

Technická zpráva

Čipové technologie v prostředí VŠ pro ID-karty a aplikace s elektronickým podpisem

CESNET, z.s.p.o., CoProSys, a.s.

Praha 2004

ABSTRAKT

Zpráva podává přehled čipových technologií pro digitální identifikaci (ID) a PKI využitelných v prostředí vysokých škol a akademické obce. Jde o dílčí výstup projektové aktivity, zastřešené sdružením Cesnet ve spolupráci s CoProSys, která se soustřeďuje na tyto úkoly:

-řešit technickou stránku integrace čipových karet do systémů PKI provozovaných v rámci akademické komunity včetně PKI/CA CESNET.

-v součinnosti se „Skupinou pro ID-karty“ přispět k technickému řešení jednotného elektronického studentského průkazu.

Tyto úkoly zpráva diskutuje v několika částech:

-Provedena stručná klasifikace čipových technologií a jejich standardů zaměřená na současnou generaci produktů (2003/2004) a na pozorovatelné průmyslové trendy. Podrobněji se text věnuje technologii čipových produktů standardizovaných podle ISO/IEC7816/14443, s duálním rozhraním, které mají předpoklad využití ve vysokoškolské praxi. Text zmiňuje přípravu čipové personalizace, kryptoovladačů a správu klíčů.

-Požadavky na funkčnost ID-karet přijaté „Skupinou pro ID-karty“ jsou přeloženy do požadavků na technickou specifikaci.

-Probrány zkušenosti s výběrem a testováním typu karty, která splňuje požadavky na funkčnost a vykazuje zpětnou kompatibilitu s Mifare pro starší aplikace.

-Předložena struktura aplikací na kartě, návrh na pilotní ověření karty a vstupy k problematice middleware pro host/PC/.

-Uvedena reference průmyslových standardů, organizací, některá fóra, iniciativy. Přehled výrobců čipů, karet, komponent a dodavatelů karetních řešení.

Část výsledků byla prezentována v rámci stejnojmenného semináře CESNET.

POUŽITÉ ZKRATKY

(podrobnější přehled pojmů a terminologie viz příloha Terminogie)

AID	Application Identifier (ID pro karetní aplikaci podle ISO 7816-5)
APDU	Application Protocol Data Unit, příkazový protokol (request – response) pro výměnu dat „karta – host“
CICC	Contactless Integrated Chip Card, název bezkontaktní karty podle ISO, viz též PICC
COS	Card Operating System
DF	Dedicated File (Adresář v souborovém systému karty) (ISO 7816)
EF	Elementary File (Soubor na kartě) buď typu „Internal EF“ nebo „Working EF“ (podle ISO 7816)
FID	File Identifier pro MF, DF, EF (podle ISO 7816)
IFD	Interface Device, akronym snímače/terminálu pro kartu podle ISO
ISF	Internal Security File, speciální typ „internal EF“ pro uložení soukromého klíče, podle G&D
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
MF	Master File (Speciální typ DF, root adresář na kartě) (ISO 7816)
PCD	(Proximity Coupling Device) - bezkontaktní snímač na frekvenci 13,56MHz splňující ISO 14443
PICC	Proximity Integrated Circuit Card, subtyp CICC

Poznámka: Pro potřeby této zprávy namísto „certifikát X.509 s dvojicí soukromého a veřejného klíče“ bude občas užit stručný termín „digitální ID“, pokud nebude na úkor přesnosti.

OSNOVA

ABSTRAKT	2
POUŽITÉ ZKRATKY	4
OSNOVA.....	5
OBSAH.....	6
SEZNAM OBRÁZKŮ A TABULEK	8
1 ÚVOD.....	9
2 RÁMEC ÚKOLU PRO PKI	11
3 POŽADAVKY NA TECHNICKÉ VLASTNOSTI A FUNKČNOST ID-KARTY	15
4 KLASIFIKACE ČIPOVÝCH TECHNOLOGIÍ	20
5 ID-KARTA S DUÁLNÍM ROZHRANÍM	38
6 INFRASTRUKTURA SMART KARET	55
7 PROFIL TECHNICKÉ PŘÍPRAVY ČIPOVÉ MIGRACE	61
8 ZÁVĚR	83
9 PŘÍLOHA Č.1 SPECIFIKACE, NORMY A PRŮMYSLOVÉ STANDARDY	84
10 PŘÍLOHA Č. 2 INICIATIVY, FÓRA, ORGANIZACE	91
11 PŘÍLOHA Č. 3 ODKAZY NA VÝROBCE A PRŮMYSL ČIPOVÝCH TECHNOLOGIÍ.....	93
12 TERMINOLOGIE	104
13 LITERATURA	109

OBSAH

ABSTRAKT	2
POUŽITÉ ZKRATKY	4
OSNOVA.....	5
OBSAH.....	6
SEZNAM OBRÁZKŮ A TABULEK	8
1 ÚVOD.....	9
2 RÁMEC ÚKOLU PRO PKI	11
2.1 Úlohy předcházející softwarové přípravě karetní aplikace	11
2.2 Stejně funkce na různých komunikačních rozhraních	13
3 POŽADAVKY NA TECHNICKÉ VLASTNOSTI A FUNKČNOST ID-KARTY	15
3.1 Karty v prostředí VŠ.....	15
3.2 kritéria funkčnosti ID-karty	15
3.3 Technické předpoklady a uživatelské aplikace.....	17
Praktické poznámky ke kartě a cílům migrace na ID-kartu VŠ	18
4 KLASIFIKACE ČIPOVÝCH TECHNOLOGIÍ	20
4.1 Základní rozdělení	20
4.1.1 Rozdělení smart karet podle použití	20
4.1.2 Hardware karty.....	21
4.1.3 Procesory a paměť	22
4.1.4 Komunikace	24
4.1.5 Standardizace smart karet.....	26
4.1.6 Operační systémy	28
4.1.7 Vlastní čipové karty prostřednictvím licence na COS.....	28
4.1.7 Klasické smart karty s pevnou instrukční sadou.	28
VM - Smart Card Virtual Machines	30
Java Card.....	30
4.1.8 Bezkontaktní rozhraní karty a JavaCard	30
4.1.9 Souborové systémy	34
4.1.10 Aplikace pro programovatelné a neprogramovatelné karty	36
4.1.11 Smart karty a bezpečnost dat	37
5 ID-KARTA S DUÁLNÍM ROZHRANÍM	38
5.1 Bezpečnostní mechanismy	39
5.2 APDU příkazy	41
5.2.1 Key management.....	44
5.2.2 Seznam příkazů APDU implementovaných na SPK2.5DI.....	44
5.2.3 Doba vykonání příkazů	46
5.2.4 Autentizace mezi kartou a terminálem	47
5.3 Výpočet digitálního podpisu.....	47
5.4 duální multiaplikační karty pro PKI	51
5.4.1 Požadavky na PKI klienta	52
5.4.2 Požadavky na zpětnou kompatibilitu karet	53
6 INFRASTRUKTURA SMART KARET	55

6.1	Protokol PC/SC	55
6.2	Middleware	55
6.2.1	CryptoAPI a OCSP	56
6.2.1.1	Životní cyklus karet	57
6.2.1.2	Klíče na kartě	59
6.3	Kritické procesy pro správu karty	59
7	PROFIL TECHNICKÉ PŘÍPRAVY ČIPOVÉ MIGRACE	61
7.1	Úkoly a etapy	61
7.2	Pracovní verze specifikace ID-karty	63
7.3	Softwarová příprava karty (čipová personalizace)	64
7.3.1	Návrh aplikační struktury karty: Úvod	64
7.3.2	Návrh proprietárního řešení bez vazby na PKCS#15	65
7.3.3	Požadavky na ID- kartu	80
8	ZÁVĚR	83
9	PŘÍLOHA Č.1 SPECIFIKACE, NORMY A PRŮMYSLOVÉ STANDARDY	84
9.1	Souhrnné odkazy	84
9.2	Norma ISO/IEC 7816	84
9.3	Norma ISO/IEC 14443 a ISO/IEC 15693	87
9.4	Smart karty a PKI	87
9.5	Průmyslové specifikace pro smart karty a aplikace	87
9.5.1	Key Management	88
9.6	Průmyslové specifikace PKCS	88
9.7	Bezpečnostní normy	90
9.8	Specifikace rozhraní karta-snímač, terminál	90
10	PŘÍLOHA Č. 2 INICIATIVY, FÓRA, ORGANIZACE	91
10.1	Technologické zdroje	91
10.2	Asociace	91
10.3	Bezpečnost a certifikace	92
11	PŘÍLOHA Č. 3 ODKAZY NA VÝROBCE A PRŮMYSL ČIPOVÝCH TECHNOLOGIÍ	93
11.1	Smart karty a vývojová podpora (SDK)	93
11.2	COS - operační systémy	95
11.3	Aplikace pro smart karty	97
11.3.1	Softwarové nástroje a knihovny pro smart karty	97
11.3.2	Firmy s komplexním programem JavaCard a produkty	98
11.3.3	Softwarové nástroje pro smart karty SIM	99
11.4	Výrobci smart karet	99
11.5	Výrobci čipů pro smart karty	100
	Odkaz - zabezpečení proti útokům na smart kartu	100
11.6	Bezkontaktní produkty a klasické aplikace	101
11.7	Snímače smart karet– výrobci s přímou distribucí	101
12	TERMINOLOGIE	104
13	LITERATURA	109

SEZNAM OBRÁZKŮ A TABULEK

Obr. 1 Základní vlastnosti ID-karty.....	16
Obr. 2 Rozšířené využití smart karet	20
Obr. 3 Rozdělení smart karet podle čipu („hw engine“) a podle komunikačního rozhraní.....	21
Obr. 4 Typická architektura smart karty s duálním rozhraním a koprocesorem	22
Obr. 5 Kontroler – logické jednotky (smart karta s koprocesory RSA a 3DES)	23
Obr. 6 Struktura ISO/IEC pro standardy smart karet	26
Obr. 7 APDU - formát příkazu.....	42
Obr. 8 Typy objektů ve FS na kartě s 2 PKI-aplikacemi. Bez PKCS#15.	65
Obr. 9 Specifikace konkrétních objektů pro PKI-aplikace (bez PKCS#15).....	68
Obr. 10 Aplikace podle PKCS#15: Vztahy mezi typy souborů/objektů	72
Obr. 11 Datová struktura a vztahy mezi objekty pro aplikace DF1 DF2 podle PKCS#15.....	75
Obr. 12 PKCS#15 – Výsledný stav návrhu PKI Cesnet, PKI Univ s konkrétními objekty	76
Obr. 13 Přístup k privátnímu klíči ve struktuře PKCS#15 (podle schématu obr.12)	77
Obr. 14 Příklad SDK s podporou karet SPK2.5DI na bezkontaktním rozhraní (Starmag, G&D)	94
Obr. 15 Příklad vývoj. prostředí pro kontaktní PKI karty (ASE, Athena)	94
Tab. 1 Seznam příkazů APDU (implementace na SPK2.5DI)	44
Tab. 2 Postup výpočtu digitálního podpisu na kartě SPK2.5DI	49
Tab. 3 Struktura karty s aplikacemi a alokovanou pamětí pro oblasti DF.....	67
Tab. 4 Popis objektů navržené datové struktury karty s aplikacemi, podle obr.9	69
Tab. 5 Použití ze strany middleware, ilustrace k aplikaci (Tab.4 a Obr.9)	71
Tab. 6 Popis souborů/objektů na kartě v případě jedné PKI-aplikace podle PKCS#15, dle obr.10	73
Diagram 1 Proces selekce karty terminálem v bezkontaktním režimu	25
Diagram 2 Aplikace na klasickém COS jen prostřednictvím příkazů oper.systemu	33
Diagram 3 Java Card Applet - data & kód	34
Diagram 4 Základní klasifikace příkazů COS (APDU, ISO/IEC 7816).....	41
Diagram 5 Životní cyklus karty.....	58
Diagram 6 Proces generování e-podpisu	79

1 ÚVOD

Klientským základem současných systémů PKI je technicky, a do jisté míry i právně podpořená identifikační funkce držitele čipové karty. Podstatou je kryptograficky zabezpečené uložení identity konkrétní osoby s možností ověření.

Praktický přínos pro autentizační úlohy a aplikace s elektronickým podpisem závisí na efektivní implementaci PKI-karty do konkrétního prostředí uživatele ve VŠ komunitě. Efektivností je míněno:

- poskytování otevřeného rozhraní *karta – host* pro uživatelsky jednoduchý přístup k aplikacím
- funkčnost na host-platformách Windows, Linux, Solaris využívaných ve VŠ
- funkčnost podle ISO/IEC7816-4,5,8, ISO/IEC14443-3,4, PKCS#11, PC/SCv.1, 2, případně podle PKCS#15 a ISO/IEC7816-9,15.
- politika trvalé správy verzí a updates middleware pod hlavičkou akademické komunity.

Roli při praktickém nastartování tohoto projektu hraje samozřejmě základní výběr čipové technologie, která umí pracovat s párem klíčů v bezkontaktním režimu a odzkoušení prototypů karetních aplikací. Přirozeným požadavkem je dospět prostřednictvím ověřovacích pilotů od prototypu k provozní verzi, kde provázány aplikace na (multiaplikační) kartě přes vrstvu middleware s různými aplikacemi na PC, na intranetu/internetu, resp. s aplikacemi fyzického přístupu, pro ovládání zařízení, peněženky aj.

Pokud karetní a softwarové řešení posuzujeme z perspektivy jeho schopnosti plnit specifické požadavky prostředí VŠ, včetně studentského průkazu, nejde o seznam rutinních úloh, i když každou jednotlivou umíme technicky zprovoznit: První PKI-úlohy v bezkontaktním režimu RSA-karty byly v ČR připraveny v rámci tohoto úkolu a prakticky předvedeny na semináři CESNET.

Ale implementace řešení zůstane na půl cesty bez podpůrné technické a organizační infrastruktury, bez správy klíčů, bez spoluúčasti systémů PKI.

Cílem zprávy je informovat o dosud provedených krocích v problematice. Dále uspořádat svodku z technických podkladů a standardů tak, aby vznikl první z řady příspěvků k posuzování kritérií a rizik při testování a pilotním nasazení čipové karty pro PKI-klienta. Prioritu mají současné i předpokládané funkční požadavky VŠ na sjednocení elektronického průkazu studenta. Technická orientace čtenáře je usnadněna přehledem terminologie a pojmů na konci zprávy a zmapováním stavu čipových technologií dostupných v letech 2003-2004.

Zpráva je součástí širšího úkolu, který byl zahájen v r.2003 a dosud pokračuje.

Úkol je zastřešený sdružením CESNET se spoluúčastí smluvního partnera CoProSys a koresponduje s připravovanou migrací na novou generaci studentských průkazů (dále též stručně „čipová migrace“). Příprava průkazů je pokusem o standardizaci různorodého karetního vybavení na školách. Standardizace je koordinována prostřednictvím iniciativy „Skupina pro ID-kartu“, která sdružuje zástupce řady vysokých škol. Záštitu nad tímto pracovním výborem poskytl CESNET, který zajišťuje

potřebné zázemí. „Skupina pro ID-kartu“ pracuje v několika sekcích pro technickou a právní problematiku související se sjednocením průkazu.

Projektová aktivita tohoto druhu otvírá experimentální a aplikační pole i pro případné potřeby dalších výzkumných projektů CESNET a VŠ.

Výstupy z úkolu, který je přes značnou dobu uplynulší od zahájení teprve na počátku praktické fáze přípravy pilotů, budou ověřovány, implementovány a dány k dispozici akademické veřejnosti.

Technická zpráva vypovídá o přípravném stadiu úkolu v období IV/2003 až II/2004.

2 RÁMEC ÚKOLU PRO PKI

Úkol má dvě odlišné fáze. První se zabývá karetní technickou problematikou, další část je převážně vývojářská na platformách PKI-klienta. Cílem je implementace čipových karet do PKI. Protože se PKI-systémy začaly uplatňovat v reálných projektech v akademickém prostředí i mimo (příkladem je řešení CA CESNET), rozšíření klientské části PKI o čipové karty se stává zcela praktickým a nezbytným úkolem.

Základní funkcí karty je prokazování totožnosti, které má dva kroky: identifikaci (dotaz - kdo jsi?) a autentizaci (dotaz – dokaž, že jsi ten, za koho se vydáváš). Na rozdíl od jiných technik identifikace, jde s pomocí PKI-karty zvládnout i ostatní atributy bezpečnosti (utajení, integritu, nepopiratelnost, neodmítnutelnost). Kartu s identifikací může mít uživatel stále u sebe a použít ji k autentizaci či k e-podpisu na různých místech, nejenom na svém PC. Před jejím používáním je třeba připravit karetní aplikace.

2.1 ÚLOHY PŘEDCHÁZEJÍCÍ SOFWAROVÉ PŘÍPRAVĚ KARETNÍ APLIKACE

Návrh datové struktury a karetních aplikací je v první řadě ovlivněn výběrem **průmyslových standardů** (zejména ISO/IEC, PKCS), **kteří budou podporováni** při řešení na straně karty a na straně terminálu (hosta).

V rámci vybrané architektury karty budou navrhovány karetní aplikace pro jednotlivé skupiny držitelů karet (například pro jednotlivé školy). Konzistentní pravidla při návrhu lze ukládat do *šablon (templates)*. Šablonu tvoří údaje vybrané ze spektra přípustných parametrů, které je nutno nastavit, aby vynutily dohodnutý stupeň bezpečnosti při užívání karty a umožnily jednotnou provozní politiku. Vývojářská skupina podle šablony (odsouhlasené určenou autoritou) finalizuje strukturu karty, podmínky přístupu k datovým objektům (file access conditions) a určí chování karty v aktivním režimu. Šablon může být víc, pro různé organizace, pro různé etapy zavádění karet do provozu.

Rozhodnutí před návrhem datové struktury karty a nastavením access conditions, se týkají chování karty od resetu k ukončení session:

- Režim práce s podpisovým klíčem, který nikdy neopustí kartu
- Autentizační mechanismy „karta-terminál“, secure messaging
- Datové formáty pro osobní údaje, případně pro digitalizované fotografie
- Chování na rozhraní „karta – PC“, s jednou otevřenou aplikací, současně otevřeno několik aplikací na kartě, použití několika soukromých klíčů
- Varianty práce s otiskem (hash). Karta může vyrobit hash nebo přijmout hash z terminálu
- Nastavení *default* hodnot pro klíče, aplikace
- Reakce karty na výjimečné stavy terminálu.

-Nastavení chování terminálu (zařízení), resp. session, po přerušení komunikace (po zdvihnutí položené karty nebo vyjmutí z kontaktní čtečky).

Typické příklady rozhodnutí a nastavení chování karty:

-Rozhodnutí o specifikaci karty vzhledem k držiteli karty:

Bude podporována pouze karta osobní (jako trvalý ID-průkaz osoby)?

Budou vyžadovány i jiné karty? (např. přenositelná karta, karta pro semestrálního hosta, služební karta pro zaměstnance, karta pro aktivaci zařízení nebo procesů) ?

-Rozhodnutí zaměřená na užití karetých aplikací

Rozhodnutí o správě obsahu karty: delegovat pravomoci pro přidávání aplikací, odblokování karty personálně (administrátor) nebo místně (autorizované pracoviště)

Bude přijat číselník karetých aplikací podle struktury AID (Application ID)?

Bude povoleno sdílení aplikací na přenositelné kartě dvěma osobami?

Bude povolena přítomnost externích aplikací na kartě (mimo VŠ, mimo CA CESNET) např. dopravní a peněžní služby?

-Rozhodnutí týkající se klíčů na kartě a certifikační politiky

Jaký postup při pozbytí platnosti, ztráty, při vypršení expirační doby (týká se certifikátu, klíčů, karty)

Může být vydán nový certifikát pro kartu ještě před vypršením platnosti starého certifikátu?

Postup při obnovení některého z podpisových klíčů

Postup při opětovném nahrání šifrovacího klíče ze zálohy.

-Nastavení funkce ochrany PINem:

Zvolit PIN ve formátu ASCII nebo číselný, s počtem znaků (4-8)?

Scénář nasazení PINů: Jaký počet různě zaměřených PINů povolit?

Kolik PINů bude generováno pro PKI-aplikace a kolik pro non-PKI aplikace (např. povolit pro aplikaci „ACS = fyzický přístup“ řešenou nezávisle na Mifare otevření dveří i bez PINu) ?

Povolit odblokování PINu jen na určených místech na autorizovaných pracovištích, kde odblokování provede držitel karty sám (jako jediný zná PUK)?

Počet neplatných pokusů pro PIN a PUK? Scénář použití PUK?

Speciální podpora PINPadů (natypování PINu bez natažení do operační paměti PC) při zvýšených nárocích na bezpečnost?

Další postup přípravy čipové personalizace:

-Design datové a aplikační struktury na kartě (včetně rozhodnutí o ponechání volné kapacity na novou aplikaci, rozhodnutí o nahrání dat specifických pro middleware)

-Příprava programu pro inicializaci karty, vygenerování struktury na kartě a pro vložení dat, která mají být nahrána (personální data).

Tento program bude součástí procesu čipové personalizace na registračním místě (RA) (Žádost o certifikát – Vystavení certifikátu)

Karetní aplikace a rozhraní ošetřené middlewarem tvoří jádro řešitelského úkolu. Spolu s technologií je třeba dodat a rozšířit patřičnou znalost potřebnou při údržbě a rozvoji, zapojit více kompetentních účastníků. Kromě technického řešení je součástí úkolu oponovat při nastavení patřičných organizačních opatření a interních procesů souvisejících s rozběhem technologie – například s životním cyklem karet, certifikátů, se správou klíčů a registračními autoritami.

2.2 STEJNÉ FUNKCE NA RŮZNÝCH KOMUNIKAČNÍCH ROZHRAŇÍCH

Základní přínosy čipových smart karet disponujícími RSA algoritmy byly ověřeny na kontaktních kartách, stručně:

- e-podpis dokumentů a emailů, přihlášení do systémů ICT.
- Nasazení PKI-karet místo soukromých klíčů uložených na disku (v soft-tokenech).
- Zjednodušení správy přístupů k systémům včetně techniky Sign-On.
- Využívání služeb dvou certifikačních autorit pomocí jedné karty (karta jako nosič dvou párů klíčů a dvou certifikátů s mechanismem automatického rozhodování, kdy má který klíč a certifikát použít).
- Bezpečná správa uživatelských účtů a navýšení bezpečnosti síťové infrastruktury.
- Uložení přístupových hesel uživatele informačního systému na kartu a jejich načítání z karty v těch případech, že IS přímo nepodporuje PKI-autentizaci.
- Zvýšení lokální bezpečnosti - Monitorování přítomnosti čipové karty ve snímači (při odebrání karty dojde k odhlášení uživatele a uzamčení počítače).
- Šifrování zpráv, šifrování komunikace mezi serverem a klientským počítačem.
- Klient PKI pracující pod OS Windows, Linux, Solaris.

Nové úkoly a faktory jsou ty, které se ve výčtu nahoře nenacházejí: 1) komunikace karty s desítkami typů čteček různé kvality, 2) plošný rozsah testování, 3) požadavek na otevřenost řešení a vlastní správu řešení, 4) rozvoj řešení bez přílišné divergence, 5) účinný helpdesk, 6) problematika distribuce karet a zřizování odpovídajících registračních autorit, 7) problematika distribuce middleware přes web. Přesto, že jsou čipové karty pro PKI rutinně podporovány řadou výrobců *kontaktních* karet (viz přílohy této zprávy), neplatí to zdaleka v případě bezkontaktní komunikace *PKI-karta - host*. Jde o nastupující technologii, která je mimoto podmínkou tohoto řešení.

Spolu s PKI-úlohami v bezkontaktním režimu karty, které byly ve zjednodušené podobě předvedeny na semináři CESNET, je součástí řešení problematika *zpětné kompatibility* se staršími karetními aplikacemi a *portability*. Zpětná kompatibilita je důležitá Mifare pro rozšíření na školách (cca 40%

studentů). V případě námi navrhovaných čipů se -- vzhledem k jejich nativní podpoře Mifare - redukuje úloha na ověření funkce přenosového protokolu ISO/IEC 14443-3 na instalovaných čtecích modulech. Za druhé se týká zpětná kompatibilita těch starších 125kHz aplikací, které musí karta převzít a podporovat jako jednu ze svých nově připravených karetních aplikací.

Úkoly při výběru a zprovoznění již dříve námi ohlášené karty, jsme rozdělili do těchto skupin:

- Příprava technologických podkladů pro práci s kartou. Příprava struktury dat na kartě, karetních aplikací řízený příkazy APDU a příprava čipové personalizace prováděné pod registrační autoritou.
- Příprava software pro práci s kartou ve Windows a Linux s výhledem na pozvolné zavádění karty jako elektronického průkazu ve VŠ.
- Průzkum zpětné kompatibility karty se stávajícími karetními aplikacemi na VŠ a s různými typy snímačů na VŠ. Podmínka zní: Nová karta bude podporovat některou ze starších technologií.
- Příprava pilotních projektů ve spolupráci se sdružením CESNET a VŠ. Pilotní projekty, které ověří praktické možnosti držitele karty při identifikaci, autentizaci a elektronickém podpisu i spolupráci se stávajícími aplikacemi.

Potřebné technické zabezpečení úkolu zahrnuje tyto složky ICT:

- procesorové čipové karty (smart karty)
- podrobnou technickou specifikaci COS
- snímače, kartové terminály, bezkontaktní čtecí moduly
- počítače (PC, servery)
- operační systémy Windows 2k, XP, W2003, Linux, Solaris
- vývojové prostředky pro typy řešených karet, toolkity pro testování, pro adaptaci a programování kryptoovladačů (middleware)
- experimentální certifikační a registrační autoritu, adresářové služby, CRL

xxx

3 POŽADAVKY NA TECHNICKÉ VLASTNOSTI A FUNKČNOST ID-KARTY

3.1 KARTY V PROSTŘEDÍ VŠ

Pro negativní zkušenosti z praxe byly ve všech VŠ odmítnuty kontaktní karty v roli studentských průkazů. Proto jsme navrhli ID-skupině typ karty, která poskytuje funkce PKI na bezkontaktním rozhraní. Jak vyplynulo, karta musí splňovat i další požadavky na funkčnost. Při generační obměně a sjednocení karet (elektronických průkazů) na školách se přihlíží k několika požadavkům na funkčnost.

Poznámka: Požadavky na funkčnost jsou zformulovány podle účastníků ID-skupiny¹. ID-karta je stručně uváděná jako IDK.

3.2 KRITERIA FUNKČNOSTI ID-KARTY

Uživatelské požadavky na technické vlastnosti a funkčnost ID-karty projednané ID-skupinou:

- [R1] IDK musí umět pracovat bezkontaktně.
- [R2] IDK musí podporovat uznávané standardy, zejména skupinu protokolů pro bezkontaktní rozhraní ISO/IEC 14443 a skupinu protokolů ISO/IEC 7816 v případě užití kontaktního rozhraní.
- [R3] IDK musí disponovat přiměřenými bezpečnostními mechanismy, které zaručí nezpochybnitelnost údajů na kartě, zcela minimálně na úrovni čipové technologie MIFARE.
- [R4] IDK musí podporovat kryptografické funkce.
- [R5] IDK má jako hardwarový token umožňovat silnou autentizaci a elektronický podpis.
- [R6] IDK by měla podporovat stávající aplikace VŠ, provozované na nejrozšířenějších čipových karetních systémech (tj. MIFARE Standard), bez nutnosti výměny provozovaných snímačů.
- [R7] IDK by měla podporovat většinu aplikací používajících čipové nebo mg karty (po nezbytných úpravách snímačů a aplikačního software).

Dlouhodobé priority programu sjednocení průkazu shrnuty ve shodě s iniciativou ID-karta:

- Standardizace IDK i služeb, které IDK používají, ve víceletém výhledu a pro celé VŠ-prostředí.
- Zajištění určitého stupně zpětné kompatibility k zavedeným starším technologiím pro překlenovací období.
- Využitelnost karty a mobilita uživatele ve VŠ-prostředí i mimo.
- Harmonizace s trendy, které jsou podporovány standardizačními organizacemi SCEN, ETSI, eEurope Smart Card Charter (eESCC).

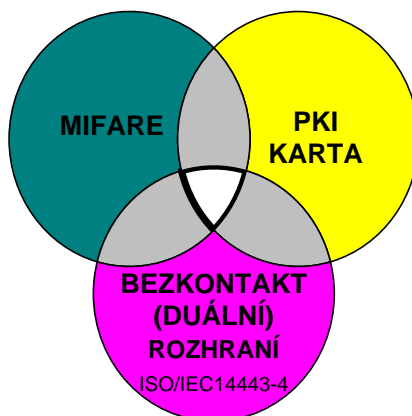
¹ Viz web-konference, materiály a zápisy ID-Karta. Viz Vítuško, EurOpen 2004

Tři vlastnosti karty, které má splňovat pro využití v prostředí VŠ, jsou znázorněny na diagramu:

DUÁLNÍ KARTA viz kritérium [R1] [R2]

PKI viz kritérium [R3] [R4] [R5] a [R2]

MIFARE viz kritérium [R6] a [R7] zabývající se podporou této technologie (ISO14443-3)



Obr. 1 Základní vlastnosti ID-karty

Výrobci a dodavatelů je v každé jednotlivé kategorii více. Průnik udávající možnost výběru se zužuje na 2-3 výrobce a 4-5 produktů podle průzkumu trhu provedeného v 2.pol. 2004 řešiteli. Karetní produkty splňující kritéria založeny na čipech Philips a Infineon

Závěr pro úkol:

Funkční požadavky jsou vstupem pro technickou stránku řešení.

Ve zprávě jsou uvedeny technické a operační charakteristiky karty, kterou řešitelé představili na semináři CESNET jako prototyp řešení.

3.3 TECHNICKÉ PŘEDPOKLADY A UŽIVATELSKÉ APLIKACE

- § Tabulka se sadou aplikací, které se (ve střednědobém a dlouhodobém horizontu) mohou stát aplikacemi nad PKI.
- § Aplikace, které jsou provozovány na některé VŠ na stávající technologii, zvýrazněny
- § Aplikace, které byly diskutovány na „ID-karta“ jako aktuální – pro update na PKI-karty, označeny kurzivou
- § Tabulka je orientačním vodítkem pro analýzu technické specifikace karty, šablon a middleware
- § Některé z uvedených aplikací mohou být v „evolučním procesu“ zavádění PKI realizovány v samostatných projektech, u některých aplikací se to předpokládá již v rámci pilotních programů.

