ karty: eOP CZE v2.1

Informace o přístupových kódech

Název:	Stav:	Počet použitých pokusů:	Délka (min/max):
PIN	zablokovaný (nelze odblokovat)	3 ± 3	5 - 15
PUK	neinicializovaný (nastavit)	3 ± 5	6 - 15
QPIN	zablokovaný (nelze odblokovat)	3 ± 3	5 - 15
IOK	platný (změnit)	0 ± 3	4 - 10
DOK	platný (změnit)	0 ± 10	4 - 10

Zaplnění karty

RSA max. 4096 b.	RSA max. 4096 b.
RSA max. 4096 b.	RSA max. 4096 b.
RSA max. 4096 b. (el. podpis)	RSA max. 4096 b. (el. podpis)
RSA max. 4096 b. (el. podpis)	RSA max. 4096 b. (el. podpis)
ECC max. 521 b.	ECC max. 521 b.
ECC max. 521 b.	ECC max. 521 b.
ECC max. 521 b. (el. podpis)	ECC max. 521 b. (el. podpis)
ECC max. 521 b. (el. podpis)	ECC max. 521 b. (el. podpis)

Nastavit PUK Odblokovat IOK

Změnit DOK Změnit IOK

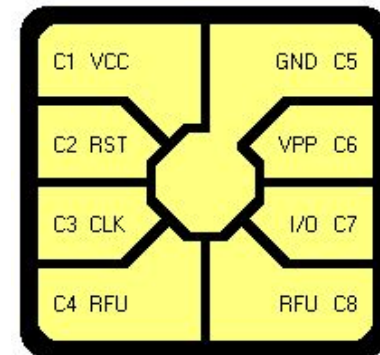
PINy

- BOK - Bezpečnostní osobní kód (4-10) pouze fyzick
- IOK - Identifikační osobní kód (4-10 číslic)
- DOK - deblokační osobní kód (4-10 číslic)
- PIN - pin (5-10)
- QPIN (asi od qualified PIN)
- PUK (PIN Unblocking Key) - (8-15 číslic)

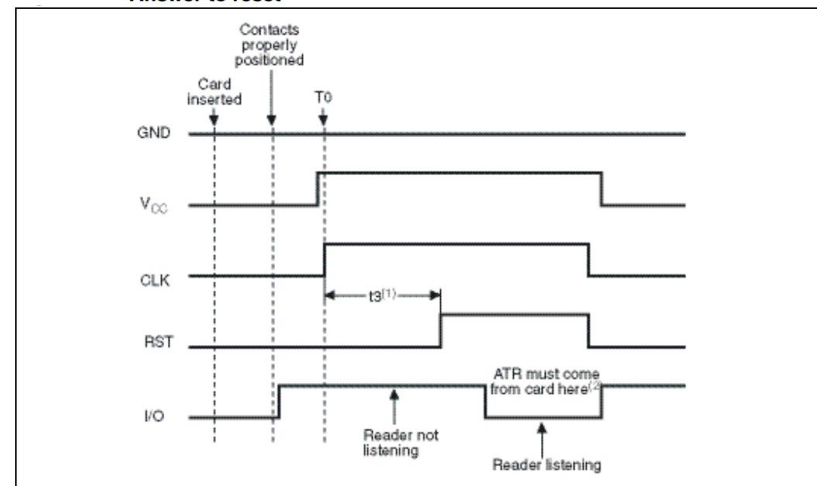


Architektura - Čip

- Kontaktní čip M7892 G12 od společnosti Infineon
- 3 Applety:
 - Systémový
 - Identifikační
 - Podepisovací - IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4 (Gemalto)
- Standard ISO 7816, CCID (Chip Card Interface Device)
- Memory 300 kBytes SOLID FLASH™ + 8 kBytes RAM
- CPU Dual 16-bit + šifrovaná RAM
- Symetrické šifrování DES, 3DES, AES up to 256-bit
- Asymetrické šifrování RSA up to 4096-bit, ECC up to 521-bit
- -25 to + 85 °C
- Pravděpodobně má ROCA zranitelnost



Answer to reset



1. $t_3 = 40\,000$ clock cycles.

2. ATR must be issued by card between 400 clock cycles and 40 000 clock cycles after RST goes high.



Architektura - APDU

Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le

CLA (1 byte): Třída.

INS (1 byte): Instrukce

P1 (1 byte): Parametr 1

P2 (1 byte): Parametr 2

Lc (1 byte): Volitelné pole, počet bajtů v poli Data

Data pole Toto volitelné pole obsahuje data

Le (1 byte): Volitelné. Určuje maximální počet bajtů v odpovědi.



