



Dodatek č. 1

ke smlouvě o poskytnutí služby č. objednatele INO/40/05/001121/2006,
č. zhotovitele 246/06 ze dne 25.10.2006
jímž se mění a doplňují čl. I., III., IV. smlouvy

Smlouva o poskytnutí služby uzavřená mezi

Hlavní město Praha

se sídlem: Mariánské nám. 2/2, 110 01 Praha 1
zastoupené: Ing. Ivanem Seyčkem, ředitelem odboru informatiky Magistrátu hl. m. Prahy
IČ: 00064581, DIČ: CZ00064581
Bank. spojení: [REDACTED]

(dále jen „objednatel“)

a

MONET+, a. s.

se sídlem: Za Dvorem 505, 763 14 Zlín - Štípa
zastoupená: Mgr. Jiřím Benešem, obchodním ředitelem, zmocněným zástupcem
IČ: 26217783, DIČ: CZ26217783
Bank. spojení: [REDACTED]

(dále jen „zhotovitel“)

se v souladu s ustanovením článku XIII. odst. 4 výše uvedené smlouvy, po dohodě smluvních stran, mění a doplňuje takto:

I.

V článku I. s názvem Popis předmětu smlouvy a cíl poskytnuté služby

se za odst. 4 písm. d) vkládá písm. e) následujícího znění:

„e) poskytnutí technické a funkční specifikace řešení včetně ověřovacích testů.“

II.

V článku III. s názvem Termíny plnění

se v odst. 1 za písm. d) vkládá písm. e) následujícího znění:

„e) provedení Ověření technické a funkční shody dodaného appletu, middleware a Technického řešení zápisu PKI appletu do čipové karty dle „Technické a funkční specifikace řešení včetně ověřovacích testů“ dle čl. I, odst. 4 písm. e) do 90-ti dnů od převzetí dle odst. 1, písm. a) a b) čl. III. smlouvy“

se v odst. 1 vypouští původní text písm. b) a nahrazuje se novým písm. b) následujícího znění:

„b) dodávka technického řešení zajištění uložení appletů na karty: 45-dní od uzavření smlouvy dle specifikace přílohy č. 1 dodatku č.1

se v odst. 1 vypouští původní text písm. c) a nahrazuje se novým písm. c) následujícího znění:

„c) poskytnutí podpory a údržby: po dobu čtyř kalendářních let od data ověření dle odst. 1. písm. e) čl. III této smlouvy nejpozději však do 90-ti dnů od převzetí díla. Podpora a údržba bude poskytnuta na základě uzavření Servisní smlouvy, která tvoří přílohu č. 1 a je nedílnou součástí této smlouvy“

III.

V článku IV. s názvem Povinnosti zhotovitele

se za odst. 3 vkládají odst. 4, 5, 6, 7, 8, 9, 10 a 11 následujícího znění:

- „4. Objednatel je oprávněn požadovat po zhotoviteli provedení Ověření technické a funkční shody dle písmena e) odst. 1 čl. III této smlouvy. Ověření lze provést až po uskutečnění dodávky dle čl. III., odst. 1, písmena a) a b) smlouvy. Tento požadavek musí být specifikován písemně.“
- „5. Zhotovitel je povinen ve lhůtě 10-dnů od doručení tohoto požadavku zahájit přípravu procesu ověření. Vlastní provádění ověření je zhotovitel povinen zahájit ve lhůtě do 15-dnů od doručení tohoto požadavku.“
- „6. Objednatel se zavazuje ve lhůtě do 10-dnů před zahájením provádění ověření poskytnout součinnost uvedenou v příloze č. 4 smlouvy a zajistit technické a organizační podmínky pro provedení ověřování, které jsou specifikovány v dokumentu „Technická a funkční specifikace řešení“ dle čl. I., odst. 4 písm. e).“
- „7. Provedení ověření je ukončeno akceptací objednatelem, která musí mít písemnou podobu.“
- „8. Pokud v rámci provádění ověření dojde ke zjištění neshody mezi dodávkou dle čl. III., odst. 1., písmene a) a b) smlouvy a dokumentem „Technická specifikace řešení“ dle čl. I. odst. 4. písm. e) je zhotovitel povinen uvést dodané řešení do stavu shodného s technickou specifikací, a to do 15-dnů od zjištění této skutečnosti, pokud se obě strany nedohodnou jinak.“
- „9. Pokud zhotovitel neučiní nápravu dle odst. 8. tohoto článku ve stanoveném termínu, má se za to, že porušil termíny plnění smlouvy, a objednatel může uplatnit sankce specifikované v čl. II., odst. 6. smlouvy.“
- „10. V případě, že neshoda specifikovaná v rámci odst. 8. čl. IV. brání provozu systému, jedná se o „Kritickou chybu“, a v takovém případě může objednatel při nesplnění lhůt k odstranění závady ze strany zhotovitele dle tohoto článku ani v prodloužené lhůtě 30-dnů, požadovat předčasné ukončení smlouvy.“
- „11. V případě předčasného ukončení smlouvy dle odst. 10. čl. IV si objednatel vyhrazuje právo požadovat částečné či úplné vrácení vzájemného plnění. Zhotovitel je povinen vyhovět takovému požadavku bezodkladně a ve vzájemně dohodnutém rozsahu.“

IV.

Ostatní ustanovení smlouvy o poskytnutí služby „Řešení PKI pro čipovou kartu“ č. objednatel INO/40/05/001121/2006, č. zhotovitele 246/06 ze dne 25.10.2006 zůstávají beze změny.

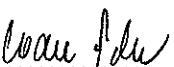

V.


1. Dodatek se vyhotovuje v pěti stejnopisech, z nichž dva obdrží zhotovitel a tři objednatel.
2. Dodatek nabývá účinnosti dnem podpisu oběma smluvními stranami.
3. Nedílnou součástí tohoto dodatku je příloha č. 1 – Technická specifikace „Řešení pro čipovou kartu“ včetně ověřovacích testů


12. pros. 2006

V Praze dne

V Praze dne


.....
za objednatele



.....
za zhotovitele

 **MONET+, a.s.** ②
Za Dvorem 505, 763 14 Zlín - Štípa
IČ: 26217783, DIČ: CZ26217783
tel.: +420 577 110 411, fax: +420 577 914 557

Příloha č. 1: Dodatek č. 1 ke Smlouvě o poskytnutí služby „Řešení PKI pro čipovou kartu“

Technická specifikace „Řešení PKI pro čipovou kartu“ včetně ověřovacích testů

Popis PKI appletu

Součástí dodávky je vlastní PKI applet *CryptoPlus XG*, který splňuje požadavky zadávací dokumentace. Podrobnosti o PKI appletu *CryptoPlus XG* jsou uvedeny v kapitole 0 tohoto dokumentu.

Popis middleware *CryptoPlus opencard*

Součástí dodávky je vlastní middleware *CryptoPlus opencard*, které spolu s appletem *CryptoPlus XG* tvoří nedílnou součást řešení pro PKI. Podrobný popis jednotlivých komponent middleware, způsobu instalace a customizace je uveden v kapitole 0.

Implementace technického řešení pro zápis appletu do čipu hybridní čipové karty

V tomto dokumentu je uveden technický popis řešení zápisu appletu, bezpečnostní koncept, časové náročnosti na zápis appletu při zvoleném řešení zápisu. Jsou také uvedeny požadavky na zajištění součinnosti ze strany MHMP. Podrobný způsob implementace technického řešení pro zápis appletu je uveden v kapitole 0.

Specifikace ověřovacích testů dodaných komponent

Akceptace funkčnosti jednotlivých komponent (i systému jako celku) proběhne po ověření požadovaných funkcí. V kapitole 0 je uvedena specifikace ověřovacích testů, která bude relevantním podkladem pro posouzení funkčnosti a pro následnou akceptaci dodávky.

Specifikace technického řešení PKI appletu

Dodavatel dodá PKI applet *CryptoPlus XG*.

Tento applet je originálním dílem Dodavatele. Lze jej implementovat na procesorovou čipovou kartu, jejíž parametry byly uvedeny v **Zadávací dokumentaci**.

Applet *CryptoPlus XG* je plně kompatibilní s middleware *CryptoPlus opencard* a tvoří tak nedělitelný celek PKI řešení na čipové kartě.

Applet *CryptoPlus XG* splňuje všechny požadavky PKI appletu, které jsou uvedeny v **Zadávací dokumentaci.**

CryptoPlus XG využívá asymetrickou kryptografii (RSA) na čipu karty. Umožňuje bezpečné uložení privátních RSA klíčů:

- všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty
- privátní RSA klíč uložený na kartě nelze z karty vyexportovat
- RSA klíče mohou být generovány v čipu anebo mohou být na kartu importovány.

Spolu s páry RSA klíčů jsou na kartě uloženy i příslušné certifikáty ve formátu X.509.

Kromě RSA klíčů (a příslušných certifikátů) mohou být na kartě uložena ještě statická data, např. jména a hesla pro identifikaci do non-PKI systémů.

Použití citlivých údajů, jako jsou např.:

- privátní RSA klíče
- statická data

je chráněno pomocí PIN.

Applet *CryptoPlus XG* podporuje (mimo jiné i):

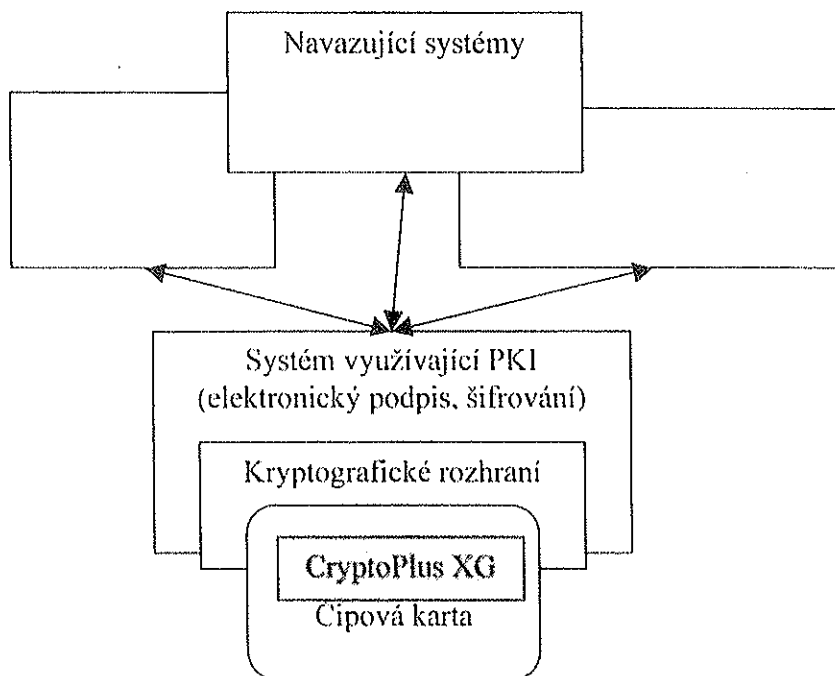
- **nahrávání kvalifikovaného certifikátu dle zákona č. 227/2000 Sb., zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) v platném znění a**
- **přístup ke kvalifikovanému certifikátu na osobních počítačích poskytnutím patřičného volně šiřitelného rozhraní.**

Applet *CryptoPlus XG* bude do čipových karet zapsán v rámci implementace technického řešení zápisu appletu do hybridních karet. Applet bude v zašifrované podobě uložen v *HSM serveru*, odkud bude řízeným procesem zapisován do kontaktních čipů.

1.1 Základní popis appletu *CryptoPlus XG*

CryptoPlus XG představuje PKI applet pro čipovou kartu s interním funkčním rozhraním, které je optimalizováno pro klientské PKI aplikace, založené na certifikátech X.509.