Kdo uživatel	popis funkce (typ aplikace)	technologie	stav nyní	vzdálený přístup
Fyzický přístup	Vstup do chráněných prostor	autent.PKI (přech.Mifare nebo 125kHz)	Mifare nebo 125kHz	<i>beze změny</i>
Studenti	Přístup k citlivějším informacím ze studijního odd. a bezpečný mail	autent.PKI /e-podpis/	osobně	<i>odkudkoliv</i>
Zaměstnanci	<i>Přístup k ekonomické agendě aj.</i>	autent.PKI	heslo	<i>dle propozic</i>
Centrum VT	Přístup k zařízení& síťový přístup	autent.PKI	karta, heslo	<i>beze změny</i>
Všichni	Zásobník hesel na kartě (Autentizace při spouštění procesů – vzdálený přístup) (Vzdálená správa webu, sítě a aktivních prvků)	logon z karty	zapam.heslo	<i>beze změny</i>
Všichni	Věrnostní aplikace bez dat na kartě (=data na serveru)	nová aplikace karty		
Všichni	Věrnostní aplikace s daty&číselníky na kartě(=bodový systém, peněženka)	nová aplikace karty		
Všichni	Distanční studium po internetu (e-learning)	autent.PKI		
Všichni	Knihovny, kopírky, postupně i menzy	autent.PKI + peněženka (přechodně Mifare nebo 125kHz)	Mifare/125kHz /	<i>obj. v knihovně zasl.elektř.publ.</i>
Všichni	Parkování	autent.PKI		
Zaměstnanci	Oběh dokladů	e-podpis		
Zaměstnanci+	Spisová a archivní služba	e-podpis		
Všichni	Elektronická podatelna VŠ	e-podpis		
Studenti	<i>Odbavení studentů na stud. oddělení prostřednictvím centrální aplikace (např. STAG), autent.PKI</i>			
Všichni	Přístup k aplikacím přes portály – jednotná strategie PKI autentizace (Sign On)			
Dle kategorie	Bezpečná výměna informací se zahr. univerzitami			
Studenti + zam.	<i>Koleje - ekon. aplikace, agenda služeb pro studenty na kolejích</i>			

§ Některé základní vlastnosti karty SPK2.5DI - plně funkční prototyp pro vývoj karetních aplikací

a middleware:

- multifunkční - několik dvojic klíčů lze generovat (nebo jen importovat)
- více aplikací – aplikace lze přidávat i mazat z karty kdykoliv během životnosti karty, kartu lze reinitializovat
- duální karta tj. bezkontaktní i kontaktní provoz na jednom čipu
- antikolizní režim, 4 kanály pro současně otevřené aplikace
- podpora 3DES i RSA, 16k EEPROM pro aplikace

Praktické poznámky ke kartě a cílům migrace na ID-kartu VŠ

1) Konvergence k stabilnímu aplikačnímu obsahu karty

- mít na jedné kartě dohromady:

- a) el. průkaz studenta / zaměstnance
- b) nástroj fyzického přístupu
- c) podpisové a šifrovací klíče
- d) klíče jako nástroj přístupu k datům: logický přístup (2-faktorová autentizace) k PC, síti, intranetu, portálu, aplikacím
- e) místo pro přidávání dalších aplikací

2) O všech aplikacích nemusí být rozhodnuto při personalizaci. Karta se chová tak trochu jako počítač, u kterého můžeme přidat nebo smazat aplikace.

3) Držitel karty dostane v podobě ID-karty nástroj, na kterém může mít uloženy certifikáty a klíče několika nezávislých nebo konkurenčních certifikačních autorit .

4) Je ověřeno, že kartu lze používat i jako kartu s jedinečným identifikátorem pro staré aplikace.

U některých systémů dalších (čip e5560), je nutno upgradovat čtečky na vyšší frekvenci a podporu ISO14443. Tento problém je částečně vyřešen na ZČU přidáním druhého modulu.

5) Vznik otevřeného prostředí: výběr technologie provést tak, aby byl pod kontrolou VŠ-komunity a nevznikala totální závislost na dodavateli karetních systémů (role standardů, zásady přenositelnosti funkcí (aplikací) na jiný HW) .

6) Dosavadní karetní aplikace (Mifare, e5560) využívají na kartě jen nějaký jedinečný identifikátor typu seriové číslo karty. Veškerá data se kontrolují v databázích nebo kontrolerech mimo kartu. Bude třeba navrhnout novou koncepci (LDAP) nebo „evoluční“ kontinuitu této dosud užitečné koncepce

7) Lze dělat PKI i bez karet?

Idea systémů PKI bez karet (tj. bez hw tokenů) je pro citlivější aplikace nad PKI riziková, téměř nemožná. Jako náběh PKI ano, v delším horizontu ne. Zkusme distribuovat 50000 souborů s klíči stejnému počtu studentů. Kolik soukromých klíčů asi bude do měsíce zkompromitováno, kolik ztraceno? K tomu připočtíme menší mobilitu uživatele, který má klíč na PC a je někde jinde...

8) Ceny karet od výrobce silně závisí na objemu odběru. Výrobce poskytuje slevy pro nekomerční oblast a pro školství. Odhad ceny se pohybuje mezi 200 – 350 Kč za nepersonalizovanou kartu. Její využitelnost je ale nesrovnatelně větší proti současným kartám ve VŠ.

4 KLASIFIKACE ČIPOVÝCH TECHNOLOGIÍ

4.1 ZÁKLADNÍ ROZDĚLENÍ

Terminologie: Čipové procesorové karty označeny stručně jako smart karty.

Mezi smart karty nejsou zahrnuty paměťové karty bez procesoru.

Oficiální akronym ISO, zahrnující paměťové i procesorové karty, je ICC (Integrated Chip Card)

Do třídy smart karet náleží:

klasické čipové procesorové karty rozměru kreditní karty,

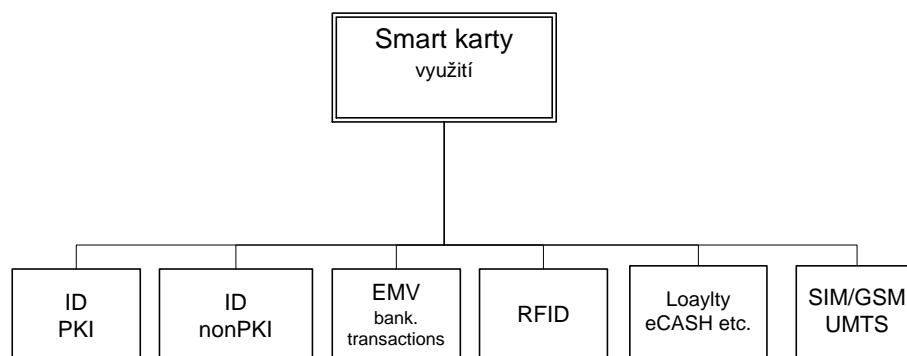
tokeny (USB-tokeny, „klíčenky“),

SIM karty,

platební čipové karty standardu EMV.

4.1.1 ROZDĚLENÍ SMART KARET PODLE POUŽITÍ

Orientační schema rozšířeného využití smart karet na diagramu:



Obr. 2 Rozšířené využití smart karet

Všechny aplikace využívají silných bezpečnostních mechanismů oproti paměťovým kartám.

-Karty ID/PKI a karty ID/nonPKI jsou nasazovány mj. jako elektronické občanské a profesní doklady, pro e-government, pro e-commerce, pro zdravotní péči atd.

-Karty EMV jsou platební čipové karty.

-Loyalty - věrnostní karty pro obchodní a čerpací sítě, elektronické peněženky.

-Karty ID/nonPKI též pro starší ID techniky, ACS (fyzický přístup) aj.

-RFID –pro logistiku, pohyb zboží, skladové systémy

-SIM pro mobilní telefonii

4.1.2 HARDWARE KARTY

Rozdělení podle základních technických charakteristik:

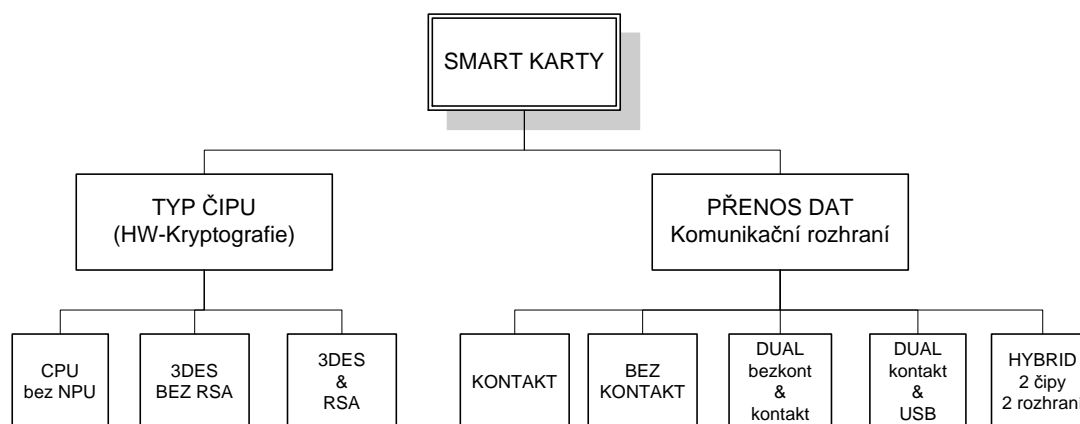
procesorové karty bez koprocesorů,

procesorové karty s přidavnými kryptografickými koprocesory

(koprocesor pro symetrickou kryptografii (3DES, resp. AES).

(koprocesor pro asymetrickou kryptografii (obvykle RSA))

Rozdělení karet podle čipu a komunikačního rozhraní přenosového protokolu je znázorněno na diagramu.



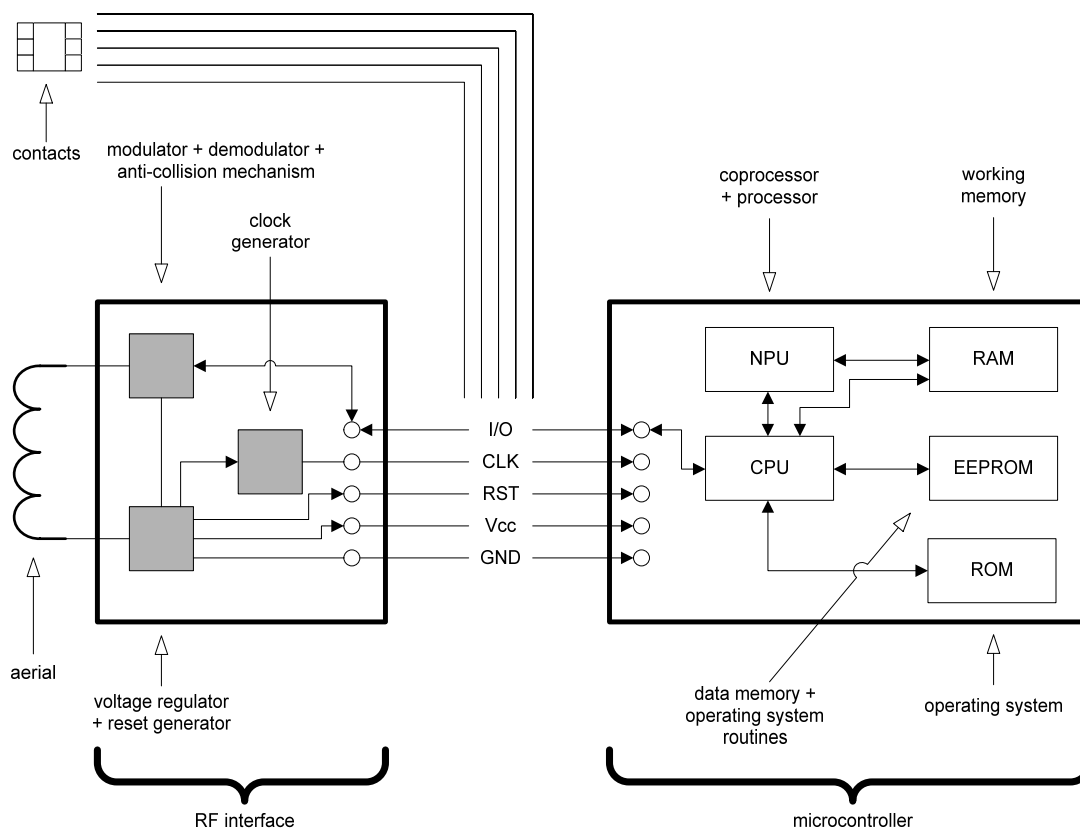
Obr. 3 Rozdělení smart karet podle čipu („hw engine“) a podle komunikačního rozhraní

Poznámka: Pojem „kontaktní karta“, „bezkontaktní karta“ nevypovídá nic o vnitřním technickém uspořádání karty (o paměti, CPU, NPU, bezpečnosti karty, aplikačních charakteristikách), ale pouze o způsobu, jak karta komunikuje s terminálem.

Čip (čipový kontroler, čipový modul) na smart kartě disponuje vlastním CPU, operačním systémem, pamětí typu EEPROM, ROM, RAM, oblastmi pro ukládání dat, kanály pro komunikaci s I/O zařízeními.

Čipový modul je umístěn na plastu (karta, USB-token, ..) s příslušným komunikačním rozhraním realizovaným kontaktním polem resp. do plastu zalisovanou anténou pro RF rozhraní.

Na obrázku je vidět zjednodušený náčrt typické architektury smart karty s duálním rozhraním



Obr. 4 Typická architektura smart karty s duálním rozhraním a koprocesorem

4.1.3 PROCESORY A PAMĚŤ

Základní řada CPU pro smart karty: 8bitové CPU

Typické příklady:

- CPU Intel 8051 a jeho modernizované a výkonnější verze 80C51
- CPU Motorola 6805 (inovovaná)
- CPU Atmel (risc architektura)

Nejvýkonnější řada: 32bitové CPU, disponuje každý větší výrobce čipů, např. často používán Intel MX51

	<i>Zápis (Write time per cell)</i>
EEPROM typicky rozsah 8kB – 128kB (až 1MB)	3-10ms
ROM typicky 64kB	-
RAM typicky 4kB	70ns
Těž Flash EEPROM	10mikrosec

EEPROM pro aplikační data

ROM obsazen OS

RAM výkon instrukcí OS

Flash EEPROM někdy doplňuje (nahrazuje) EEPROM pro rychlejší práci s pamětí.

Koprocesor 3DES velmi rychlý (operace v desítkách mikrosekund)

Koprocesor pro asymetrické kryptografické algoritmy. (Příklad: FAME-X)

-RSA

-ECC (Eliptické křivky)

Specializovaná jednotka právě jen na výpočty pro algoritmus RSA (algoritmus pro eliptické křivky).

Až 140bitové interní operace, obvykle pouze umocňování a celočíselná modulo aritmetika. Tato aritmetika je nedílnou částí RSA algoritmů s veřejným klíčem, v generování ECC digitálních podpisů a v Diffie - Hellman algoritmu výměn klíče.

Metody Chinese Remainder Theorem (CRT) pro efektivní umocňování.

RNG (Random Number Generator)

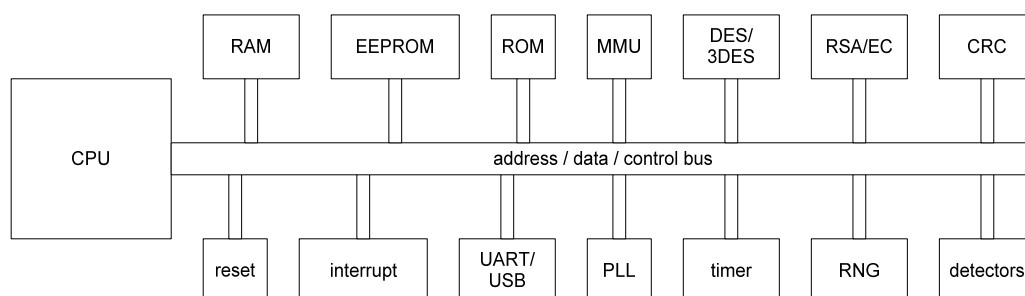
Kvalita RNG rozhoduje o kvalitě kryptografie na kartě.

Kapacita - obsazení paměti EEPROM pro PKI:

Velikost digitálního ID pro e-podpis se pohybuje typicky kolem 3kB (záleží na šifře – délce klíče, počtu a obsahu jednotlivých položek certifikátu). Je třeba počítat ještě s režii pro souborový systém na čipu. Lze rezervovat místo pro komplexní profily systémů jako je CA/PKI od Entrust nebo Baltimore, které mohou na čipu zabírat až 6kB.

Jako minimální velikost paměti pro ID-kartu lze doporučit 16kB.

Uspořádání sběrnice kontroleru smart karty. Pro výkon kryptografických operací je rozhodující 3DES NPU a RSA NPU. Na čipech Philips a Infineon jsou implementovány s rozšířenou sběrnici.



Obr. 5 Kontroler – logické jednotky (smart karta s koprocesory RSA a 3DES)

Příklady kontrolerů (tj. čipů), kterými se osazují duální karty a které podporují MIFARE:

Philips MIFARE ProX

Infineon SLE66CL160S.

Philips SmartMX (přímý 32bitový následovník MIFARE ProX). CPU Intel MX51, úplná kompatibilita s 80C51. Technologie CMOS 0,18.

Maximální frekvence CPU 30MHz (internal) 10MHz (external)

SmartMX podporuje tři komunikační rozhraní – ISO/IEC14443A,B, ISO/IEC7816 a USB1.1.

Všechny funkce SmartMX včetně kryptografických operací FameEX – RSA a 3DES a AES jsou využitelné i přes bezkontaktní rozhraní.

Podpora COS: SmartMX podporuje snadnou implementaci současných operačních systémů s pevnou instrukční sadou i systémů, založených na otevřených platformách včetně Java Card a Multos.

Optimalizace jazyka C.

FameXE engine

Kryptografie veřejného klíče. Podpora RSA s operandem délky až 5kb,

HW akcelerátor 3DES, 3DES výpočet pod 50microsec

4.1.4 KOMUNIKACE

Rozdělení smart karet podle komunikačního rozhraní karty

Bezkontaktní karty (proximitní karty): normovány podle ČSN ISO/IEC 14443-x, x=1,2,3,4.

Kontaktní karty. Společným základem kontaktních karet jsou pravidla definovaná základní sadou norem ISO/IEC 7816-x, resp. českých ekvivalentů ČSN EN 27816-x.

Hybridní karty: karty opatřené dvěma čipy, každý čip obvykle komunikuje přes jedno rozhraní.

Duální karty: karty s jedním čipem, který komunikuje přes bezkontaktní i kontaktní rozhraní.

Bezkontaktní karty - klasifikace podle čtecí vzdálenosti:

Close-Coupled Cards	0 mm - 10 mm
Proximity Cards	10 mm - 100 mm
Vicinity Cards	100 mm - 500 mm

Pro řešení úkolu připadají v úvahu proximity karty. Jde o stejnou nebo návaznou kategorii jako MIFARE (kompatibilita čteček). V této třídě jsou přenosové charakteristiky komunikace přes elektromagnetické pole optimální (na rozdíl od malé datové propustnosti Vicinity-karet).

Pro projekt (splňující [R1]-[R7]) jsou důležité tyto parametry a prvky:

duální smart karta s bezkontaktním rozhraní podle ISO/IEC 14443, části 1-4 a kontaktní rozhraní podle ISO/IEC 7816 část 1-3.

Bez ohledu na použité komunikační rozhraní pracuje duální karta po navázání komunikace v nižších vrstvách s APDU příkazy podle ISO/IEC 7816-4, -8, resp. -9. a vrací response-APDU.

Není proto přesné považovat ISO/IEC 7816 jen za standard kontaktních karet.

Karta, která navíc podporuje Mifare, pracuje takto: v případě, že inicializační proces karta-snímač detekuje snímací technologii Mifare na vrstvě ISO 14443-3, je inicializován režim karty Mifare.

Na diagramu jsou znázorněny procesy při navazování spojení v bezkontaktním režimu.

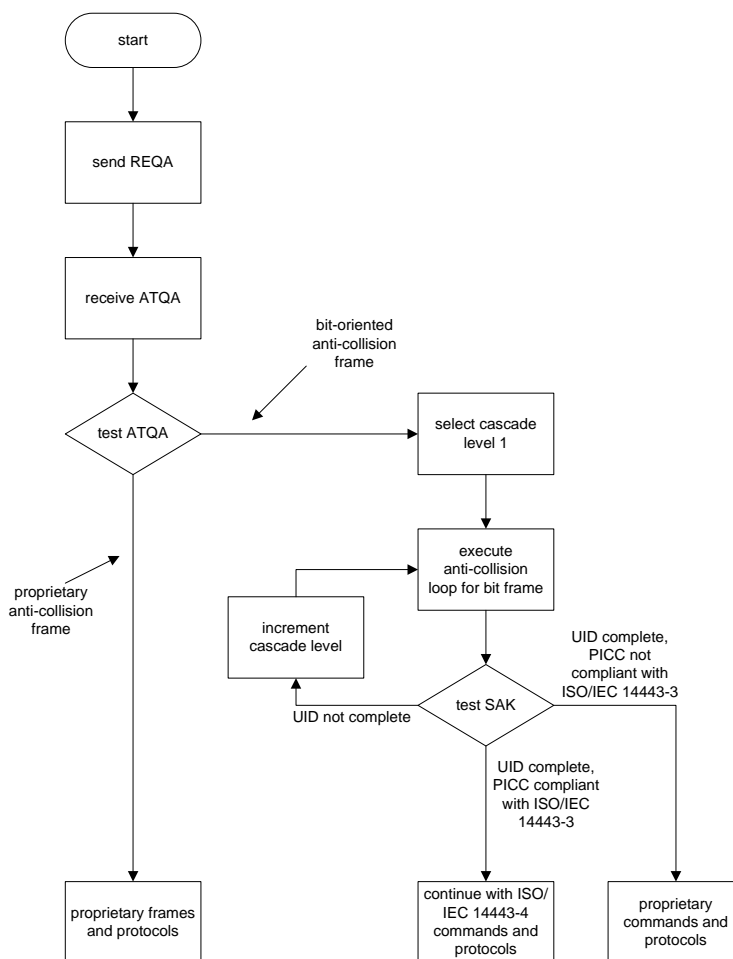


Diagram 1 Proces selekce karty terminálem v bezkontaktním režimu

1) Duální karta s jedním čipem pracujícím s bezkontaktním i kontaktním rozhraním.

Příklad: SPK 2.5DI s čipovým kontrolerem Philips MifareProX a operačním systémem Starcos 16K. Jde zároveň o prototyp vybraný k pilotnímu ověření

2) Hybridní karta s dvěma čipy. Jeden čip s bezkontaktním rozhraním, druhý čip s kontaktním rozhraním.

Příklad: Karta CyberFlex Access 32K s čipem na platformě JavaCard pracujícím s kontaktním rozhraním a čipem MIFARE pro bezkontaktní provoz.

Slabinou obdobného řešení vzhledem k [R1]-[R7] je, že hybridní karta této koncepce nemůže pracovat jako PKI karta v bezkontaktním režimu.

Přenosový protokol

TPDU (Transmission Protocol Data Unit)

Přenosový protokol. Terminál (master) komunikuje s kartou (slave) tak, že APDU je konvertován do TPDU a zaslán smart kartě přes seriové (či jiné) rozhraní.

V prostředí komunikace smart karet přes kontaktní rozhraní je obvykle ve smart kartě implementován některý z těchto protokolů (nebo oba dva):

protokol T=0 (asynchronní, half duplex, bajtově orientovaný, ISO7816-3)

protokol T=1 (asynchronní, half duplex, blokově orientovaný, ISO7816-3, Amd.1)

Ve standardizační přípravě je:

protokol T=2 (asynchronní, full duplex, blokově orientovaný, ISO10536-4) (optimalizace T=1)

V prostředí komunikace proximitních smart karet přes bezkontaktní rozhraní je obvykle ve smart kartě implementován

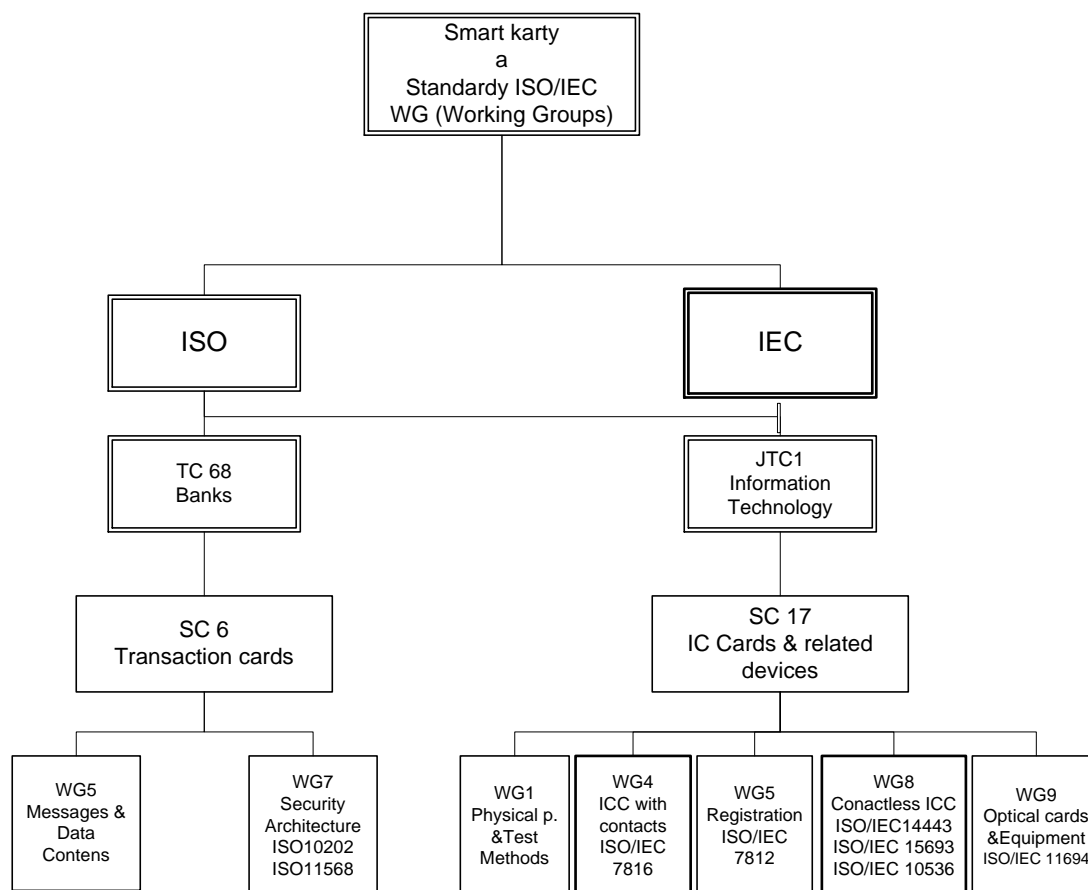
protokol T=CL (asynchronní, half duplex, blokově orientovaný, ISO14443A-4)

protokol pro MIFARE ISO/IEC 14443A-3

Přenosové protokoly, kterými je schopna komunikovat duální karta SPK2.5DI jsou T=0, T=1, T=CL

4.1.5 STANDARDIZACE SMART KARET

Přehledné schéma struktury pracovních skupin ISO/IEC (všechny nejsou zobrazeny). Nejdůležitější jsou pro smart technologii na úrovni vydavatele karet, programátora a držitele karty WG4 a WG8.



Obr. 6 Struktura ISO/IEC pro standardy smart karet

Standardizované vlastnosti smart karet.

- § Existují standardy pro fyzické, mechanické, elektrické i softwarové vlastnosti. Sada standardů ISO/IEC 7816-x, ISO/IEC 14443-x a ETSI SMG9 je podstatnou skupinou norem pro výrobu smart karet i pro aplikační programátory v oboru smart karet.
- § Přehled hlavních standardů a jejich částí je uveden a podrobněji odkazován na externí dokumenty a adresy v příloze zprávy.
- § Odkaz na souhrn většiny relevantních norem a standardů pro smart karty:
 - <http://forum.afnor.fr/afnor/WORK/AFNOR/GPN2/Z15Y/PUBLIC/WEB/ENGLISH/commerce.htm>
 - <http://www.tfn.net/techno/smartcards/standards.html>
 - ISO/IEC JTC1 Information technology SC 17 Identification cards and related devices (www.iso.ch/meme/JTC1SC17.html)

§ Standardy pro komunikaci karty a aplikace na kartě:

- § Z pohledu komunikačního rozhraní a aplikačního programování jsou nejdůležitější informace v těchto dokumentech:
- § ISO/IEC 7816-4 (zde zejména příkazy APDU, platné nezávisle na tom, jestli karta komunikuje bezkontaktním nebo kontaktním rozhraním. Viz též tabulka příkazů APDU implementovaných na kartě)
- § ISO/IEC 7816-5, 6, 8, 9
- § ISO/IEC 7816-15 integrace normy PKCS#15
- § ISO/IEC 14443A-3 na této vrstvě bezkontaktně komunikuje MIFARE
- § ISO/IEC 14443A-4 na této vrstvě bezkontaktně komunikuje COS
- Průmyslové specifikace RSA :
 - § PKCS# x x=11, x=15 pro kryptografické operace
- Rozhraní PC - čtečka
 - § PC/SC průmyslový standard pro rozhraní PC-snímač ve verzi 1 a v nové verzi 2

Standardy přenosových protokolů

TPDU (Transmission Protocol Data Unit)

protokol T=0	(ISO/IEC 7816-3)
protokol T=1	(ISO/IEC 7816-3, Amd.1)
protokol T=2	(ISO/IEC10536-4)
protokol T=CL	(ISO/IEC 14443-3,4)

Standardy pro datové objekty

Datový objekt je formalizovaný podle pravidel Basic Encoding Rules (BER, ASN.1) podle standardu ISO/IEC 8825.

Tagy pro SM (secure messaging) jsou v ISO/IEC 7816-4.

4.1.6 OPERAČNÍ SYSTÉMY

§ Operační systémy (Smart Card Operating Systems)

§ Konvence: Pro operační systém smart karty bude používán akronym COS.

§ COS patří mezi tzv. „embedded OS“.

§ Rozdělení podle způsobu řízení operací na kartě a aplikačních profilů:

-karty se souborovými operačními systémy, pevná příkazová (instrukční) sada, příklady:
(Starcos/G&D, Cryptoflex-Cyberflex/Schlumberger, SIMphonIC/Oberthur, DKCCOS/Datakey..)

-karty na bázi otevřené platformy, příklady:
(Java Card, jayaCard OpenSource COS, Multos, ...)

Poznámka: V posledních 10 letech vznikly a rozvíjejí se trendy, kdy se nezávisle napsaný kód COS portuje na vybraný typ hardware karty, a je podporována přenositelnost karetních aplikací (viz dále). Přesto pořád setrvává tradice odběru karet i COS od jednoho výrobce

Důvody:

-Tradice. Dříve jiné karetní systémy, než hw+cos od jednoho výrobce, nebyly k dispozici

-Oficiální záruka naprosté kompatibility a korektního chování aplikací na kartě z odlišných zdrojů chybí.

-Snaha o přenositelnost aplikací je, ale kartu s runtime systémem a základní aplikací obvykle dodá tentýž výrobce.

Vývojové nástroje a emulátory

Pro vývojářskou přípravu smart karet (nikoliv jen aplikací) je zapotřebí tool pro embedded software

a) C kompilátor pro čip

b) čip simulátor pro debug (first level)

c) obvodový emulátor (ICE) s reálným čipem pro základní testy technologie programování a testy paměti

d) vývojářské karty s ROM-loaderem, který obsahuje čip pro alfa a beta testování.

Vlastní čipové karty prostřednictvím licence na COS

-COS lze opatřit jako software (viz seznam poskytovatelů výukových i licencovaných COS)

a „customizovat“ a implementovat na vhodný čip nezávisle na výrobci HW, viz předchozí odstavec.

-Zákazníkem kontrolovaná profilace řešení, týkající se adaptace vlastního čipu a vlastního software (adaptace COS). Dnes je tato low-level činnost realizovatelná za nižších nákladů než v 90. letech.

-Open Source čipové projekty díky tomu existují.

Ve všech obdobných projektech je podstatné - a realizačně nejdražší – dodržet kritéria průmyslové standardizace, bezpečnosti a spolehlivosti.

4.1.7 KLASICKÉ SMART KARTY S PEVNOU INSTRUKČNÍ SADOU.

Klasické karty nejsou programovatelné (v tom smyslu, že na ně nelze ukládat aplikační spustitelný kód, ale jen aplikační data).

Na kartu lze zasílat příkazy, které vykoná operační systém karty (COS).

Příkazy lze zaslat prostřednictvím API karetního snímače, PC/SC nebo OpenCard API.