Case 1:
No Command data,
No Response required

CLA	INS	P1	P2
-----	-----	----	----

Case 2:
No Command data,
Yes Response required

CLA	INS	P1	P2	Le
-----	-----	----	----	----

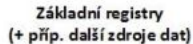
Case 3:
Yes Command data,
No Response required

CLA	INS	P1	P2	Lc	Data Field
-----	-----	----	----	----	------------

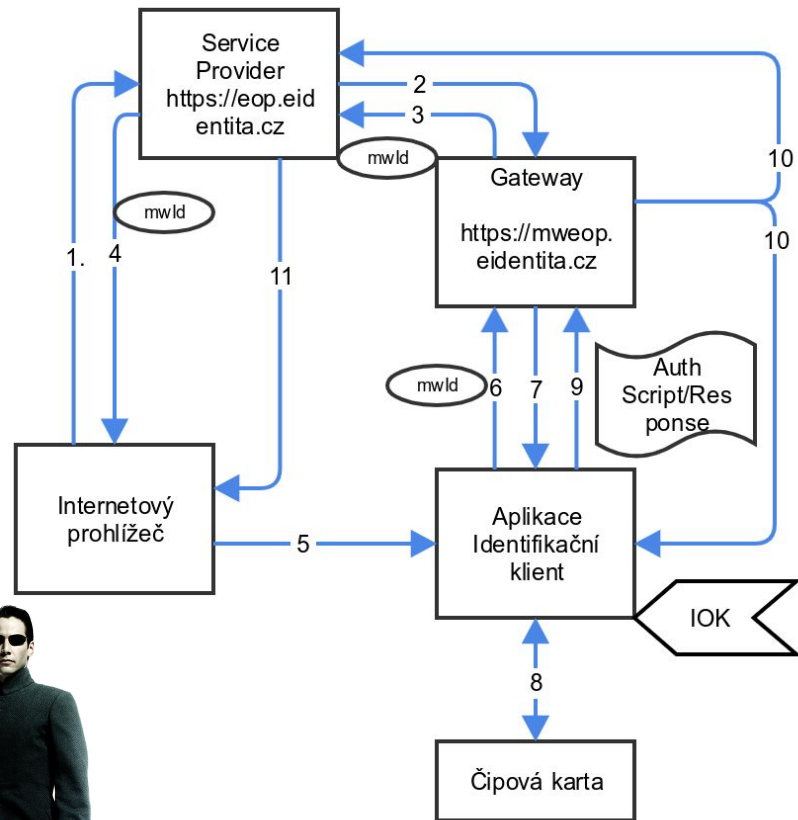
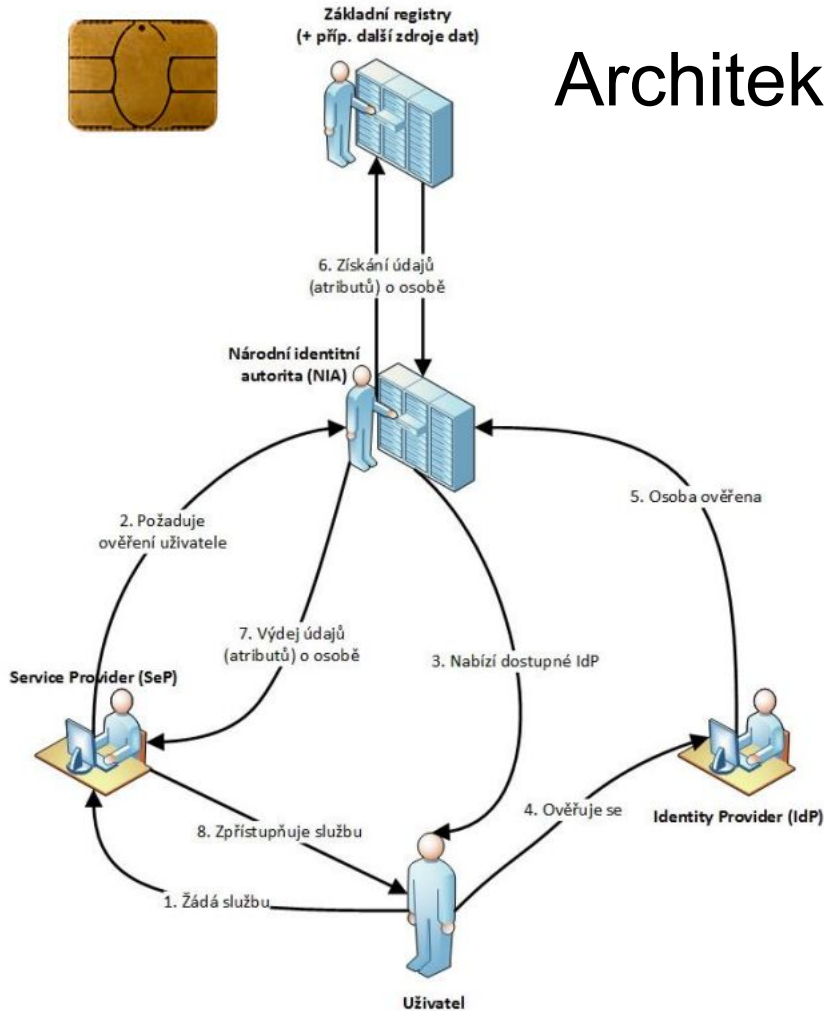
Case 4:
Yes Command data,
Yes Response required