Následující obrázek ukazuje klientské PKI řešení, ve kterém je barevně zvýrazněna role produktu *CryptoPlus XG*:



Obrázek 1: PKI klientské řešení

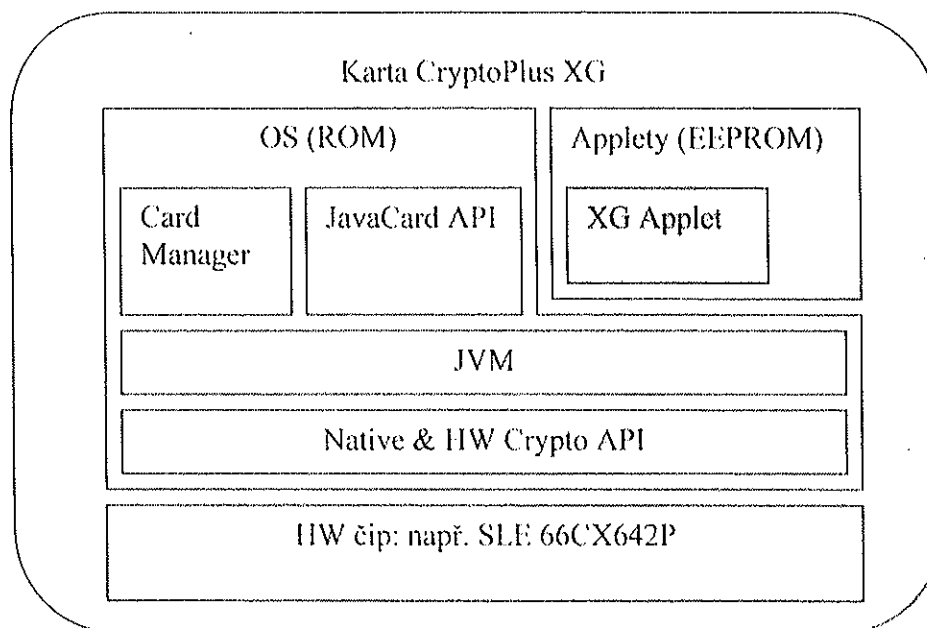
Jak je z obrázku patrné, applet *CryptoPlus XG* spolu s čipovou kartou zde slouží především jako zařízení podporující systém využívající PKI (tj. na principech asymetrické kryptografie s podporou certifikátů X.509) pro vytváření a ověřování elektronického podpisu a pro šifrování a dešifrování dat.

Dvojice čipová karta a applet *CryptoPlus XG* je zde v roli bezpečného zařízení pro vytváření elektronického podpisu (SSCD – *Secure Signature Creation Device*) a bezpečného dešifrování transportních šifrovacích klíčů.

Je zřejmé, že čipová karta nedokáže v PKI systému pracovat samostatně. Pro využití jejích funkcí je nutné realizovat příslušná kryptografická rozhraní, přičemž nejrozšířenější standardy jsou CSP (Cryptographic Service Provider – kryptografický modul pro systémy Microsoft Windows) a PKCS#11 (obecné, platformě nezávislé rozhraní pro kryptografická zařízení).

Tato rozhraní Dodavatel implementuje ve formě *CryptoPlus opencard* middleware.

Další obrázek ukazuje vnitřní architekturu čipové karty s appletem *CryptoPlus XG*:



Obrázek 2: Vnitřní architektura čipové karty

Z obrázku je patrné, že funkčnost celého produktu je postavena na platformě JavaCard, která zajišťuje především širokou flexibilitu, a to zejména z pohledu nezávislosti na konkrétní HW platformě (škálovatelný výkon i paměť, možnost výběru HW s potřebnými bezpečnostními certifikáty).

Funkčním jádrem *CryptoPlus XG* je tzv. XG Applet, který realizuje ISO 7816-4 kompatibilní souborový systém doplněný o funkce související s PKI. Díky tomuto řešení je možné budovat standardizované SW řešení využívající výhody čipových karet (mobilita, bezpečnost).

Z hlediska funkcionality *CryptoPlus XG* appletu mohou případně PKI aplikace využít:

- podporu souborového systému s možností nastavení rozličných přístupových podmínek (zajištění integrity nebo utajení mechanismy tzv. „secure messaging“ s využitím 3DES klíčů (různé typy klíčů vhodné pro různé účely), ochrana operací pomocí různých PIN (8 lokálních + 8 globálních PIN objektů)
- dvouúrovňová hierarchie adresářů
- podpora RSA algoritmů 1024, 1536, 2048bitu, vč. HW generování klíčů, vytváření elektronického podpisu, dešifrování dat a klíčů
- interní podpora výpočtu podpora haš algoritmů (SHA-1, MD5)
- podpora podpisových schémat zahrnující i externě počítané hodnoty haš algoritmy, které nejsou běžně přímo podporovány HW karty (např. rodina SHA-2)
- integrované bezpečnostní politiky importu RSA klíčů (pokud je povolen import privátního RSA klíče, pak jen šifrovaným kanálem)

Podmínkou vytvoření bezpečné aplikace jako celku je však správná inicializace (resp. mapování) souborového systému s odpovídajícím nastavením přístupových podmínek.

Mapování pro PKI aplikace je mapování *CryptoPlus* v souladu se schváleným personalizačním profilem, který odráží požadavky na

- bezpečnostní politiky a
- rozdělení dostupné paměti mezi podporované typy objektů (PKI, datové objekty, atributy, ..)

Přesné znění schváleného personalizačního profilu je uvedeno v kapitole 1.4.

Applet *CryptoPlus XG* umožňuje implementaci na různých HW platformách. Pro projekt PKI řešení pro čipovou kartu byla zvolena karta GemXpresso R3.2 E64PK. Na této karetní platformě byl proveden elementární vývoj řešení, včetně ověřovacích a implementačních testů. Tato karta zcela vyhovuje požadavkům, je plně funkční s optimálním využitím výkonu.

Applet *CryptoPlus XG* je však možno provozovat i na jiných HW platformách, které splňují následující specifikaci čipu:

- Vyhovění Java Card, Open Platform 2.0.1, ISO 7816
- Certifikace čipu dle CCEAL5 a / nebo FIPS140-1 level2
- Existence kryptografického koprocessoru pro podporu symetrické (DES, 3DES) i asymetrické (RSA) kryptografie
- Paměť o velikosti 64kB
- Soulad s normami ČSN EN ISO7816, část 1-4, podpora protokolů T=0 a/nebo T=1, ČSN EN ISO/IEC 10373
- Podpora klíčů RSA až do velikosti 2 048 bitů
- Podpora HW ochrany proto fyzickému a časovému útoku
- PseudoHW generátor náhodných čísel resp. true random number generátor
- Minimální množina algoritmů:
 - Symetrická kryptografie:
 - javacard.security.KeyBuilder.TYPE_DES_TRANSIENT_RESET
 - javacard.security.KeyBuilder.LENGTH_DES3_2KEY
 - javacard.security.Signature.ALG_DES_MAC8_NOPAD
 - javacardx.crypto.Cipher.ALG_DES_ECB_NOPAD
 - Asymetrická kryptografie:
 - javacard.security.KeyPair
 - javacard.security.KeyBuilder.TYPE_RSA_PUBLIC
 - javacard.security.KeyBuilder.TYPE_RSA_CRT_PRIVATE
 - javacard.security.KeyBuilder.LENGTH_RSA_512 (je-li vyžadován klíč RSA512)
 - javacard.security.KeyBuilder.LENGTH_RSA_1024 (je-li vyžadován klíč RSA1024)
 - javacard.security.KeyBuilder.LENGTH_RSA_1536 (je-li vyžadován klíč RSA1536)
 - javacard.security.KeyBuilder.LENGTH_RSA_2048 (je-li vyžadován klíč RSA2048)
 - javacardx.crypto.Cipher.ALG_RSA_NOPAD
 - Hashovací algoritmy:
 - javacard.security.MessageDigest.ALG_MD5
 - javacard.security.MessageDigest.ALG_SHA
 - Generátor čísel:

- javacard.security.RandomData.ALG_SECURE_RANDOM
- Podpora změny Histo-bytu ATR
 - visa.openplatform.OPSystem.setATRHistBytes
- Paměťové nároky:
 - Transient memory: min 600 B pro applet, doporučujeme 1kB
 - Podpora transient paměťových alokací
 - javacard.framework.JCSystem.CLEAR_ON_DESELECT
 - javacard.framework.JCSystem.CLEAR_ON_RESET
 - APDU buffer min. 260 B (celé APDU: 5 byte hlavička + 255 byte data)
 - Transaction buffer min. 300 B
 - Persistent memory: min 20 kB volné paměti pro applet a jeho data

1.2 Popis funkcí appletu

1.2.1 Základní vlastnosti

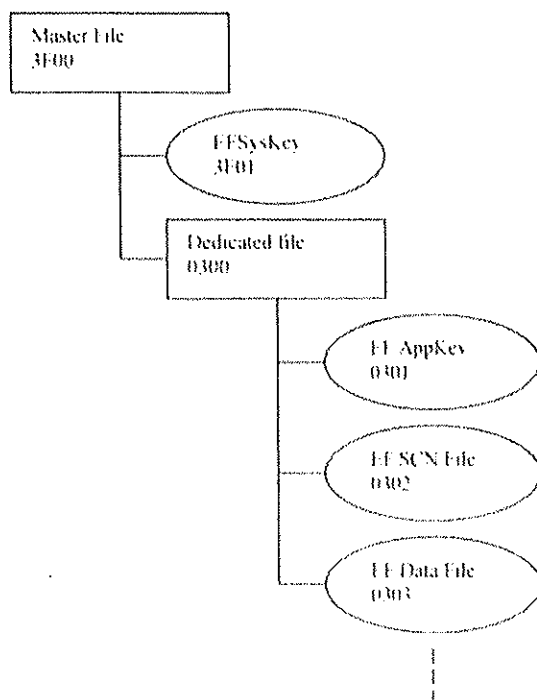
Následující tabulka sumarizuje základní vlastnosti appletu *CryptoPlus XG*:

Vlastnost	Popis
Applet, verze	<i>CryptoPlus XG</i> applet, v1.10
Kryptografické algoritmy	<ul style="list-style-type: none"> • RSA 1024, 1536, 2048 bitů <ul style="list-style-type: none"> ○ HW generování klíče ○ import klíče ○ elektronický podpis s výpočtem haš na kartě (MD5, SHA-1), padding na kartě (EMSA-PKCS1-v1_5, EMSA-PKCS1 bez DER kódování OID hašovací funkce) ○ elektronický podpis s výpočtem haš mimo kartu (MD5, SHA-1, SHA256, SHA384, SHA512, RIPEMD128, RIPEMD160), padding na kartě (EMSA-PKCS1-v1_5, EMSA-PKCS1 bez DER kódování OID hašovací funkce) ○ elektronický podpis s výpočtem haš mimo kartu (spojení hodnot haš SHA-1, MD5), padding na kartě (EMSA-PKCS1 bez DER kódování OID hašovací funkce) ○ dešifrování dat (symetrických klíčů) RSA klíčem s odstraněním paddingu RSAES-PKCS1-V1_5 ○ obecná operace s RSA klíčem (bez paddingu) – umožňuje realizaci vlastního paddingu v SW • výpočet haš SHA-1 a MD5 pro použití v operaci vytvoření elektronického podpisu • 3DES algoritmus (klíč 112 bitů) pro <ul style="list-style-type: none"> ○ šifrování PIN (ECB režim)

	<ul style="list-style-type: none"> ○ šifrování importovaného privátního klíče (ECB režim) ○ zajištění integrity přenášení APDU příkazů (CBC-MAC režim) • HW true random number generátor
Souborový systém	<ul style="list-style-type: none"> • ISO 7816-4 s podporou „secure messaging“ • 2-úrovňová hierarchie adresářů • podpora selekce přes AID (i částečný název) • podpora globálních i aplikačních PIN objektů (až 8 objektů na adresář) • různé typy 3DES klíčů • implementované bezpečnostní politiky pro uložení RSA klíčů (privátní klíče nelze exportovat, import, pokud je možný, pak pouze s použitím šifrovaného kanálu) • optimalizováno pro výkon (s ohledem na použití JavaCard) • podpora životního cyklu (personalizační fáze, uživatelská fáze – pozor, tyto fáze jsou nad rámec fází definovaných v OpenPlatform)

1.2.2 Organizace souborového systému

Souborový systém *CryptoPlus XG* appletu je dvouvrstvý – příklad hierarchie je naznačen na následujícím obrázku:



Obrázek 3: Souborový systém *CryptoPlus XG* appletu

Další podkapitoly stručně popisují typy souborů *CryptoPlus XG* appletu.

1.2.2.1 Master File (MF)

Základní adresář, který může obsahovat soubory (tzv. Elementary Files) a další adresáře (tzv. Dedicated Files).

1.2.2.2 Dedicated File (DF)

Typicky představuje adresář aplikace. Kromě číselné adresy může mít i textový nebo binární název do maximální délky 16B.

Obsahuje soubory realizující danou aplikaci.

DF již nemůže obsahovat další vnořené DF.

1.2.2.3 Elementary File (EF)

Datový soubor aplikace.

CryptoPlus XG applet rozlišuje několik typů souborů (viz. další podkapitoly), speciální místo má soubor EFSysKey (System Key File), který je (kromě MF) na kartě vždy přítomen a který obsahuje inicializační 3DES klíč, bez jehož znalosti nelze na kartě vytvářet nové soubory (DF ani EF).

Datové soubory se dělí podle různých kritérií.