Tento druh programátorské přípravy karetní aplikace vyžaduje podrobnou technickou dokumentaci s popisem příkazů na úrovni bitů.

Příklady klasických karetních COS:

- G&D, Starcos
- Gemplus, GEMSafe
- IBM, MFC 4.1
- Schlumberger (Axalto), Multiflex, Cyberflex, Cryptoflex, MicroPayflex

Smart karty se podle aplikačního hlediska rozdělují:

- Programovatelné karty (runtime)
- Klasické neprogramovatelné karty s pevnou instrukční sadou jejich COSu (Fixed-command smart cards)

Nástroje pro vývojáře

jsou dostupné jako:

- SDK pro smart karty
- softwarové balíky specifické pro aplikaci nebo třídu aplikací

Aplikace pro smart karty jsou psány ve vyšších jazycích, případně i v asemblerech.

Příklady:

„Basic Card“ od firmy Zeitcontrol – vývoj v mutaci Basic. Podpora souběžného vývoje aplikace karty a host-terminálu.

„MULTOS“ - smart karta opatřená operačním systémem MULTOS od MAOSCO. MULTOS karta může být personalizována (programována) v C, Java, Basic, MEL (assembler).

„DKCCOS“. Datakey ve svém operačním systému DKCCOS podporuje i assembler.

Vývoj a běh aplikací na klasické kartě s pevnou instrukční sadou:

- § Klasické, neprogramovatelné karty: je třeba chápat tak, že na kartě samé nelze spustit běh kódu poslaného na kartu. Lze jen z hostu vyvolat příkaz COSu, který zařídí operaci s aplikačními daty. (Jde o klasické smart karty s pevnou instrukční sadou).
- § Do karty lze poslat příkazy (APDU) přes snímač smart karty (API) nebo přes PC/SC API či OpenCard API.
- § Je zapotřebí disponovat detailní technickou specifikací karty včetně:
 - popisu příkazů na bitové úrovni
 - souborového systému
 - access controls (access conditions) pro soubory
 - klíče k odblokování karty.

VM - Smart Card Virtual Machines

Pro smart karty existuje několik operačních platform typu „virtual machine“ (VM). Nejrozšířenější jsou:

- MULTOS virtual machine
- Java Card virtual machine

Přenositelnost VM: Neplatí striktně, že je možné použít kartu s operačním systémem od jednoho výrobce a provozovat VM od jiného výrobce.

Příklady VM pro smart karty:

MAOSCO MULTOS, (C kód)
IBM Java Card Open Platform
Zeitcontrol BasicCard, (Basic kód)
Keycorp OSSCA, (Forth kód)
Exceldata, (Java kód)
jayacard.org, (Java kód)

Java Card

Současná verze Java Card je 2.2.

Každý výrobce definuje svojí vlastní mutaci (Java byte code set). Přenositelnost aplikací (apletů) se postupně zvyšuje. Cílem je dosáhnout spolehlivé přenositelnosti od výrobce k výrobci. Java Card Forum řeší problémy interoperability v nejnovějších verzích specifikace Java Card.

Někteří výrobci Java Cards a Java Card SDK:

Schlumberger: Cyberflex
Gemplus: GemXpresso
Giesecke & Devrient: Sm@rtCafe

4.1.8 BEZKONTAKTNÍ ROZHRAŇÍ KARTY A JAVACARD

Funkční požadavek [R1] na bezkontaktní provoz je v současném prostředí JavaCard splnitelný.

-JavaCard oficiálně podporuje bezkontaktní rozhraní karty (platí až od současné ver. 2.2).

-Průměrný faktor rozdílu výkonnosti mezi Java Card VM 2.2 a operačním systémem s pevnou instrukční sadou na „klasické“ smart kartě se udává v rozmezí 10-30% v neprospěch JavaCard.

(Zdroj: Trusted-Logic, 2004 aj.).

Rozdíl

- není významný při komunikaci přes kontaktní rozhraní
- je významný při bezkontaktním provozu

-Design Java Card aplikací pro bezkontaktní provoz: údajně náročnější a náchylný na méně standardní postupy a návrhářské triky pro snížení režie (konference eSMART'04, TL, 09/04). Virtual Machine 2.2 při podpoře rychlých procesů na bezkontaktním rozhraní preferuje „výkonnost na účet portability aplikací“

-Pro bezkontaktní provoz je obvyklé řešení „hrubou silou“: Trendem je implementace JavaCard na výkonnějším, ale dražším hardware smart karet (32bitové CPU, 64-128kB EEPROM).

Pro případné masové nasazení ve VŠ vzniká problém cenové přiměřenosti.

-Problémem může být emulace Mifare, související s požadavky na zpětnou kompatibilitu [R6] - pokud není ve smartkartě použit vhodný čip (např. kontroler Philips), garantující podporu této technologie.

-Na trhu se objevují (resp. připravují) JavaCards s RSA pro bezkontaktní (duální) provoz. Připravujeme jejich praktické ověření pro některé typy PKI aplikací na 1.kv./05.

Závěr:

Pro masové nasazení ve VŠ řešitelé nedoporučují orientaci na JavaCard / bezkontakt ISO 14443-3,4:

-v současné verzi 2.2

-při současných cenách na trhu 32bitových smart karet typu JavaCard.

Závěr vyhodnocuje i další argumenty, specifické pro prostředí VŠ:

-Charakter pro VŠ připravovaných nebo uvažovaných karetých aplikací nevyžaduje velký objem dat, resp. aplikační kód na kartě. Například autentizace uživatele a elektronický podpis nevyžadují ukládání dat z aplikací na karty uživatelů, ale stačí jejich centralizované zpracování.

-V dohledu nejsou nové požadavky na datově náročné typy aplikací (Současně používané čipové karty buď jen čtou SerialID nebo disponují 1kB paměti).

-V případě budoucí potřeby lze vlastními silami uskutečnit převod víceméně standardizovaných aplikací (ISO7816-4 a výše) do požadovaného prostředí.

Trendy kolem standardů:

-Konvergence ke standardu ISO/IEC 7816-4 (a výše, zejména ISO/IEC 7816-5, 8, 9).

-Novější implementace systémového prostředí vznikají vesměs podle ISO/IEC 7816-4,8,9. Trend se týká standardizace karetých části aplikace, APDU příkazů a systému souborů (resp. „emulace“ file systému v runtime systémech).

-Časová náročnost na jednorázový převod (přepsání) aplikace z jednoho karetního prostředí do druhého je díky standardizaci teoreticky nižší. „Teoreticky“ proto, že když se hovoří o zásahu do karetní aplikace, je nutno současně zvážit dopad změn na middleware, počínaje kryptoovladači.

Bez kontroly kódu pro middleware nelze se zárukou „karetní převody“ provádět.

Vývoj a správa karetních aplikací: Porovnání klasického COS a JavaCard

	Aplikace klasického COS (s pevnou sadou příkazů)	Aplikace JavaCard
Podpora ISO/IEC 7816	Ano	Ano
Dostupnost vývojových nástrojů	Solidní dodavatelé poskytují vývoj. nástroje a technickou specifikaci	Dodavatel poskytuje, část lze získat z různých zdrojů
Možnost vývoje aplikace nezávisle na dodavateli	Ano	Ano
Přenositelnost na vyšší verzi operační platformy (OS, JC) stejného výrobce	Podle listu kompatibility výrobce Obvykle ano, s manuální optimalizací vzhl. k inovaci HW	Teoreticky ano, prakticky po seznámení s doporučením implementátora JC po důkladném otestování
Přenositelnost aplikace na kartu jiného výrobce	Ne bez přepsání aplikace. Pracnost je menší při dodržení norem ISO7816-4,8,9 a PKCS#15	Teoreticky ano, současná specifikace JC negarantuje 100% kompatibilitu
Struktura aplikace	Na kartě jen data aplikace Na hostu řídicí kód (prostřednictvím CSP, PKCS#11, S-card apod)	Na kartě kód i data aplikace. Implikuje větší variabilitu a složitost aplikací, které nemusí být uniformní vzhledem ke standardům. Větší odpovědnost vývojářů za bezpečnost.
Náročnost vývoje a údržby	Nížší. Těžiště je ve správě middleware	Vyšší a komplexnější

Typ multiaplikační smart karty #1

Aplikace na kartě = aplikační data + služby operačního systému

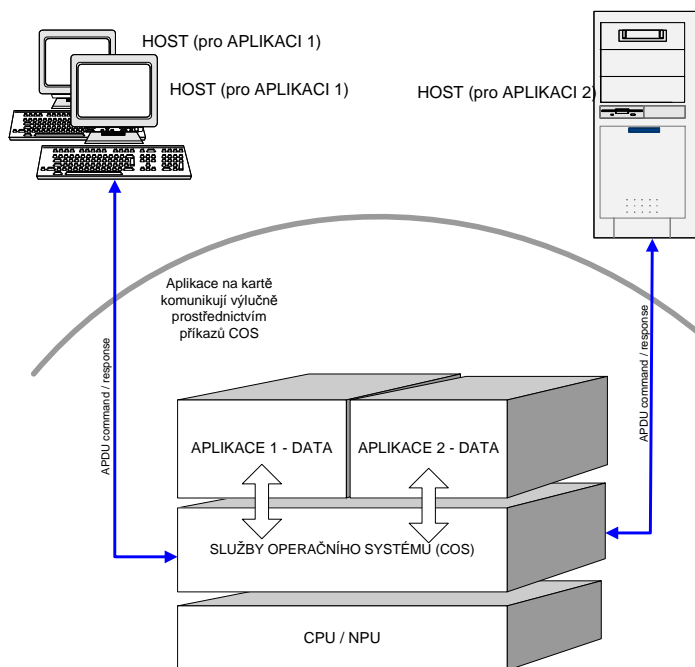


Diagram 2 Aplikace na klasickém COS jen prostřednictvím příkazů oper.systému

Typ multiaplikační smart karty #1

Aplikace na kartě = aplikační data + služby operačního systému

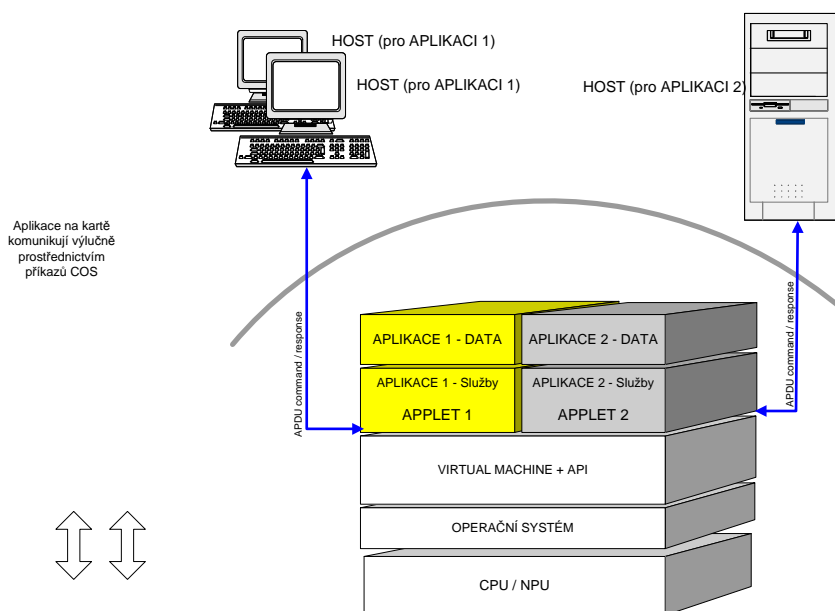


Diagram 3 Java Card Applet - data & kód

4.1.9 SOUBOROVÉ SYSTÉMY

Soubory

Všechny soubory uloženy v EEPROM (resp. v modifikacích této paměti, jako např. Flash EEPROM). V současných COS se neuzívá přímá fyzická adresace údajů na kartě. Standardem je objektově orientovaná správa souborů *file management* (a TLV-kódování datových objektů). Informace typu *access condition* jsou umístěny přímo v souborech.

Podle ISO/IEC 7816-4 jsou rozlišeny soubory:

MF (Master File) jako povinný a jedinečný „root“ na kartě,

DF (Dedicated Files) jako „adresáře“. Reprezentují a identifikují aplikace na kartě

EF (Elementary Files) jako datové soubory různé organizace (linear fixed, linear variable, transparent, cyclic, executable).

Soubory se tvoří příkazem CREATE FILE, parametry určují pravidla pro přístup do souboru (Access Conditions). Pro každou operaci nad souborem pravidla zvlášť určují, za jakých okolností lze se souborem danou operaci provést.

Každý soubor má *file descriptor* (užívaný název v oblasti smart karet: hlavička souboru, *file header*).

Minimální penzum informací v hlavičce:

Jméno (File name, např. FID='0003 ')

Typ (File type, např. EF)

Struktura (File structure, linear fixed)

Velikost (File size, 10rec, rec 10B)

AC (Access Conditions, Read Binary po zadání PINu)

Atribut (worm)

Link do stromové struktury (pod DF2)

Každý soubor má FID (File Identifier) (2bytes). DF soubory mají kromě FID také 1-16 bytový DF Name, který umožňuje jednoznačnou identifikaci karetní aplikace (mezinárodně). Aby nedocházelo ke kolizím v názvech, používá se DF Name pro uložení tzv. AID (Application Identifier). AID je definovaný v ISO/IEC 7816-5 (viz též ISO/IEC 7816-15). Jde (zjednodušeně) o správu identifikátorů aplikací různých dodavatelů na jedné kartě. AID obsahuje povinný, 5 bytů dlouhý RID (Registered Identifier), který je poskytovateli aplikace přiřazován určenou autoritou a 0-11 bytů PIX (Proprietary Application Identifier Extension), který může poskytovatel využít pro další identifikaci (rozlišení) aplikace, např. verze.

Soubory na kartě jsou uspořádány ve struktuře typu strom. Proto je nutno pro soubory specifikovat rodičovské vazby. Jsou užívány dva druhy nástrojů, pointery a alokační tabulky. Podle toho rozlišen *Pointer-based file management* a *FAT-based file management*.

Specifikum práce file managementu na kartě je mj. v ošetření charakteristik EEPROM paměti, kde roli hraje stránkování paměti i omezený počet zápisových a mazacích cyklů EEPROM. Správa souborů na kartě se musí preventivně vypořádat s potencionálními problémy interní bezpečnosti dat v EEPROM a soukromých klíčů zvlášť. Základní mechanismy: velikost každého souboru (header + body) musí být předdefinována. Informace *file managementu* od obsahu souborů jsou striktně odděleny (na separované stránky paměti).

Při řízení práce s volnou (velmi omezenou) pamětí je základním požadavkem udržení dobře definovaného stavu stromové struktury v každém okamžiku session. (Kartě může být kdykoliv přerušeno napájení ze snímače). V opačném případě může dojít k narušení bezpečnosti.

Operační systém rovněž řeší fragmentaci paměti (garbage collection).

4.1.10 APLIKACE PRO PROGRAMOVATELNÉ A NEPROGRAMOVATELNÉ KARTY

Aplikace pracující se smart kartami se skládá z částí: 1.karetní aplikace, 2.host-aplikace.

Vývojář flexibilně kontroluje host-aplikaci, tj. vždy může doplnit aplikaci kódem, který vykoná žádanou manipulaci s daty na hostu. Není tomu tak obecně v případě karetní aplikace.

a) Karta s pevnou instrukční sadou: není programovatelná

Při návrhu host-aplikace pracující s kartou smí vývojář použít pouze některý příkaz z omezené instrukční sady, kterou podporuje COS. COS s pevnou instrukční sadou nelze rozšířit o nový příkaz nebo novou službu. To je jen v pravomoci výrobce operačního systému karty v době vývoje karty.

b) Programovatelná karta:

Při návrhu aplikace nemusí vývojář použít příkaz z instrukční sady, která je na kartě implementována. Napíše program realizující *nový příkaz* a provede jeho load na kartu. Tím je implementován na kartě *nový příkaz*, který host-aplikace použije k přístupu na kartu.

Aplikace je pod vývojářskou kontrolou nejen na straně straně hostu, ale i na straně karty.

Na každé programovatelné kartě běží VM (virtual machine), který interpretuje natažený kód. V prostředí programovatelných karet vznikla větší vývojářská flexibilita, za kterou se platí určitou ztrátou výkonu. Cílem v kategorii nejrozšířenějších programovatelných karet JavaCard je portabilita aplikací (appletů), nezávisle na výrobci karty a runtime systému.

Mezi programovatelné karty patří například Multos card, Microsoft's Smart Card for Windows, Zeitcontrol's Basic Card, většina Java Cards.

Rizikové faktory, které je třeba vzít do úvahy při bližším průzkumu nebo výběru technologie JavaCard:

-Problémy s binární kompatibilitou. Přenést applet z jedné karty na druhou znamená mít zdrojový kód a překompilovat jej.

-Není plně zaručena zdrojová kompatibilita mezi mnoha různými verzemi JavaCard specifikací.

-Značný rozdíl v rychlosti mezi konkurenčními implementacemi JVM (Java Card Virtual Machine), (zdroj: IBM, Buhler, bup@zurich.ibm.com).

(Například, jestliže applet, použitý pro bezkontaktní provoz, při změně JVM poběží 2-3x pomaleji, stává se karta nepoužitelnou)

Zatím je pro uživatele bezpečnější vybrat jednoho komplexního dodavatele karet i jeho implementaci JavaCard (JVM) a na této platformě vyvíjet a podporovat své aplikace.

Což se příliš neliší od postupu používaného u karet opatřených pevnou instrukční sadou.

4.1.11 SMART KARTY A BEZPEČNOST DAT

Bezpečnostní certifikace PKI-karet (tokenů, HSM).

Americká norma FIPS (vydaná NIST) může mít úrovně 1 až 4. Pokud karta získá certifikaci, většinou je to FIPS 140-2 level 2.

Evropská norma ITSEC má úrovně E1 Basic až E6 High. Čipové karty/tokeny dosahují většinou úrovně E4 High.

Norma CC (Common Criteria) - EAL. Tato norma je následovníkem ITSEC. Celkem má 7 úrovní. Čipové karty/ tokeny s certifikací E4 High zhruba odpovídají EAL 5.

Bezpečnostní firmy/asociace vydávají proprietární certifikáty pro karetní produkty, které byly odzkoušeny s jejich systémem (např. Entrust ready).

5 ID-KARTA S DUÁLNÍM ROZHRAŇÍM

Identifikační funkce karty, svodka

Smart karty budou v rámci projektu aplikačně připravovány a testovány, jak na bezkontaktním, tak i kontaktním rozhraní pro identifikaci osob, zejména technikou identifikace na bázi certifikátů.

Jak bylo uvedeno v kap. 2, základní úlohy jsou:

-ověřování identity okolí, se kterým držitel karty komunikuje (osob, technických i programových prostředků, procesů),

-nabídnout okolí, se kterým držitel karty komunikuje, bezpečné ověření své identity.

Funkční vlastnosti požadované karty implikují technické vlastnosti karty:

(Poznámka: Odkazované funkční požadavky [Rx] uvedeny v kap. 3.2.)

- § provoz karty na bezkontaktním rozhraní ISO/IEC 14443, přenosový protokol T=CL.
(Důsledek [R1] a [R2])
- § provádění kryptografických operací na kartě prostřednictvím koprocesorů RSA a 3DES (především e-podpis klíčem, který je uložen na kartě, bezpečná a autorizovaná aktualizace dat, silná autentizace)
(Důsledek [R4], [R5], [R3] ve spojení s požadavkem na rychlost operací při bezkontaktní komunikaci implikuje implementaci s koprocesory. Technologie RSA a 3DES převažují. Existují implementace karet s AES i 3DES. Otázka ceny)
- § možnost kryptografického ověření pravosti karty, vysoký stupeň ochrany proti různým formám útoků a kopírování karty
(Důsledek [R3] a automatický důsledek současné sofistikované technologie smart karet)
- § technická a bezpečnostní podpora pro více aplikací na kartě, možnost jejich výmazu a aktualizace
(Důsledek [R6] – podpora starších aplikací i nových aplikací založených na páru klíčů)
- § možnost uložení dat, a to jak v elektronické, tak vizuální formě, v rozsahu 8kB a více (vede ke kapacitě EEPROM 16kB nebo 32kB)
(Velikost jednoho digitálního ID - dvojice klíčů + certifikát - pro e-podpis se pohybuje kolem 2-3kB (záleží na šifře – délce klíče, počtu a obsahu jednotlivých položek certifikátu). Je třeba počítat ještě s daty uživatele, režii pro souborový systém. Aplikace na kartě typu přístup ke službám, peněženka, bezpečné úložiště hesel aj. zaberou max. 1-2kB. Oblast Mifare 1kB. Lze rezervovat místo pro profily middleware, systémů jako je Entrust Ready aj., které mohou na čipu zabírat až 6kB. Jako minimální velikost paměti EEPROM pro ID-kartu lze doporučit 16kB).
- § bezpečná úložiště malých (řádově několik kB) dat, která je třeba chránit.
(Na správě soukromých klíčů je karta postavena, není třeba zmiňovat. Ale dat, jako jsou hesla, šifrovací klíče, sdílená tajemství, certifikáty, kódy atd. se to týká rovněž).
- § vícekanálová komunikace karetních aplikací s host-aplikacemi

(Možnost mít s kartou položenou na snímači otevřeno několik karetních aplikací naráz, používat současně několik klíčů na kartě, jde o přidanou funkcionalitu některých typů smart karet, např. i SPK 2.5DI)

§ Funkčnost technologie Mifare Standard na kartě, separované od ostatní struktury karty, podle ISO/IEC 14443A-3

(Důsledek požadavku [R6], [R7])

5.1 BEZPEČNOSTNÍ MECHANISMY

Import/Export klíčů

§ RSA páry klíčů pro PKI je možné na kartě vygenerovat nebo je importovat z certifikační autority.

Poznámka: Kvalita implementovaných šifrovacích algoritmů a zejména generátoru náhodných čísel by měla být u smartkarty obecně o něco nižší, než např. v případě kryptografického modulu HSM chránícího soukromý klíč CA. Tento faktor je v praxi smart karet spíše akademický (např. nemají za úkol generovat klíč CA) a je bohatě vyvážen bezpečným prostředím karty pro neexportovatelné a *non-readable* soukromé klíče.

Poznámka: Délka soukromého klíče 1024 bitů pro klienta je optimální ve střednědobém výhledu z pohledu doporučení kryptoanalytiků i z pohledu časových nároků na kryptooperace při bezkontaktním provozu karty.

Je zapotřebí vygenerovat podpisový pár a šifrovací pár klíčů.

Existují asi tyto základní možnosti, které se promítnou do certifikačních politik:

RSA pár **vytvořen přímo na kartě** - jednoznačně nejbezpečnější. Soukromý klíč z této dvojice nelze exportovat z karty (nelze jej ani číst). Proto odpadá možnost zálohování soukromého klíče. To je problém při ztrátě či krádeži karty v případě šifrovacího soukromého klíče vzhledem k archivu zašifrovaných dokumentů držitele karty.

Nevadí u podpisového klíče. Lze vygenerovat nový podpisový pár v rámci nového procesu žádosti o certifikát a zároveň zneplatnit starý certifikát.

Závěr: Generování RSA páru na kartě je vhodné pro podpisovou dvojici klíčů.

Poznámka: Problém ztráty karty, ve které je nezálohovaný pár asymetrické šifry RSA tkví v tom, že je sice možné přečíst držitelem karty digitálně podepsané emailové zprávy, ale není možné přečíst zprávy, které byly držiteli karty zaslány a byly šifrované.

RSA pár pro šifrování je vytvořen **v nějakém software (například určenou autoritou)** s provedením zálohy (stanovit roli odpovědnosti za zálohu). Potom RSA pár pro šifrování v podobě souboru bude importován do smart karty.

Export uloženého soukromého šifrovacího klíče z karty už nebude možný. Proto musí být záloha vytvořena před importem.

Poznámka:

Pokud je zvoleno takové provozní řešení na straně klienta, kdy soukromý klíč uživatele ukládán na přenositelné medium, které nepodporuje asymetrickou kryptografii (např. USB flash disk, MIFARE paměť na kartě chráněné symetrickou šifrou), jde jen a jen o ekvivalent výrazně slabšího řešení na bázi soft-tokenů ukládaných na disketu. Obecně veškerá řešení, kdy je soukromý klíč během zpracování natažen do operační paměti PC, jdou na úkor bezpečnosti. Každé obdobné řešení má dvě vady:

-neposkytuje úroveň bezpečnosti a mobility jako standardní PKI-karta (PKI-token)

-jde o odklon od průmyslového trendu který vyžaduje proprietární vývojovou podporu navíc.

5.2 APDU PŘÍKAZY

Klasifikace příkazů na ID-kartě (ISO/IEC 7816)

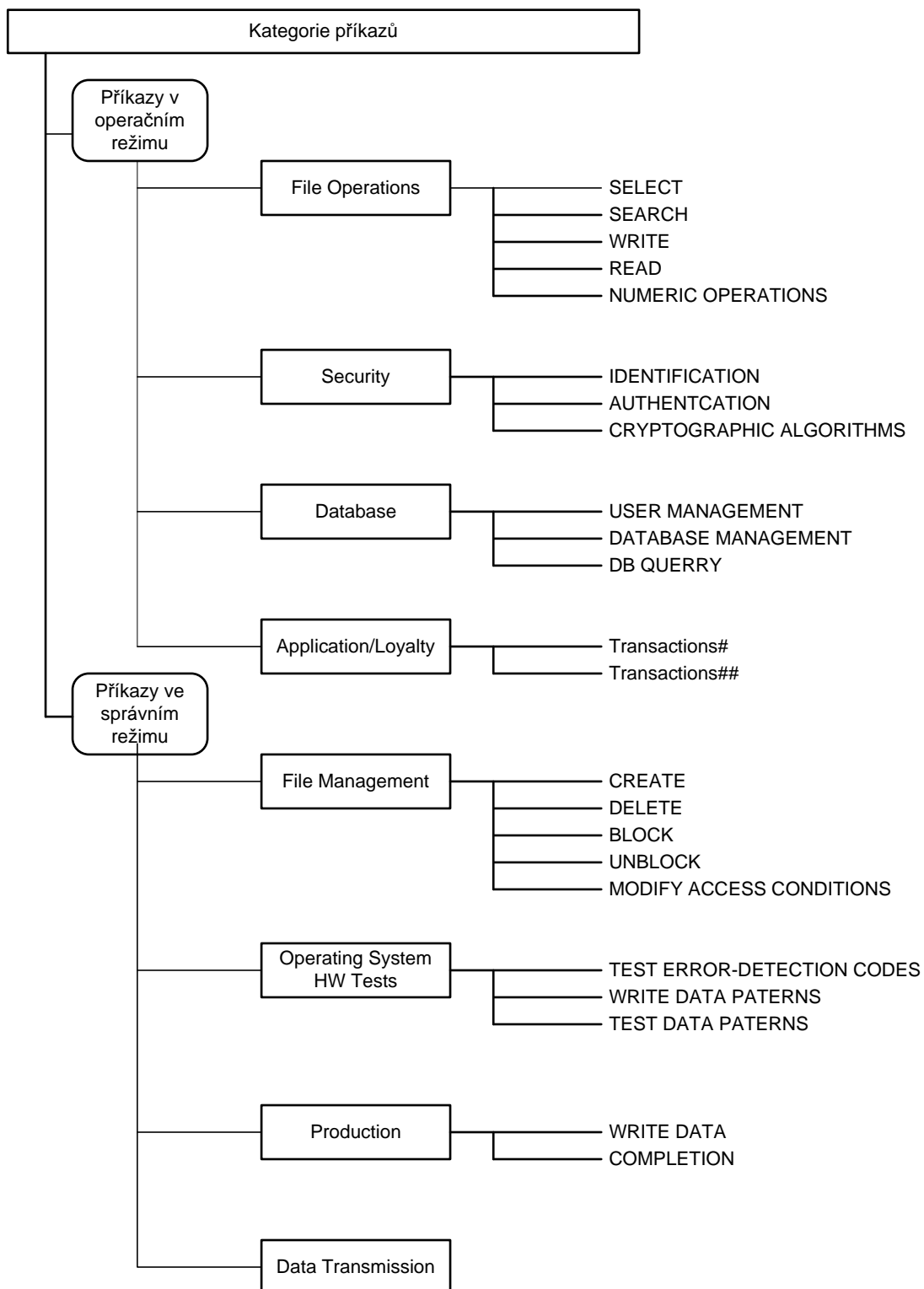


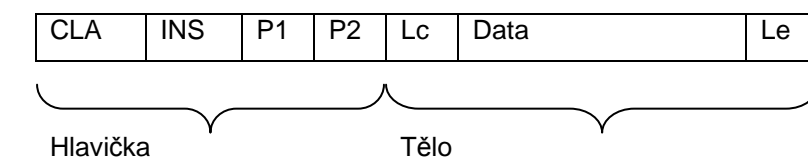
Diagram 4 Základní klasifikace příkazů COS (APDU, ISO/IEC 7816)

Poznámka: Hodnoty v následujících tabulkách jsou uváděny hexadecimálně.

APDU

Pro přenos dat mezi terminálem a kartou se používá tzv. APDU (Application Protocol Data Unit). Jedná se o strukturu přenášených dat, která je nezávislá na použitém přenosovém protokolu (T=1, T=CL apod.). Rozlišují se dva typy APDU – *command APDU* (posílaný terminálem) a *response APDU* (posílaný kartou).

Command APDU



CASE 2:

Příkaz, při kterém se přenášejí data pouze z karty na terminál. Obsahuje hlavičku a Le byte.

Příklad: READ BINARY (přečte data z EF souboru s transparentní strukturou. P1/P2 udává ofset (zde 32), Le udává počet čtených bytů (zde 16)):

CLA	INS	P1	P2	Le
00	B0	00	20	10

CASE 3:

Příkaz, při kterém se přenáší data pouze z terminálu na kartu. Obsahuje vše kromě Le.

Příklad: UPDATE BINARY (zapiše data (zde samé nuly) do EF souboru s transparentní strukturou. P1/P2 udává ofset (zde 32), Lc udává počet zapisovaných bytů (zde 4)):

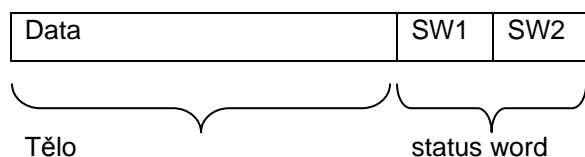
CLA	INS	P1	P2	Lc	Data
00	D6	00	20	04	00 00 00 00

CASE 4:

Příkaz, při kterém se data přenášejí v obou směrech.

Příklad: GENERATE PUBLIC KEY PAIR (vygeneruje klíč s identifikátorem určeným v P2 (zde 5) o délce určené v datové části APDU (zde 1024 bitů), vrátí modulus)

CLA	INS	P1	P2	Lc	Data	Le
00	46	00	05	02	04 00	00

Response APDU

5.2.1 KEY MANAGEMENT

Global key – klíč v MF, který je označen jako globální, lze použít ve všech DF souborech (reprezentujících jednotlivé aplikace). Typickým příkladem je PIN sdílený více aplikacemi.

Volby: Asym, 3DES, PIN

Default key – V každém elementárním souboru typu ISF (Internal Security File) lze jeden z klíčů každého typu označit jako default. Při použití tohoto klíče potom není nutné uvádět jeho identifikátor.

Volby: 3DES, PIN

Session key – dočasný klíč sloužící ke zvýšení bezpečnosti. Při každé transakci (session) je použit jiný klíč odvozený ze sdíleného symetrického klíče a náhodného čísla, které si terminál s kartou mezi sebou vymění pomocí EXCHANGE CHALLENGE.