CLA	INS	P1	P2	Lc	Data Field	Le
-----	-----	----	----	----	------------	----

Response APDU		
Body (optional)		Trailer (required)
Data Field		SW1 SW2



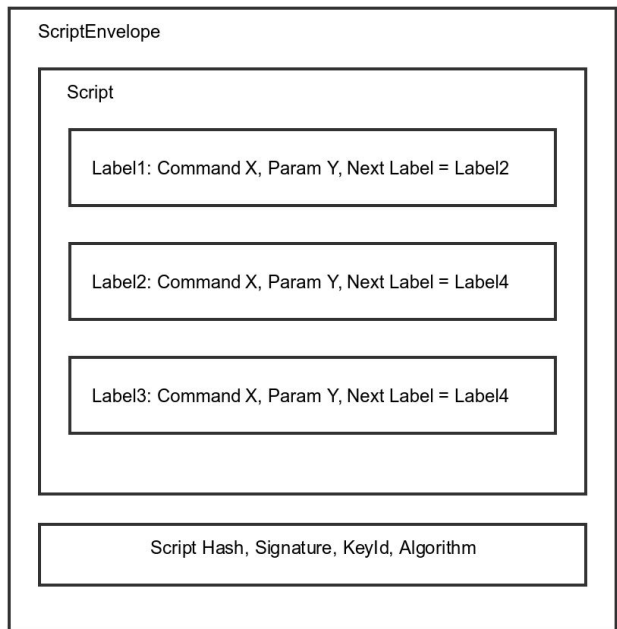
Architektura - Infrastruktura



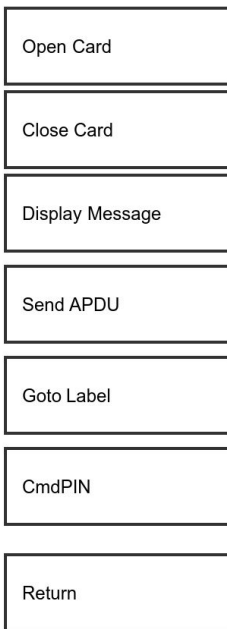


Architektura - Skripty

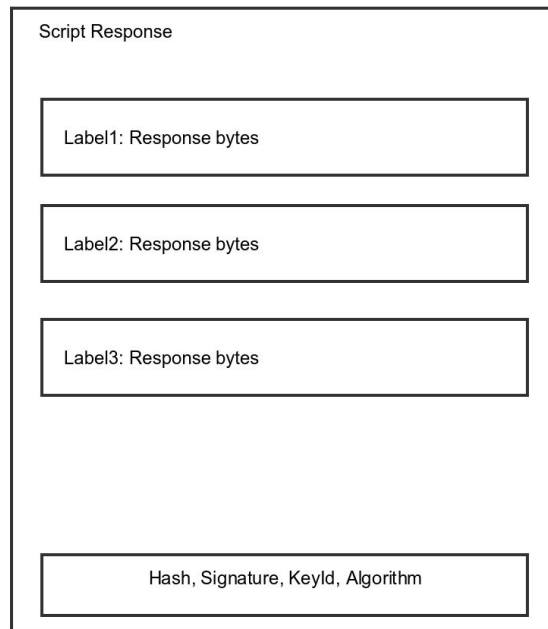
Skript - zadání úlohy



Příkazy



Odpověď - odeslání výsledků



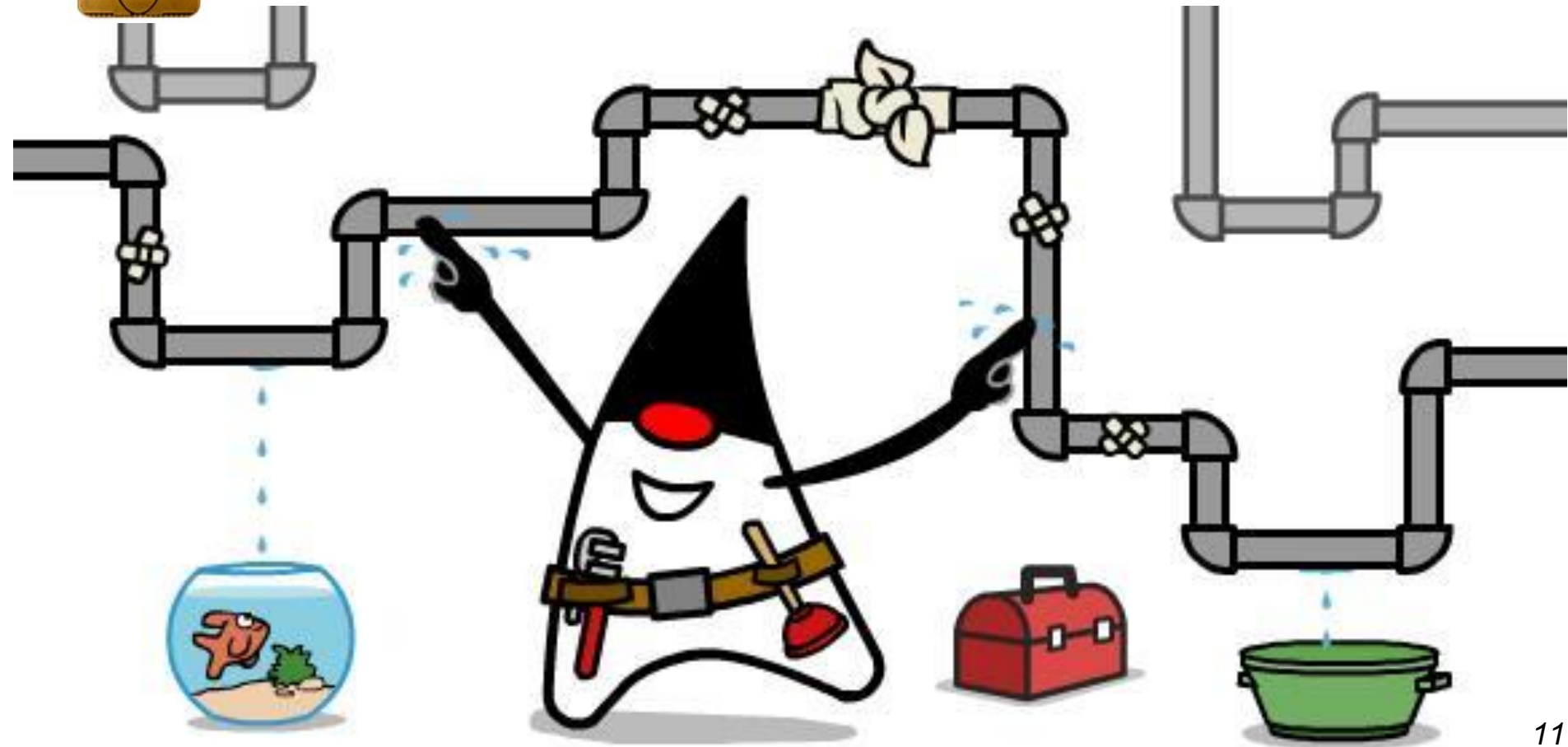


Další obsah karty

- Tagy - počet pokusů, sériové číslo certifikátu, číslo klíče
- Identifikátory aplikací
 - 0xD2, 0x03, 0x10, 0x01, 0x00, 0x01, 0x00, 0x02, 0x02 - **Správa karty**
 - 0xD2, 0x03, 0x10, 0x01, 0x00, 0x01, 0x03, 0x02, 0x01, 0x00 - **Identifikace**
- Soubory - certifikáty
 - Krátký - Autorizační - sériové číslo (číslo občanky)
 - Dlouhý - Identifikační - sériové číslo, jméno, příjmení, pohlaví, stav, adresa, rodné číslo
- Secure Messaging



Java knihovna





Java knihovna

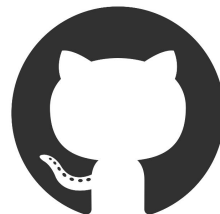
<https://github.com/ParalelniPolis/obcanka-public/java>

Repozitář si nejdříve forkněte, usnadní vám to vytváření pull requestů se změnami.