Typy souborů dle struktury:

- transparentní soubory – lineární datové soubory bez definované struktury
- strukturované soubory
 - lineární s konstantní délkou záznamu – obsahují lineárně adresovatelné záznamy konstantní délky (tj. v rámci souboru mají jednotlivé záznamy stejnou délku, adresují se indexem od 1 do n)
 - lineární s proměnnou délkou záznamu – obsahují lineárně adresovatelné záznamy, každý záznam může mít jinou délku

Typy souborů dle významu (tj. XG Applet interpretuje jejich obsah, který má přesně definovanou strukturu):

- soubory 3DES klíčů (3DES Key Files) – obsahují 3DES klíče (max 4 klíče v jednom souboru). 3DES klíče mohou být různých typů (tzv. Administration Key a Log Key).
- soubory PIN objektů (Secret Code Files) – obsahují PIN objekty (max. 8 PINů/PUKů v jednom souboru)
- soubory RSA klíčů (Public Key Files) – obsahují RSA klíče (jeden klíč v každém souboru). RSA klíč je uložen ve dvou částech:
 - veřejná část u které lze nastavit přístupová práva na úrovni souborového systému;
 - privátní část u které jsou předdefinovaná přístupová práva (update pouze se šifrováním administračním klíčem, čtení je zakázáno)
- soubory čítače transakcí (Transaction Manager Files) – soubor drží číslo transakce realizované log klíčem, řeší obranu proti tzv. replay attack při ustavování klíče sezení s použitím „Log Key“

1.2.3 Přístupové podmínky

Přístupové podmínky jsou děleny do několika skupin:

- přístupové podmínky v rámci souborového systému – řídí přístup k jednotlivým souborům. Je možné kombinovat zabezpečení Secure Messaging a použití až dvou PIN objektů. Rozlišují se tyto skupiny operací, pro každou skupinu se nastavují vlastní práva:
 - skupina 0: operace vytváření senzitivních souborů (DF, 3DES klíče, soubory s PIN), operace přepsání dat v souboru (tzv. UPDATE)
 - skupina 1: operace vytváření datových souborů, operace přidání záznamu do strukturovaného souboru, operace 'OR' zápisu do souboru (tzv. WRITE)
 - skupina 2: operace čtení dat ze souboru
- přístupové podmínky pro použití privátního klíče – nastavují podmínku použití konkrétního privátního klíče (možno nastavit použití definovaného PIN – globální/lokální + číslo PIN objektu)

1.2.4 Skupiny příkazů *CryptoPlus XG* appletu

Příkazy ISO 7816-4 je možné rozdělit do několika kategorií, tak jak je uvedeno v následujících podkapitolách.

1.2.4.1 Administrativní příkazy

Příkaz	Stručný popis
Append Record	Přidá záznam do strukturovaného souboru
Create File	Vytvoří nový soubor nebo adresář
Erase Card	Inicializuje souborový systém, veškerá paměť je nulována
Freeze Access Conditions	Modifikuje přístupové podmínky na soubor
Get Challenge	Generuje náhodná čísla
Get Info	Vrací různé informace o kartě nebo o souborech
Get Response	Vrací data připravena v rámci předchozího příkazu
Read Binary	Čte data z transparentního datového souboru
Read Record	Čte záznam ze strukturovaného souboru
Select File	Změní adresář nebo otevře soubor
Select Admin Key	Ustaví administrativní klíč sezení
Set Card Status	Mění fázi životního cyklu karty
Set Secret Code	Mění nebo odblokuje PIN
Update Binary	Modifikuje obsah transparentního datového souboru
Update Record	Mění záznam strukturovaného souboru
Verify	Autentizace ke kartě
Write Binary	Provede „WRITE“ zápis do transparentního datového souboru

1.2.4.2 Příkazy pro transakce

Příkaz	Stručný popis
Select Trans Key	Ustaví transakční klíč sezení (s použitím tzv. „Log Key“)

1.2.4.3 Příkazy pro PKI

Příkaz	Stručný popis
Create Private Key File	Vytvoří chráněný prostor pro privátní RSA klíč
Generate Key Pair	Provede HW generování RSA klíče
InitHashedData	Nastaví hodnotu haš, která se má podepsat
Load Private Key	Importuje privátní RSA klíč
PSO_Decipher	Pomocí privátního RSA klíče dešifruje blok dat (s volitelným odstraněním PKCS#1 paddingu)
PSO_ComputeDigitalSignature	Vytvoří elektronický podpis
PSO_HashData	Provádí výpočet haš z dat (data mohou být posílána po blocích)
PSO_InitOperation	Inicializuje operaci s RSA klíčem

1.2.5 CryptoPlus XG – parametry a vlastnosti kryptografických funkcí

1.2.5.1 Šifrovací algoritmy

Algoritmus	Délka klíče	Režim	Poznámka
RSA	1024, 1536, 2048	RSAS-EMSA1-V1_5-Decrypt	Rozšifrování symetrického klíče s paddingem PKCS#1 v1.5, typ 2
RSA	1024, 1536, 2048	RAW Encrypt (PKCS#1 RSADP)	Základní operace s privátním klíčem bez kontroly formátu vstupních a výstupních dat – použitelná pro vytváření vlastního paddingu pomocí SW.
3DES	112	ECB	Zajištění utajení dat při komunikaci mezi obslužným SW a kartou. Šifrovaná data jsou: <ul style="list-style-type: none"> • privátní RSA klíč při importu • hodnota PIN při požadavku na šifrovaný přenos
3DES	112	CBC-MAC	Zajištění integrity přenosu APDU příkazů.

1.2.5.2 Podpisová schémata

Asymetrický algoritmus	Délka klíče	Padding	Hašovací funkce
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA-1, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA-1, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID	SHA-1, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID	SHA-1, výpočet hodnoty haš proveden v SW

		hašovací funkce	
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	MD5, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	MD5, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	MD5, výpočet hodnoty haš proveden na čipu
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	MD5, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	RIPEMD160, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	RIPEMD160, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	RIPEMD128, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	RIPEMD128, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA256, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA256, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1-v1_5	SHA384, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	SHA384, výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	EMSA-PKCS1 bez DER kódování OID hašovací funkce	spojení SHA1a MD5 (tzv. SSL), výpočet hodnoty haš proveden v SW
RSA	1024, 1536, 2048	vytvoření paddingu v SW	výpočet hodnoty haš proveden v SW

1.2.5.3 Algoritmy generování asymetrických klíčů

Asymetrický algoritmus	Délka klíče	Metoda generování náhodných čísel
RSA	1024, 1536, 2048	True random

1.2.5.4 Metody generování náhodných čísel

Poznámka: Náhodný generátor je mj. používán jako zdroj dat pro generování klíčů (RSA, 3DES, atp.)

Název	Poznámka pro GemXpresso E64 PK
True random	<ul style="list-style-type: none">Firmware čipu provádí kontrolu kvality náhodných číselvýrobce čipu deklaruje, že dodávaná náhodná čísla jsou kryptograficky kvalitní v celém rozsahu provozních podmínek čipu

1.2.5.5 Hašovací funkce

Jméno haš funkce	Výstupní délka (bitů)
SHA-1	160
MD5	128

1.2.6 Podporované standardy, normy a protokoly

- PKCS#1
- PKCS#7 (s využitím SW)
- PKCS#10 (s využitím SW)
- PKCS#11 (SW rozhraní)
- PKCS#12 (s využitím SW)
- SSL, TLS, S/MIME, EAP (s využitím SW)
- X.509v1 – v3
- CSP (Cryptographic Service Provider, SW rozhraní)
- ISO 7816-1,2,3,4
- protokol T=0
- SHA-1, MD5, RIPEMD128, RIPEMD160, SHA256, SHA384, SHA512
- 3DES, RSA
- JavaCard 2.1.1
- OpenPlatform 2.0.1' level 2

1.3 Způsob zajištění bezpečnosti

Bezpečnost PKI appletu a z něj odvozeného řešení je postavena na těchto základních stavebních kamenech

1. bezpečná platforma karty
2. bezpečnostní funkce implementované appletem
3. správné využití bezpečnostních funkcí a vlastností appletu v PKI profilu

4. odpovídající implementace middleware
5. odpovídající využití middleware aplikacemi
6. správné zacházení s kartou

1.3.1 Bezpečná platforma karty

Bezpečnostní požadavky na platformu karty byly specifikovány výběrovým řízením. Karty splňující tyto požadavky lze považovat za kvalitní základ budování dostatečně bezpečného PKI řešení.

1.3.2 Bezpečnostní funkce implementované appletem

Applet implementuje tyto základní bezpečnostní funkce

- kvalitní souborový systém ISO7816-4 kompatibilní s možností definice široké škály přístupových podmínek
 - 3 skupiny oprávnění
 - definice PIN objektů
 - definice 3DES klíčů
- využití transakčních mechanismů při vykonávání bezpečnostních operací
- využívání tzv. principu „Secure Messaging“ pro kryptografické zabezpečení zpráv vyměňovaných mezi kartou a middleware s možností
 - šifrování specifických částí
 - podepisování (MAC) specifických částí
- podpora aplikací vynuceného zabezpečení pomocí Secure Messaging (tj. karta akceptuje zabezpečení vybraných zpráv i když to není explicitně požadováno v nastavení konkrétního oprávnění)
- vynucení bezpečnostních politik ochrany RSA klíčů appletem
 - šifrovaný zápis privátních klíčů
 - zakázání exportu privátního klíče
- nadstandardní implementace PKI funkcí
 - automatická detekce podpisových schémat
 - automatické doplnění padding široké množiny podpisových schémat

1.3.3 Správné využití bezpečnostních funkcí a vlastností appletu v PKI profilu

Schválený PKI profil *CryptoPlus opencard* plně využívá bezpečnostních funkcí appletu *CryptoPlus XG*.

Přiřazení přístupových podmínek vychází ze zásady povolení výhradně takových oprávnění, která jsou minimální pro dosažení požadované funkčnosti (tj. operace, které jsou nad rámec implementace PKI aplikací s použitím middleware jsou zakázány).

Profil *CryptoPlus opencard* umožňuje uložení jedné skupiny PKI (či obecných datových) objektů do různých souborů. Díky tomuto principu je možné na kartu nahrávat objekty (klíče, certifikáty, ..), které jsou ve správě konkrétních subjektů, popř. jsou na kartu nahrány tak, že není možné za žádných okolností modifikovat.

1.3.4 Odpovídající implementace middleware

Dodávaný middleware vybudovaný na platformě *CryptoPlus* přebírá mnohá bezpečnostní nastavení přímo z karty, tj. je svým způsobem univerzální a pracuje v takovém režimu, v jakém je vyrobena karta.

Platforma *CryptoPlus* však může definovat dodatečné bezpečnostní politiky, které mohou být – vzhledem k omezeným prostředkům čipové karty – na čipu jen těžko implementovatelné (např. ověřování řetězce importovaného certifikátu, atp.)
Popis funkcí middleware je předmětem kapitoly č. 0.

1.3.5 Odpovídající využití middleware aplikacemi

Celková bezpečnost PKI řešení je do jisté míry ovlivněna i aplikacemi, které využívají middleware. Middleware platformy *CryptoPlus* dokáže – nezávisle na aplikacích – vynutit některé politiky (zadávaní PIN, import klíčů, certifikátů, atp.). Nicméně, kompletní ovlivnění správného zacházení s kartou ze strany aplikace není na úrovni middleware možné, proto by i vlastní aplikace měly pamatovat na základní pravidla bezpečnosti.

1.3.6 Správné zacházení s kartou

Správné zacházení s kartou je jeden z nejdůležitějších momentů budování bezpečného systému s čipovými kartami.

Čipová karta je zařízení, které se dokáže bránit sofistikovaným technickým i technologickým útokům, neubrání se však rizikovým zacházením ze strany majitele karty.

Proto je nutné spolu s rolloutem karet investovat do osvětové kampaně, která uživateli vysvětlí nejzásadnější bezpečnostní rizika způsobena nesprávným používáním karty.

Držitel karty musí kartu vnímat jako silně personální záležitost – PKI karta je pro držitele bránou do dimenze elektronického světa. privátní objekty na kartě jsou pak zhmotněním jeho identity ve virtuálním světě.

1.4 Personalizační profil PKI appletu

V této kapitole je uveden personalizační profil PKI appletu, který byl schválen ze strany MHMP.

Personalizační profil definuje vlastnosti (počet, velikost, ochrana, ...) objektů PKI karty.

Na 64kB kartě s tímto personalizačním profilem zůstane ještě asi 20kB volného místa pro další applety.

Typ: JavaCard 64k

Mapování: CryptoPlus2, v5

Bezpečnostní politiky:

Root certifikát: ANO

Personalizovaný root certifikát: ANO, device CA

Kontrola platnosti klientského certifikátu: NE

Modifikace device klíče a certifikátu: Zakázána

Vytváření objektů a mazání uživatelských objektů: PIN

Použití privátního klíče: PIN

Čtení veřejných informací: FREE

Zajištění integrity-modifikace: 3DES Usr (uložen v SW)

Import privátního klíče: ANO

Expirace karty: ANO, generuje SKC

PIN: konstantní „1111“, max. 3 neúspěšné pokusy

PUK: konstantní „44444444“, max. 5 neúspěšných pokusů

Alokovaný prostor:

RSA klíče 1024 bitů: 2

RSA device klíč 1536 bitů: 1
RSA klíče 2048 bitů: 2
Certifikáty CA: 2 certifikáty 4KB
Device certifikát: 1 certifikát / 1KB
Klientské certifikáty: 4 certifikáty / 8KB
Počet tajemství PKCS#11: 4
Chráněné hodnoty tajemství PKCS#11: 3KB
Dodatečné atributy PKCS#11: 1KB
AID: A0 00 00 00 28 80 10 24 00
Logické číslo: 16 číslic, generuje SKC

Typ – typ HW čipové karty, je navržena karta s 64KB EEPROM a operačním systémem JavaCard, HW generátor RSA

Mapování – definuje typ a verzi použitého mapování paměti souborového systému PKI appletu. Navrhovaná verze 5 nabízí nejvíce možností (rozšířená podpora ukládání PKCS#11 atributů objektů).