Volby: DES

Poznámka: hodí se pro kontrolní součty (e-peněženka)

Karta má chránit data. Jak, to se nastaví při čipové personalizaci (access conditions). Všechny neplatné pokusy odmítne, platný pokus přijme.

Derived key – Každá karta vlastní svůj symetrický klíč. Pro jednodušší správu klíčů na terminálu jsou tyto klíče pro každou kartu odvozeny z tzv. master klíče a sériového čísla karty. Terminálu pak stačí udržovat pouze master klíč.

Poznámka: Default, session a derived klíče nelze použít s asymetrickými klíči.

Poznámka: Asymetrický klíč nelze označit jako default

Z asymetrického klíče nelze z principu odvodit další klíč (ani session, ani derived)

5.2.2 SEZNAM PŘÍKAZŮ APDU IMPLEMENTOVANÝCH NA SPK2.5DI

Tab. 1 Seznam příkazů APDU (implementace na SPK2.5DI)

Název	Použití		Výstup
File management			
CREATE	Vytvoření souboru		
DEFRAGMENT FILE	Defragmentace souboru		
DELETE FILE	Smazání souboru		
LOCK FILE	Dočasné uzamčení souboru		
REGISTER DF	Alokace paměti pro DF		
SELECT FILE	Aktivace souboru	P	

Data management			
DECREASE	Snížení čítače v compute souboru		Nová hodnota čítače
ERASE OBJECT FILE	Smazání obsahu object souboru		
GET DATA	Čtení dat ze souboru typu object	P	Čtená data
INCREASE	Zvýšení čítače v compute souboru		Nová hodnota čítače
PUT DATA	Zápis dat do souboru typu object	P	
READ BINARY	Čtení dat ze souboru typu binary	P	Čtená data
READ RECORD	Čtení ze souboru typu linear fixed	P	Čtený záznam
UPDATE BINARY	Zápis dat do souboru typu binary	P	
UPDATE RECORD	Zápis do souboru typu linear fixed	P	
Other (Transmission management, card life cycle management)			
GET RESPONSE	Čtení odpovědi (pouze T=0)	P	Odpověď case 4 příkazu
MANAGE CHANNEL	Otevírání a zavírání logických kanálů	P	Počet otevřených logických kanálů
TERMINATE CARD USAGE	Ukončení životního cyklu karty	P	
PIN management			
CHANGE REFERENCE DATA	Změna PINu při znalosti současného PINu	P	
RESET RETRY COUNTER	Nastavení nového PINu pomocí PUK	P	
VERIFY AND CHANGE	Změna PINu pomocí PUK nebo stávajícího PINu		
Key management			
GENERATE PUBLIC KEY PAIR	Generování nového key pairu	P	Veřejný klíč
KEY STATUS	Zjištění čítače chybných pokusů		Čítač chybných pokusů
LOCK KEY	Nevratné znepřístupnění klíče		
READ PUBLIC KEY	Čtení IPF		Veřejný klíč
WRITE KEY	Zápis klíče		
Authentication			
EXCHANGE CHALLENGE	Výměna náhodných čísel	P	Náhodné číslo
EXTERNAL AUTHENTICATE	Autentizace terminálu kartou	P	
GET CARD DATA	Zjištění sériového čísla karty		Sériové číslo karty

GET CHALLENGE	Generování náhodného čísla	P	Náhodné číslo
INTERNAL AUTHENTICATE	Autentizace karty terminálem	P	Autentizační data
MUTUAL AUTHENTICATE	Vzájemná autentizace karty a terminálu		Autentizační data
VERIFY	Autentizace držitele karty (ověření PINu)	P	
Cryptographic functions			
COMPUTE SIGNATURE	Výpočet e-podpisu	P	e-podpis
CRYPT	Šifrování symetrickým klíčem		Zašifrovaná / odšifrovaná data
ENCIPHER / DECIPHER	Šifrování asymetrickým klíčem	P	Zašifrovaná / odšifrovaná data
HASH	Výpočet / nastavení hash	P	Hodnota hash
MANAGE SECURITY ENVIRONMENT	Nastavení parametrů pro následující kryptografické výpočty	P	
PERFORM SECURITY OPERATION	Viz COMPUTE SIGNATURE, ENCIPHER / DECIPHER, HASH, VERIFY CERTIFICATE a VERIFY SIGNATURE	P	
VERIFY CERTIFICATE	Bezpečné uložení veřejného klíče s ověřením certifikátu	P	
VERIFY SIGNATURE	Ověření e-podpisu	P	

Ve sloupci tabulky výstup jsou uvedené pouze typické výstupní hodnoty. Za různých okolností může mít příkaz jiný výstup (např. po nastavení hodnoty hash (která byla již vypočítána mimo kartu) pomocí příkazu HASH karta nic nevrací). Všechny příkazy navíc vrací *status word*. Jedinou výjimkou je TERMINATE CARD USAGE, který nevrací nic (při úspěchu).

Třetí sloupec označuje příkazy, které jsou definovány ISO/IEC normou. Neznamena to, že je příkaz implementován *plně* podle dané normy.

5.2.3 DOBA VYKONÁNÍ PŘÍKAZŮ

Přístup k souborům

READ BINARY (20 bytes)	4,6 ms	
READ BINARY (240 bytes)	6,2 ms	
READ RECORD (20 bytes)	1,4 ms	(1 rec fix length)
READ RECORD (240 bytes)	3,1 ms	(1 rec fix length)
UPDATE BINARY (20 bytes)	14, 7 ms	

UPDATE BINARY (240 bytes) 28,0 ms

Key Management, autentizace

INTERNAL AUTHENTICATE	2,6 ms	3DES
EXTERNAL AUTHENTICATE	35,2 ms	3DES
GET CHALLENGE	6,8 ms	
VERIFY PIN	39,8 ms	
WRITE KEY (15bytes)	19,9 ms	(Secure Write)
WRITE KEY (249 bytes)	33,9 ms	(Secure Write)

CREATE DF 25,3 ms

SELECT FILE 1,3 ms

CRYPT (8 bytes) 3,2 ms (3DES)

MANAGE SECURITY ENV 2,6 ms

VERIFY CERTIFICATE 113 ms (195 bytes certification)

GENERATE PUB KEY PAIR 9 508 ms (1024bit)

Generování páru klíčů je samozřejmě časově nejnáročnější proces (odehraje jen několikrát v průběhu životního cyklu karty). Pro generování klíčů je výhodné použít kontaktní rozhraní.

5.2.4 AUTENTIZACE MEZI KARTOU A TERMINÁLEM

Autentizace držitele karty se provádí prostřednictvím PIN (PUK). Příkaz VERIFY

tj. karta ověřuje identitu držitele

Autentizace zařízení - 3DES, RSA. Příkaz EXTERNAL AUTHENTICATE

tj. karta ověřuje identitu zařízení

Autentizace karty - 3DES, RSA. Příkaz INTERNAL AUTHENTICATE

tj. karta prokazuje svou identitu nějakému subjektu (např.terminálu)

Vzájemná autentizace příkazem MUTUAL AUTHENTICATE.

5.3 VÝPOČET DIGITÁLNÍHO PODPISU

**Postup výpočtu digitálního podpisu pomocí StarCOS SPK 2.5 DI
(Ilustrační příklad)**

Vstupy: KIDpk – *kartový* identifikátor soukromého klíče pk (velikost 1 byte)

HASH – SHA-1 otisk (hash) podepisovaných dat (20 bytes)

KIDpin – *kartový* identifikátor PINu, který chrání použití soukromého klíče KIDpk (1 byte)

Výstup: SIG – podpis dat podle PKCS#1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002, Sekce 8.2.1

Předpoklady: karta byla resetována, příkazem SELECT vybrán odpovídající DF soubor reprezentující aplikaci na kartě se soukromým klíčem pk, který má být použit k podpisu

Tab. 2 Postup výpočtu digitálního podpisu na kartě SPK2.5DI

	Karta		Terminál														
1		☞	PIN = uživatelem zadaný PIN VERIFY PIN: <table border="1"> <thead> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>DATA</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>20</td> <td>00</td> <td>KIDpin</td> <td>08</td> <td>PIN</td> <td></td> </tr> </tbody> </table>	CLA	INS	P1	P2	Lc	DATA	Le	00	20	00	KIDpin	08	PIN	
CLA	INS	P1	P2	Lc	DATA	Le											
00	20	00	KIDpin	08	PIN												
2	RESPONSE: <table border="1"> <thead> <tr> <th>Data</th> <th>SW</th> </tr> </thead> <tbody> <tr> <td></td> <td>90 00</td> </tr> </tbody> </table>	Data	SW		90 00	è	Je-li SW = 90 00, pokračuj dál. Je-li SW tvaru 63 Cx, jdi na krok 1. Jinak konec (chyba)										
Data	SW																
	90 00																
3		☞	MANAGE SECURITY ENVIRONMENT: <table border="1"> <thead> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>DATA</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>22</td> <td>81</td> <td>B6</td> <td>06</td> <td>84 01 KIDpk 80 01 12</td> <td></td> </tr> </tbody> </table>	CLA	INS	P1	P2	Lc	DATA	Le	00	22	81	B6	06	84 01 KIDpk 80 01 12	
CLA	INS	P1	P2	Lc	DATA	Le											
00	22	81	B6	06	84 01 KIDpk 80 01 12												
4	RESPONSE: <table border="1"> <thead> <tr> <th>Data</th> <th>SW</th> </tr> </thead> <tbody> <tr> <td></td> <td>90 00</td> </tr> </tbody> </table>	Data	SW		90 00	è	Je-li SW = 90 00, pokračuj dál, jinak konec (chyba)										
Data	SW																
	90 00																
5		☞	PUT HASH: <table border="1"> <thead> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>DATA</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>2A</td> <td>90</td> <td>81</td> <td>14</td> <td>HASH</td> <td></td> </tr> </tbody> </table>	CLA	INS	P1	P2	Lc	DATA	Le	00	2A	90	81	14	HASH	
CLA	INS	P1	P2	Lc	DATA	Le											
00	2A	90	81	14	HASH												
6	RESPONSE: <table border="1"> <thead> <tr> <th>Data</th> <th>SW</th> </tr> </thead> <tbody> <tr> <td></td> <td>90 00</td> </tr> </tbody> </table>	Data	SW		90 00	è	Je-li SW = 90 00, pokračuj dál, jinak konec (chyba)										
Data	SW																
	90 00																
7		☞	COMPUTE SIGNATURE: <table border="1"> <thead> <tr> <th>CLA</th> <th>INS</th> <th>P1</th> <th>P2</th> <th>Lc</th> <th>DATA</th> <th>Le</th> </tr> </thead> <tbody> <tr> <td>00</td> <td>2A</td> <td>9E</td> <td>9A</td> <td></td> <td></td> <td>00</td> </tr> </tbody> </table>	CLA	INS	P1	P2	Lc	DATA	Le	00	2A	9E	9A			00
CLA	INS	P1	P2	Lc	DATA	Le											
00	2A	9E	9A			00											
8	RESPONSE: <table border="1"> <thead> <tr> <th>Data</th> <th>SW</th> </tr> </thead> <tbody> <tr> <td>SIG</td> <td>90 00</td> </tr> </tbody> </table>	Data	SW	SIG	90 00	è	Pokud SW = 90 00, pak je SIG požadovaný podpis, jinak chyba										
Data	SW																
SIG	90 00																
9			Konec														

Výpočet digitálního podpisu (e-podpisu) na kartě (viz předchozí obr.) probíhá ve stepech 1 až 9. Čísla 1 až 9 v prvním sloupci označují jednotlivé kroky komunikace “host (terminál) – karta” probíhající na bázi APDU příkazů.

1. Terminál požádá uživatele o zadání PINu, převede jej do tvaru podle ISO/IEC 7816-4 a pošle jej společně s KIDpin na kartu příkazem VERIFY PIN.
2. Karta *mimo jiné*: v ISF vyhledá záznam s daným KID, zkontroluje, že se jedná o PIN a zkontroluje, že nastavená bezpečnostní pravidla umožňují PIN v dané chvíli použít. Pokud je PIN blokováný, vrátí 69 83, jinak porovná PIN v ISF se zadaným PINem. Pokud se shodují, nastaví čítač chybných pokusů na původní hodnotu (nastavenou při personalizaci) a vrátí hodnotu 90 00, jinak sníží čítač chybných pokusů. Pokud je čítač roven nule, PIN je zablokováán a vrátí hodnotu 69 83, jinak vrátí 63 Cx, kde x je hodnota čítače. Pokud dojde k nějaké chybě, vrátí odpovídající chybový kód.
3. Terminál pošle příkaz MANAGE SECURITY ENVIRONMENT, ve kterém uvede, že se jedná o výpočet podpisu (bytes 81 B6), KID privátního klíče, který má být použit (KIDpk), a identifikátor algoritmu (byte 12 – označuje RSASSA-PKCS1-v1_5 s SHA-1 hashem)
4. Karta *mimo jiné*: ověří platnost parametrů, zkontroluje, že klíč s daným KID existuje, je kompletní, může být použit k výpočtu podpisu. V případě úspěchu jsou parametry kartou dočasně uloženy a karta vrátí hodnotu 90 00, jinak vrátí odpovídající chybový kód.
5. Terminál pošle kartě SHA-1 hash pomocí příkazu PUT HASH.
6. Karta si *mimo jiné*: hash dočasně uloží a pokud nedojde k chybě, vrátí hodnotu 90 00.
7. Terminál pošle požadavek na výpočet digitálního podpisu pomocí příkazu COMPUTE SIGNATURE.
8. Karta *mimo jiné*: ověří, že byly nastaveny parametry pomocí MANAGE SECURITY ENVIRONMENT, že byl nastaven platný hash, že délka hashe odpovídá požadovanému algoritmu a že nastavená bezpečnostní pravidla umožňují klíč v dané chvíli (tj. byl správně ověřen PIN). V případě úspěchu vypočítá digitální podpis a vrátí jej s návratovým kódem 90 00, jinak vrátí odpovídající chybový kód.

Poznámka:

Kroky 1, 3, 5 ukazují APDU příkazy typu request podle ISO 7816 (CLA='00'). Příkaz je vždy iniciovaný aplikací (host), provedení je zprostředkováno kryptografickými mechanismy hostu (moduly CSP, PKCS#11) a příkaz zaslaný na kartu prostřednictvím příslušných vrstev protokolů

APDU --- T=x,

kde T je transmission protocol, T = 0 nebo 1 v případě, že je aktivní kontaktní rozhraní. T=CL při bezkontaktním provozu.

Kroky 2, 4, 6, 8 ukazují APDU typu response. V příkladu znázorněné kroky 2, 4, 6 a 8 *nepopisují detailně akce*, které vykonává operační systém karty – pouze věci zajímavé pro výstup z procesu

(response kódy). Proto v tabulce zdůrazněno „mimo jiné“. Cílem příkladu není popisovat programový kód aplikace resp. kryptoovladačů, ani procesy v pozadí OS karty či kód StarCOSu (který není dostupný ve zdrojové formě).

5.4 DUÁLNÍ MULTIAPLIKAČNÍ KARTY PRO PKI

Komunikace PKI/ID-karty s aplikací resp. se systémovou vrstvou odpovědnou za kryptografické operace (např. ověření e-podpisu) je běžná přes kontaktní rozhraní typu T=0, T=1. (ISO 7816). Tento typ komunikace nepokrývá veškeré požadavky kladené na ID-kartu vzhledem ke striktní podmínce [R1].

Komunikace PKI/ID-karty prostřednictvím *bezkontaktního rozhraní* (ISO 14443,1-4, T=CL) klade větší nároky na optimalizaci výkonu HW karty a na COS (nutná např. kratší odezva příkazů a operací s daty předávaných na kartu). Bezkontaktní rozhraní pro PKI/ID-karty bylo ohlášené v r.2002² (G&D) a je dostupné od r. 2003.

Důvody ve prospěch duální karty jsou:

- § podporovat současný průmyslový trend v ID kartách je lepší, než jednoúčelovou technologií 10-15 let starou.
- § kombinace rozhraní ISO/IEC14443-4, ISO/IEC14443-3 (Mifare) a ISO/IEC7816 pokrývá výčet všech známých aplikací VŠ³. Nepatří tam žádná, která by nešla upgradovat. Některé aplikace řešitelné ihned, jiné s určitou pracností.
- § část strojového parku snímačů 125kHz na školách pochází z 90.let. Po přirozené výměně vznikne prostor pro čtečky ISO/IEC14443 a pro duální kartu.
- § Ostatní důvody jsou z PKI:
- § software bude udržovatelné podle *Public Key Cryptography Standards* – PKCS#11, PKCS#15, CSP
- § datové aplikace karty podle ISO/IEC7816-4, 5, 8 budou mít dobrý základ přenositelnosti na následnou platformu
- § uložení dvou tří párů klíčů včetně příslušných certifikátů X.509
- § digitální identita v přenositelné podobě: kapacita paměti čipové karty je dostatečně velká pro na jedné kartě sdílení několik konkurenčních certifikátů a několik aplikací.

bezpečnostní:

- použité prostředky garantují dostatečnou bezpečnost (3DES, RSA),
- bezpečnost manipulace s kartou je založená na dvou faktorech, které jsou vzájemně propojeny: disponování předmětem (karta) a disponováním znalostí (PIN), lze přidat třetí – biometrický faktor, za cenu zvýšených nákladů,

² IBM 1999, první funkční prototypy duální ID-karty (impl.3DES) na čipu Philips

³ Seznam zasílali v r.2002 respondenti jednotlivých škol skupině ID-karta v dotazníkové akci.

PIN a jeho chování či rozsah lze nastavit/vypnout v závislosti na karetní aplikaci,

lze též nastavit povinnost zadat PIN na snímači opatřeném pinpadem.

(věc politiky: nastavení při inicializaci karty a datové struktury, resp. administrátorem)

– kryptografická identita klienta je bezpečně uložena v kartě,

– kryptografické algoritmy jsou prováděny přímo v čipu karty;

Výhody pro držitele karty:

– vysoký stupeň ochrany proti kompromitaci, defraudaci,

– jednoduché použití všude, kde je instalován odpovídající middleware a PC/SC čtečky, ve VŠ pak prioritně bezkontaktní čtečky

– rozšíření funkčnosti při zachování stejné identifikace;

výhody pro VŠ organizaci:

– jednotný prostředek autentizace studenta, zaměstnance, hosta, zároveň pro větší počet aplikací,

– možnost využití externích certifikačních autorit, jestliže se organizace (škola) rozhodne, že nebude budovat vlastní CA.

5.4.1 POŽADAVKY NA PKI KLIENTA

Stručná rekapitulace přístupu ke správě klíčů:

Na straně serverové části CA/PKI se bezpečnost opírá o zabezpečení soukromého klíče CA: Certifikační a bezpečnostní politika týkající se ochrany soukromého klíče CA je v certifikační autoritě pracující s citlivými daty řešená spolehlivě (pomocí HSM nebo oddělením serveru s CA od sítě).

Na opačné straně infrastruktury se důvěryhodnost identity uživatele (osoby) opírá o *ochranu soukromého klíče uživatele* - ta je z principu ponechána na uživatelově odpovědnosti.

Bezpečnost správy a přechovávání soukromých klíčů se řeší dvojím způsobem: pomocí *soft-tokenů* nebo *hardwarových tokenů*.

-*Soft-tokeny*. Pro klíče a certifikáty pro osoby ukládané jako zašifrované soft-tokeny na desktopech platí, že kompromitace klíčů při masovějším nasazení je statisticky nevyhnutelná. Vydat a udržovat sto tisíc certifikátů s příslušnými klíči jen jako data na studentských počítačích (i sdílených), znamená zvýšené organizační nároky na společně využívanou techniku ve VŠ. Znamená to iniciovat permanentní řetěz řešení problémů se ztrátou, napadením viry, útoky ze sítě, prozrazením hesla k souboru (lidský faktor), revokací, expirační dobou. Užití soft-tokenů při přístupu k citlivějším datům a podepisování citlivých zpráv je kvůli lidskému faktoru poměrně riziková záležitost (známé incidenty z obdobné bankovní praxe).

-*HW-tokeny*. čipové karty s certifikátem a privátními klíči – poskytují řádově vyšší ochranu soukromého klíče uživatele i vyšší mobilitu uživatele. Jde o preferovaný způsob zavádění PKI.

Soukromý podpisový klíč je z principu neodmítnutelnosti odpovědnosti uložen výhradně na čipové kartě uživatele, *na níž byl vytvořen* a kterou nikdy neopustí. Pokud o něj uživatel přijde, musí požádat o vygenerování nové dvojice klíčů (resp. napřed o novou kartu) v souladu s platnou certifikační politikou.

Soukromý šifrovací klíč je uložen na čipové kartě uživatele, *na níž byl importován*. Jeho kopie je navíc zálohována prostřednictvím předem určené odpovědné autority. Pokud o šifrovací klíč uživatel přijde, požádá autoritu o nové vytvoření „uživatelského profilu“ obsahujícího starý šifrovací klíč (přesněji dvojici klíčů - veřejný a soukromý).

S ohledem na průkaznost a mobilitu certifikátů (soukromých klíčů) proto praktická využitelnost e-podpisu a PKI úzce souvisí s technicky propracovaným řešením pro čipové karty a demonstrací jejich funkčnosti pro používané OS a aplikace. Masové nasazení v praxi může být s výhodou realizováno prostřednictvím studentského průkazu nové generace.

Úkoly, týkající se podpory řešení PKI-klienta.

Byly shrnuty následovně:

- varianty datové struktury a aplikací na kartě
- systematická práce na modulu CSP, později PKCS#11
- testy nových produktů v oblasti bezkontaktních/duálních PKI-karet
- testy v oblasti bezkontaktních/duálních PKI-karet
- rozšíření certifikačních politik CA - zohlednění čipového media
- příprava prototypu registrační autority realizující žádost o certifikát vydáním čipové karty

5.4.2 POŽADAVKY NA ZPĚTNOU KOMPATIBILITU KARET

Standard ISO/IEC 14443A

Protože většina (viz poznámka) současně provozovaných aplikací čipových karetních systémů na VŠ je založena na standardu Mifare (ISO/IEC 14443-3), ve skupině pro ID-karty vznikl požadavek zpětné kompatibility navrhované ID-karty právě s technologií Mifare.

Poznámka: Statistika ze škol (II/2003), viz Skupina pro ID karty - ČVUT, OU, JU, UJEP, UK, UP, UPCE, VŠE, VUT, VŠZ a ZČU. Přibližně 164000 uživatelů. Cca 37% VŠ nepoužívalo čipovou technologii, 31% VŠ využívalo Mifare, 23% H4002/125kHz atd.

SPK2.5DI podle technické specifikace i testování požadavek kompatibility splňuje. Nicméně závěry bude možno učinit až po rozsáhlejších testování (několik desítek karet) v praktických podmínkách (pracoviště na 3-4 VŠ, různé snímače založené na různých čtecích modulech (RC500 a výše).

Srovnávací testy: Předmětem navržených srovnávacích testů bylo ověření chování vzorků karet v laboratorní i běžné praxi . Jako vzorky sloužily karty SPK25.DI, originál Philips Mifare, Studentský průkaz Mifare od výrobce Siemens.

Interní testy (pracoviště Coprosys) karta-čtečka prošly. Byl testován OEM čtecí modul pro technologii Mifare typu RC500.

Dále použit: Mifare toolkit Philips, referenční snímač RD700/Pegoda, 100MHz osciloskop, sampler.

Pokračování testů: Pro externí testy několik vzorků karet SPK2.5DI zapůjčeno na VŠ pro testování na provozních aplikacích a na provozovaných čtečkách.

Metody přípravy testů, komunikace karta - snímač

Cílem testů bylo verifikovat správnou funkčnost protokolu mezi PCD a kartou.

Pro terminologii testů viz specifikaci ISO/IEC 14443-3.

Zkušebně postaveno monitorovací zařízení na krystalu pro VF signál 13.56MHz (rezonanční obvod karty), a data transfer 106 kHz (modulace)

-Odchycení komunikace, analýza logu.

-Sledování Manchester modulace a loop REQA – AC - SEL - HALT pro detekci kolize,

-Detekce seriového čísla (UID)

-Citlivost modulace - čtecí modul opakovaně vysílá request (REQA – hex26) a detekuje ATQA. Výstup

- na připojeném displeji, přijímané hodnoty ATQA. Následně sledovány modulační charakteristiky prostřednictvím sampleru.

6 INFRASTRUKTURA SMART KARET

6.1 PROTOKOL PC/SC

- § Standardizace rozhraní pro snímače smart karet je proti ostatním komponentám ICT o několik let opožděna: pro kontaktní, bezkontaktní rozhraní, dokonce i v případě USB rozhraní. API jsou založena většinou na proprietárních řešeních. Hlavní proud standardizačního úsilí se týká specifikace Personal Computer/Smart Card (akronym PC/SC). PC/SC specifikace ve verzi 1 byla implementována ve Windows a Linuxu. Nová specifikace PC/SC ver.2 zahrnuje i bezkontaktní rozhraní.
- § Informace o verzích a částech standardu na adrese <http://www.pcscworkgroup.com>.
 - Part 1 - Přehled architektury a relevantních standardů
 - Part 2 - Požadavky na rozhraní pro kompatibilní karty a snímače (od fyzických, elektrických, příkazových charakteristik smart karet k přenosovým protokolům T=x)
 - Part 3 - Požadavky na rozhraní zařízení připojených k PC (monitor, keypad atd.)
 - Part 4 - Informace týkající se návrhu terminálů s USB a PS/2 rozhraní
 - Part 5 – ICC (Integrated Chip Card) Resource Manager
 - Part 6 - ICC Service Provider s popisem technických a softwarových aspektů CSP (Crypto Service Provider) a ICC Service Provider.
 - Part 7 – Popis PC/SC specifikace z aplikační perspektivy
 - Part 8 – Doporučení pro ICC Security, zahrnuje funkce a mechanismy, které by měly být podporovány ze strany PC/SC smart karet, např. MF, DF, EF, jejich AC (access conditions), return kódy aj.
- § Seznam PC/SC snímačů podporovaných ve Windows a kompatibilních s PC/SC (v.1), např. na adrese <http://www.microsoft.com/hcl/default.asp> (Smart Card Readers).
- § PC/SC řešení a implementace týkající se Linuxu pro řadu typů snímačů smart karet: <http://www.linuxnet.com>
- § Konektivita snímače s využitím CSP (Cryptographic Service Provider): <http://www.wave.com/technology/csp.html>

Poznámka: Spolupráce mezi ovladačem terminálu pro připojení karty SPK2.5DI dle standardu PC/SC a modulem CSP, který tuto kartu používá jako prostor pro uchovávání soukromých klíčů je otestována s kladným výsledkem. Jiné standardy než PC/SC zatím nebyly soustavně testovány v jiném režimu než Mifare. Problematika je důležitá z pohledu podpory dalších aplikací na školách, kde figurují bezkontaktní čtečky různého typu, pořízené v různé době a jejich technická katalogizace není provedena.

6.2 MIDDLEWARE

PKCS#11, MS CAPI a podpora tokenů v oblasti programování.

K realizaci přicházejí do úvahy dvě řešení. Pomocí **Microsoft Cryptographic API (MS CAPI)** nebo na základě **Cryptoki (standard PKCS#11)**. Obě bude nutno naprogramovat.

CSP bude součástí každého cílového řešení pro komunikaci s ID/PKI-kartou ve Windows, které poskytuje služby systém (CryptoApi), jako „kryptografický ovladač karty„.

CSP je komponenta middleware, která *musí* znát kartu včetně nestandardizovaných vlastností).

CSP bude hlavní součástí middleware určeného pro Windows platformu pravděpodobně v distribuci CESNET.

6.2.1 CRYPTOAPI A OCSP

Aplikace pro komunikaci s kartou využívají:

- pro kryptografické účely CryptoAPI
- pro ostatní - rozhraní SCard

§ SCard

- zajišťuje abstrakci nekryptografických funkcí smartcards (zejména práce se soubory)

§ CryptoAPI:

spravuje úložiště certifikátů

- poskytuje podporu šifrování a rozhraní kryptografických služeb CSP (Cryptographic Service Provider). Podpora zahrnuje certifikáty X.509, CRL prostřednictvím obecných kódovacích /dekódovacích funkcí, rozboru a ověření certifikátu. Podporují se také požadavky na certifikáty PKCS#10 a PKCS#7 pro podepsaná a zabalená data.

§ CSP (odpovídá výrobce karet, resp. dodavatel CSP)

realizuje kryptografické funkce

spravuje úložiště privátních klíčů

- pomocí software (např. registry)
- pomocí hardware (např. čipová karta)

§ Správce zdrojů (resource manager)

je zodpovědný za správu všech přístupů na všechny karty vložených do všech čteček
všechny požadavky na smartcard jdou přes resource manager

§ Ovladače čteček

zajišťují komunikaci se čtečkou (příkazy typu: resetuj kartu, pošli na kartu APDU, odpoj kontakty, rozsviť diodu, ...)

čtečka a její ovladače by měly být kompatibilní s PS/SC specifikacemi

Modul CSP komunikuje prostřednictvím rozhraní PC/SC a čtečky s kartou. Aplikace (s příkazem pro generování) volá systémovou vrstvu CryptoApi. CryptoApi aktivuje CSP. CSP „zná kartu“ a realizuje příkaz vygenerovat pár klíčů na kartě. CSP umožňuje pracovat se soukromým klíčem a certifikátem uloženými na kartě SPK2.5DI, a to jak v kontaktním režimu (ISO/IEC 7816), tak při použití *bezkontaktního* rozhraní (ISO/IEC 14443A). Základní testy na aplikacích e-mail -Outlook,

browser IE. Funkce podepsání e-mailu, ověření podpisu příjemcem, šifrování a dešifrování zprávy, komunikace browser –server s výměnou certifikátů funkční na bezkontaktní i kontaktní čtečce.

Čtečky se vyrábí v několika provedení: sériové čtečky (připojené k sériovému portu COM a napájené přes rozhraní PS/2), USB čtečky, PCMCIA čtečky (pro notebooky), pinpad (čtečka s klávesnicí a displejem), PC klávesnice se čtečkou čipových karet a biometrické čtečky využívající jako přístupové heslo biometriku (např. otisk prstu).

Některé technologické zásady řešení snímačů:

http://www.technick.net/index.php?load_page=http%3A//www.technick.net/cir_smartcardemu.php

API snímačů.

Většina snímačů je opatřena vlastním kontrolerem. Implementace příslušného API je více či méně proprietárního původu. Výrobci snímačů drží API buď pod svou kontrolou (velká většina) nebo poskytují vývojářům veřejnou podporu (SDK od www.traditor.fi nebo API od www.spyrus.com).

6.2.1.1 Životní cyklus karet

Z obrázku (Diagram 5) jsou zřejmé jednotlivé role, známé na VŠ, kde provozují karetní systémy.

- výrobce (vendor)
- vydavatel (issuer)
- držitel karty (cardholder)

1) Obchodně technické vztahy s výrobcem

- otázka dohody grafického provedení bílých karet a velmi kvalitního statického potisku (neměnné logo aj., ochranných prvků aj.
- otázka garance skladovaných karet (typicky 3 roky a více)
- otázka, zda bude zahrnut místní mezičlánek pro provedení designu karty a jak garance
- otázka dodací lhůty. 1000 – 5000 karet je komorní zakázka s nízkou prioritou, která má čekací dobu na výrobní-personalizační linky výrobce třeba 3-4 měsíce.

2) Vydavatelem bude patrně (každá) škola.

Riziko je, že role vydavatele ID-karet je náročnější organizačně i technicky, než např. distribuce karet Mifare. Vhodná je softwarová spoluúčasť technické jednotky (údržba, rozvoj). Nutná provázanost s registrační autoritou (RA).