Členění knihovny:

- core - základní funkce
- desktop_lib - funkce specifické pro desktop
- android_lib - funkce specifické pro android
- desktop_app - příkladové desktop aplikace
 - HelloWorld
 - Authenticate
- android_app - příkladová android aplikace
- tools - různé nástroje

Apache Licence





Java knihovna - příklad

```
public class HelloWorld {
    public static void main(String[] args) {
        DesktopCardInterface ci = DesktopCardInterface.create();
        try {
            downloadCertificates(ci);
        } catch (CardException e) {
            e.printStackTrace();
        }
    }

    private static void downloadCertificates(ICardInterface ci) throws CardException {
        Card cm = new Card(ci);
        String cardID = cm.getCardNumber();
        System.out.println("cardID = " + cardID);
        System.out.println("iokState = " + cm.getIokState());
        System.out.println("cm.getIokTryLimit() = " + cm.getIokTryLimit());

        Certificate longCert = cm.getCertificate(Certificate.CertificateType.IDENTIFICATION);
        Certificate shortCert = cm.getCertificate(Certificate.CertificateType.AUTHORIZATION);
        try {
            FileOutputStream fos = new FileOutputStream("long.crt");
            fos.write(longCert.getData());
            fos.close();
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```




Java knihovna - důležité třídy

I	ICardInterface
(m)	transmit(ICommandAPDU) IResponseAPDU
(m)	createCommand(byte[]) ICommandAPDU
(m)	getATR() byte[]

↑

C	DesktopCardInterface
(m)	getCardTerminalWithCard() CardTerminal
(m)	create() DesktopCardInterface
(m)	create(Card) DesktopCardInterface
(m)	destroy() void
(m)	getATR() byte[]
(m)	transmit(ICommandAPDU) IResponseAPDU
(m)	createCommand(byte[]) ICommandAPDU

C	Card
(m)	Card(ICardInterface)
(m)	selectApplication(byte[]) boolean
(m)	getCardNumber() String
(m)	getSerialNumber() byte[]
(m)	getKeyChecksumValue() byte[]
(m)	getData(int, int) byte[]
(m)	getDokState() DokState
(m)	getDokTryLimit() int
(m)	getDokMaxTryLimit() int
(m)	getIokState() IokState
(m)	getIokTryLimit() int
(m)	getIokMaxTryLimit() int
(m)	changePIN(PINType, String, String) CardAuthorizationResult
(m)	unblockIOK(String, String) CardAuthorizationResult
(m)	getCertificate(CertificateType) Certificate
(m)	readFile(int) byte[]
(m)	createEncryptionToken() EncryptionToken



Java knihovna - důležité třídy

I	IResponseAPDU	
(m)	getData()	byte[]
(m)	getSW()	int
(m)	getSW1()	int
(m)	getSW2()	int
(m)	getBytes()	byte[]

I	ICardInterface	
(m)	transmit(ICommandAPDU)	IResponseAPDU
(m)	createCommand(byte[])	ICommandAPDU
(m)	getATR()	byte[]

I	ICommandAPDU	
(m)	getData()	byte[]

C	CardException	
----------	----------------------	--

C	Client	
(m)	getSessionState(String)	State
(m)	getMWID()	String
(m)	askGateway(String, byte[])	GatewayResponse

C	ScriptPlayer	
(m)	ScriptPlayer(ScriptExecutor, Client)	
(m)	start()	boolean

C	ScriptExecutor	
(m)	ScriptExecutor(ICardInterface)	
(m)	getCardInterface()	ICardInterface
(m)	execute(ScriptEnvelope, IUIEntryProvider)	ScriptResponse



Inspirace

- Dokumentace
- Knihovny v jiném jazyce
- Podpora pro jiné platformy: iOS, OSX
- Open-source klon existující aplikace
- Zranitelnost
- Podpůrné nástroje: Emulátor karty, Síťová karta
- Infrastruktura: Síťová karta, Proxy, Gateway
- Přihlašování na web
- Javascript WebUSB podpora
- Zařízení používající občanku
- Volební systém