Bezpečnostní politiky – politiky, které budou aplikovány v rámci prvotní inicializace profilu *CryptoPlus opencard*

- Na kartě bude vyhrazen prostor pro kořenové certifikáty
- V procesu zápisu PKI appletu bude do karty zapsán kořenový certifikát tzv. *device certifikační autority*, která vydává certifikáty pro karty.
- Nebude omezení na import klientských certifikátů dle certifikátů CA, které jsou na kartě uloženy.
- Certifikát karty, tzv. *device certifikát*, nebude možno z karty smazat ani jej modifikovat.
- Operace vytváření, mazání a modifikace dalších objektů budou chráněny PIN
- Operace s privátním klíčem budou chráněny PIN
- Veřejné informace (veřejné klíče, certifikáty, veřejné datové objekty) je možné číst bez nutnosti zadání PIN
- Zápis údajů na kartu bude dodatečně chráněn **3DES** Ussr klíčem (je zakódován do klientských knihoven CSP, PKCS#11)
- Na kartě bude povolen import privátních klíčů (např. z PKCS#12 souborů, při archivaci klíčů v rámci MS CA 2003. ...), export není možný
- Karta bude mít nastavenou expiraci na 4 roky, po konci platnosti karty na ni nebude možné nahrát nový certifikát, všechny ostatní funkce zůstanou zachovány
- PIN bude konstantní s hodnotou „1111“, maximální počet následujících neúspěšných pokusů bude nastaven na 3.
- PUK bude konstantní s hodnotou „44444444“, maximální počet následujících neúspěšných pokusů bude nastaven na 5.
- **Alokovaný prostor** – popisuje rozložení paměti:
 - na kartě bude alokovan prostor pro 5 párů (soukromý + veřejný) RSA klíčů (2x 1024 bitů, 1x 1536 bitů, 2x 2048 bitů),
 - na kartě bude prostor pro uložení dvou certifikátů CA: komprimovaná délka obou certifikátů nesmí překročit 5KB
 - na kartě bude prostor pro uložení 1 certifikátu karty (*device*), komprimovaná délka nepřekročí 1KB.

- na kartě bude prostor pro uložení 4 uživatelských certifikátů; komprimovaná délka všech certifikátů nesmí přesáhnout 8KB
- na kartě bude prostor pro vytvoření čtyř obecných datových (ne PKI) objektů
- chráněné hodnoty tajemství (hodnotu je možné přečíst až po zadání PIN) mohou mít max. délku 3KB
- dodatečné atributy objektů PKCS#11 (např. ID klíčů a certifikátů, atd.), mohou mít max. délku 1KB

AID – je interní identifikátor aplikace. Jeho hodnota je přidělena Dodavatelem tak, aby byly karty akceptovány v rámci dodávaných komponent middleware.

Logické číslo – definuje aplikační číslo kontaktní karty. Hodnoty *logického čísla karet* jsou ve formátu 16 číslic. Číslo generuje SKC, systém pro zápis PKI appletů tato čísla akceptuje a zapisuje je do kontaktních čipů. SKC garantuje unikátnost logických čísel karet (nebudou existovat 2 karty se stejným logickým číslem).

1.5 Licenční politika

Licence *CryptoPlus XG* appletu je spolu s licencí middleware *CryptoPlus opencard* vztažena k použitým čipovým kartám. Podrobnosti o licencování appletu *Cryptoplus XG* jsou uvedeny ve společné kapitole 1.12 této specifikace.

Specifikace technického řešení middleware

Dodavatel pro MHMP dodává vlastní řešení middleware *CryptoPlus opencard*.

Dodávaný middleware splňuje všechny požadavky, které jsou uvedeny v Zadávací dokumentaci. (V některých vlastnostech *CryptoPlus opencard* požadavky převyšuje.)

Dodavatel - jako výrobce (vykonavatele majetkových práv) software *CryptoPlus* middleware - opravňuje MHMP prostřednictvím licenční smlouvy k používání

- middleware *CryptoPlus opencard* a
- obslužného software

na libovolném počtu uživatelských stanic s možností volné instalace (bez omezení licenčním číslem apod.), a to v počtu 50 tisíc uživatelů (počet vydaných karet).

1.6 Platforma *CryptoPlus*

CryptoPlus opencard je klonem otevřené platformy *CryptoPlus*.

CryptoPlus je originálním produktem Dodavatele. První verze *CryptoPlus* byla uvedena na trh v roce 2000. Od té doby je software *CryptoPlus* neustále zdokonalován, aby akceptoval nové trendy v oblasti IT bezpečnosti a aby byl stále o několik kroků před konkurencí.

Platforma *CryptoPlus* je určena pro zabezpečení PKI systémů a je praxí ověřená v mnoha implementacích.

1.7 *CryptoPlus opencard* middleware

CryptoPlus opencard middleware je soubor knihoven, které zprostředkují operačnímu systému funkce PKI čipových karet. Zároveň poskytují rozhraní pro použití *CryptoPlus opencard* dalším aplikacím. Aplikace a systémy pak mohou využívat *CryptoPlus opencard* např. pro:

- autentizaci
- zabezpečení dat (elektronický podpis, šifrování)
- bezpečné uložení citlivých aplikačních dat
- atd ...

Pro použití PKI dat implementuje *CryptoPlus opencard* dvě standardizovaná rozhraní:

- **Cryptographic service provider (CSP)** pro použití přes CryptoAPI Microsoft, buď přímo anebo prostřednictvím high-level komponent, jako je např. CAPICOM. CSP je standardně digitálně podepisováno společností Microsoft.
- **PKCS#11** pro non-Microsoft aplikace

Důležitou vlastností *CryptoPlus opencard* middleware je jeho nativní integrace do operačního systému. Kryptografické knihovny v operačním systému nepůsobí jako cizorodé těleso, naopak, standardizovaným způsobem rozšiřují kryptografický subsystém o schopnost používat karty *CryptoPlus opencard*. Funkce *CryptoPlus opencard* tak mohou používat i

aplikace, které původně nebyly navrženy pro spolupráci s čipovými kartami. Jestliže tyto aplikace používají jedno z uvedených standardních programových rozhraní, je vysoká pravděpodobnost jejich interoperability s *CryptoPlus opencard*.

Některé aplikace vyžadují registraci elektronických identit, před jejich použitím. Pro **automatickou registraci certifikátů** do MS Windows implementuje *CryptoPlus opencard* vlastní Certificate Store Provider. Ten po vložení karty uživateli automaticky zaregistruje všechny certifikáty, uložené na kartě. Po vyjmutí karty jsou certifikáty automaticky odregistrovány. Tímto způsobem se maximálně podporuje mobilita uživatele – *CryptoPlus opencard* zpřístupní elektronické identity uživatele na libovolném počítači, kde je nainstalováno *CryptoPlus opencard*.

Použití statických dat pro řešení Single Sign-On je implementováno proprietárními algoritmy aplikace *PassPro Tools*. Podrobnosti o *PassPro Tools* viz kapitolu 1.9.1.

CryptoPlus opencard middleware umožňuje pracovat současně s několika čtečkami připojenými k počítači.

Použití *CryptoPlus opencard* middleware je vázáno na čipové karty, v nichž je implementován PKI applet *CryptoPlus XG* a struktura *CryptoPlus opencard*.

CryptoPlus opencard je kompletně lokalizován do:

- češtiny
- angličtiny
- slovenštiny
- němčiny

Uživatel si může použítý jazyk zvolit pomocí grafického uživatelského rozhraní.

1.8 Řešení na bázi standardů

CryptoPlus opencard je budováno na základě standardních formátů a rozhraní. Díky použitým standardům lze:

- Garantovat vysokou míru interoperability s jinými subsystemy a aplikacemi, které akceptují standardy.
- Garantovat možnost případného upgrade a/nebo budoucího rozšíření systému.

Pro uložení dat se využívá standardních formátů:

- X.509 pro formát certifikátů
- PKCS#12 pro uložení páru klíčů a certifikátu. Tento formát je využíván při importu RSA klíčů na kartu *CryptoPlus opencard*

Pro šifrování, integritu apod. jsou užívány standardní algoritmy:

- Asymetrická šifra RSA
- Symetrické šifrování: 3DES, DES, RC2, RC4, RC5
- Hashovací funkce: SHA-1, RIPEMD160, MD5

Pro integraci karet *CryptoPlus opencard* do operačních systémů, resp. aplikací jsou dodána standardní rozhraní:

- Cryptographic Service Provider (CSP) pro použití v OS Windows a aplikacích kompatibilních se standardy Microsoftu
- Certificate Store Provider pro automatickou registraci certifikátů z karty do OS MS Windows
- PKCS#11 pro použití v „non-Microsoft“ aplikacích

Pro komunikaci operačního systému se čtečkou karet se využívá standardních rozhraní:

- PC/SC pro integraci čtečky do OS MS Windows
- PC/SC Lite pro integraci čtečky do OS Linux. (Instalace ovladačů čtečky do Linuxu je závislá na verzi použité distribuce Linuxu, resp. na verzi jádra.)

1.9 Komponenty *CryptoPlus opencard middleware*

CryptoPlus opencard middleware je souborem následujících komponent:

- Knihovny pro operační systém
 - Cryptographic Service Provider (CSP) - implementace kryptografického rozhraní pro operační systém MS Windows a CryptoAPI.
 - Knihovna PKCS#11 – implementace standardního kryptografického rozhraní hardwarového tokenu pro aplikační využití.
 - Certificate Store Provider – podpora pro automatickou registraci certifikátů z karty do operačního systému MS Windows.
 - Podpůrné knihovny, používané ostatními komponentami.
- *PassPro Tools* – software pro automatizované přihlašování do aplikací pomocí údajů z karty. Viz kapitulu 1.9.1.
- *Správce karty* – grafická aplikace pro správu dat na kartě. Podrobnosti viz v kapitole 1.9.2.
- Instalační software pro grafickou anebo bezobslužnou instalaci. Viz kapitolu 1.11.

1.9.1 *PassPro Tools*

PassPro Tools je jednoduchý **Single Sign-On** subsystém pro autentizaci uživatele do non-PKI aplikací. Je navržen pro starší typy aplikací, do nichž se uživatel autentizuje jménem a heslem.

Je typické, že uživatel má pro každý non-PKI systém jiné jméno a heslo. Někteří uživatelé mají tolik autentizačních údajů, že si je nemohou zapamatovat a raději si tyto údaje zaznamenávají na snadno dostupná místa. Takové praktiky znamenají velké bezpečnostní riziko.

PassPro Tools umožní uživateli zaznamenat si jména a hesla do bezpečného úložiště – na čipovou kartu, kde musí být vytvořeny kontejnery pro uložení statických dat. Použití autentizačních údajů je chráněno pomocí PIN (stejný PIN jako pro PKI objekty).

Kromě bezpečného uložení umí *PassPro Tools* autentizační údaje automaticky použít:

- detekuje zobrazení formuláře pro přihlášení uživatele
- nalezne na kartě autentizační údaje pro daný formulář
- automaticky vyplní údaje do formuláře
- automaticky stiskne tlačítko spouštějící proces přihlášení uživatele

Tento postup zajistí automatické přihlášení uživatele do:

- standardních aplikací (EXE)
- webových formulářů (pouze v prohlížeči MS Internet Explorer)

1.9.2 Správce karty

Správce karty je klientská grafická utilita pro práci s daty na kartě *CryptoPlus opencard*. Pomocí *Správce karty* lze:

- zobrazit data uložená na kartě
- mazat data z karty
- importovat data na kartu
- exportovat (některá) data z karty do souboru
- měnit PIN, PUK karty
- odblokovat kartu
- atd...

Program také umožňuje vygenerovat diagnostiku *CryptoPlus opencard*, která může být při potížích cenným zdrojem informací pro pracovníky podpory *CryptoPlus opencard*.

Použití webového rozhraní zjednodušuje ovládání programu pro méně zkušené uživatele.

1.10 Kompatibilita *CryptoPlus opencard* s aplikacemi třetích stran

Jedním z hlavních úkolů *CryptoPlus opencard* middleware je: zpřístupnit PKI data karty *CryptoPlus opencard* aplikacím.