Proces vydání má několik stepů a je zakončen předáním karty držiteli, odpovídá RA. Vytvoření aplikace, generování páru klíčů a následný proces žádosti o certifikát bude zakončený nahráním certifikátu na kartu. Držitel obdrží kartu a PIN. Při distribuci PINu půjde o poměrně sofistikovanou proceduru (vzpomeňme na bankovní karty).

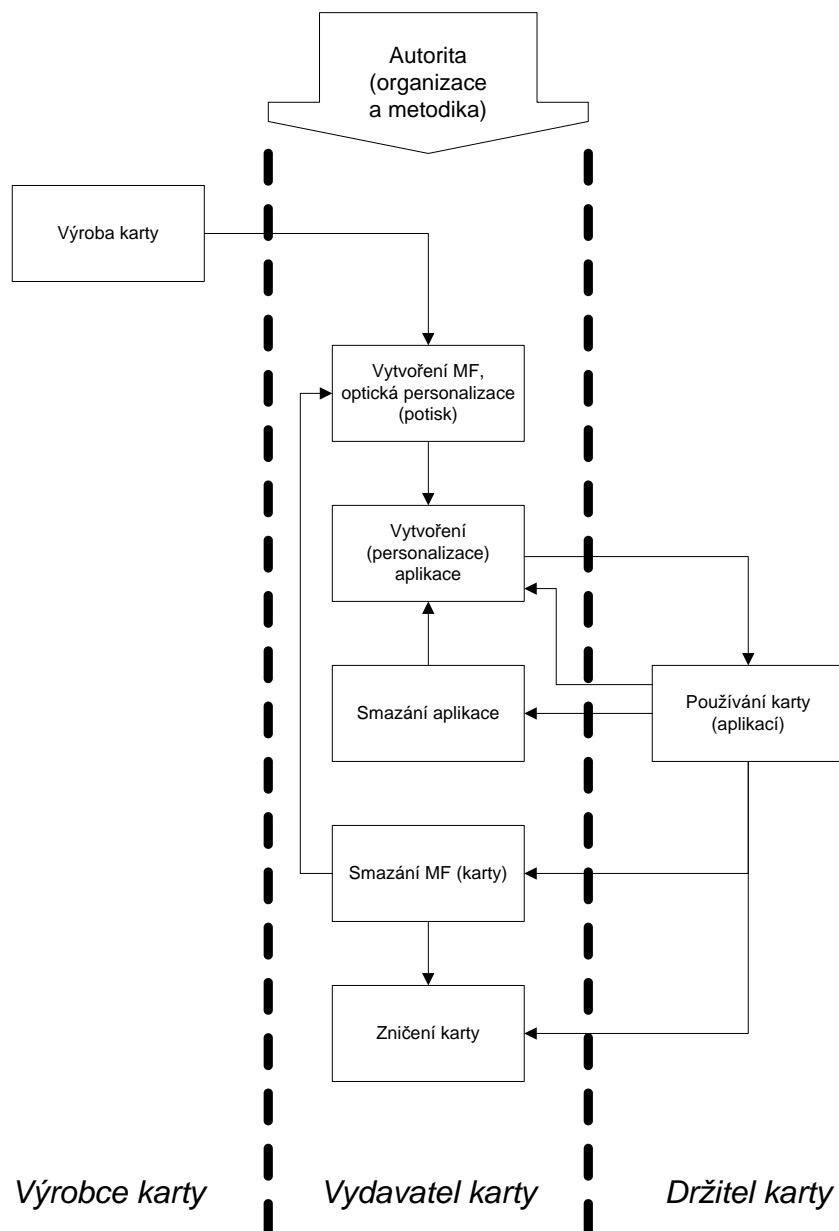


Diagram 5 Životní cyklus karty

Metodická kontrola (nejlépe externí) autority s určitými pravomocemi musí vynutit soulad s příslušnými politikami a prováděcími směrnicemi pro vydavatelskou jednotku.

3) Držitel karty se obrátí na vydavatele (např. na RA nebo určenou autoritu):

- v případě blokace PINu. (V příkladové „šabloně“, viz Poznámka za Tab.4 v kapitole popisující tvorbu aplikací nebo kap.Rámec úkolu pro PKI, je politika na kartě nastavena tak, že odblokování provádí držitel pouze na dedikovaném místě.

- v případě změny nebo přidání aplikace
- v případě krádeže/ztráty/zrušení karty
- v případě obnovy šifrovacího klíče

Musí být též upraveny expirační procedury (klíč, certifikáty)

Musí být upraveny postupy, týkající se koexistence certifikátu VŠ a jiného certifikátu (např. CESNET) na kartě.

6.2.1.2 Klíče na kartě

Klíče pro správu aplikací na kartě, rekapitulace, viz též 5.2.1.

- § Globální klíč – používá se pro sdílení klíče (nebo PINu) mezi více karetními aplikacemi
- § Default klíč - v případě více klíčů stejného typu lze jeden klíč nastavit jako default. (Pokud prostředky mimo kartu při použití klíče neurčí specifický klíč, karta použije default)
- § Derivované klíče – slouží pro zjednodušení správy klíčů – každá karta má klíč derivovaný z nějakého master klíče (pomocí např. sériového čísla karty). Komunikujícímu systému pak stačí znát jeden klíč pro více karet (a samozřejmě odvozovací postup)
- § Session klíče – pro každou transakci jiný (odvozuje se z klíče uloženého na kartě)
- § Každý klíč si udržuje tzv. KFPC – Key Fault Presentation Counter – určuje, kolik nekorektních pokusů použít klíč vede k jeho zablokování (např. 3x chybně zadaný PIN)

6.3 KRITICKÉ PROCESY PRO SPRÁVU KARTY

Následující odstavce popisují typické situace týkající se správy karty/aplikací a **příklad** jejich řešení.

1. Žádost o certifikát pro e-podpis

- probíhá v těchto krocích:

- a) generování dvojice klíčů (key pairu) na kartě
- b) export veřejného klíče a vytvoření žádosti o certifikát
- c) vytvoření certifikátu certifikační autoritou
- d) uložení certifikátu na kartu

- Zásada: žádnou z těchto operací nemůže provést držitel karty, ale pouze oprávněná autorita. Ta je kartou ověřena pomocí symetrického klíče, který je uložen v odpovídajícím DF.

2. Obnova certifikátu pro e-podpis

- např. při expiraci, při ztrátě karty nebo při zablokování PINu
- řešeno generováním nového key pairu, viz odstavec 1

3. Žádost o certifikát pro šifrování

- probíhá v těchto krocích:

- a) generování (a uchování v archívu) key pairu mimo kartu
- b) vytvoření certifikátu certifikační autoritou
- c) uložení key pairu na kartu
- d) uložení certifikátu na kartu

- Zásada: prováděno pouze oprávněnou autoritou, viz odstavec 1

- je navíc nutný další symetrický klíč (uložený v daném DF), kterým bude chráněn privátní klíč při ukládání na kartu

4. Obnova certifikátu pro šifrování

- řešeno pomocí archívu šifrovacích klíčů

- viz odstavec 3, kroky c, d

5. Změna PINu

- držitel karty si může změnit PIN, pokud zná stávající PIN a ten není zablokovaný

- změnu lze provést na jakémkoliv terminálu (PC), který má patřičný software (tj. na dedikovaném pracovišti)

6. Ztráta PINu

- držitel si může změnit PIN, pokud zná PUK

- změnu lze provést na jakémkoliv terminálu, který má patřičný software (tj. na dedikovaném pracovišti)

7. Vytvoření nové karetní aplikace

- je možné pouze po prokázání pravosti pomocí symetrického klíče, který je uložen v MF

8. Smazání karetní aplikace nebo celé karty

- je možné pouze po prokázání pravosti pomocí symetrického klíče, který je uložen v MF

7 PROFIL TECHNICKÉ PŘÍPRAVY ČIPOVÉ MIGRACE

Implementace karet ní technologie do systémů PKI a zároveň do „klasických aplikací“ v prostředí VŠ je víceletou řešitelskou a investiční akcí. Technické řešení má v optimálním případě splňovat požadavky formulované v ID-skupině a již diskutované ([R1] až [R7]). Projekt zahrnuje vývojové práce, pilotní ověření prototypů a přípravu technické základny pro čipovou personalizaci a podporu registračních autorit.

7.1 ÚKOLY A ETAPY

Profil (draft) jednotlivých okruhů (úkolů a etap) technické přípravy načrtnut v bodech [1] – [16].

(Kartou se rozumí nová ID-karta splňující požadavky na funkčnost [R1] až [R7]):

- [1] Výběr a testování typu (typů) karty, technická dokumentace včetně technické specifikace, vývojářské toolkity
- [2] Smluvní zajištění a otestování základní optické personalizace na průmyslové bázi v kvalitě úměrné předpokládané životnosti karty (4-5 let)
- [3] Zajištění koncové optické personalizace (potisk prvků specifických pro uživatele, obvykle v místě vydání karty).
- [4] Iterační procesy spojené s čipovou personalizací (analýza, návrh, implementace prototypu, implementace finálního řešení). Týkají se rovněž všech bodů [5] až [14].
- [5] Návrh a odladění datové struktury, aplikační architektury karty včetně administrace. Návrh prototypu pro základní pilotní ověření. Finální návrh konfrontovaný se známými a hlavně předpokládanými potřebami VŠ.
- [6] Řešení správy klíčů na kartě a pinů, distribuce pinů (pinových obálek).
- [7] Struktura a počet aplikací na kartě pro PKI v rámci kapacity EEPROM.
- [8] Adaptace aplikací ze staré generace karet (řešení zpětné kompatibility).
- [9] Integrace karty do procesů týkajících se žádosti o certifikát a odraz v certifikačních politikách.
- [10] Softwarové zajištění čipové personalizace (vývoj), technické řešení aktualizace aplikací na kartě (výmaz, přidání)
- [11] Konzolidace bezpečnostní politiky pro karty a certifikační politiky CA, jejíž certifikáty bude karta obsahovat.
- [12] Optimalizace řešení pro využití karty jako nosiče více certifikátů a klíčů pro více autorit (CA), s nimiž vysokoškolská organizace (nebo uživatel) vyžaduje vytvoření důvěryhodné zóny.
- [13] Zajištění funkčnosti „kryptoovladačů“ a middleware (na bázi PKCS#11 a CSP) pro vybraný typ (typy) karty a pro používané SW platformy (Windows, Unix/Linux). Vývojová podpora pro middleware v rozsahu potřebném pro zajištění volné nekomerční distribuce pro akademickou komunitu.

- [14] Návrh a technické zajištění distribuce karet uživatelům přes registrační místa (RA), řešení správy šifrovacích klíčů, řešení CMS (Card Management System) pro správu životního cyklu karet.
- [15] Samostatným okruhem řešení je kompatibilita karet se stávajícími (zejména bezkontaktními) snímači karet a technická doporučení, týkající se pořizování nových snímačů pro VŠ.
- [16] Samostatným okruhem řešení je dosažení kompatibility karet s hybridními snímači vyvíjenými v ZČU na bázi bezkontaktních snímačů starší generace (125kHz).

Stav v jednotlivých bodech

-Každý z bodů [1], [4], [5]-[8], [10], [13], [15] byl nebo je předmětem analýzy, určité fáze vývoje a testování v rámci úkolu (CoProSys).

-Dokončení těchto dílčích úkolů je plánováno na I/2005 pro vybraný prototyp karty (CoProSys).

-Piloty na VŠ menšího rozsahu lze zahájit souběžně s dokončováním předchozích úkolů. (VŠ ve spolupráci s CoProSys)

Poznámka: (Další typy karet, produktů). Případný požadavek na profilaci a odzkoušení řešení založeném na dosud netestovaném typu karty lze odhadnout na 3 čiměsíce. Za předpokladu, že bude k dispozici podrobná technická specifikace ověřovaného produktu (není samozřejmostí!) a vývojový toolkit.

K dalším bodům:

Body [2] a [3] se týkají optické personalizace, která není předmětem tohoto úkolu. Musí být ale částečně připravena pro potřeby ověřovacího provozu. Při vydávání několika set karet není vhodné pracovat s „bílymi kartami“.

Body [9], [11], [12] se promítnou do certifikačních politik. Řešení bude nutné konzultovat a řešit v součinnosti s administrátorem CA CESNET a s dalšími VŠ autoritami, včetně ZČU.

Bod [14] je kritickou částí projektu pro organizační složitost. Nebyl ještě rozpracován.

Nelze vynechat komentář porovnávající technickou stránku řešení s ostatními aspekty projektu. Technická stránka řešení je po vynaložené práci řešitelů dostatečně čitelná a může být dále vedena jako standardní IT-projekt a podprojekty. Nicméně jde o snažší část realizace ve srovnání s organizačními procesy, distribučními, servisními a školicími požadavky provádějícími vznikající projekt čipové migrace. Operativní stupeň koordinace (systémové integrace) bude v dalších etapách nutný.

Příklad: Koordinace je nezbytná například při specifikaci obsahové stránky a datové struktury na kartě, zejména co se týče povinného využití identifikačních údajů na kartě. Jde o záležitost v kompetenci VŠ, která by mohla být řešena v rámci Skupiny pro ID-karty.

Poznámka: Příklady identifikačních dat, která mohou být uložena na kartě nebo využívána pomocí karty:

-Seriové číslo karty (dosud nejčastější užitý identifikátor, není invariantní při ztrátě karty)

-Certifikát (veřejný, není invariantní kvůli době expirace – kontinuita přes atributy)

Položky, které jednoznačně identifikují uživatele/studenta na certifikátu a kartě, je nutné teprve stanovit, včetně jejich formátu.

Je možné zavést *bezvýznamový identifikátor*, po vzoru MPSV.

-E-podpis dokumentu prostřednictvím soukromého klíče.

7.2 PRACOVNÍ VERZE SPECIFIKACE ID-KARTY

Viz též kap.5.

Neoficiální specifikace požadavků na funkce a parametry ID-karty. Slouží jako pracovní podklad pro skupinu ID-karty:

Duální rozhraní kontaktní/bezkontaktní, na jednom čipu

Minimálně 16 kB EEPROM pro aplikace

Rychlé symetrické šifrování (3DES, ...)

Asymetrický kryptografický koprocesor (**RSA min. 1024b**), generování páru klíčů

Komunikace prostřednictvím rozhraní ISO 14443A, ISO 7816

Update dat funkcí a aplikací v průběhu života karty

Na zřeteli dále

-požadavek na interoperabilitu, který v praxi sleduje **vzájemnou spolupráci karty a čtečky karet od různých výrobců.**

-**požadavek zpětné kompatibility (čtečky a aplikace Mifare)**

Všechny tyto požadavky splňuje karta G&D SPK 2.5DI.

S kartou SPK 2.5DI lze zajistit aplikační kontinuitu (běh aplikací, dosud závisejících na kartách starší generace) v případech, že použité bezkontaktní snímače již pracují (nebo budou upraveny) podle norem ISO 14443-3 a ISO 14443-4.

7.3 SOFTWAREVÁ PŘÍPRAVA KARTY (ČIPOVÁ PERSONALIZACE)

Dodané karty SPK2.5DI byly inicializovány prostřednictvím toolkitu vyžádaného od výrobce G&D.

Realizováno několik variant návrhu datové struktury (viz dále).

Ověřena podpora: výmaz souborů a reinicializace, přidávání aplikací (novinka umožňující zvýšit morální životnost karty).

Detekovatelné a funkční je rovněž rozhraní Mifare (std,1kB)

Čipová personalizace karty zahrnuje:

Podklady pro aplikace na kartě.

Předběžné kapacitní výpočty (viz dále Tab. 3).

Vytváření objektů na kartě - návrh datových struktur, počet a umístění klíčů na kartě, pravidla pro přístup k souborům aplikacím, pravidla práce s identifikátory, autentizace, key management, PIN a jeho vlastnosti aj.

7.3.1 NÁVRH APLIKAČNÍ STRUKTURY KARTY: ÚVOD

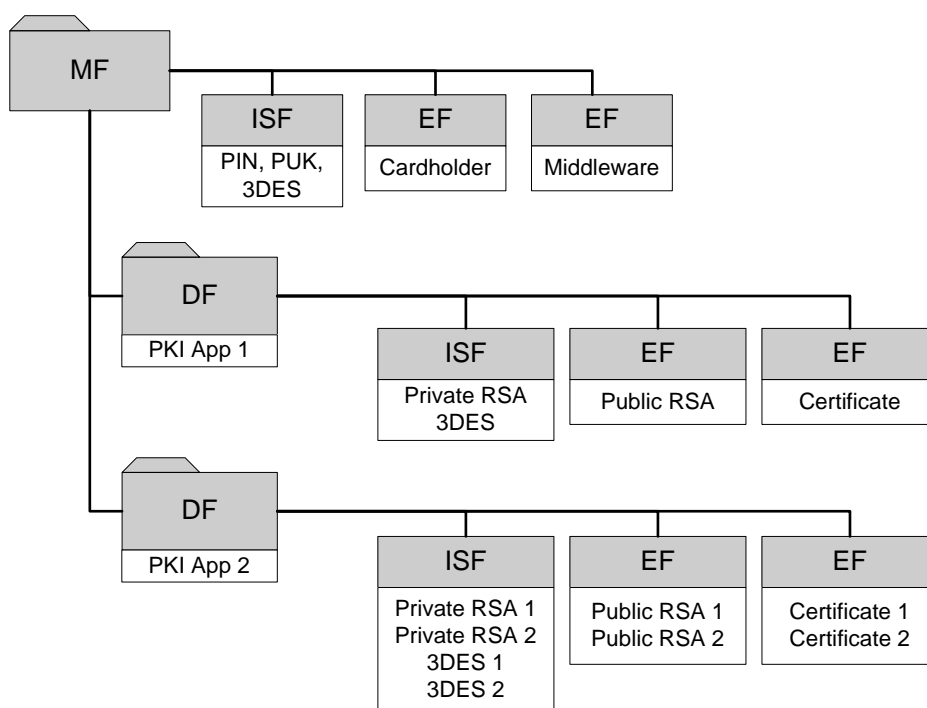
Při návrhu karty je nutno učinit řadu rozhodnutí, která ovlivňují chování karty i organizační postupy spojené s předávkou karty, s užíváním karty a ukončením provozu karty (tj. s celým životním cyklem karty).

Dále jsou popsána dvě z mnoha možných řešení. První je proprietární návrh aplikace (nazván proprietární, protože nepoužívá PKCS#15), druhý návrh vychází z normy PKCS#15, vydané též v podobě ISO/IEC 7816-15 (2004).

V obou případech jde o řešení základní multiaplikační struktury pro PKI aplikace (pro PKI-klienta).

Pro popis použita standardní terminologie (viz např. 4.1.9 a dále 7.3.2).

- **NÁVRH DATOVÉ STRUKTURY KARTY**
- =Typy objektů a jejich uspořádání=
-
- Typy objektů: pro PKI aplikace
- Aplikace: 2 DF
- Varianta: Proprietární řešení, tj. nonPKCS#15
- Odkaz: (následující popis a tabulka)



Obr. 8 Typy objektů ve FS na kartě s 2 PKI-aplikacemi. Bez PKCS#15.

7.3.2 NÁVRH PROPRIETÁRNÍHO ŘEŠENÍ BEZ VAZBY NA PKCS#15

Komentář k obr.8, Typy objektů ve File Systému na kartě s dvěma PKI-aplikacemi. Řešeno bez pravidel normy PKCS#15. Takový způsob nazván proprietárním.

MF obsahuje informace společné všem aplikacím, především:

- informace o držiteli karty (například jméno, adresa, fotka)
- PIN držitele pro přístup k privátním klíčům, sdílený aplikacemi
- PUK pro odblokování PINu
- informace využívané v middleware

- symetrický klíč pro autentizaci zařízení, které je oprávněno manipulovat s aplikacemi na kartě (přidávání a mazání aplikací, př. výmaz celé karty)

DF PKI App 1 je PKI aplikace s podpisovým RSA key parem. Tento key pair je generován kartou, privátní část je uložena v ISF, veřejná v jednom EF souboru. Další EF soubor obsahuje certifikát k tomuto páru. Pro vygenerování key pairu a uložení nového certifikátu je nutná autentizace zařízení, které tyto operace provádí. Tato autentizace probíhá pomocí symetrického klíče v ISF (Internal Security File).

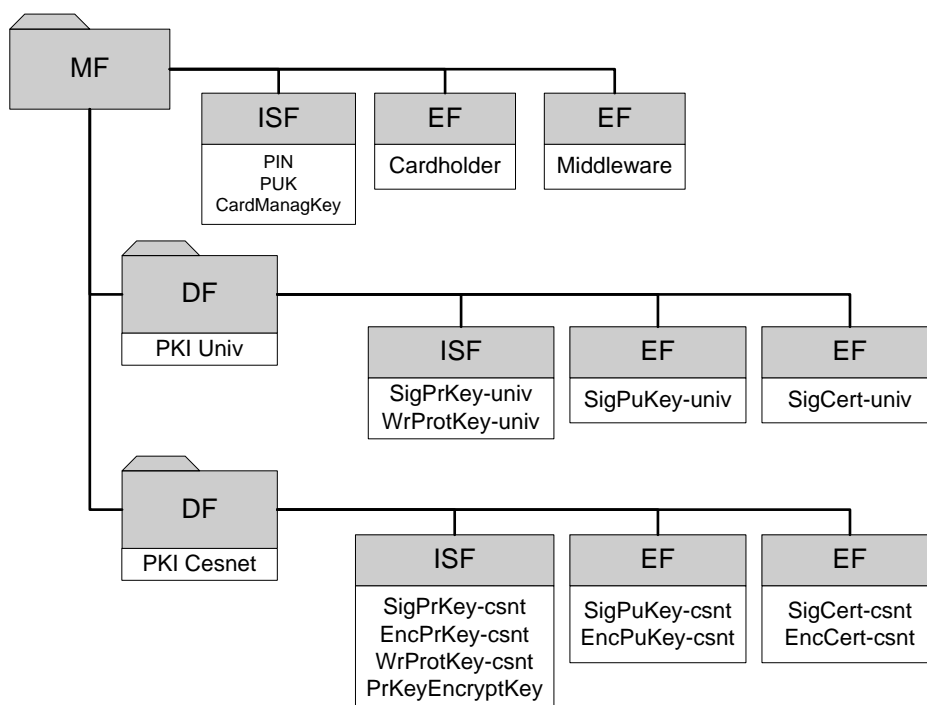
DF PKI App 2 je předchozí aplikace rozšířená o šifrovací key pair. Ten není generován kartou, ale je na kartu importován. K zabezpečení přenosu privátního klíče na kartu slouží další symetrický klíč v ISF.

V následující tabulce je zobrazena aplikační struktura karty s objekty a jejich alokovanou pamětí, včetně režijních nároků.

Tab. 3 Struktura karty s aplikacemi a alokovanou paměť pro oblasti DF

File	File ID	Type	Size of data [B]	Size overhead [B]
MF	3F00	N/A	1470	36
ISF	N/A	N/A	88	8
User PIN		<i>PIN</i>	8	16
User PUK		<i>PUK</i>	8	16
Admin key		<i>3DES</i>	16	16
EF cardholder	2F01	transparent	1143	23
Cardholder name			32	
Address			64	
Photo			1024	
EF user	2F02	transparent	87	23
User data			64	
EF middleware	2F03	Linear fixed	116	20
middleware data (3x32B)			96	
DF Cesnet PKI application	4F00	N/A	4302	36
ISF	N/A	N/A	832	8
SM confidentiality key		<i>3DES</i>	16	16
Authentication key		<i>3DES</i>	16	16
Signature private key		<i>RSA</i>	364	16
Encryption private key		<i>RSA</i>	364	16
IPF	4F01	N/A	339	21
Signature public key		<i>RSA</i>	147	12
Encryption public key		<i>RSA</i>	147	12
EF cert	4F02	transparent	3095	23
Signature certificate			1536	
Encryption certificate			1536	
DF University PKI application	5F00	N/A	2195	36
ISF	N/A	N/A	420	8
Authentication key		<i>3DES</i>	16	16
Signature private key		<i>RSA</i>	364	16
IPF	5F01	N/A	180	21
Signature public key		<i>RSA</i>	147	12
EF cert	5F02	transparent	1559	23
Signature certificate			1536	
TOTAL SIZE			7967	

- **NÁVRH DATOVÉ STRUKTURY KARTY**
- =Konkrétní objekty=
-
- Typy objektů: viz předchozí schema „Typy objektů“
- Aplikace: (DF) PKI Univ, (DF) PKI Cesnet
- Varianta: Proprietární řešení, tj. nonPKCS#15
- Odkaz: (následující popis a tabulka)



Obr. 9 Specifikace konkrétních objektů pro PKI-aplikace (bez PKCS#15)

Specifikace konkrétních objektů pro PKI aplikace (ve verzi bez PKCS#15)

Popis typů z obr.8 byl nahrazen konkrétními objekty pro navržené aplikace (obr.9)

Popis objektů uveden v následující tabulce Tab. 4.

Pro bližší technické podrobnosti o objektech MF, DF, EF a násl. viz ISO/IEC7816-4, 8.

Tab. 4 Popis objektů navržené datové struktury karty s aplikacemi, podle obr.9

MF	Master File	Hlavní soubor karty („kořenový adresář“)
DF	Dedicated File	Soubor (adresář) pro uložení karet aplikací
ISF	Internal Secret File	Soubor pro uchování tajných klíčů
EF	Elementary File	Soubor pro uložení dat
PIN	Personal Identification Number	Kód pro ochranu citlivých údajů před použitím nepravé osoby (autentizace držitele karty)
PUK	Personal Unblocking Key	Slouží ke změně a odblokování PINu
CardManagKey	Card Management Key	Symetrický (3DES) klíč pro správu karty (např. mazání aplikace, přidání aplikace, smazání celé karty). Slouží k autentizaci (EXTERNAL AUTHENTICATE) zařízení, které správu provádí.
Cardholder		Soubor pro uchování informací o držiteli karty (jméno, adresa, fotka)
Middleware		Data pro interní potřebu middleware
PKI Univ		PKI aplikace univerzity
SigPrKey-univ	University Signature Private Key	Privátní část dvojice klíčů pro podpis v rámci univerzitní infrastruktury
SigPuKey-univ	University Signature Public Key	Veřejná část dvojice klíčů pro podpis v rámci univerzitní infrastruktury
SigCert-univ	University Signature Certificate	Certifikát k veřejnému klíči pro podpis v rámci univerzitní infrastruktury
WrProtKey-univ	University Write Protection Key	Symetrický (3DES) klíč pro autentizaci zařízení, které je oprávněno modifikovat (nikoliv použít) údaje univerzitní PKI aplikace, tzn. vygenerovat na kartě novou dvojici klíčů a uložit nový certifikát
PKI Cesnet		PKI aplikace CESNETu
SigPrKey-csnt	Cesnet Signature Private Key	Privátní část dvojice klíčů pro podpis v rámci PKI CESNET
SigPuKey-csnt	Cesnet Signature Public Key	Veřejná část dvojice klíčů pro podpis v rámci PKI CESNET
SigCert-csnt	Cesnet Signature Certificate	Certifikát k veřejnému klíči pro podpis v rámci PKI CESNET
EncPrKey-csnt	Cesnet Encipherment Private Key	Privátní část dvojice klíčů pro šifrování v rámci PKI CESNET
EncPuKey-csnt	Cesnet Encipherment Public Key	Veřejná část dvojice klíčů pro šifrování v rámci PKI CESNET
EncCert-csnt	Cesnet Encipherment Certificate	Certifikát k veřejnému klíči pro šifrování v rámci PKI CESNET
WrProtKey-csnt	Cesnet Write Protection Key	Symetrický (3DES) klíč pro autentizaci zařízení, které je oprávněno modifikovat (nikoliv použít) údaje CESNET PKI aplikace, tzn. vygenerovat na kartě novou dvojici klíčů, uložit nový šifrovací klíč, uložit nové certifikáty
PrKeyEncrypt-Key	Private Key Encryption Key	Symetrický (3DES) klíč, slouží k ochraně privátního klíče při importu na kartu.

Poznámky k vlastní karetní aplikaci:

Uvedené poznámky tvoří v praxi podklad pro vytvoření závazné provozní *šablony (template)* pro kartu a aplikace (viz kapitola Rámcem úkolu pro PKI). Níže popsané chování aplikace, nastavení atributů a klíčů lze určit odlišně. Pak bude aplikace vygenerována a provozována pod jinou *šablonou*.

1. Oba podpisové privátní klíče jsou generovány na kartě a nikdy ji neopustí. Jejich použití pro podpis je podmíněno zadáním správného PINu (příkaz VERIFY), jejich změna je umožněna pouze takovému zařízení, které prokáže znalost odpovídajícího WrProtKey.

2. Naopak šifrovací key pair je generován mimo kartu (a zálohován příslušnou autoritou pro případ ztráty karty). Na kartu jej lze uložit opět pouze po prokázání znalosti WrProtKey (konkrétně WrProtKey-csnt) a navíc privátní klíč musí být šifrován klíčem PrKeyEncryptKey.

3. Použití privátní šifrovací klíče lze opět pouze po zadání správného PINu.

4. PIN je sdílený pro všechny aplikace, které PIN používají pro ochranu citlivých dat. Rozhodnout, zda u některé aplikace povolit bezpinový provoz (typicky fyzický přístup).

Rozhodnout, zda budou pro PIN použity všechny znaky ASCII nebo jen čísla.

5. Po několika (např. čtyřech, maximálně 14) po sobě jdoucích špatných zadáních PINu dojde k jeho zablokování. Odblokovat (a zároveň nastavit na jinou hodnotu) lze PIN pouze při znalosti kódu PUK. Pokud dojde i k zablokování PUKu (počet pokusů může být jiný než u PINu), nelze již PIN odblokovat a tudíž nelze použít žádný z privátních klíčů na kartě. Jediné, co lze s takovou kartou dělat, je celou ji smazat (a znovu reinicializovat). Bezpečnost lze dále zvýšit prostřednictvím klíče CardManagKey (povolit zablokování tohoto klíče s následným vyřazením karty).