Díky standardizovaným rozhraním lze *CryptoPlus opencard* middleware použít v mnoha aplikacích třetích stran.

V následujícím přehledu jsou uvedeny vybrané aplikace, které byly úspěšně testovány na kompatibilitu a interoperabilitu s *CryptoPlus opencard* middleware. Mnohé z uvedených aplikací jsou v současné době prakticky provozovány v různých organizacích.

- **Klientská autentizace webovým prohlížečem na HTTPS spojení**
 - MS Internet Explorer (od verze 5)
 - Netscape (od verze 4.7)
 - Mozilla (od verze 0.9, vč. Firefox)
- **Autentizace do domény MS Windows (2000 i 2003)**
 - Smart Card Logon
 - pomocí *Run as*
 - Terminálové služby (*Terminal Services*) – MS Windows Server i Citrix Metaframe
 - přes Wi-Fi
 - přes RAS
 - přes VPN
- **Elektronický podpis a šifrování e-mailů**
 - MS Outlook
 - MS Outlook Express
 - Mozilla (vč. Thunderbird)
 - Netscape
 - Novell GroupWise
- **Elektronický podpis webových formulářů**

- MS Internet Explorer (od verze 5, s použitím CAPICOM)
- Netscape (od verze 4.7)
- Mozilla (od verze 0.9)
- **Certifikační autority**
 - MS Windows Server 2000 i 2003
 - Entrust
 - Baltimore (UniCERT) WebRAO
 - Novell Certificate Server 2
 - První certifikační autorita (I.CA)
 - CA České pošty (PostSignum)
 - AEC (Trustport)
 - CA EVPÚ (pozn.: první akreditovaná CA na Slovensku)
 - ...
- **Bezpečné uložení klíče, podpora šifrování**
 - AreaGuard (SODATSW)
 - Protect (ICZ)
 - PGP (od verze 8)
 - SafeEnterprise ProtectFile
 - Entrust Desktop Solutions
- **Elektronický podpis maker a dokumentů**
 - MS Office (od verze 2000)

Počet kompatibilních aplikací se neustále rozšiřuje. Díky standardním rozhraním lze *CryptoPlus opencard* middleware používat i v aplikacích, které nejsou v seznamu uvedeny.

1.11 Instalace *CryptoPlus opencard*

Před použitím je nutno *CryptoPlus opencard* middleware instalovat na uživatelský počítač. Součástí dodávky je proto také instalační program.

CryptoPlus opencard middleware lze instalovat několika způsoby:

- Běžným instalačním programem
 - pro MS Windows (setup.exe)
 - pro Linux (balíček RPM)
- Bezobslužnou instalací, např.
 - pomocí SMS serveru (MS *Systems Management Server*),
 - pomocí skupinových politik (*Group Policy*) domény MS Windows (instalace *.MSI)
 - pomocí ZENworks systému Novell

Pozn.: Vytvoření transformačního souboru (*.MST) pro bezobslužnou instalaci pomocí skupinových politik, ani vytvoření konkrétního balíčku pro ZENworks není součástí dodávky. Je možno/nutno řešit separátně pro konkrétní systém a požadovanou konfiguraci produktu.

Uživatelská instalace je velmi jednoduchá, grafický průvodce provede uživatele celou instalací. Díky sofistikovanému řešení autodetekce možných problémů instalaci zvládne i méně zkušený uživatel.

Obdobný instalační nástroj software *CryptoPlus* používají tisíce klientů internetového bankovníctví několika českých bank. Drtivá většina z nich dokázala samostatně a bez potíží produkt instalovat.

Součástí instalace není zadávání žádného licenčního čísla. Po instalaci není vyžadován žádný způsob registrace produktu.

1.12 Licenční politika

Licence *CryptoPlus opencard* middleware a appletu *CryptoPlus XG* (jako nedílné součásti) jsou vztaženy k použité čipové kartě. Počet licencí odpovídá počtu použitých čipových karet v systému.

Licence *CryptoPlus opencard* middleware a appletu *CryptoPlus XG* opravňují uživatele nevýhradním a časově neomezeným způsobem applet *CryptoPlus XG* a middleware *CryptoPlus opencard* instalovat a dále ho v systému používat. Applet *CryptoPlus XG* a middleware *CryptoPlus opencard* nemá omezení licenčními čísly ani registrací.

Instalace a používání *CryptoPlus opencard* middleware a appletu *CryptoPlus XG* musí být v souladu s dodanou instalační a uživatelskou dokumentací.

1.13 Customizace *CryptoPlus opencard* middleware

Součástí dodávky je také customizace (přizpůsobení) *CryptoPlus opencard* middleware konkrétní implementaci. Prostřednictvím customizace je možné ovlivnit fungění a bezpečnostní vlastnosti použitého software, customizací se software jednoznačně identifikuje s grafickými prvky projektu.

Customizace *CryptoPlus opencard* middleware, uvedená v následujících podkapitolách, byla schválena ze strany MHMP.

Customizace se vztahuje na:

- kryptografické knihovny
- aplikaci „*Správce karty*“

1.13.1 Customizace kryptografických knihoven

Kryptografické knihovny jsou programové moduly, které rozšiřují operační systém resp. aplikaci o funkce podporované čipovou kartou.

V současné době jsou dodávány dva typy kryptografických knihoven:

- CSP pro Microsoft Windows
- Modul PKCS#11 (Cryptoki) používaný zejména produkty, které nejsou platformně vázané pouze na Windows (např. Netscape, Lotus Notes 6, Baltimore, Entrust. ...)

1.13.1.1 Bezpečnostní politiky

Kryptografické knihovny jsou implementovány v souladu s bezpečnostními politikami na kartě, nicméně je možné specifikovat dodatečné bezpečnostní politiky aplikované SW knihovnami:

- Délka PIN, který je SW knihovnami akceptován. Povolený rozsah je 4 až 8 číslic.
- Vynucení zadání PIN při každé operaci elektronického podpisu s hash algoritmy MD2, MD5, SHA-1 a RIPEMD160 (tj. mimo SSL autentizaci).
- Podpora šifrovaného ověření PIN (není možné v případě, že se používají některé PINPad čtečky)
- Povolení importu pouze těch klientských certifikátů, které vydaly důvěryhodné certifikační authority. Důvěryhodné CA z pohledu čipové karty jsou ty, které mají na kartě bezpečně uložen svůj certifikát (vázáno na bezp. politiku karty uložení certifikátů CA). Pro karty *opencard* nebude tato politika aplikována, na kartu bude možno ukládat certifikáty libovolné certifikační authority.
- Povolení kontroly časové platnosti karty. SW knihovna nedovolí import certifikátu, jenž začíná platit později, než skončila doba platnosti karty (vázáno na bezp. politiku uložení časové platnosti karty). Interval platnosti karty definuje SKC, do kontaktního čipu bude doba platnosti zavedena v procesu zápisu PKI appletu.

1.13.1.2 Název knihovny

Oba zmíněné moduly jsou v rámci systému identifikovány názvem (nejedná se o název souboru). Tento název se příliš často neobjevuje před zraky klienta, nicméně jsou okamžiky, kdy je nutné, aby klient věděl, kdy vybrat správný kryptografický modul (např. při generování žádosti o certifikát se program může zeptat, který modul má použít).

Pro karty *opencard* jsou definovány tyto názvy:

CSP pro systémy Microsoft Windows:

opencard CryptoPlus CSP v1.0

PKCS#11 pro Netscape

opencard CryptoPlus

1.13.2 Jméno karty

Pokud požadovaný typ karty není k dispozici, systém vyzve klienta, aby vložil kartu s určitým názvem.

Karty v operačním systému ponese název: *opencard CryptoPlus*

1.13.3 Uživatelské rozhraní

Kryptografické knihovny komunikují s uživatelem vždy, když potřebují použít čipovou kartu. Před dotazem na PIN je zobrazeno dialogové okno.

Vzhledem k tomu, že toto okno se zobrazuje minimálně při prvním použití karty (modul CSP) nebo při každé operaci výpočtu digitálního podpisu (pokud je nastaveno v bezpečnostních politikách), je bude zde umístěno logo produktu/služby která využívá customizovanou verzi *CryptoPlus opencard*.

PKCS#11 disponuje funkcí pro zadání PIN, implementace *CryptoPlus opencard* však dovoluje tzv. automatické přihlášení k PKCS#11 – PIN dialog se automaticky zobrazí pokud

požadovaná operace vyžaduje PIN. Automatické přihlášení k PKCS#11 je možné úplně zakázat.

1.13.4 Customizace Správce karty

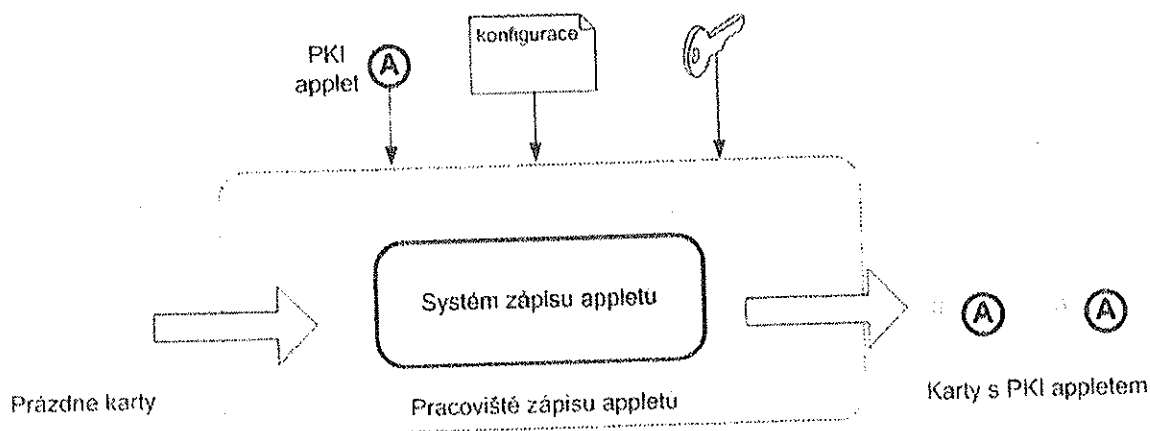
Správce karty umožňuje správu čipové karty, tj. zobrazení její struktury, mazání a import certifikátů, správu RSA klíčů, správu PIN, atp.

Současná verze správce se vyznačuje tím, že je v ní zabudován internetový prohlížeč. S využitím této technologie lze snadno uživateli prezentovat mnoho zajímavých informací, dát mu k dispozici odkazy na různé webové servery (server společnosti, server s technickou podporou, atp.).

Specifikace technického řešení zápisu appletu do čipové karty

1.14 Technický popis řešení zápisu appletu

PKI applet bude do kontaktních čipů zapisován na *pracovišti zápisu appletů*.



Obrázek 4: Schéma Systému zápisu appletů

Vstupem *pracoviště zápisu appletů* budou:

- Prázdné karty (bez appletu, v bezkontaktním čipu budou mít zapsáno logické číslo karty a interval doby platnosti)
- Klíče pro zápis appletu a způsob použití těchto klíčů (viz kapitolu 1.14.3)
- PKI applet
- Konfigurace zápisu appletu

Výstupem procesu budou karty s PKI appletem. Vzniklá karta bude plně kompatibilní s dodaným middleware. Na kartě bude uložen RSA klíč a certifikát karty (tzv. *device* certifikát C.509). Na kartě bude uložen také kořenový certifikát certifikační autority, která *device* certifikát vydala.

Zápis appletu do čipů bude proveden *Systémem zápisu appletů*, který dodá Dodavatel. Kromě *Systému zápisu appletů* dodá Dodavatel také: PKI applet a konfiguraci *Systému zápisu appletů*.

Prázdné karty a klíče pro zápis appletů zajistí MHMP (SKC). SKC zajistí také informace, potřebné pro konfiguraci – zejména informace o práci s klíči dodaných karet.

1.14.1 Postup zápisu appletů do kontaktních čipů

Zápis PKI appletu je proces, který z „prázdného“ kontaktního čipu (tedy čipu dodaného od výrobce PKI čipů) vytvoří plně funkční PKI čipovou kartu, se kterou bude možno pracovat prostřednictvím PKI middleware.

Zápisem appletu se myslí:

- zápis kódového balíku (package) Java appletu na čipovou kartu

- instalace appletu
- vytvoření struktury karty (přiřazení logického čísla, prostory pro klíče, certifikáty, data) podle schváleného customizačního protokolu.

Technický popis zápisu appletů je uveden v kapitole 1.15.6.

Po skončení zpracování (na výstupu) má karta:

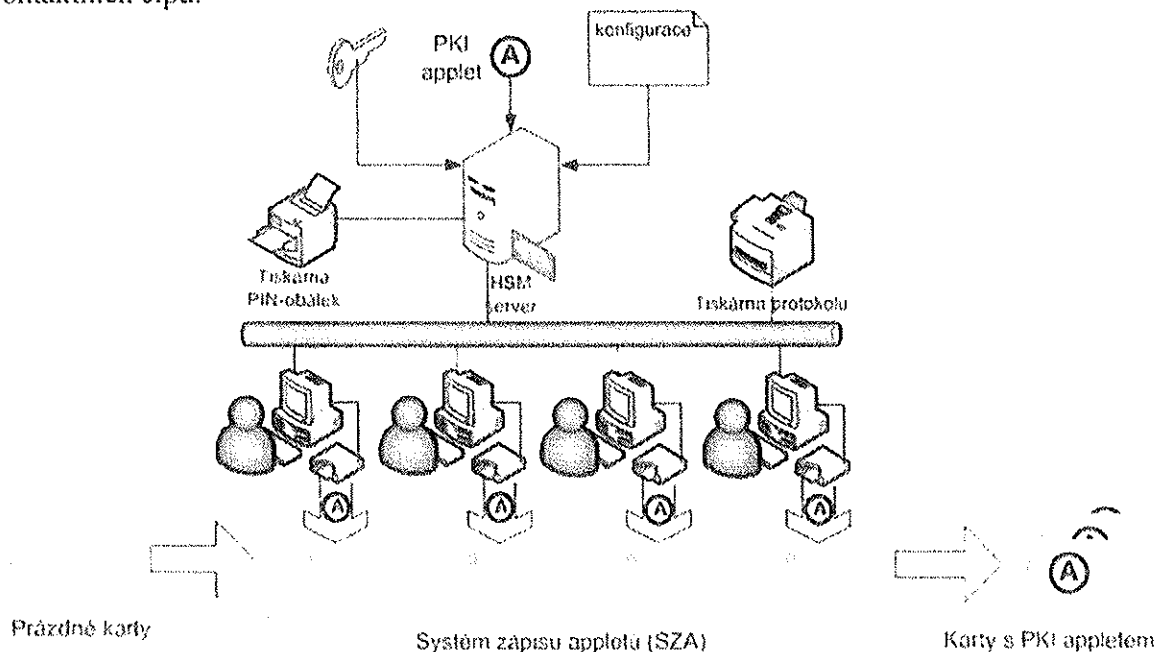
- implementovanou podporu PKI
- změněn klíč pro nahrávání / mazání appletů (pokud je požadováno),
- změněno ATR pro jednoznačnou identifikaci typu karty v PC/SC systémech,
- vytvořenu strukturu a nastavena přístupová práva a
- zapsáno logické číslo (*Card Logical Number*, CLN), které bylo kartě přiděleno v SKC,
- zapsán interval platnosti, který byl přidělen v SKC,
- nastaveny hodnoty PIN a PUK.

Takto je karta připravena k použití s dodávaným middleware.

Pozn.: ATR (*Answer to Reset*) je řetězec, kterým se karta identifikuje do PC/SC subsystému po připojení napájení. Pro UKP je třeba vytvořit unikátní ATR, aby bylo možné snadno rozlišit UKP od jiných typů karet.

1.14.2 Systém zápisu appletů

Dodavatel dodá *Systém zápisu appletů*, který bude řídit a realizovat zápis PKI appletů do kontaktních čipů.



Obrázek 5: Detailní schéma Systému zápisu appletů

Systém zápisu appletů (SZA) se skládá z těchto komponent:

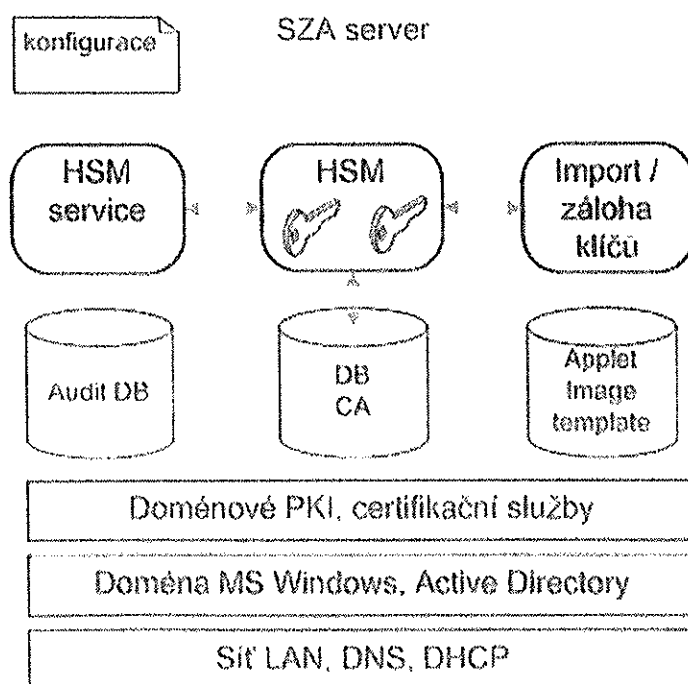
- *Obslužné pracoviště zápisu appletu (OPZA)*. Počítač s připojenou čtečkou čipových karet. Na počítači je instalován *Modul realizace zápisu appletu karty (MRZAK)*, který řídí proces zápisu appletu do kontaktních čipů karet. *OPZA* při svých operacích využívá HSM. Vkládání karet do čtečky zajišťuje lidská obsluha.

- *SZA server*. Server domény MS Windows, v němž je instalován *Host Security Module* (HSM). *SZA server* je pilířem a jádrem funkčnosti systému SZA. Zajišťuje bezpečnostní, kryptografické, konfigurační, síťové i datové služby systému. Poskytuje různé typy služeb pro pracoviště *OPZA* i systém SZA jako celku. Jeden *SZA server* obsluhuje a poskytuje služby několika *OPZA*.
- Tiskárna pro tisk protokolů, např. protokoly o zavedení klíčů do HSM, protokoly o provedení personalizace, atp.
- Tiskárna PIN-obálek. Jehličková tiskárna, která do neprůhledných PIN-obálek tiskne hesla pro autentizaci k HSM.

1.14.2.1 Funkce SZA serveru

SZA server je pilířem systému SZA. Mezi funkce *SZA serveru* patří:

- Podpora sítě LAN a protokolu TCP/IP.
- Realizace domény MS Windows.
- Realizace PKI a certifikačních služeb na doméně MS Windows.
- Hostování kryptografického modulu (HSM).
- Poskytování kryptografické podpory pro *OPZA* a systém SZA obecně.
- Podpora zavádění a zálohování klíčů HSM.
- Úložiště konfiguračních údajů systému SZA a úložiště appletu, který má být nahráván do čipových karet.
- Podpora auditu a úložiště auditních záznamů.
- Podpora tisku bezpečnostních protokolů.
- Hostování databáze certifikační autority (pro vydávání C.509)



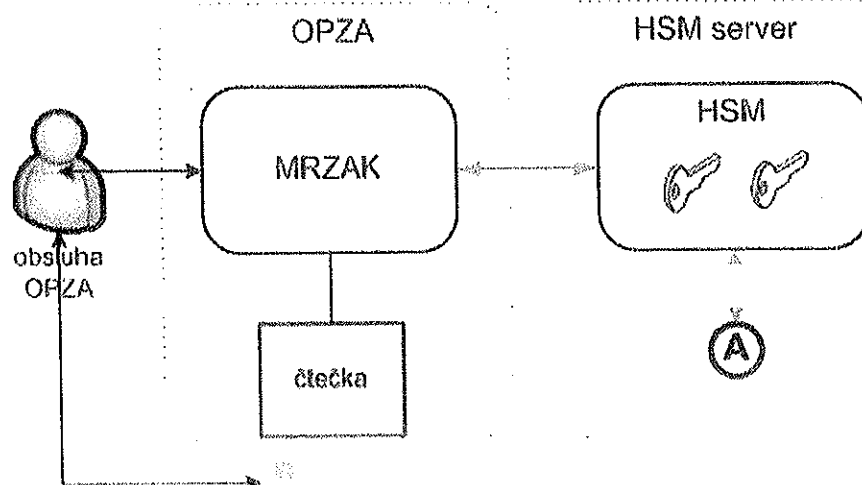
Obrázek 6: Schéma a komponenty SZA serveru

SZA server se skládá z následujících komponent:

- **Domény** MS Windows a Active Directory, které jsou postaveny nad operačním systémem MS Windows 2003. Doména slouží mj. ke správě uživatelských identit, definici uživatelských rolí a vynucení bezpečnostních politik.
- Podpory sítě a protokolu TCP/IP. Operační systém *SZA serveru* je konfigurován tak, aby poskytoval služby **DNS a DHCP**.
- **Certifikačních služeb**, reprezentujících PKI systém v doméně MS Windows. Certifikační služby jsou standardní součástí operačního systému. Pomocí doménového PKI jsou vydávány certifikáty, které slouží k vytvoření bezpečného a oboustranně autentizovaného SSL kanálu mezi *OPZA* a *SZA serverem*.
- Hardwarového kryptografického modulu (**HSM**). HSM je bezpečný hardware, který slouží k ukládání citlivých informací (zejména klíčů). HSM také provádí kryptografické operace s klíči.
- **HSM service**, což je služba (service) operačního systému, která poskytuje podporu kryptografických operací pro *OPZA* a pro zápis appletů obecně. Kryptografické zabezpečení je nezbytnou součástí procesu zápisu appletů do čipových karet.
- Softwarové aplikace pro **zavádění a zálohování klíčů** HSM. Klíče do HSM musí být zavedeny bezpečným a definovaným způsobem. Součástí procesu zavádění klíčů je i tisk protokolu o provedení citlivé operace. Výsledkem některých operací s klíči také může být tisk citlivých informací do PIN-obálek.
- **Konfigurace** systému *SZA*. Všechny konfigurační údaje, nezbytné pro provoz systému *SZA* jsou uloženy v centrálním *SZA serveru*.
- V HSM *SZA serveru* je uložen zašifrovaný a podepsaný PKI **applet**, který je zapisován do kontaktních čipů.
- Centrální **audit** *SZA*. Eventlog *SZA serveru* slouží jako centrální úložiště auditních záznamů celého *SZA*, tedy nejen samotného *SZA serveru*, ale také jednotlivých *OPZA*.
- V HSM je implementována **certifikační autorita pro vydávání certifikátů C.509**. HSM je také bezpečným úložištěm klíčů této autority.
- **SQL databáze**, v níž jsou uloženy informace pro podporu certifikační autority při vydávání C.509.

1.14.2.2 Funkce *OPZA*

Na *Ohslužném pracovišti zápisu appletu (OPZA)* se provádí samotný zápis appletu do čipové karty. Na *OPZA* je instalován softwarový *Modul realizace zápisu appletu karty (MRZAK)*. *MRZAK* je grafická aplikace, pomocí níž obsluha provádí zápis appletů do čipových karet.



Obrázek 7: Schéma obslužného pracoviště

Mezi základní funkce *MRZAK* patří:

- Řízení a kontrola procesu zápisu appletu do čipové karty.
- Řízení a ovládání čtečky, včetně detekce chybových a problémových stavů.
- Transfer dat do čtečky a karty:
 - řídicí signály pro čtečku
 - řídicí signály pro čipovou kartu
 - data pro čipovou kartu (PKI applet)
 - ...
- Zpracování odezvy od čtečky a karty.
- Žurnálování procesů.
- Grafická konzola obsluhy, pomocí níž lze mimo jiné
 - vizualizovat informace o probíhajícím procesu zápisu appletů
 - převzít plnou kontrolu nad zápisem appletů
 - řídit procesy zápisu appletů (start, pozastavení, obnova, ukončení, ...)
 - signalizovat možné problémy procesu zápisu appletu (chybové hlášení, varování, ...)
- Bezpečná komunikace s HSM.
- Využití kryptografických služeb HSM.

Pro správnou funkci *MRZAK* je nutno:

- instalovat a konfigurovat *MRZAK* na počítači *OPZA*
- instalovat na *OPZA* funkční čtečku čipových karet
- navázat spojení *MRZAK* s HSM serverem.

Obsluhu pro *MRZAK* zajistí SKC. Školení obsluhy provede Dodavatel.

1.14.2.3 Zápis appletu z pohledu obsluhy

Obsluha *MRZAK* bude z uživatelského hlediska velmi jednoduchá:

- Po přihlášení obsluhy do operačního systému se automaticky spustí aplikace *MRZAK*.
- Po spuštění *MRZAK* provede autodetekci systému.