6. Ke změně neblokovaného PINu není třeba PUK, stačí znalost původního PINu.

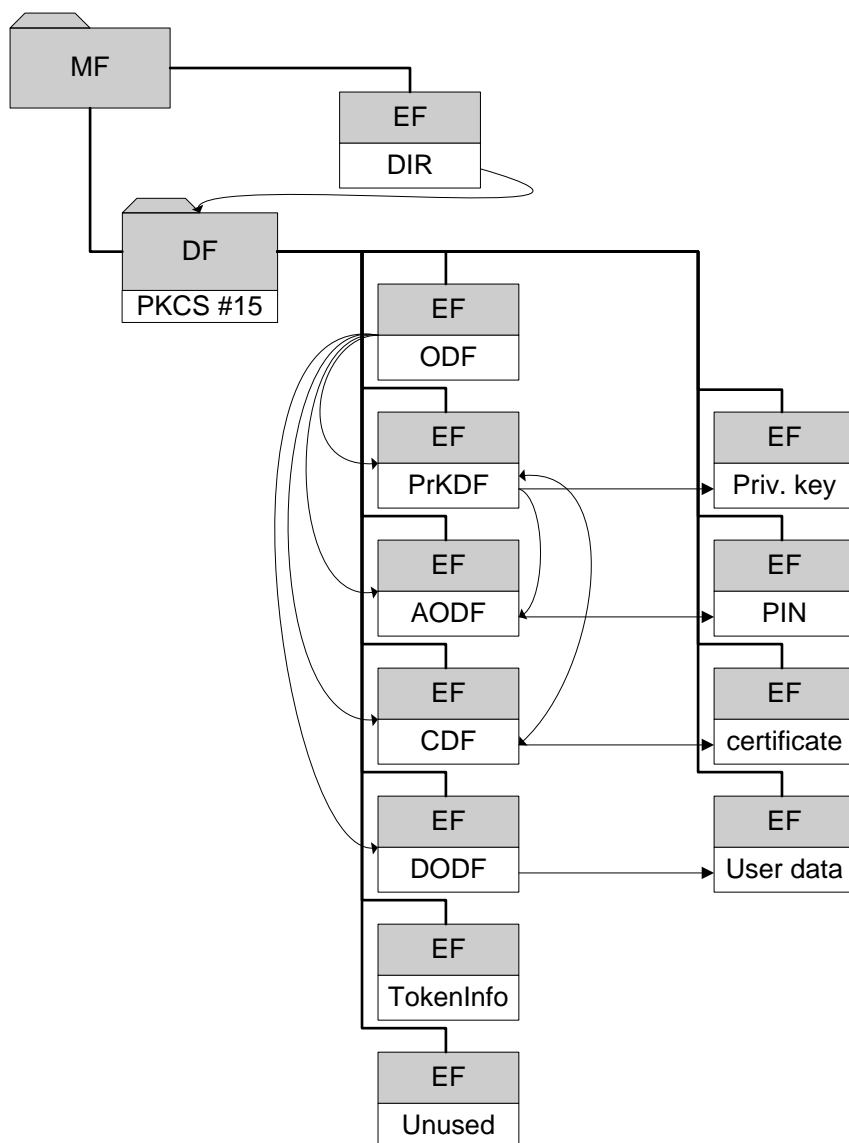
7. Všechny symetrické klíče používají tzv. derivování klíčů. Tento proces usnadňuje key management symetrických klíčů tak, že každá karta má svůj vlastní klíč odvozený ze sériového čísla karty a nějakého master klíče. Příklad: CESNET vygeneruje 3DES klíč MasterWrProtKey-csnt, který distribuuje na místa, kde se provádí personalizace a generování klíčů. Terminál, který tyto operace provádí, si přečte sériové číslo karty a pomocí klíče MasterWrProtKey-csnt odvodí konkrétní WrProtKey-csnt pro danou kartu. Opačný postup, tedy odvození MasterWrProtKey-csnt ze znalosti dvojice (WrProtKey-csnt, sériové číslo) samozřejmě nesmí být triviální.

Použití ze strany terminálu (middleware) Viz aplikace, Tab.4 a Obr.9

Tab. 5 Použití ze strany middleware, ilustrace k aplikaci (Tab.4 a Obr.9)

PIN	Ověření znalosti PINu kartou pomocí VERIFY	Middleware, App
	Změna PINu při znalosti původní hodnoty	App
	Odblokování PINu pomocí PUK	App
PUK	Odblokování PINu pomocí PUK	App
CardManagKey	Přidání / smazání aplikace, smazání karty	App
Cardholder	Čtení	App
Middleware	Čtení / zápis	Middleware
SigPrKey-*	Použití k podpisu	Middleware, App
	Změna (generování nového)	App
SigPuKey-*	Čtení	Middleware, App
	Změna	App
SigCert-*	Čtení	Middleware, App
	Změna	App
WrProtKey-*	Použití	App
EncPrKey-csnt	Použití k odšifrování	Middleware, App
	Změna (import nového)	App
EncPuKey-csnt	Čtení	Middleware, App
	Změna	App
EncCert-csnt	Čtení	Middleware, App
	Změna	App
PrKeyEncryptKey	Použití	App

PKCS#15 aplikace - typy souborů a objektů a vztahy mezi nimi



Obr. 10 Aplikace podle PKCS#15: Vztahy mezi typy souborů/objektů

K obr. 10 Aplikace podle PKCS#15

Obrázek ukazuje příklad rozvržení souborů v jedné PKCS#15 aplikaci.

Tab. 6 Popis souborů/objektů na kartě v případě jedné PKI-aplikace podle PKCS#15, dle obr.10

EF DIR	Adresář karetních aplikací podle ISO 7816-5
ODF	Object Directory File – obsahuje ukazatele na další EF soubory (PrKDF, PuKDF, CDF, AODF), které obsahují adresáře objektů daného typu
TokenInfo	Obecné informace o tokenu (kartě), například podporované algoritmy
PrKDF	Adresář privátních klíčů, pro každý privátní klíč uchovává: název klíče, identifikátor, způsob použití klíče, odkaz na autentizační objekt, kterým je omezen přístup ke klíči a odkaz na umístění klíče samotného
PuKDF	Adresář veřejných klíčů, pro každý veřejný klíč uchovává: název klíče, identifikátor, způsob použití klíče a odkaz na umístění klíče samotného. Pokud klíč patří k nějakému privátnímu klíči v PrKDF, musí mít oba klíče (veřejný a privátní) stejný identifikátor (znázorněno šipkami v obrázku)
CDF	Adresář certifikátů, každý záznam obsahuje především identifikátor a odkaz na umístění certifikátu. Pokud certifikát patří k nějakému klíči v PrKDF nebo PuKDF, musí mít stejný identifikátor (znázorněno šipkami v obrázku)
AODF	Adresář autentizačních objektů, v příkladu má jediný záznam o PINu (který je umístěn v MF kvůli sdílení oběma aplikacemi). Záznam obsahuje např. povolené znaky v PINu, délku PINu a odkaz na umístění

EF Unused – udržuje informace o volných místech v jednotlivých datových souborech (nikoliv v adresářích ODF, PrKDF, PuKDF, CDF, AODF). Pomáhá při vytváření, modifikaci a mazání objektů. (V našem případě nemusí být použit, protože vytváření/modifikace/mazání objektů nebude hostu -tj. middlewaru - umožněno.)

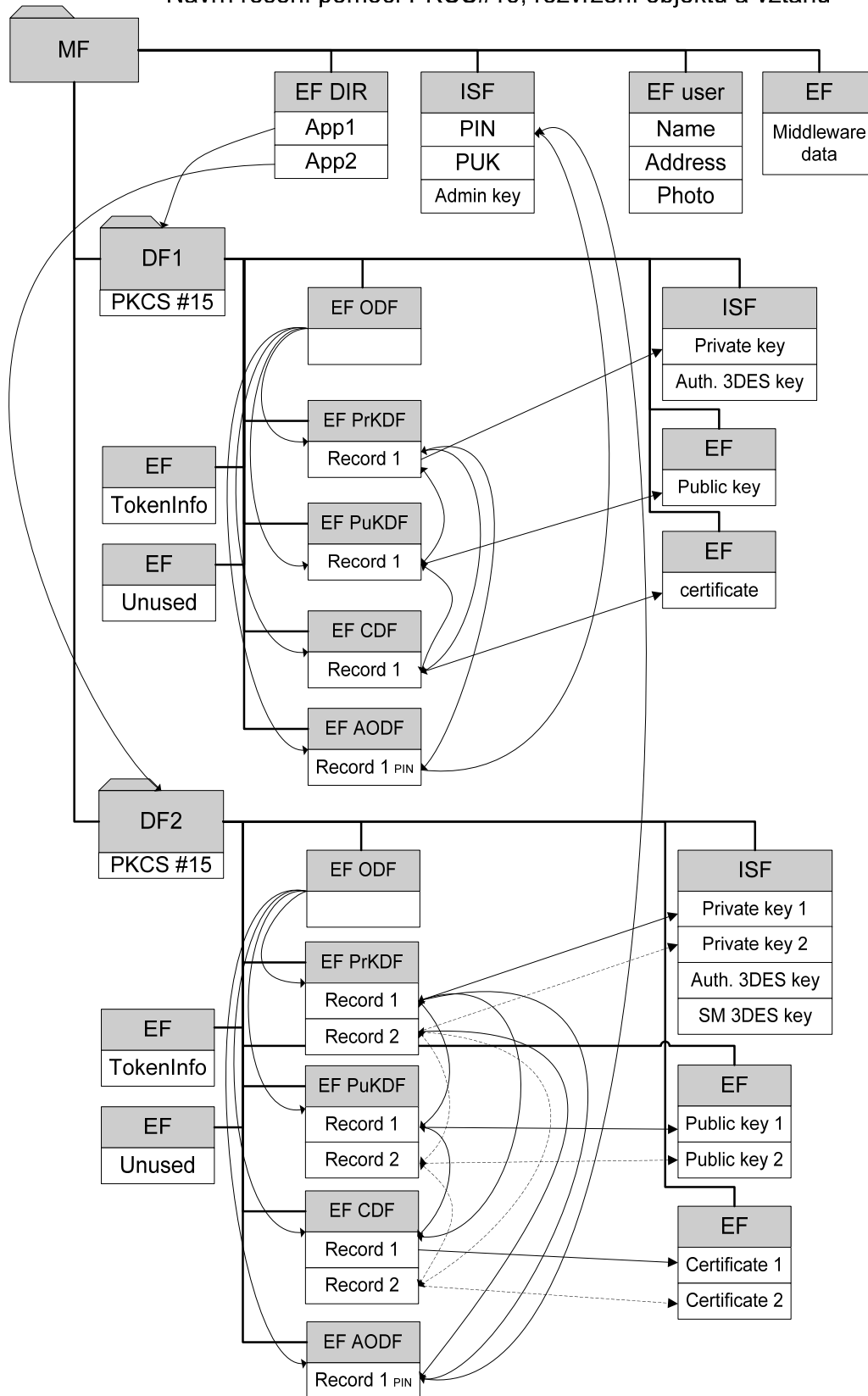
K obr. 11

Obrázek ukazuje rozložení souborů a typů objektů na kartě se dvěma PKCS#15 aplikacemi.

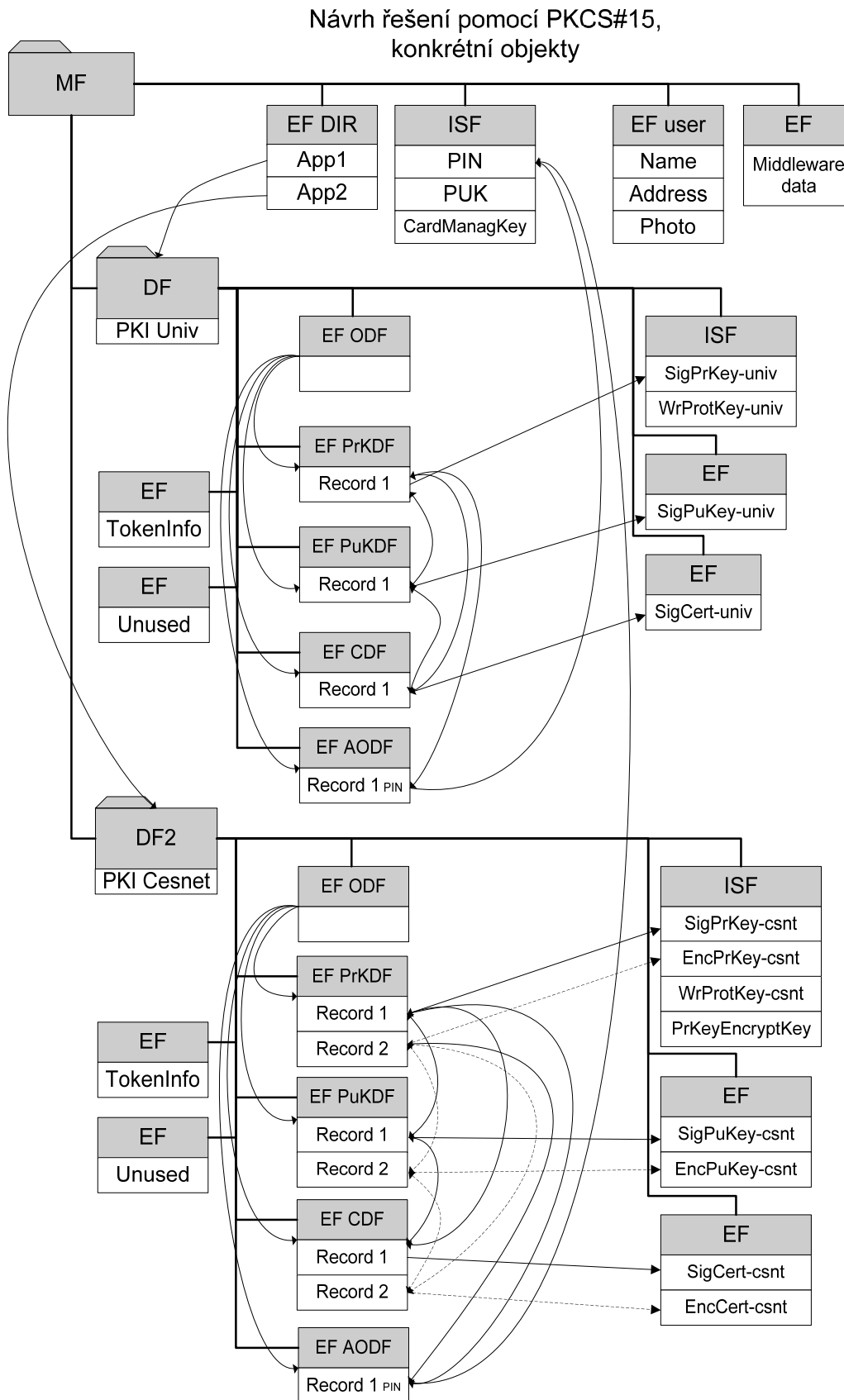
K obr. 12

Jde o schema datové struktury karty PKCS#15 podle obr. 11, doplněné o názvy konkrétních objektů. Platí zde vše, co bylo popsáno u obr.9. včetně Tab.4 a poznámek

Návrh řešení pomocí PKCS#15, rozvržení objektů a vztahů

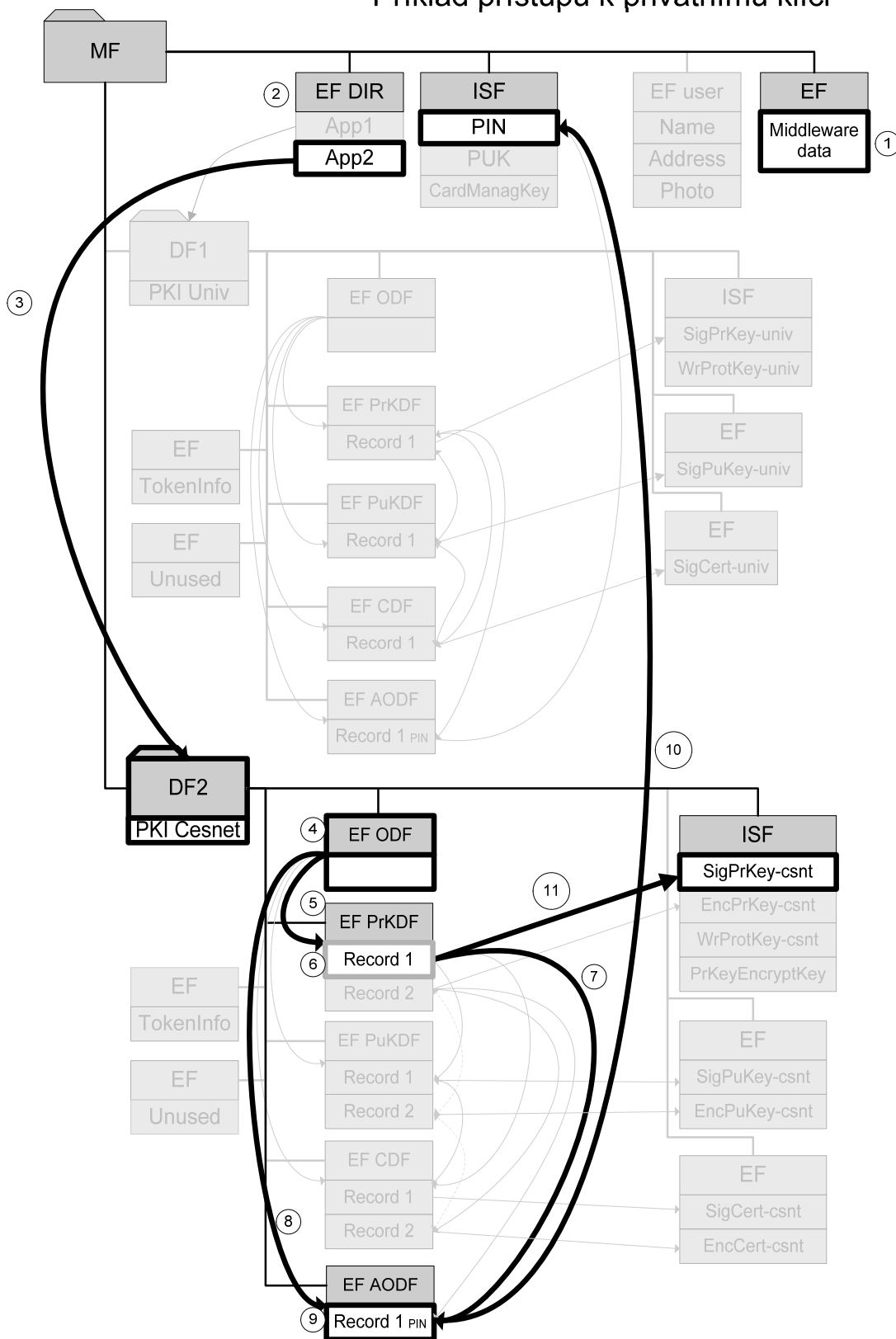


Obr. 11 Datová struktura a vztahy mezi objekty pro aplikace DF1 DF2 podle PKCS#15



Obr. 12 PKCS#15 – Výsledný stav návrhu PKI Cesnet, PKI Univ s konkrétními objekty

Příklad přístupu k privátnímu klíči



Obr. 13 Přístup k privátnímu klíči ve struktuře PKCS#15 (podle schématu obr.12)

Příklad postupu při vytváření podpisu pomocí CSP

Předpoklad: v systémovém úložišti je již nainstalován použitý certifikát společně s odkazem na CSP, container a typ klíče (AT_SIGNATURE nebo AT_KEYEXCHANGE). Instalace může být provedena nějakou utilitou automaticky při vložení karty do čtečky.

Aplikace, která potřebuje podepsat data privátním klíčem, který odpovídá nějakému (danému) certifikátu, nejprve pomocí funkcí CryptoAPI vyhledá v úložišti certifikátů tento certifikát a zjistí tak název CSP, název kontejneru a typ klíče. Poté přes CryptoAPI volá funkce daného CSP pro výpočet hashe podepisovaných dat a nakonec funkci pro výpočet podpisu. Tato funkce tedy obdrží: podepisovaný hash, název kontejneru a typ klíče.

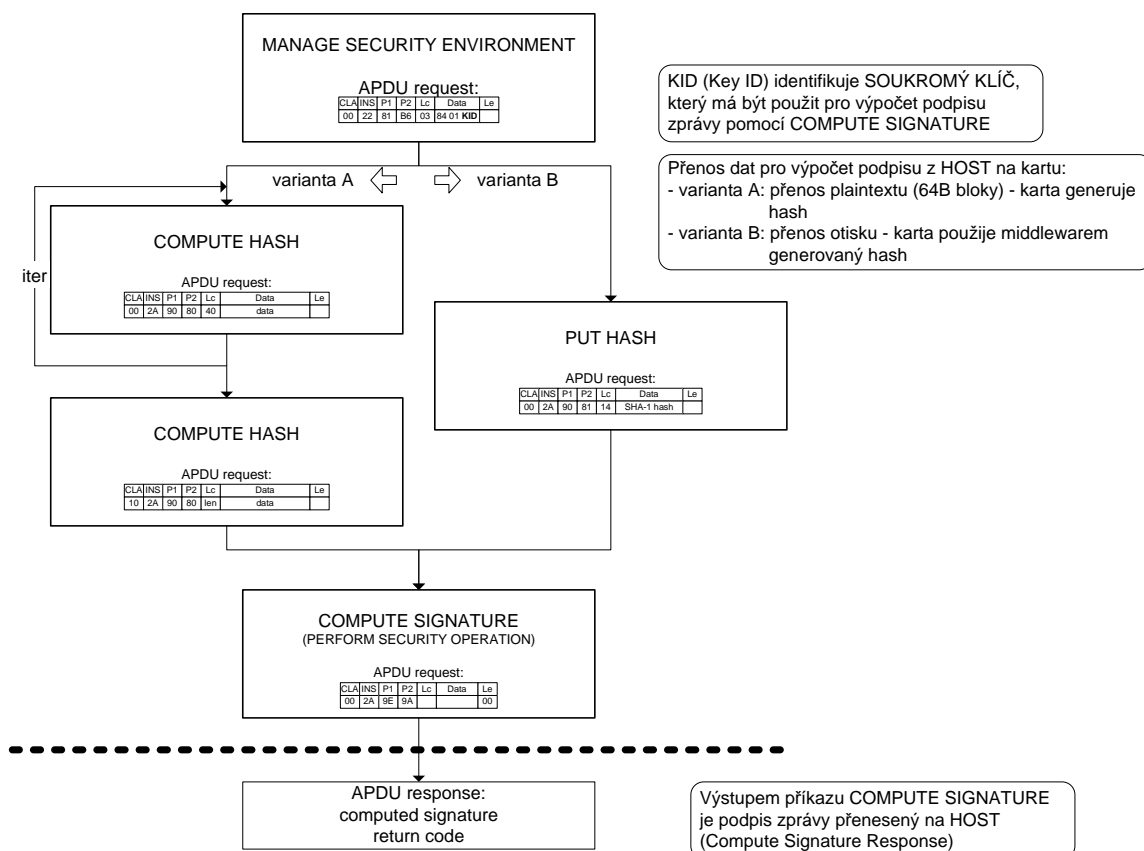
Objekty (především klíče) mají dva identifikátory:

- „karetní“ - identifikace klíče v ISF (tzv. KID)
- „aplikační“ – identifikace v rámci PKCS#15

Další postup lze sledovat na obr.13, Přístup k privátnímu klíči.. Čísla 1., 2., ..., označující jednotlivé kroky jsou na obr. zakroužkována:

1. CSP vyhledá na kartě v souboru „EF Middleware Data“ údaje o daném kontejneru – tak zjistí název (label) karetní aplikace a identifikátor klíče daného typu.
Jde o PKCS#15 - identifikátor (= identifikace v rámci PKCS#15 aplikace)
2. V „EF DIR“ vyhledá karetní aplikaci podle názvu (labelu) a zjistí AID DF souboru
3. Provede SELECT daného DF souboru.
4. Načte „EF ODF“
5. Z dat v ODF zjistí FID souboru „EF PrKDF“
6. V PrKDF vyhledá záznam o klíči s daným identifikátorem (byl zjištěn v kroku 1)
7. Z tohoto záznamu zjistí **identifikátor autentizačního objektu**, kterým je privátní klíč chráněn.
8. Z dat v ODF zjistí FID souboru „EF AODF“
9. V AODF vyhledá záznam o **autentizačním objektu** podle identifikátoru zjištěného v předchozím kroku
10. Informace zjištěné v nalezeném záznamu v AODF plus uživatelem zadaný PIN jsou použity k sestavení příkazu VERIFY. Proveden Verify. Pokud ověření PINu selže, proces končí.
11. Informace ze záznamu v PrKDF (krok 7) zahrnují i KID (identifikátor klíče v rámci ISF), který je použit k vykonání příkazu MANAGE SECURITY ENVIRONMENT (oznámí kartě, se kterým klíčem se bude dále pracovat), pošle na kartu hash ze vstupu příkazem PUT HASH a nakonec pošle kartě příkaz PERFORM SECURITY OPERATION (COMPUTE SIGNATURE). V případě úspěchu karta vrátí požadovaný podpis (viz následující diagram).

ID-karta: Proces generování elektronického podpisu



- Proces e-podpisu:
- ID-karta: SPK2.5DI
- APDU příkazy: ISO/IEC 7816-4
- Komunikace „ ID Karta - HOST“ :
- prostřednictvím bezkontaktního rozhraní, ISO/IEC 14443A (transmission protocol T=CL)
- nebo pomocí kontaktního rozhraní, ISO/IEC 7816 (transmission protocol T=1 nebo T=0)

Diagram 6 Proces generování e-podpisu

Poznámka: Část datových struktur a entit na kartě je standardizována (ISO/IEC 7816-4, -8), část vykazuje specifické implementační rysy (adresace internal security files, APDU Create File).

Tyto implementační (proprietární) rysy COS neovlivňují funkčnost řešení podle architektury PKCS#15. (Jde o tvrzení opírající se o částečné zkušenosti v dosavadních variantách přípravy karet aplikací PKI). Nicméně PKCS#15 nezahrnuje celou oblast řešení/uspořádání objektů na kartě. Norma sice usnadňuje portabilitu aplikací, ale nemůže ji sama o sobě zaručit.

Závěr:

Pro velkou flexibilitu možností při čipové personalizaci je nutno provést návrh struktury karty a kompletní funkčnosti ve verzích:

Pro první pilotní nasazení ve VŠ navrhnout jednodušší verzi pro jeden pár klíčů podpisový a jeden pár klíčů šifrovací.

Vznikne jednodušší prototyp řešení určený pro pilotní provoz.

Další verze s dvěma páry podpisových klíčů (použití pro dvě certifikační autority) bude implementována až po shromážděných připomínkách a námětech.

Výhodou je, že karta se dá reinitializovat, aplikace na kartě se dají odstraňovat i přidávat.

Veškeré personalizační aplikace budou v souladu s průběžně vznikajícím provozním řádem („provozní politikou“).

7.3.3 POŽADAVKY NA ID- KARTU

Souhrn nutných technických vlastností karty (rekapitulace předchozích odstavců):

-Soulad se specifikací ISO/IEC 7816 (pro kontaktní provoz), ISO/IEC 14443 (pro bezkontaktní provoz) a to včetně ISO/IEC 14443-4 a výše

-RSA 1024 pro podpis standardně

-RSA 2048 pro podpis pro speciální bezpečnostní aplikace (stačí výhledově)

-kompatibilita pro práci s X.509v3 certifikáty

-Velikost paměti minimálně 16KB, pro podpisové a šifrovací klíče, certifikáty a pro další aplikace

Požadavky na komunikační rozhraní systému s kartou

podpora PKCS#11 v.2.01 a podpora CSP nejlépe pod vlastní kontrolou nebo od výrobce karty po důkladném otestování modulu i servisní podpory

využití Microsoft CryptoApi (nebo bez)

PC/SC kompatibilní (viz ISO 7816)

podpora pro W2k a vyšší (NT4 je samostatný problém, lépe se vyhnout) a Linux (Solaris)

Podpora ISO/IEC 7816 –1/2/3/4 a dále

Bezkontaktně ISO/IEC 14443A

Podpora protokolů T=0, T=1 a T=CL (bezkontaktně)

odzkoušená součinnost se základními aplikacemi na desktopu e-mail, IE a jeho klientskou SSL autentizací (IE5.5 a výše)

Metodika přípravy PKI karet zahrnuje:

- Zajištění dodávek bezpečnostních tokenů (karta, čtečka, softwarové toolkity, technická specifikace karty v souladu s řešením verzí kryptomodulů na bázi CSP a PKCS#11)
- Postupy přípravy (vývoj, čipová personalizace), testování, design (optická personalizace předcházející předání uživateli)
- Implementace, otestování a aktualizace CSP, PC/SC nad aplikacemi používaných browserů a poštovních klientů
- Vypracování zásad provozní přípravy, návrhu optimálního koordinovaného postupu v této oblasti a udržování těchto manuálů
- Promítnutí do certifikačních politik a prováděcích směrnic PKI CESNET a PKI VŠ připravených spolupracovat na úkolu

Předkladatelé zprávy doporučují po dosavadních zkušenostech s výběrem a testováním IDK tyto preference:

- *Funkčnost:* Jednočipový produkt s duálním komunikačním rozhraním je vhodnější volba než hybridní dvoučipová karta.
Není nutné omezovat požadavky [R1]-[R7] z kap.5: Prototyp IDK má obojí funkčnost, jako token pro PKI i jako karta se zpětnou kompatibilitou s Mifare.
- *Požadavek na kontinuitu IDK a čipových aplikací pro IDK:*
 - Dlouhodobá podpora typové řady IDK výrobcem (verze, následovníci produktu, akceptace ISO 14443-4, ISO 7816-x, x=1-8, využitelnost otevřených standardů PKCS#11 a PKCS#15, podpora normy PC/SC ver.2 pro snímače)
 - Přenositelnost čipových aplikací prostřednictvím adaptace kódu na COS další generace, případně i na produkty jiného dodavatele, a to bez mimořádných investic.
- *Ověřovací pilot:* podpora pro zorganizování několikaměsíčního pilota v reálném prostředí. Využití nejlepších testerů, jaké lze najít – studentů.
- *Aplikační potenciál:* vytypovat a přizpůsobit praktické aplikace ve VŠ pro IDK a PKI.
- *Technická podpora mobility klienta a uživatelské jednoduchosti:* zahrne technickou podporu mobilního PKI-klienta na bázi IDK pro všechny rozšířené platformy (OS).

Systémová integrace: Role systémového integrátora, resp. dozoru nad technickou podporou nových karetých aplikací nad PKI, má připadnout nikoliv dodavatelům pro VŠ, ale subjektu z akademické obce, například sdružení CESNET.

Rizika týkající se podpory a řízení rozvoje čipových aplikací v akademické komunitě. Lze zopakovat víceméně známé pravdy:

(-) Ztráta kontroly nad „technologickým obsahem“ by se negativně promítla do „škálovatelnosti řešení“, servisu a řízení dalšího rozvoje. Middleware (kryptoovladače) na bázi komerčních licencí by prodražily řešení.

(-) Rizika jednorázově zakoupeného balíku řešení (pro design a čipovou personalizaci, pro middleware) od externího dodavatele na klíč převažují v dlouhodobém horizontu nad výhodami. Každá technická změna je placeným požadavkem na dodavatele. Kromě toho projekt čipové migrace nemá povahu statického systému, jako např. dřívější dodávky přístupových a menzovních systémů na klíč.

(+) Trendy a inspirace u obdobných evropských (a v poslední době asijských) projektů jsou řešiteli pasivně sledovány, zaslouží větší pozornost.

(+) Požadavky na harmonizaci (eEurope Smart Card Charter aj.) je vhodné podrobit bližšímu průzkumu. Otevírá cestu k širší interoperabilitě.

Rekapitulace závěrů:

Karta nemá být „černá skříňka“ jako některé současné karetní systémy na školách. Údržba i inovace datové struktury, přístupových PINů a hesel, aplikací na kartě a jejich administrace má být v kompetenci akademické komunity, nikoliv výlučně výrobce či dodavatele.

Karta má akceptovat současné průmyslové standardy uváděné v textu zprávy.

Přítomnost a tradice výrobce na evropském a regionálním (ČR) trhu. Je žádoucí pro reference pro obchodní vztahy „výrobce – zákazník“ (dodržování závazků, typ a délka garance skladovaných i neskladovaných karet). Zkušenosti s řešeními typu „campus“ a odpovídající slevové programy.

Typ výrobku (tj. typ karty včetně čipu a operačního systému) má mít delší životnost a návaznost v inovačním programu výrobce (návazností se rozumí „rozumný“ stupeň zpětné kompatibility aplikací při přechodu na novější produkt)

Vysoká a rovnoměrná jakost dodávek (v případě požadavku několika desítek dodávek pro akademickou komunitu v průběhu mnoha let jde o vysoce netriviální požadavek, který se týká mechanické odolnosti karty i zabudované antény, vlastnosti plastu, kvality optické personalizace i koncového potisku na VŠ, kvality snímání v bezkontaktním poli, doba odezvy na aplikační příkazy)

Karta má jako HW v průměru zůstat funkční po dobu studia, během této doby může dojít k update aplikací nebo k reinicializaci bez ztráty funkčnosti.

Technická podpora a odezva ze strany výrobce. Netriviální v problémech rozhraní „karta – bezkontaktní snímač“, „karta – CSP/PKCS#11-PC“, podpora komunikace PC/SC v.2

Technologická otevřenost (poskytnutí technické specifikace, řešení technických requestů, kvalita SW-tookitů a low-level podkladů pro vývoj aplikací na kartě).