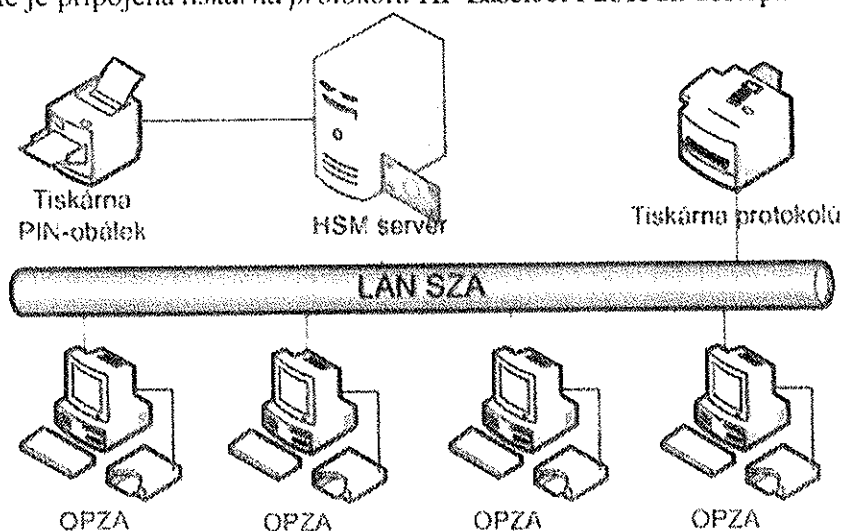
- Pokud kontrola nezjistí žádné potíže, nabídne se obsluze zahájení procesu zápisu appletů.
- Obsluha bude vždy vyzvána k vložení prázdné karty, po vložení karty začne automatický proces zápisu appletu.
- Obsluha bude o procesu zápisu srozumitelně informována.
- Po dokončení zápisu appletu do karty bude obsluha vyzvána k vyjmutí karty ze čtečky.
- Pokud v průběhu zápisu appletu do karty nastane problém, je o něm obsluha informována prostřednictvím grafického rozhraní aplikace.

Technicky je proces zápisu appletu popsán v kapitole 1.15.6.

1.14.2.4 Fyzická struktura Systému zápisu appletů

Fyzicky se SZA skládá z počítačů, spojených navzájem do sítě LAN:

- *HSM server* běží na počítači s operačním systémem MS Windows 2003 Server Standard edice. Je dodán v provedení, které je určeno do rack-u. V *HSM serveru* je instalován kryptografický modul Protect Server Gold CSA 8000 PL220. Na *HSM serveru* běží mj. tiskový server pro ostatní počítače v síti. Díky tomuto tiskovému serveru mohou *OPZA* tisknout na *tiskárnu protokolů*.
- Všechna *OPZA* jsou desktopová PC s LCD monitorem, klávesnicí a myši. Běží pod operačním systémem MS Windows XP Professional SP2. Ke každému *OPZA* je přes USB konektor připojena čtečka čipových karet typ Omnikey 5312.
- K *HSM serveru* je připojena jehličková tiskárna EPSON LQ630 pro tisk do PIN-obálek.
- Do sítě je připojena *tiskárna protokolů* HP LaserJet P2015dn dostupná všem PC SZA

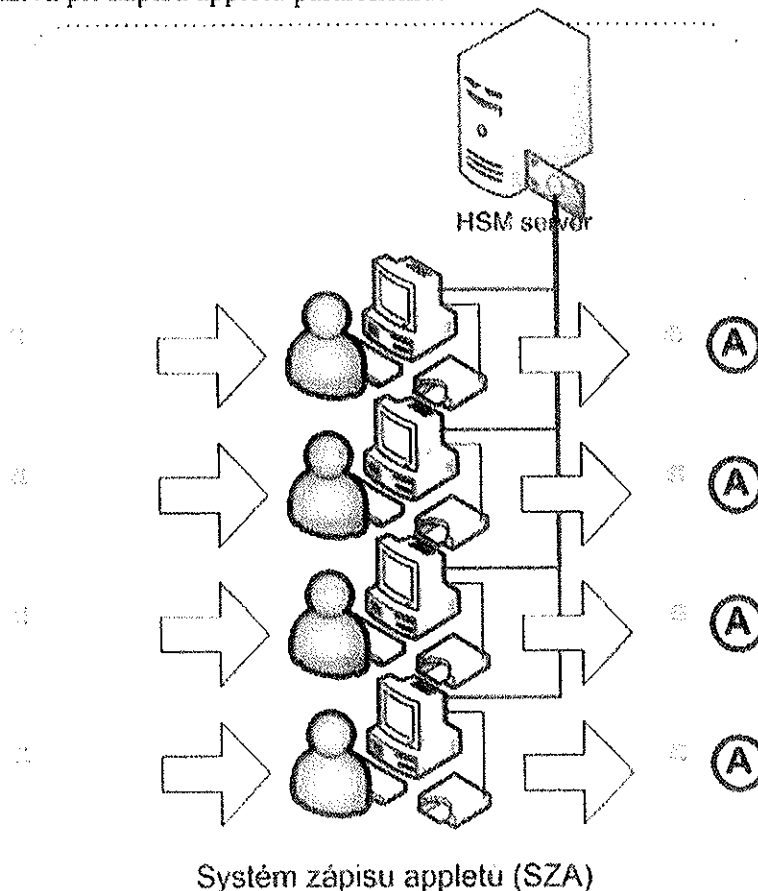


Obrázek 8: Schéma síťového propojení SZA

Všechna PC budou vybavena síťovou kartou. Síťová komunikace s HSM poběží nad protokolem TCP/IP, zabezpečení bude zajištěno protokolem SSL. Předpokládá se, že síť a síťové prvky (IP adresy, kabely, routery, switche,...) k propojení jednotlivých zařízení zajistí SKC. SKC také zajistí, aby do LAN SZA nebylo možno přistupovat z jiných sítí.

1.14.2.5 Paralelismus a škálovatelnost zápisu appletů

Návrh SZA využívá při zápisu appletů paralelismus.



Obrázek 9: Paralelismus zápisu appletů

Jednotlivá OPZA provádějí zápis appletů nezávisle na ostatních. Všechna OPZA využívají a sdílejí jediný HSM server.

Díky paralelismu zápisu appletů na jednotlivých OPZA může SZA dosahovat vysokého výkonu a velké průchodnosti. Přidáváním OPZA lze výkon SZA dále škálovat.

Při eventuální poruše jednoho z OPZA nedojde k zastavení činnosti SZA – ostatní OPZA mohou nadále pracovat a zapisovat applety.

1.14.3 Oprávnění pro zápis appletů do čipu

Zápis appletu do čipu je bezpečnostně citlivá operace. Vydavatel karet nemá zájem, aby si na karty mohl kdokoli zapisovat applety, popř. mazat stávající. Naopak, snaží se vybudovat mechanismy který by zabránily neoprávněné správě appletů. Cílem je zajistit, aby applety do čipu mohl zapisovat/mazat jen vydavatel anebo jím pověřené osoby.

Správu appletů na kartách, kompatibilních se standardem Open Platform 2.0.1, zajišťuje základní aplikace *Card Manager*. *Card Manager* umožní zápis / mazání appletů až po úspěšné autentizaci proti jeho klíčům.

Klíč nebo sada klíčů, kterými je karta chráněna při převzetí pro zápis PKI appletu, je v tomto dokumentu nazýván CMCV (*Card Manager – Card Vendor*).

Je možné, že pod tímto označením bude jeden rodinný klíč nebo tři různé rodinné klíče používané pro různé účely. Přesný popis algoritmu odvození klíče konkrétní karty z klíče/klíčů CMCV musí zajistit MHMP, resp. SKC. Dodavatel musí popis odvození klíče znát, jinak nebude schopen do karet zapisovat PKI applety.

Bližší informace o klících *Card Manager* viz dokumentace OpenPlatform 2.0.1.

1.14.4 Výměna klíčů pro zápis appletů

Předpokládá se, že Dodavatel pro zápis PKI appletů převezme prázdné karty, na nichž bude nastaven klíč CMCV. Tento klíč bude znát SKC (MHMP), ale může jej znát i dodavatel karet – oba by pak mohli pomocí klíče CMCV zapisovat applety do karty.

Aby se dodavateli karet zabránilo v neoprávněném přístupu na kartu, budou v průběhu zápisu PKI appletu klíče v čipových kartách vyměněny. Klíč CMCV bude nahrazen klíčem odvozeným od CMUKPF (*Card Manager – UKP Family*), jehož výhradním vlastníkem bude SKC (MHMP).

Po provedení výměny klíčů již nebude možné na kartu nahrávat (mazat) applety pomocí klíče CMCV, ale pouze klíči odvozenými od CMUKPF. Tím je garantováno, že pouze SKC (MHMP) může provádět správu appletů na kartách.

Technické podrobnosti výměny klíčů jsou popsány v kapitole 1.15.5.

1.14.5 PIN a PUK karet po uložení PKI appletu

Předpokládá se, že prázdné PKI karty budou před vydáním v SKC dále personalizovány. Proto budou mít všechny karty po zápisu appletů nastaveny stejné (známé) hodnoty PIN a PUK:

PIN = 1111

PUK = 44444444

Návazné procesy SKC pak mohou díky znalosti PIN a PUK do kontaktního čipu zapisovat PKI objekty.

Před vydáním karty držiteli by SKC mělo nastavit kartě náhodný PIN i PUK. Jejich hodnoty by měly být vytištěny do neprůhledné PIN-obálky a spolu s kartou předány držiteli.

Součástí dodávky Dodavatele proto bude také:

- softwarový modul (knihovna, DLL) pro vygenerování a nastavení náhodných hodnot PIN a PUK karty,
- dokumentace technologie nastavení nových hodnot PIN a PUK PKI karty.

Dodaný software umožní volajícímu procesu zjistit nově vygenerované hodnoty pro vytištění do PIN-obálek. Software bude určen pro operační systém MS Windows.

Generování a zápis PIN a PUK bude realizován prostřednictvím standardního PC/SC rozhraní čtečního/zapisovacího zařízení.

1.14.6 Integrace PKI karet do SKC

Výsledkem zápisu PKI appletu bude kompletně funkční PKI karta. Každá PKI čipová karta bude mít své unikátní logické číslo (*Card Logical Number*, CLN) – toto číslo kartám přiděluje SKC.

Předpokládá se, že SKC bude PKI čipové karty evidovat ve svých databázích. Součástí dodávky Dodavatele bude také:

- software pro
 - přečtení CRN kontaktního čipu
 - přečtení CLN z PKI karty
 - přečtení doby platnosti karty
- dokumentace s popisem čtení CLN a dalších dat z karty.

Tento software, resp. tuto dokumentaci bude moci SKC použít pro čtení dat potřebných k evidenci PKI karet.

1.15 Bezpečnostní koncept řešení zápisu appletu

Zápis appletu do čipových karet je bezpečnostně citlivá operace.

Předpokládá se proto, že celá procedura bude prováděna v režimovém pracovišti s řízeným přístupem.

Kryptografické klíče, které jsou pro zápis appletů nezbytné, budou chráněny v HSM.

HSM (*Host Security Module*) je bezpečný hardware, který slouží pro

- bezpečnou správu,
- bezpečné uložení a
- použití

kryptografických klíčů.

HSM bude poskytovat kryptografické služby pro všechny OPZA (MRZAK). Veškeré operace s klíči budou prováděny uvnitř HSM, klíče nikdy neopustí prostředí HSM. MRZAK bude využívat pouze výsledky kryptografických operací s klíči.

1.15.1 Základní vlastnosti HSM

Modul HSM obsahuje kryptografickou kartu ProtectServer Gold CSA 8000 PL220. Kryptografická karta zajišťuje bezpečné uložení klíčů, při pokusu o útok na tuto kartu automaticky všechny uložené klíče smaže. HSM nabízí standardní rozhraní PKCS#11, upravené pomocí funkcionálního modulu dle specifických požadavků na zápis appletů.

HSM má vnitřní hierarchii klíčů; hlavním (master) klíčem je KLM (*Key Local Mater*). Tento klíč je bezpečnostně nadřazený ostatním klíčům.

Pomocí klíče KLM lze dělat zálohy ostatních klíčů v HSM. HSM vygeneruje záložní soubor s klíči, šifrovanými (wrapovanými) klíčem KLM.

Klíč KLM musí být kryptograficky stejně silný nebo silnější než zálohované klíče. Vzhledem k tomu, že klíče *Card Manager* kontaktních čipů jsou typu 3DES dvojitá délka (112 bitů), používá se pro KLM klíč AES 256 bitů, případně 3DES dvojitá délka (112 bitů).

1.15.1.1 Technické parametry HSM

HSM modul Gold CSA 8000 PL220 je kryptografický PCI adaptér navržený pro bezpečné použití v kritických aplikacích. HSM modul splňuje vysoké požadavky na bezpečnost a aplikační přizpůsobivost.