Trend rozšířeni duální technologie (SPK2.5DI) určené pro testy: *rostoucí*.

Poznámka: Existuje nárůst využití bezkontaktního rozhraní na navrženém čipu (např. pilotní bezkontaktní projekty VISA), masové využití pro ID a PKI aplikace na kontaktním rozhraní SPK2.x (SPK2.3 na kontaktním rozhraní nabízí např. První certifikační jako HW-tokeny)

Morální životnost duální technologie SPK2.5DI: *dostatečné argumenty ve prospěch řešení podporující podmínky R1 až R7*.

Poznámka: součást hlavní vývojové řady produktů předního světového výrobce G&D sleduje trendy poptávky po ID kartách, kontinuální podpora ze strany výrobce se osvědčila v dřívějších projektech.

Know-how pro řešení vlastními silami: *Ano*.

Poznámka: Předkladatelé zprávy mají profesní zkušenosti s čipovou personalizací této kategorie produktů s designem karetních aplikací i s řešením v oblasti správy klíčů a PKI.

Řešením projektu předají své zkušenosti do prostředí VŠ v rámci rozsáhlé kooperace.

8 ZÁVĚR

Předkladatelé zprávy navrhuji zahájit ověřovací piloty s čipovým produktem SPK 2.5DI, což je duální karta s RSA koprocesorem, odzkoušená jak pro základní funkcionalitu pro PKI, tak pro zpětnou kompatibilitu s technologií Mifare. Karta SPK 2.5DI splňuje podle dodané technické dokumentace a provedených testů na vzorcích karty požadavky R1 až R7. Pro aktivity spojené s dalším postupem navrhuji předkladatelé rozšířit rámec spolupráce se sdružením CESNET a zájemci ze strany VŠ.

P.S. Řada mezinárodních čipových projektů je v různém stadiu realizace. Zejména postupují projekty migrace papírových občanských dokladů na čipové ID-karty. Tyto projekty jsou založeny na standardech ISO 7816 s využitím duálního rozhraní karet podle ISO 14443. Vesměs je pamatováno na integraci e-podpisu, alespoň přes kontaktní rozhraní. Jde právě o technologie, navržené pro ID-karty pro VŠ a popsané v tomto příspěvku. Dnešní iniciativa bude zítra nutností. Leitmotivem je zvládnout technologii pro ID-karty už proto, že nabízí užitečný a dostupný stavební prvek pro většinu IT aplikací pod kontrolou akademické komunity.

9 PŘÍLOHA Č.1 SPECIFIKACE, NORMY A PRŮMYSLOVÉ STANDARDY

9.1 SOUHRNNÉ ODKAZY

Existují standardy pro fyzické, mechanické, elektrické i softwarové vlastnosti. Odkaz na souhrn většiny norem a standardů pro smart karty. Na některých odkazech lze získat rovněž dokumenty standardů:

<http://www.tfn.net/techno/smartcards/standards.html>

<http://forum.afnor.fr/afnor/WORK/AFNOR/GPN2/Z15Y/PUBLIC/WEB/ENGLISH/commerce.htm>

ISO/IEC JTC1 Information technology SC 17 Identification cards and related devices (www.iso.ch/meme/JTC1SC17.html)

Sada standardů ISO/IEC 7816-x, ISO/IEC 14443-x a ETSI SMG9 obsahuje podstatné normy pro aplikační programátory v oboru smart karet.

ISO/IEC 10373 Identification cards -- Test methods.

ISO/IEC 14443 Remote coupling communication cards. (Contactless cards)

ISO TC 68 Banking and related financial services SC 6

(www.iso.ch/meme/TC68SC6.html)

Security architecture of financial transaction systems using integrated circuit cards (parts 1-8).

NIST (<http://csrc.ncsl.nist.gov/>) FIPS 140-1 nově FIPS 140-2

(<http://csrc.nist.gov/publications/fips/fips1401.htm>)

"Security Requirements for Cryptographic Modules"

Secure Electronic Information in Society (SEIS) (www.seis.se) card

WIM - Smart karta pro Wireless Interface Module (podpora WAP)

Specifikace: WAP WIM Wireless Application Protocol Identity Module Specification (www.wapforum.org)

9.2 NORMA ISO/IEC 7816

Pro osvojení technických základů smart karet je norma ISO/IEC 7816 nezbytná.

Standardy ISO zahrnují (resp. postupně připravují a zahrnou) metodiku zjišťování kompatibility karet s ISO/IEC 7816. ISO FCD 10373-3 specifikuje testovací metody pro vyhodnocení ISO /IEC 7816-3.

Základní standard pro karty pracující na kontaktním rozhraní. Part 4 a navaz. Part 8, 9 se týká zároveň chování bezkontaktních ID-karet ISO/IEC 14443-4, vyšších vrstev nad přenosovým protokolem.

Jednotlivé dokumenty mají toto uspořádání:

ISO/IEC 7816-1 (Part 1) - Cards with contacts: Physical characteristics
(fyzické charakteristiky karet)

ISO/IEC 7816-2 (Part 2) - Cards with contacts: Dimensions and location of the contacts
(velikost a umístění kontaktu, čipu, magnetického proužku, atd.)

ISO/IEC 7816-3 (Part 3) - Cards with contacts: Electrical interface and transmission protocols
(definice elektrických signálů, napájení, postup resetování, přenos dat na fyzické úrovni, přenosové protokoly (T=0 a T=1 protokoly))

ISO/IEC 7816-4 (Part 4) - Organisation, security and commands for interchange
- popis souborové struktury, APDU, secure messaging, návratové kódy, příkazy pro:
- práci s obsahem EF souboru,
- práci s logickými kanály
- ověření PINu
- ověření znalosti klíče (Get challenge, internal authentication a external authentication)

ISO/IEC 7816-5 (Part 5) - Registration of application providers
- popisuje způsob číslování aplikací a přidělování jednoznačných identifikátorů (AID)

ISO/IEC 7816-6 (Part 6) - Interindustry data elements for interchange
- popisuje způsob uložení informací, které jsou pro mnohé aplikace společné (identifikátory, jméno, fotografie, držitelem upřednostňované jazyky...)

ISO/IEC 7816-7 (Part 7) - Commands for SCQL
- příkazy pro Structured Card Query Language (SCQL)

ISO/IEC 7816-8 (Part 8) - Security related interindustry commands
Commands for security operations
- příkazy pro digitální podpis, hashování, šifrování, ...

ISO/IEC 7816-9 (Part 9) - Additional interindustry commands and security attributes
Commands for card management
- životní cyklus karty, příkazy pro práci se soubory, pro prohledávání obsahu souboru

ISO/IEC 7816-10 (Part 10) - Cards with contacts: Electrical interface for synchronous cards
- popis ATR pro synchronní karty

ISO/IEC 7816-11 (Part 11) - Personal verification through biometric methods
- příkazy pro aktivaci-deaktivaci aplikací na kartě, nahrávání a spouštění kódu

ISO/IEC 7816-12 (Part 12) - Cards with contacts: USB electrical interface and operating procedures
(draft)

ISO/IEC 7816-15 (Part 15) - Cryptographic token information in IC Cards
(2004) Cryptographic information application

Poznámka k ISO/IEC 7816 (podrobnější vymezení):
Part 1: Physical characteristics

Defines the physical dimensions of contact smart cards and their resistance to static electricity, electromagnetic radiation and mechanical stress. It also prescribes the physical location of a IC card's magnetic stripe and embossing area.

Part 2: Dimensions and Location of Contacts

Defines the location, purpose and electrical characteristics of the card's

metallic contacts:

Part 3: Electronic Signals and Transmission Protocols

Defines the voltage and current requirements for the electrical contacts defined in Part 2 and asynchronous half-duplex character transmission protocol (T=0).

Protocol type T=1, asynchronous half duplex block transmission protocol.

Revision of protocol type selection

Electrical characteristics and class indication for integrated circuit(s) cards operating at 5V, 3V and 1,8V

Part 4: Inter-industry Commands for Interchange

ISO 7816-4 is an International Standard that establishes a set of commands across all industries to provide access, security and transmission of card data. Within this basic kernel, for example, are commands to read, write and update records.

There is an urban legend often repeated by smart card sales people that ISO 7816-4 is so complex and so poorly written that it is impossible to implement. Strictly compliant implementations of ISO 7816-4 have been created. These claims are intended to excuse lack attention to complying with the standard in the hopes of selling non-standard cards.

Impact of secure messaging on the structures of APDU messages

Clarifies the construction of secure message variants of commands in Part 4.

http://perso.wanadoo.fr/dgil/scm/iso7816_4.html

Standardizace identifikátorů karetních aplikací

Podle 7816-5 se skládá Application Identifiers (AIDs) ze dvou částí. 1) 5-bytes Registered Application Provider Identifier (RID) jednoznačně přiřazený výrobcí. 2) Proprietary Application Identifier Extension (PIX), kterým výrobce identifikuje aplikaci (variable).

Registrační autoritou RIDs je Copenhagen Telephone Company Ltd.

Part 6: Inter-industry data elements

Describes encoding rules for data needed in many applications e.g. name and photograph of owner, his preference of languages etc.

Technical Corrigendum 1: Interindustry Data Elements

Amendment 1: IC manufacturer registration

Part 7: Interindustry commands for Structured Card Query Language (SCQL)

Defines how to treat the data on the card as an SQL database.

Part 8: Security related interindustry commands

Adds symmetric and asymmetric key capabilities to Part 4.

Part 9: Additional interindustry commands and security attributes

Adds commands needed for personalization such as Create File and Delete File as well as search commands to Part 4.

Part 10: Electronic signals and answer to reset for synchronous cards

Defines basic communication protocols for synchronous (T=14) smart cards.

Part 15: Cryptographic token information in IC Cards

A standardized way to keep cryptographic material on a smart card and to access public keys and certificates stored therein.

9.3 NORMA ISO/IEC 14443 A ISO/IEC 15693

ISO/IEC 14443 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards.

Standard (parts 1-4) specifikuje komunikaci (transmission, anticollision, selection, command exchange) of chipcards in ranges up to 10cm. Jsou definovány protokoly A a B. Další protokoly jsou C, D a E.

ISO/IEC 15693 - Identification cards - Contactless integrated circuit(s) cards - Vicinity cards.

9.4 SMART KARTY A PKI

„Symbioza“ PKI a smart karet se promítá do řady standardizačních aktivit:

RSA (www.rsa.com) specifikovala PKCS#15 "Cryptographic Token Information Syntax Standard", týkající se souborové a datové struktury smart karty (kryptografického tokenu) pro PKI.

„Global Mobile Commerce Forum“(global.mobilecommerce.com), Radicchio (www.radicchio.org) – rámec pracovní skupiny sledující možnosti využití PKI smart karet na bezdrátových sítích(wireless networks).

PKI Forum (pkiforum.org) se zabývá rovněž specifikacemi pro e-podpisy s dopady na PKI smart karty.

MasterCard inicializoval skupinu pro tvorbu draftů týkajících se digitální uživatelské identity a ID procedur pro vystavení, revokaci, správu ID. Skupina zahrnuje ACI Worldwide, Unisys a významné výrobce smart karet - Gemplus, Bull Smart Cards & Terminals, Giesecke & Devrient a Schlumberger.

ETSI Technical Committee Security se podílí na standardech formátu PKI certifikátů, viz ES 201 733.

„Smart Card Constituency“ – jako součást integračního úsilí „eEurope“ (http://europa.eu.int/comm/information_society/eeurope/index_en.htm) se podílí na množině specifikací pro interoperabilitu smart karet.

SIMalliance (www.simalliance.org) – skupina výrobců karet: navrhuje specifikace protokolů pro konektivitu smart karet typu GSM SIM na internet (TCP/IP stacks).

E-Europe projekt pro mapování problematiky smart karet a karetních aplikací a publikování tutoriálů a dokumentů typu „white papers“
<http://www.eeurope-smartcards.org/B2-Index.htm>

9.5 PRŮMYSLOVÉ SPECIFIKACE PRO SMART KARTY A APLIKACE

Zdroje: Průmyslová konsorcia, společnosti, user groups

PC/SC group. Specifikace pro komunikaci „smart karta – PC“ (<http://www.pcscworkgroup.com>).

GlobalPlatform (www.globalplatform.org) je standardizační konzorcium iniciované asociací Visa. Drafty založené na Visa Open Platform týkající se multiaplikačních smart karet.

Java Card Forum (www.javacardforum.org) and JavaSoft (www.javasoft.com) specifikace pro Java Card.

OpenCard Framework (www.opencard.org) – Standardy pro práci s Javou zaměřenou na smart karty.

STIP - Small Terminal Interoperability Platform konzorcium (www.stipgroup.org)

EMV specifikace. Europay, MasterCard and Visa vytvořily normu „Integrated Circuit Card Specifications for Payment Systems“, stručně EMV, pro platební systémy založené na čipových kartách. Základ specifikace založen (s mírnými úpravami) na ISO/IEC 7816. (<http://www.emvco.com/>).

CEPS (jeden z typů elektronické peněženky, které přežily do současnosti). Specifikace Europay www.europay.com, CEPS dokumenty na <http://www.cepsco.com/>

Inspirativní představa interoperability ve spojení se smart kartami je v materiálu "Government Smart Card Interoperability Specification", dostupnost na csrc.nist.gov/smartcard/GSCISV2-0.pdf.

9.5.1 KEY MANAGEMENT

Popis řízení klíčového hospodářství - generování klíčů, jejich použití a případné zničení, volba kryptografických algoritmů, velikosti klíčů, kryptografických politik a výběr kryptografických modulů. Popis úrovně řízení v jednotlivých organizacích, příslušné politiky a prováděcí směrnice.

Příručka pro popis klíčového hospodářství viz (<http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html>).

viz rovněž:

ČSN ISO/IEC 11770-1 Informační technologie - Bezpečnostní techniky - Správa klíčů -

Část 1: Struktura

ČSN ISO/IEC 11770-2 Informační technologie - Bezpečnostní techniky - Správa klíčů -

Část 2: Mechanismy používající symetrické techniky

ČSN ISO/IEC 11770-3 Informační technologie - Bezpečnostní techniky - Správa klíčů -

Část 3: Mechanismy používající asymetrické techniky

9.6 PRŮMYSLOVÉ SPECIFIKACE PKCS

Public Key Cryptographics Standards zajišťují průmyslové sjednocení metod pro ochranu informace při přenosu a vzájemnou autentizaci účastníků na síti.

(www.rsa.com).

PKCS #1:RSA Cryptography Standard

PKCS #3:Diffie-Hellman Key Agreement Standard

PKCS #5:Password-Based Cryptography Standard

PKCS #6:Extended-Certificate Syntax Standard

PKCS #7:Cryptographic Message Syntax Standard

PKCS #8:Private-Key Information Syntax Standard

PKCS #9:Selected Attribute Types

PKCS #10:Certification Request Syntax Standard

PKCS #11:Cryptographic Token Interface Standard

PKCS #12:Personal Information Exchange Syntax Standard

PKCS #13: Elliptic Curve Cryptography Standard

PKCS #15: Cryptographic Token Information Format Standard

Stručná anotace PKCS

PKCS#1 popisuje postup (rsaEncryption) pro zašifrování dat.

Použití při konstrukci digitálního podpisu a digitálních obálek v návaznosti na PKCS #7. Obsah podepsované zprávy je nejprve vyjádřen pomocí otisku této zprávy (SHA1). Potom je oktetový řetězec reprezentující otisk zašifrován soukromým RSA klíčem podepisující strany. Obsah zprávy a zašifrovaný otisk zprávy je pak vyjádřen ve formátu definovaném PKCS #7.

Při vytváření digitální obálky zpráva nejprve zašifrována symetrickou šifrou (3DES). Použitý symetrický klíč je v zašifrované podobě rovněž součástí zprávy zformátované dle PKCS #7 (klíč je zašifrován veřejným RSA klíčem adresáta).

PKCS#3 - definuje asymetrický algoritmus (protokol) DH - Diffie-Hellman. DH používá se k ustanovení šifrovacího symetrického klíče relace. Klíč se vypočte na obou stranách relace zároveň z privátního klíče a veřejného klíče protistrany.

PKCS#7 - standard definuje formát šifrovaných dat, digitálně podepsaných dat, dat s kontrolním součtem, dat, která jsou zároveň šifrovaná a digitálně podepsaná, obecných dat a dat zašifrovaných "jiným způsobem". Rozšíření PKCS#7 se nazývá CMS - Cryptographic Message Standard. Norma použita pro standard zabezpečení elektronické pošty - S/MIME.

PKCS#10 - definuje podobu žádosti o certifikát. Standardní žádost o certifikát obsahuje kromě veřejného klíče, také další údaje žadatele. Žádost je podepsána soukromým klíčem žadatele. (CA ověří, že žadatel má k danému veřejnému klíči i příslušný soukromý klíč). Tento standard neřeší některé speciální žádosti (např. žádost o DH certifikát) a tak vznikl standard CRMF (Certificate Request Message Format), který je určitou nadmnožinou PKCS#10.

PKCS#11 - standard specifikuje kryptografické rozhraní mezi aplikací a kartou. Na jeho základě lze definovat programátorské (aplikační) rozhraní (API) pro karty, obecněji pro hardwarové bezpečnostní tokeny (čipové karty, USB tokeny, kryptografické akcelerátory, HSM moduly, ...). Pokud se aplikace obrací na token, používá pro přístup k tokenu většinou PKC#11 nebo CSP.

Aplikační rozhraní, založené na PKCS#11 se nazývá CryptoKI. Primárním významem Cryptoki je nízkourovňové programové rozhraní, které abstrahuje detaily těchto zařízení a poskytuje tak aplikacím společný model kryptografického zařízení zvaného "kryptografický token". To má výrazný vliv na možnost vývoje přenositelných aplikací. Cryptoki se na token dívá jako na zařízení, které ukládá objekty (data, klíče, certifikáty) a vykonává kryptografické funkce.

PKCS#12 - tento standard se zabývá importem/exportem digitálních ID do/z tokenů a navrhuje formát. Digitálním ID = soukromý klíč + certifikát (+veřejný klíč PK). Exportovat samozřejmě nelze soukromé klíče, jen PK a vlastní certifikát. Pokud jde o import, tak do tokenů lze importovat digitální ID právě ve formátu dle tohoto standardu, tj. pomocí souborů s příponou P12 a PFX.

PKCS#15 - navrhuje "rozložení" a způsob uchování informací uvnitř tokenu. Viz příklady návrhu prototypu karty v této zprávě.

9.7 BEZPEČNOSTNÍ NORMY

Smart Card Security Users Group (SCSUG) a bezpečnost podle Common Criteria (ISO 15408),
<http://csrc.nist.gov/cc/sc/scslist.htm>

Inspirativní mohou být tyto materiály
- Smart Card Security User Group Smart Card Protection Profile
<http://csrc.nist.gov/cc/sc/scscug.pdf>

9.8 SPECIFIKACE ROZHRAŇÍ KARTA-SNÍMAČ, TERMINÁL

- § Standardizace rozhraní pro snímače smart karet je proti ostatním komponentám ICT o několik let opožděna: pro kontaktní, bezkontaktní rozhraní, dokonce i v případě USB rozhraní. API jsou založena většinou na proprietárních řešeních. Hlavní proud standardizačního úsilí se týká specifikace Personal Computer/Smart Card (akronym PC/SC). PC/SC specifikace ve verzi 1 byla implementována ve Windows a Linuxu. Nová specifikace PC/SC ver.2 zahrnuje i bezkontaktní rozhraní.
- § Informace o standardech na adrese <http://www.pcscworkgroup.com>.
- § Jeden z hlavních proudů současných průmyslových trendů v oblasti moderních čipových karet se týká rozšíření a standardizace bezkontaktních snímačů čipových karet podle ISO 1443A,B. Bezkontaktní rozhraní je též zahrnuto do specifikace rozhraní PC/SC ve verzi 2.
- § Seznam PC/SC snímačů podporovaných ve Windows a kompatibilních s PC/SC (v.1), např. na adrese <http://www.microsoft.com/hcl/default.asp> (Smart Card Readers).
- § PC/SC řešení a implementace týkající se Linuxu pro řadu typů snímačů smart karet: <http://www.linuxnet.com>
- § Z pohledu ID-smart karet marginální průmyslové standardy jsou:
 - OTA (Open Terminal Architecture)
Tento standard vznikl z iniciativy Europay International (<http://www.europay.com>), architektura pro tvorbu přenositelných terminálových aplikací. Podpora „Forth virtual machine“.
 - POS / EFT_POS (Electronic Funds Transfer Point Of Sale)
Platební terminály pro čipové karty se soustřeďují s praktických důvodů na podporu specifikace asociací pro platební karty EMV.

10 PŘÍLOHA Č. 2 INICIATIVY, FÓRA, ORGANIZACE

10.1 TECHNOLOGICKÉ ZDROJE

Smart Card Solutions Limited

Vývoj COS (card operating systems) a karetních aplikací

Smart Card Technical Resources

Obecné i nízkourovňové technické informace o smart kartách a datových rozhraních

Smart Cards for Windows

Aktuality a zdroje o řešení fy Microsoft v oblasti technologie smart karet.

Smartcard Focus

Databáze snímačů smart karet, databáze karetních aplikací, standardů a odkazů.

10.2 ASOCIACE

Card Europe

Card Europe je nezisková organizace zabývající se nasazováním a využíváním smart karet (např. www.cardeurope.demon.co.uk)

GlobalPlatform

GlobalPlatform sleduje a porovnává zájmy vydavatelů, výrobců, průmyslových skupin, veřejných entit, k určení požadavků a technologických standardů pro multiaplikační smart karty. GlobalPlatform řídí a rozvíjí specifikace „Open Platform specifications“ původně vytvořené asociací VISA.

(www.globalplatform.org)

JavaCard Forum

Domovské fórum skupiny „JavaCard Forum group“ která pracuje na příslušných standardech a sleduje kompatibilitu JavaCard Smart Cards.

(www.javacardforum.org)

PC/SC Workgroup

Kritické technické dokumenty vztahující se k integraci smart karet a všech ICCs s platformou PC

(www.pcscworkgroup.com)

Smart Card Alliance

Nezisková organizace působící v americkém karetním průmyslu (smart karty)

(www.smartcardalliance.org)

Smart Sign Project

Projektové směry integrující karetní technologie s PKI do otevřených interoperabilních řešení.

(<http://smartsign.sourceforge.net/about.html>)

10.3 BEZPEČNOST A CERTIFIKACE

Referenční odkaz:

Smart Card Security Users Group (SCSUG) a bezpečnost podle Common Criteria (ISO 15408),

<http://csrc.nist.gov/cc/sc/sclist.htm>

Příklady organizací pro testování (a certifikaci) smart karet.

Pozn. Některé laboratoře poskytují testovací utility.

Collis

(<http://www.collis.nl/conclusion>)

Cygnacom CEAL

(www.cygnacom.com/ceal.html)

Domus ITSEC Laboratory

(www.domus.com)

FIME (<http://www.fime.com>)

Gilles Leroux

(<http://www.gilles-leroux.com>)

ICC Solutions

(<http://www.iccsolutions.com>)

InfoGuard Labs

(<http://www.infogard.com>)

Integri

(<http://www.integri.be>)

Micropross

(<http://www.micropross.com>)

Tuvit

(<http://www.tuvit.net>)

Laboratoře s osvědčením od NSA a NIST: CC (Common Criteria)

Computer Sciences Corp.

Cygnacom Solutions

Science Applications International Corp.

11 PŘÍLOHA Č. 3 ODKAZY NA VÝROBCE A PRŮMYSL ČIPOVÝCH TECHNOLOGIÍ

Poznámka: Pro vyhledání detailnějších odkazů lze například použít adresu:

<http://www.netinformations.com/>

11.1 SMART KARTY A VÝVOJOVÁ PODPORA (SDK)

Výrobci, dodavatelé smart karet a souvisejících technologií, kteří poskytují vývojovou podporu (SDK)

Poznámka: Subjektivní výběr s přihlédnutím k internetovým citacím a odkazům. Na obr. několik ilustračních příkladů - obrazovek při přípravě karetních aplikací.

Alegra Technologies (Pittsburg)

<http://www.alegratechnologies.com/about.htm>

Athena SmartCard Solutions (Japan)

<http://www.athena-scs.com/>

Axalto - Schlumberger

<http://www.axalto.com> aj.

Gemplus

<http://store.gemplus.com>

G&D (Giesecke&Devrient)

<http://www.gdai.com>

Net Informatique Services

<http://www.nis-infor.com/>

Nexsmart Technologies (CA)

<http://www.nexsmart.com/>

Oak-Tech.com (Hong Kong)

<http://www.hkoak-tech.com>

Schlumberger Smart Card Store (viz též Axalto)

spec. <http://www.scmegastore.com/>, [www.axalto](http://www.axalto.com) a další

SDLOGIC Technologies, Inc. (CA)

<http://www.sdlogic.com/index.asp>

SmartcardFocus

Richmond,UK

<http://www.smartcardfocus.com/>

SMART-SOLUTIONS.CA

Bedford

<http://www.smart-solutions.ca/>

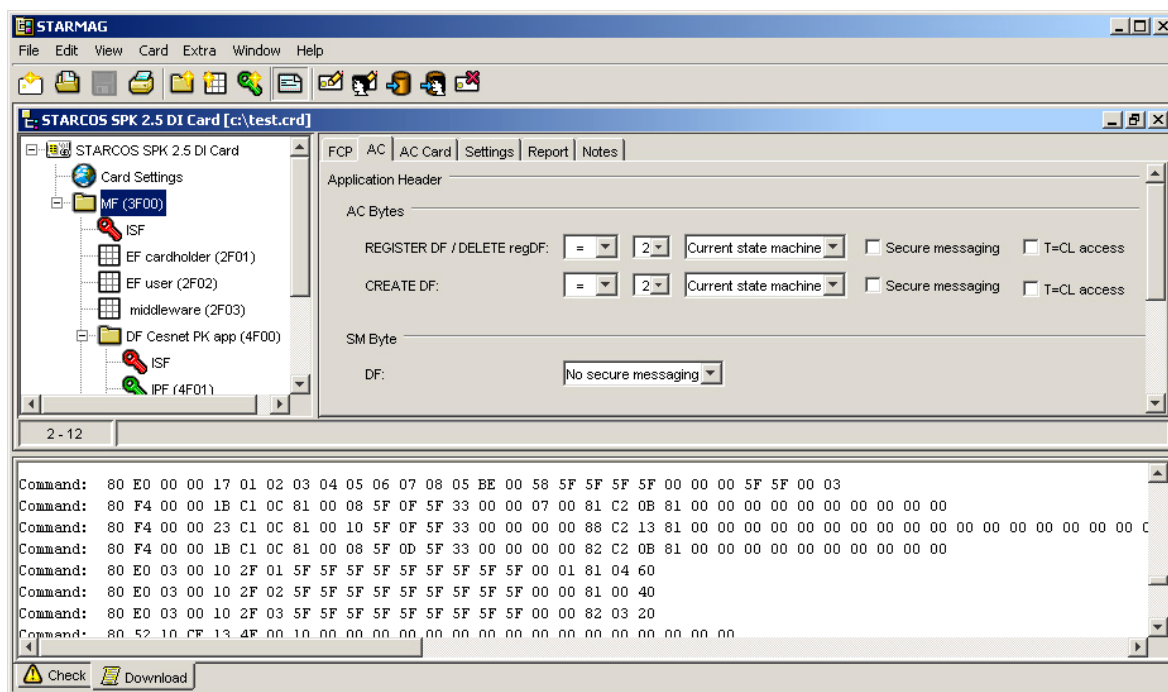
ZeitControl

Cardsystems GmbH

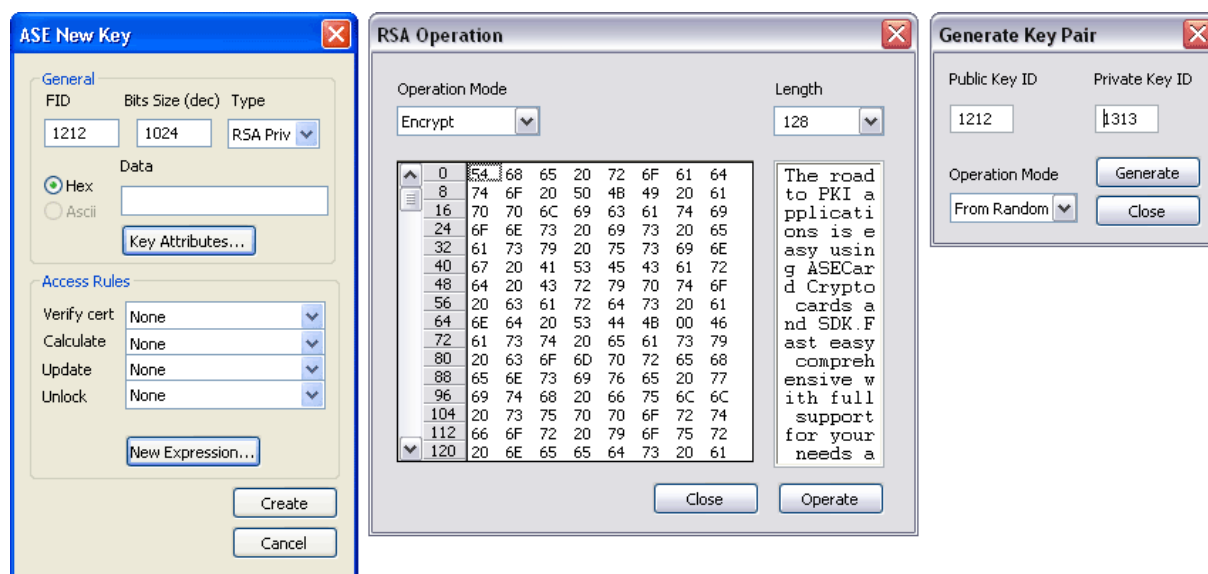
<http://basiccard.com/> (firma používá víc adres)

###

Ilustrace práce s SDK ve Windows:



Obr. 14 Příklad SDK s podporou karet SPK2.5DI na bezkontaktním rozhraní (Starmag, G&D)
(Nástroj pro přípravu karetních aplikací PKI Cesnet, PKI University)



Obr. 15 Příklad vývoj. prostředí pro kontaktní PKI karty (ASE, Athena)

11.2 COS - OPERAČNÍ SYSTÉMY

Průřezová problematika spojená s vývojem COS a čipových systémů je například na adresách:

<http://www.smartecos.com>
<http://www.chipcardstore.com>
<http://www.openavr.org/>

Klasické smart karty s pevnou instrukční sadou.

Příklady klasických karet opatřených COS od vybraných výrobců:

G&D (Giesecke&Devrient)
(<http://www.gdm.de>, www.gdai.com)
Starcos

Gemplus
(<http://store.gemplus.com>)
(<http://www.gemsafe.com>)
GEMSafe

IBM
(<http://www.comcard.de>)
MFC 4.1

Schlumberger
(<http://www.cardstore.slb.com>)
Multiflex
Cyberflex
Cryptoflex
MicroPayflex

JavaCards

-Většina výrobců a dodavatelů řešení má ve výrobním programu rovněž karty na platformě JavaCard (např. Datakey, Gemplus, Giesecke&Devrient, Schlumberger, Sony....) a dodává je i s aplikacemi.

-Specifikace, dokumentace a referenční implementace v oblasti Java Card platform:

Sun's Java Card Technology
viz kap. Asociace ... pro Java Card Forum

Výrobci Java Cards a Java Card SDK, výběr:

Schlumberger Java Card and Software Development Kit (SDK)
Cyberflex, <http://www.cardstore.slb.com>

Aspects Software:
<http://www.aspects-sw.com>

Gemplus: GemXpresso
<http://www.gemplus.com>

Oberthur: Galactic
<http://www.oberthursc.com>

G&D (Giesecke & Devrient): Sm@rtCafe
<http://www.gdm.de>, www.gdai.com

IBM: <http://www.zurich.ibm.com/csc/infosec/smartcard.html>
Fujitsu: <http://edevice.fujitsu.com/fj/CATALOG/PDF/a05000263e.pdf>

Příklady Open Source projektů resp. výukových projektů

Open source COS project - University of Michigan (starší)
(www.citi.umich.edu).

Simple Operating System for Smartcard Education (SOSSE)
COS pro Atmel kontrolery.
www.opensc.org/sosse/, www.mbsks.franken.de/sosse/.

SmarteC free SDK pro operační systém SmarteCOS
(<http://www.smartecos.com>)

COS – software, binární (zdrojový) kód

Uvedené produkty vesměs nejsou vázány na specifické smart karty (hardware od dodavatele)
Některé níže uvedené zdroje lze použít k výukovým účelům, příp. licencovat pro vlastní karty

AMOS-SC and AMOS-SIM
American Microdevice Manufacturing, Inc.

Exceldata
<http://www.exceldata.es>
M.MAR ISO - ISO 7816 Card

IBM MFC
Schilling
Smart Card Projects
www.de.ibm.com

IBM Java Card Operating System
Peter Buhler
zurich.ibm.com

Gator and SCOS
Amazing Smart Card Technologies
www.amazingtechnologies.com

Smart Card for Windows
Microsoft Corporation

OSSCA
Keycorp Limited
<http://www.keycorp.net>

DKCCOS
Datakey
<http://www.datakey.com>

Secure Java O/S
www.jayacard.org

Siemens CardOS M3 and M4
Information and Communication Group,
Smart Cards and Security
http://www.siemens.com/sbs/en/offerings/services/SmartCard/Products/cardos_m4.html

Simple Operating System for Smartcard Education
<http://www.franken.de/users/mbsks/sosse/index.html>

11.3 APLIKACE PRO SMART KARTY

Dodavatelé řešení (Solution Providers)

ACG AG

Čipy a smart karty pro e-komerci, internet homebanking

Aigner Technologies

smart karty, věrnostní karty, zařízení typu čteček, a Card-Printer

BMIT Solutions

Smart karty, PKI and biometrika.

Cylink

Poskytuje autentizační řešení k zabezpečení e-komerce pomocí USB-tokenů, smart karet, toolkitů, serverů.

Chipcards Ltd.

Řešení pro platební systémy a smart karty.

Datacard Group

Poskytuje personalizační řešení, personalizační výrobní linky, smart karty, související HW a SW.

DBC Braincon Technologies

Výrobce HW, v repertoáru smart karty a ID karty, Proxy, Mifare, EDP-Security, konzultační služby

Eletek Smart Solutions

Eletek je poskytovatel řešení pro karetní produkty, zařízení pro personalizaci a další, je rovněž výrobcem snímačů a OEM čtecích modulů (Dodávky pro UK Praha)

Labcal Technologies

Labcal Technologies nabízí PKI systémy a řešení s integrací smart karet a biometricky

RSA Security

Dodává smart karty zejména na podporu svých ID/PKI řešení

Siemens SmartCard Services

Rozsáhlé spektrum služeb a řešení na bázi smart karet

11.3.1 SOFTWAREVÉ NÁSTROJE A KNIHOVNY PRO SMART KARTY

Příklady známějších poskytovatelů software, SDK, utilit a knihoven

Card-Lab

(Card-Lab podporují simulátory, např. pro Multos)

(<http://www.card-lab.com>)

DataKey SignaSURE DTK

(<http://www.datakey.com>)

Flint Smart

(<http://www.flint.co.uk>)

G&D, Giesecke & Devrient STARMAG STARCOS Tool Kit

(<http://www.gdm.de>, www.gdai.com)

Metrowerks - a Java Card development system

(www.metrowerks.com)

Schlumberger - Cyberflex Java Card development kit

(cardstore.slb.com)

Smart Dynamics EZ Formatter

(<http://www.smartdynamics.com/software.htm>)

Utimaco
(<http://www.utimaco.com>)

Příklady řešení v oblasti utilit, softwarových nástrojů pro karetní rozhraní a middleware

Utility pro Win PC/SC a WinSCard APDU View Utility
<http://www.fernandes.org/apduview/index.html>.

PC/SC driver a utility, open source
<http://www.dbasko.com>

Software pro podporu PKCS#11 ve Win98, NT4.0, W2k, XP, Linux, MAC OS X pro G&D Starcos a Rainbow iKey USB Token.
<http://www.aeteurope.nl/html/aet.html>

Utility a knihovny pro Windows rozhraní (wincard.dll):
<http://www.fernandes.org/apduview/index.html>

SCEZ Library
(<http://www.franken.de/crypt/scez.html>)

UMich Library – starší věci
(<http://www.citi.umich.edu/projects/smartcard/sc7816.html>)

PC/SC software
(<http://www.pcsc.pl/VAS/index.html>)

tfn - PC/SC varia, SDK pro Scard
(<http://www.tfn.net/techno/smartcards/software.html>)

ActiveX Component
(<http://www.prioregroup.com/>)

11.3.2 FIRMY S KOMPLEXNÍM PROGRAMEM JAVA CARD A PRODUKTY

Aspects Software
(www.aspects-sw.com)

Datakey - Model 330J
(www.datakey.com)
Fujitsu - HIPERSIM
(www.fujitsu.com)

Gemplus - GemXpresso
(www.gemplus.com)

G&D (Giesecke & Devrient) -Sm@rtCafé
(www.gdm.de, www.gdai.com)

IBM Java Card -JCOP
<http://www.zurich.ibm.com/csc/infosec/smartcard.html>.

Oberthur -GalactiC
(www.oberthurusa.com)

Schlumberger -Cyberflex
(www.cardstore.slb.com)

11.3.3 SOFTWAREVÉ NÁSTROJE PRO SMART KARTY SIM

Okruh smart karet typu SIM je zatím pro akademickou komunitu marginální, může mít svůj význam při „customizaci“ čipů, při řešení identifikace (autentizace) a aplikací v rámci sítí a zařízení (GSM brány, datové bezdrátové sítě) disponujících čipy (smart kartami)SIM.

Komerční podpora nástrojů „SIM Application Toolkit (SAT)“, např.

- Gemplus (GemXplore98)
- Giesecke & Devrient (StarSIM)
- Multos (Multos SIM Card)
- Oberthur (SIMphonic)
- Orga (SIMtelligence)
- Schlumberger (SIMera)

11.4 VÝROBCI SMART KARET

Austria Card

Produkce čipových karet, rozvoj zejména v oblasti platebních karet s licenční podporou G&D.

www.austriacard.at

Axalto

Úplné technické i aplikační spektrum založené na čipových kartách, rozsáhlý program PKI/ID karet, snímače, terminály. Viz Schlumberger, který vystupuje pod hlavičkou Axalto.

www.axalto.com

Compelson Laboratories

Nabídka smart karet (ID/PKI a SIM), utilit, SDK, snímačů s obchodním zastoupením v ČR

www.compelson.com (též www.compelson.cz)

Datakey

Produkce čipových karet a čteček, zejména pro identifikaci a PKI, včetně USB-tokenů. Utility a softwarová nadstavba pro firemní produkty

www.datakey.com

De La Rue

ID-karty, bankovní karty, e-payment, e-commerce, e-government

www.delarue.com

Euclid Limited

Nabídka řešení od požadavků na libovolné plastové karty, od plastových/mg/čipových vstupenek ke standardním čipovým produktům.

www.euclid.ltd.uk

Gemplus

Nabízí úplné technické i aplikační spektrum bankovních (EMV) i smart karet (PKI/ID), hardware i software, aktivní účast na rozvoji standardů

www.gemplus.com

G&D (Giesecke & Devrient)

Nabízí úplné technické i aplikační spektrum čipových karet (včetně EMV, PKI/ID) i tokenů, bezpečnostní, průmyslová, věrnostní, campus-řešení, pokrývá e-payment, e-commerce, e-government, dodává nástroje pro vývojáře, aktivní účast na rozvoji standardů

www.gdai.com

ICcard Technology Corporation

Výrobce celého spektra IC-karet, smart karet pro ID/PKI, PVC karet.

<http://www.cardic.com.tw/>

Infineon Technologies AG

Vývoj nových technologií (IC) a produkce čipů, též čipové karty a software

www.infineon.com

I'M Technologies
Výrobce smart karet především pro mobilní telefonii (GSM SIM karty, WCDMA USIM karty)
<http://www.imcorporation.com/>

Litronic, (nyní divize SAVLINK Corp.)
Poskytuje řešení pro smart karty, čtečky s kombinovanými rozhraními, bezpečnostní middleware, toolkity pro vývoj karetých aplikací (software developer toolkits), bezpečnostní aplikace v rámci PKI (účast na karetých projektech DoD a CAC (USA))
<http://www.ssplitronic.com/>

Neuron Electronics Inc.
Vyrábí karty, snímače pro smart karty, USB čtečky aj.

Oberthur Card Systems
Výrobce platebních karet, smart karet, karet pro bezpečné transakce nad PKI

ORGA

OTI - On Track Innovations Ltd
Výrobce smart karet a karetých aplikací, v repertoáru zejména bezkontaktní a duální karty, snímače karet, tokeny, podpora řešení na bázi ID/PKI

Philips (Philips Semiconductors)
Vývoj a produkce čipů, čipové karty, vývojové nástroje, standardizační aktivity v oblasti čipových technologií
Samsung

Schlumberger Limited (viz Axalto, SchlumbergerSema)
Řešení fy Schlumberger v oblasti smart karet zahrnuje rozsáhlý repertoár karet, terminálů, vývojových nástrojů, podporu integrátorům.

Sony
Výroba širšího spektra čipových technologií včetně smart karet

Worldtronic

11.5 VÝROBCI ČIPŮ PRO SMART KARTY

Výrobci čipů (kontrolerů, IC) pro smart karty, výběr:

Advanced Logic
Atmel
Hitachi
Infineon
Inside Technologies
Microchip
NEC
Philips Semiconductors
Samsung
Semiconductor
STMicroelectronics
Texas Instruments
Toshiba
Xicor.

Odkaz - zabezpečení proti útokům na smart kartu

Rozsáhlá problematika, mimo rámec zprávy. Dvě reference přiloženy:

<http://www.cl.cam.ac.uk/Research/Security/tamper>
<http://www.cryptography.com/dpa/technical/index.html>

11.6 BEZKONTAKTNÍ PRODUKTY A KLASICKÉ APLIKACE

<http://www.ask.fr/>

<http://www.insidefr.com/products/kits.htm>

<http://www.epicard.com/contactless/products/>

<http://www.supertechsystems.com>

<http://smartechnology.com.au/index1.htm>

<http://www.topcard-monetique.com/anglais/summary/summaryd.htm>

<http://www.epsys.no/sreaders.htm>

<http://www.athena-scs.com>

<http://www.omron.com/card/rfid/prod/v720/kit.html>

<http://www.microchip.com/1000/pline/tools/index.htm>

<http://www.ehag.ch/HTML-Files/RFID/inside.htm>

Poznámka: viz též výrobci podle jednotlivých kategorií:

<http://www.contactlessnews.com/vendors/38.php>

11.7 SNÍMAČE SMART KARET– VÝROBCI S PŘÍMOU DISTRIBUCÍ

Příklady výrobců snímačů smart karet s přímou distribucí a prodejem

Advanced Card Systems Ltd. – Snímače(s EMV certifikací), vývojové nástroje, biometrické skenery se čtečkami smart karet.

<http://www.acs.com.hk>

ASK

výrobce snímačů kontakt/bezkontak, vč.bezkontaktních „handheld“ čteček, couplers (bezkontaktních čtecích modulů), bezkontaktních procesorových karet, bezkontaktních papírových vstupenek a labelů (ISO14443,RFID, mj. podpora specifikace Calypso)

(<http://www.ask.fr>)

Athena

(<http://www.athena-scs.com>)

Výrobce čteček, vč. tzv. „embedded readerů“ montovatelných podle uživatele, vesměs kontaktní provedení. Smart karty pro PKI, kontaktní (COS: AsepCOS, SW tools pro Win, SDK)

Bull SCT – Výrobce čteček a POS terminálů

(<http://www.cp8.bull.com>)

CardTronics Corp. - Poskytovatel zákaznických zařízení/rozhraní pro smart karty pro OEM a systémové integrátory, operátory.

Chery Corp. – výrobce čteček / integrovaných čteček na klávesnici / biometrických prvků softwarové nástroje k e-podpisu.

např. klávesnice typu Chery 14100 má senzor pro logon přes otisk palce i smart čtečku

(<http://www.cherycorp.com/english/advanced-line/index.htm>)

Datamega
(<http://www.datamega.com>)

DeLaRue
(<http://www.delarue.com>)

Dione PLC - Poskytovatel MSys (management systems) výrobce terminálů a pinpad pro smart /EMV karty

(<http://www.dione.co.uk>)

viz též informace o dodavatelích smart-card snímačů na adrese:

http://www.applegate.co.uk/elec/pselect/ps_4892.htm

Eletek Smart Solutions

Výrobce snímačů a OEM čtecích modulů (Dodávky pro UK Praha)

poskytovatel řešení pro karetní produkty, zařízení pro personalizaci

Elk Technologies – Průmyslové, mechanicky odolné, vlhkotěsné, spolehlivé čtečky pro smart karty.

Epsilon Electronics
(<http://www.eps.no>)

Fischer International Systems
(<http://www.fisc.com>)

Gemplus – výrobce většího spektra smart karet, systémů, řešení, čteček kontaktních, bezkontaktních (access control),

klávesnice se čtečkou, podpora pinpadu a biometricky

(<http://www.gemplus.com>)

Ingenico – výrobce čteček a POS terminálů

Labcal Technologies – Snímače smart karet podporující čipovou technologii (smart karty) v oblasti PKI prostřednictvím nabídky přenositelného bezpečného tokenu pro certifikáty a klíče.

Litronic
(<http://www.litronic.com>)

Micropross – Výroba snímačů pro smart karty s dodáním pro výrobce a vývojáře

Omniquey – Snímače pro karty (včetně distribuce smart karet)
(<http://www.omnikey.com>)

ORGA Orga Card Systems
(<http://www.orga.com>)

Philips Semiconductors – čtečky, čipy a čipové karty
(<http://www.semiconductors.philips.com/markets/identification>)

Pro-Active - CompactFlash čtečky pro smartkarty určené pro Pocket PCs.

Rainbow Technologies
(<http://www.rainbow.com>)

Schlumberger – nyní Axalto
(<http://www.slb.com/smartcards>) (Axalto)

SmartCard Laboratory
(<http://www.smartcardlab.com>)

SCM Microsystems, Inc. - Design, vývoj a dodávky technologií pro rozhraní smart karet. Řešení pro OEM a čteček pro PC.

(<http://www.scmmicro.com>)

SDLogic Technologies
(<http://www.sdlogic.com>)

SecureTech

(<http://www.securetech-corp.com>)

Sagem – mj.výrobce čteček (multi-biometrika)
(www.sagem.com)

Todos
(<http://www.todos.se/argosminiindex.htm>)

Towitoko Inc. – Vyrábí cenově dostupné čtečky pro smart karty
(<http://www.towitoko.de>)

Vasco - vyrábí mj. USB čtečky s pinpady (smart čtečky s dispejem a klávesnicí)

Utimaco Safeware AG – produkty pro řešení bezpečnosti přístupu v ICT a datových medií, biometrické čtečky a čipové karty
(<http://www.utimaco.com>)

Zeitcontrol CardSystems GmbH – karetní systémy, širší spektrum produkce,
např. dceřinná firma Cybermouse – PC/SC čtečky
(<http://www.cybermouse.de>)

- - -

12 TERMINOLOGIE

AID Application Identifier (ID pro karetní aplikaci podle ISO 7816-5)

Anti-collision

Mechanismus užitý při bezkontaktní komunikaci karty k prevenci konfliktu mezi různými signály od různých karet vyžadujících komunikaci ve stejný okamžik (pro proximitní karty viz ISO14443).

APDU (Application Protocol Data Unit)

Základní příkazový protokol pro smart karty podle ISO7816-3 a ISO7816-4. Jako aplikační vrstva (OSI model vrstva 7) je nezávislá na přenosovém TPDU. Na bázi protokolu probíhá komunikace „terminál – karta“ typu „command message“, kdy terminál posílá zprávu na kartu (C-APDU) nebo typu „response message“, kdy karta posílá odpověď na terminál (R-APDU).

ATR (Answer To Reset) (ISO 7816-3)

Zpráva, kterou vrací smart karta při aktivaci napájecím proudem nebo když je aktivován reset pin. ATR indikuje typ karty, komunikační protokol a další informace. Viz Session.

ATQA Answer to request (typ A) - odpověď karty na REQA

Autentizace

Proces, v němž karta, terminál nebo osoba (entita) prokazují svou identitu

-Externí autentizace

Procedura pro autentizaci terminálu vzhledem ke kartě. V případě multiaplikační karty se autentizuje terminál vůči aplikaci

-Interní autentizace

Procedura, ve které se karta autentizuje, prokazuje svoji identitu vůči terminálu. V případě multiaplikační karty se autentizuje vůči terminálu aplikace.

BER (Basic encoding rules of ASN.1)

(BER, ASN.1, podle ISO8825) definuje formát a pravidla pro formalizovaný zápis datových objektů.

Bezkontaktní karta viz contactless

CAP soubor (Converted (Card) Applet File)

Zkonvertovaný applet - soubor aplikace natažený do JavaCard. Je vytvořen ve vývojovém prostředí konverzí Java class file.

CICC Contactless Integrated Chip Card, akronym bezkontaktní karty podle ISO, viz též PICC

CLA (Class byte) (ISO7816)

Identifikační byte, část hlavičky příkazu APDU. (1) Identifikuje třídu aplikací a jejich „command set“, příklady: ('A0' pro GSM, '0X' pro ISO příkazy, '8X' pro proprietární příkazy) & (2) indikuje užití SM (secure messaging) a logických kanálů.

CMS (Card Management System)

Software, nástroje a služby pro správu karet, jejich životního cyklu a karetních aplikací.

Contact Smart Card, kontaktní karta

Smart karta, která operuje se snímačem prostřednictvím kontaktního fyzického rozhraní (na rozdíl od bezkontaktního rozhraní).

Contactless, bezkontaktní karta

Smart karta, která komunikuje se snímačem pomocí radiofrekvenčního signálu bez potřeby fyzického kontaktu.

klasifikace podle čtecí vzdálenosti:

Close-Coupled Cards 0 mm - 10 mm

Proximity Cards 10 mm - 100 mm

Vicinity Cards 100 mm - 500 mm

COS (Card Operating System), viz OS

CQL (Card Query Language)

Subset SQL (Structured Query Language) implementovaný na smart kartě.

CRC (Cyclic Redundancy Check)

CryptoAPI (Cryptographic Application Programming Interface)

Systémová vrstva MS Windows zprostředkující přístup ke společným kryptografickým funkcím.

CryptoKI

Viz PKCS#11

CryptoKI realizuje koncepci otevřených kryptografických modulů. Požadavky na jejich funkční schopnosti jsou v normě PKCS#11.

Primárním významem *Cryptoki* (resp. PKCS#11) je nízkourovňové programové rozhraní, které abstrahuje detaily připojených kryptografických zařízení (smart karet) a poskytuje tak aplikacím společný model kryptografického zařízení zvaného "kryptografický token". To usnadňuje vývoj přenositelných aplikací. *Cryptoki* se na token dívá jako na zařízení, které ukládá (resp. má uloženy) objekty (data, klíče, certifikáty) a vykonává kryptografické funkce.

Knihovny CryptoKI (PKCS#11) jsou součástí middleware. Nezávislost na platformě (OS).

CSP (Cryptographic Service Provider)

Softwarový modul, řízený systémovou vrstvou Windows CryptoAPI. Realizuje kryptografické funkce, spravuje úložiště privátních klíčů pomocí software (registry) nebo pomocí hardware (smart karta).

CSP oslovuje kartu při plnění požadavků aplikace na operace se soukromými klíči, musí znát specifické vlastnosti karty.

CSP je jako tzv. kryptografický ovladač součástí middleware pro Windows.

DES (Data Encryption Standard)

Šifrovací standard. Symetrický šifrovací algoritmus. Silnější varianta se nazývá 3DES (Triple DES). 3DES/DES a nově standard AES jsou implementovány prakticky všemi výrobci čipů pro smart karty.

DF (Dedicated File)

Součást organizace paměti EEPROM na smart kartách podle ISO7816: DF je logická jednotka, která jako adresář v souborovém systému karty adresuje jako rodič jeden nebo více EF (elementary files). Obsahuje *file control information* a informaci o alokaci paměti V multiaplikačních kartách každý DF koresponduje s nějakou aplikací. Master file MF náleží logicky rovněž mezi DF.

DF Name

Řetězec bytes, který jednoznačně identifikuje DF na kartě.

Directory File

Directory file je EF soubor umístěný v MF(master file), který obsahuje identifikátory aplikací na kartě. (Directory File není povinný, ale např. PKC#15 požaduje jeho použití, je-li na kartě víc PKC#15 aplikací).

Dual Interface

Dvojitý komunikační rozhraní u karty. Smart karta s jedním čipem komunikujícím přes dvě rozhraní, (např. kontaktní a bezkontaktní rozhraní), je označována sufixem DI.

Dual Slot

Snímač smart karet , který je přizpůsobený k současné komunikaci dvou karet (např. karta koncového uživatele a karta autorizovaného admina)

EEPROM (Electrically Erasable Programmable Read-Only Memory)

Typ stálé (non-volatile) paměti. Ve smart kartách EEPROM typicky obsahuje aplikační data.

EF (Elementary File)

Organizační jednotka paměti u smart karty pod správou COS: Nejmenší logická jednotka typu soubor, která může být chráněna bezpečnostními mechanismy COS. Rodičem souboru EF je DF (resp. MF). EF může obsahovat data s různými typy organizace.

EMV (Europay - Mastercard - Visa)

Průmyslový standard pro platební čipové karty, navržený částečně nad ISO7816 (ale s vlastní specifikací EMV2000).

ETSI (European Telecommunications Standards Institute)

FID File Identifier pro MF, DF, EF (podle ISO 7816)

FLASH Memory.

Typ stálé paměti používaný někdy ve smart kartách pro urychlení operací s daty (doplnění EEPROM).

IC (Integrated circuit)

Synonymum: čip

IFD (Interface Device), akronym snímače/terminálu pro kartu podle ISO

Inicializace karty

První krok čipové personalizace před vydáním karty (issuing process). Cílem je příprava datové struktury, load všech dat společných pro jednotlivé aplikace do EEPROM.

ISF (Internal Security File)

Klon EF souboru implementačně specifický pro COS firmy G&D. „Internal EF“ pro uložení soukromého klíče.

ISO (International Standards Organization)

Standardy ISO pro průmysl smart karet zejména zahrnují:

ISO/IEC 7816-1:1998 Physical Characteristics of IC cards.

ISO/IEC 7816-2:1999 Position of Module and Contacts on IC cards.

ISO/IEC 7816-3:1997 Exchange protocol with IC cards (i.e., communication between readers and cards).

ISO/IEC 7816-4:1995 Command set for microprocessor cards.

ISO/IEC 7816-5:1994 Numbering system and registration procedure for application identifiers.

ISO/IEC 7816-6:1996 Inter-industry data elements.

ISO/IEC 7816-7:1999 Inter-industry commands for Structured Card Query Language (SCQL).

ISO/IEC DIS 7816-8 Security related inter-industry commands.

ISO/IEC DIS 7816-9 Additional inter-industry commands and security attributes.

ISO/IEC DIS 7816-10 Electronic signals and answer to reset for synchronous cards.

ISO/IEC 7816-15 (2004)

ISO 14443-1,2,3,4 Proximity cards (contactless).

ITSEC (Information Technology Security Evaluation Certification)

Kriteria pro vyhodnocení bezpečnosti software a IT komponent.

Java Card

termín označující čipovou procesorovou kartu (smart kartu) obsahující JCVM (Java Card Virtual Machine) a JCRE (Java Card Runtime Environment). Karty Java Card určeny k běhu aplikací napsaných v Javě.

Termín Java Card užíván rovněž jako synonymum „Java Card OS“ - softwarové platformy založené na Javě, patřící k otevřeným operačním systémům pro smart karty.

JCF (Java Card Forum)

Průmyslová asociace zabývající se od r. 1997 technologiemi a specifikacemi pro Java Card, jejich rozvojem.

JCRE (Java Card Runtime Environment)

JavaCard operační („runtime“) prostředí, které řídí load appletu a inicializační operace pro applet na kartě.

Součástí je JCVM (Java Card Virtual Machine) a Java Card API.

Lifecycle

Doba mezi vydáním karty a zrušením karty resp. dobou expirace karty.

Memory Card, Paměťová karta

Karta obsahující paměťový čip pro čtení a zápis a některé bezpečnostní funkce řešené hardwarově (Wired logic card). Na rozdíl od smart karty nemá CPU. (Občas ještě není rozlišován tento rozdíl a paměťovou kartu řadí mezi smart karty).

MF (Master File)

Hlavní dedikovaný soubor (viz DF) na smart kartě zřizovaný při inicializaci smart karty: Tento soubor je 1. jediný na kartě 2. povinný, (obdobu root adresáře).

Open Smart Card Operating System

Operační systém, který je deklarován jako otevřený pro implementaci (load) a běh aplikací dodaných třetí stranou, bez nutné účasti výrobce operačního systému na řešení. Například Java Card, Multos, Windows for Smart Cards (WSC) patří mezi otevřené systémy v tomto smyslu. Termín Open Smart COS nevypovídá sám o sobě o míře standardizace a interoperability mezi implementacemi jednotlivých výrobců.

OS (Operating System), COS

Termín používaný podle souvislosti buď

- obecně pro označení systémového prostředí na smart kartě, zajišťující bezpečný přístup k datům na kartě a správu souborů, nebo
- pro označení typu plnohodnotného operačního prostředí, které se vyznačuje pevnou sadou instrukcí (klasický COS na smart kartě, na rozdíl od runtime systémů) nebo
- pro označení systémové vrstvy nad HW, na kterou je implementován runtime-systém.

Paměťová karta viz Memory Card, Wired logic card.

Personalizace

Proces, během kterého je karta přizpůsobena koncovému uživateli, jak datově, tak designem:

Grafická (optická) personalizace včetně potisku, ochranné prvky na kartě.

Čipová („elektrická“) personalizace modifikuje informace v čipu (např. jsou nahrány karetní aplikace)

PCD (Proximity Coupling Device) - bezkontaktní snímač na frekvenci 13,56MHz splňující ISO/IEC 14443.

PICC Proximity Integrated Circuit Card, subtyp CICC.

PIN (Personal Identification Number)

Číslo nebo alfanumerický resp. ASCII kód, který musí držitel karty natypovat do terminálu nebo pinpadu připojeného ke kartě, aby se prokázal jako oprávněný držitel.

PKCS (Public-Key Cryptography Standards)

Průmyslové standardy vydávané pod patronací RSA Security.

PKCS #1 RSA Standard

PKCS #3: Diffie-Hellman Key-Agreement Standard

PKCS #5: Password-Based Cryptography Standard

PKCS #6: Extended-Certificate Syntax Standard

PKCS #7: Cryptographic Message Syntax Standard

PKCS #8: Private-Key Information Syntax Standard

PKCS #9: Selected Attribute Types

PKCS #10: Certification Request Syntax Standard

PKCS #11: Cryptographic Token Interface Standard

PKCS #12: Personal Information Exchange Syntax Standard

PKCS #13: Elliptic Curve Cryptography Standard

PKCS #15: Cryptographic Token Information Format Standard.

POS Terminal (Point Of Sale Terminal)

POS terminály jsou ruční / stolní programovatelná zařízení opatřená snímačem pro on-line nebo off-line transakce (např. platební, věrnostní) pomocí čipových karet s příslušnou aplikací nebo karet s magnetickým pruhem. POS bývají opatřena pinpadem pro zadání PINu.

REQA Request command (typ A)

RSA (Rivest-Shamir-Adleman)

Rozšířený asymetrický šifrovací algoritmus obvykle implementovaný na smart kartách určených pro ID/PKI v koprocesorech.

SAK Select Acknowledge

Session

Časový úsek mezi dvěma resety karty nebo mezi zapojením a odpojením napájení

SHA-1 (Secure Hash Algorithm 1)

Základní hašovací algoritmus na smart kartách, který nahrazuje MD5

SIM (Subscriber Identification Module)

Smart karta pro GSM systémy

Smart Card, smart karta

Čipová procesorová karta. Do této třídy karet se obvykle nezahrnují paměťové čipové karty bez CPU.

SW1-SW2

Status bytes

Terminál

Zařízení, které může komunikovat se smart kartou.

Terminál může operovat samostatně (standalone mode) nebo musí být napojen na centrální IS pro přístup k aplikaci.

TLV (Tag Length Value)

Datový objekt, vytvořený podle pravidel Basic Encoding Rules (BER, ASN.1, viz ISO8825) je kódován podle tzv. TLV-struktury, jejíž pole jsou: 1. tag (label objektu), 2. length (délka objektu), 3. value (aktuální data). Objekt s touto strukturou se nazývá TLV-objekt. Tagy pro frekventované datové struktury, pro datové objekty z průmyslových aplikací, jsou klasifikovány v ISO7816-6. Tagy pro SM (secure messaging) jsou v ISO7816-4. Data, která jsou interpretována operačním systémem karty, jsou ukládána jako TLV-objekty. Typicky APDU.

TPDU (Transmission Protocol Data Unit)

Přenosový protokol. Terminál (master) komunikuje s kartou (slave) tak, že APDU je konvertován do TPDU a zaslán smart kartě přes seriové (či jiné) rozhraní.

Při komunikaci přes kontaktní rozhraní je obvykle ve smart kartě implementován protokol T=0 (asynchronní, half duplex, bajtově orientovaný) nebo T=1 (asynchronní, half duplex, blokově orientovaný) protokol T=CL (asynchronní, half duplex, blokově orientovaný, ISO14443-3,4) je pro bezkontaktní rozhraní

WIM (WAP Identity Module)

SIM karta, specificky vyvinutá pro přístup na internet.

Wired logic card

Paměťová karta se zadržovanou bezpečnostní logikou (včetně autentizačního mechanismu)

13 LITERATURA

Smart Card Manufacturing: A Practical Guide

Yahya Haghiri, Thomas Tarantino

John Wiley & Sons,2002

Smart Cards: A Developer's Toolkit

Tim Jurgensen, Scott Guthery

<http://www.amazon.com/exec/obidos/ASIN/0130937304/smartcarddevelopA/>

Smart Card Developers Kit

Scott Guthery and Tim Jurgensen

<http://www.amazon.com/exec/obidos/ASIN/1578700272/smartcarddevelopA/>

Smart Card Handbook by Wolfgang Rankl and Wolfgang Effing, 3rd ed.

John Wiley & Sons,2003

<http://www.amazon.com/exec/obidos/ASIN/0471988758/smartcarddevelopA/>

Java Card Technology for Smart Cards

Z.Chen, Addison-Wesley Prof, 2000

Giesecke & Devrient : Starcos 2.5DI Reference Manual

Philips Semiconductors: MIFARE ProX P8RF5016 - Secure Dual Interface Smart Card IC, rev.1.4

Philips Semiconductors: MIFARE & I.CODE

Philips Semiconductors: MIFARE MF RC500 - Highly Integrated ISO 14443A Reader IC, rev. 2.0