Charakteristické parametry:

Bezpečnost

- V procesu certifikace FIPS 140-2 level 3
- Automatický výmaz paměti při detekci pokusu o fyzické vniknutí do modulu
- 4MB baterií zálohované bezpečné paměti pro uložení klíčů, certifikátů a dalších citlivých dat (baterie zajišťuje i zdroj energie pro mechanismy detekce a reakce na fyzické útoky)
- True Random Number Generator generátor náhodných čísel (splňuje kritéria ANSI X9.31 a je certifikován na FIPS 140)
- Podpora čipových karet pro transfer a zálohu klíčů
- Přímé propojení se čtečkou čipových karet a PIN pad zařízením

Výkon

- Jsou dostupné modely s různým výkonem
- Redundance pro škálovatelnost a rozložení výkonu a vysokou spolehlivost
- Podpora vícevláknového zpracování operací v rámci jednoho procesu (thread-safe)

Správa

- GUI aplikace pro správu (založené na Java)
- Řádkové utility pro správu (vhodné pro scripty)
- Nástroje pro bezpečnou aktualizaci firmware v produkčním prostředí
- Vzdálená správa síťových HSM

Nástroje

- PKCS#11 rozhraní
- Java JCA/JCE provider
- CSP pro Microsoft CryptoAPI
- implementace OpenSSL engine
- EFT command set pro podporu zpracování platebních transakcí
- SDK pro vývoj vlastních aplikací

Kryptografické algoritmy

- Symetrické – AES, DES, 3DES, CAST-128, RC2, RC4, SEED, další na vyžádání; podpora režimů zahrnuje ECB, CBC, OFB64, CFB-8 (BCF), další na vyžádání
- Asymetrické – RSA (do 4096 bitů), DSA, ECDSA (do 512 bitů), Diffie Hellman (DH), další na vyžádání

Kompletní výpis algoritmů, vč. podpisových a autentizačních schémat je popsán v příručkách jednotlivých kryptografických knihoven

Připojení

- PCI 2.2 rozhraní (32 nebo 64 bitů, 33 nebo 66MHz)
- podpora 3.3V i 5V úrovní

Rozměry

- 231mm x 18,7mm x 105,5mm

Napájení

- +3,3V/655mA, +5V/645mA, +12V/27mA

Provozní prostředí

- teplota 0° – 40°C
- relativní vlhkost 5 – 95% (nekondenzující)

1.15.1.2 Použitý server pro provoz HSM

Pro instalaci HSM serveru bude použit HP ProLiant DL360R04p X3.0-2MB/800, 1GB SCSI
Tento server bude umístěn v RACKu SKC, součástí dodávky není monitor, klávesnice, myš.

Charakteristické vlastnosti:

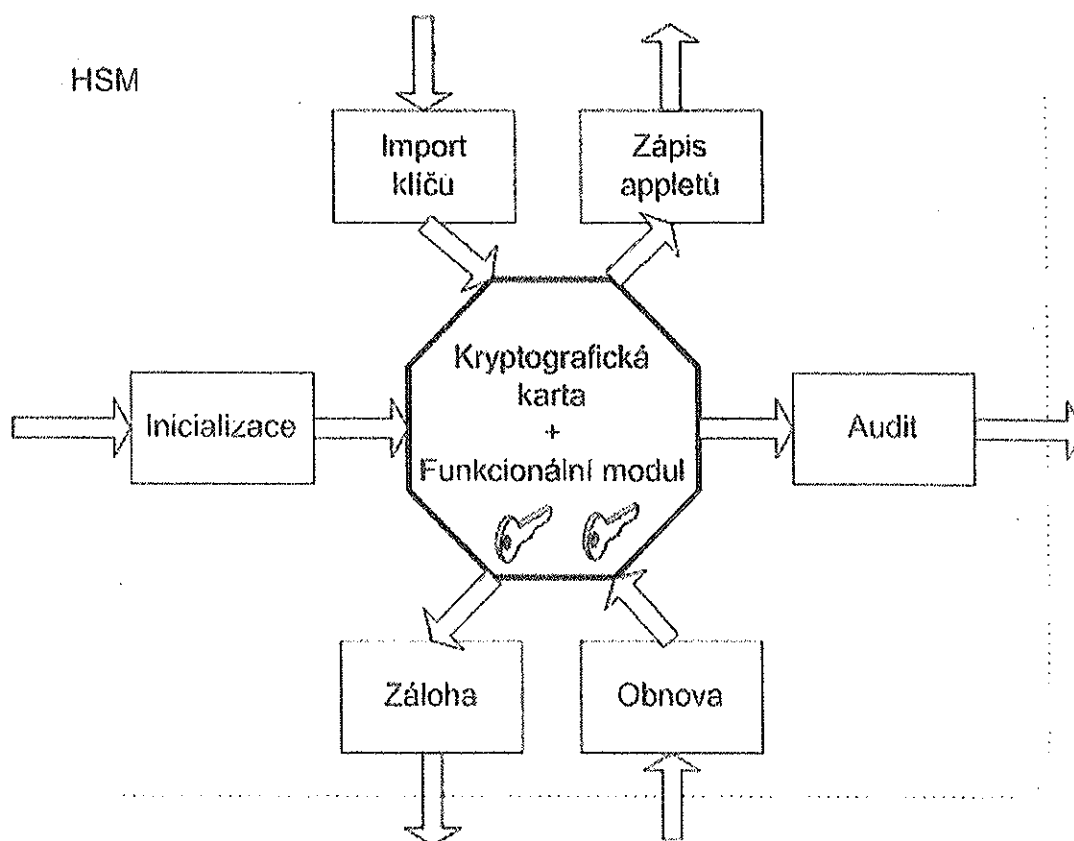
- Procesor: Intel Xeon Processor 3.0-GHz/800MHz / 2-MB level 2 cache
- Memory: 1 GB (2 x 512 MB) PC2-3200 DDR2 400 SDRAM
- Network Controller: Embedded NC7782 Dual Port PCI-X 10/100/1000T Gigabit network adapter
- Storage Controller: Embedded U320 Smart Array 6i Controller
- Remote Management: Integrated Lights-Out (iLO) Standard Management (embedded)
- Power Supply One 460W power supply (redundant power supply optional)
- 460W HP redundant power supply with IEC cord only
- 72.8GB 15,000 rpm, U320 Universal Hot Plug drive, 1"
- HP DVD+R/RW 8X Slim

1.15.2 Modulární struktura HSM

Systém zápisu appletů (SZA) je vybaven HSM pro zabezpečení zápisu appletů.

Podpora zápisu appletů však není jedinou funkcí HSM. HSM implementuje také řadu servisních funkcí, které obecně souvisí se správou klíčů:

- *Inicializace HSM* – zajistí správnou inicializaci kryptografických tokenů na HSM, inicializaci bezpečnostního režimu HSM, generování KLM klíčů se zálohou na čipové karty, tisk PIN obálek s hesly, atp..
- *Import klíčů* do HSM, pro bezpečné zavedení nových klíčů.
- *Záloha*, pro bezpečné zálohování klíčů. Klíče jsou před zálohováním zašifrovány (wrapovány) klíčem KLM.
- *Obnova*, pro bezpečnou obnovu klíčů. Obnovované klíče jsou do HSM vkládány zašifrované (wrapované) klíčem KLM. Po zavedení HSM provede dešifrování (unwrap) klíče. Klíč KLM je v případě potřeby rekonstruován z čipových karet.
- *Audit*, pro zaznamenání a kontrolu operací s klíči.



Obrázek 10: Modulární struktura HSM

Jádrem HSM je bezpečný hardware (kryptografická karta). Pro podporu zápisu appletů je nutno do kryptografické karty zavést *funkcionální modul* – software pro řízení jádra HSM.

1.15.3 Seznam klíčů v HSM

V HSM systému zápisu appletů budou uloženy tyto klíče:

- **KLM (Key Local Master)**– Master klíč HSM používaný pro zálohování ostatních klíčů. Je generován v HSM, rozložen Shamirovým algoritmem na čipové karty. Vlastníkem klíče a správcem čipových karet s jeho komponentami je SKC.
- **CMCV (Card Manager – Card Vendor)**– klíč/klíče chránící zápis/mazání appletů na dodané (čisté) kartě. Tento klíč musí být k dispozici, aby bylo možné do karet ukládat applety. Je obvyklé, že CMCV dodává dodavatelem karet. Hodnota klíče bude vložena do HSM pověřenými pracovníky dodavatele karet. Klíč CMCV nikdy neopustí prostředí HSM (s výjimkou prováděné zálohy, šifrované klíčem KLM).
- **TKCMCV (Transport Key – Card Manager – Card Vendor)**. Šifrovací klíč pro bezpečné zavedení klíče CMCV do HSM.
- **CMUKPF (Card Manager – UKP Family)** – rodinný klíč UKP pro ochranu zápisu/mazání appletů na kartě se zapsaným appletem (pro budoucí přihrávání dalších appletů na kartu). Klíč bude pracovníky SKC předán pověřeným pracovníkům Dodavatele. CMUKPF bude při předání zašifrovaný klíčem TKCMUKPF. Klíč bude zaveden do HSM, nikdy neopustí prostředí HSM. Bude využit při procesu zápisu appletů do karet.

- **TKCMUKPF** (*Transport Key - Card Manager – UKP Family*). Transportní klíč pro ochranu klíče CMUKPF. Pracovníci SKC jej předají rozložený ve 3 PIN-obálkách 3 definovaným pracovníkům Dodavatele. TKCMUKPF bude zaveden do HSM a nikdy jej neopustí. Bude použit výhradně pro bezpečné zavedení klíče CMUKPF do HSM.
- **KAPPL** (*Key Applet*) – klíč, kterým je zašifrována binární podoba appletu. Klíč KAPPL obecně slouží k šifrování dat (nejen binárního kódu appletu). Klíč je generován přímo v HSM, hodnota je při generování rozložena do tří obálek, které převezmou pracovníci Dodavatele. Vlastníkem a držitelem klíče je Dodavatel.
- **CPLUSFK** (*CryptoPlus Family Key*). Rodinný klíč appletu *CryptoPlus opencard* pro vytváření bezpečného kanálu mezi PKI kartou a čtečkou, např. při importu privátního klíče na kartu. Od CPLUSFK budou v procesu zápisu appletu diverzifikovány klíče pro jednotlivé karty. Vlastníkem a držitelem klíče je Dodavatel.
- **KRCA** (*Key Root CA*). Asymetrický klíč device certifikační autority. Tímto klíčem budou podepisovány certifikáty karet. KRCA bude vygenerován v HSM a nikdy jej neopustí.

Postup zavádění klíčů do HSM je naznačen v kapitole 1.15.4.

Ceremonie generování / zavádění / zálohování klíčů HSM bude detailně popsána v dokumentaci dodané s HSM. V této dokumentaci bude také uveden seznam uživatelských rolí, které mohou pracovat s HSM. Pro každou roli bude definováno, jaké operace a s kterými klíči mohou příslušní uživatelé provádět.

Předpokládá se, že SKC deleguje do jednotlivých rolí své důvěryhodné zástupce.

1.15.4 Zavedení klíčů do HSM

Některé klíče budou generovány přímo v HSM, jiné budou do HSM ceremoniálně zavedeny. V následujících podkapitolách budou uvedeny podrobnosti zavedení / generování jednotlivých klíčů.

Postup zavedení některých klíčů, jejich vlastníkem je Dodavatel není uveden.

1.15.4.1 Key Local Master (KLM)

KLM se generuje v HSM a je zálohován na N karet z nichž M postačuje k rekonstrukci klíče. Používá se například rozdělení na 3 karty, z nichž 2 postačují k rekonstrukci. Při poškození některé karty tak zůstávají 2 karty, z nichž lze KLM rekonstruovat.

1.15.4.2 Card Manager – Card Vendor (CMCV)

CMCV je nutno do HSM ceremoniálně zavést. CMCV bude do HSM zaveden zašifrovaný klíčem TKCMCV a algoritmem 3DES. V HSM bude CMCV dešifrován pomocí TKCMCV.
 $\text{Šifrovaný CMCV} = 3DES[\text{TKCMCV}](\text{CMCV})$.

Pro kontrolu úspěšného zavedení HSM vypočte a zobrazí kontrolní sumu klíče CMCV:
 $\text{Kontrolní suma} = 3 \text{ MSB z } 3DES[\text{CMCV}](00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00)$

Poznámka: 3 MSB jsou horní 3 byte z vygenerovaného kryptogramu (*Most Significant Bytes*).

1.15.4.3 Transport Key – Card Manager – Card Vendor (TKCMCV)

Klíč CMCV bude zaváděn do HSM jako zašifrovaný. Před zavedením CMCV bude nutno zavést do HSM transportní klíč TKCMCV.

TKCMCV do HSM zavedou 3 bezpečnostní úředníci, každý bezpečnostní úředník zavede pouze jeden fragment TKCMCV1, TKCMCV2 a TKCMCV3. V HSM bude z fragmentů sestaven kompletní TKCMCV = TKCMCV1 XOR TKCMCV2 XOR TKCMCV3.

Pro kontrolu úspěšného zavedení HSM vypočte a zobrazí kontrolní sumu klíče TKCMCV:
Kontrolní suma = 3 MSB z 3DES[TKCMCV](00 00 00 00 00 00 00 00)

1.15.4.4 Card Manager – UKP Family (CMUKPF)

CMUKPF je nutno do HSM ceremoniálně zavést. CMUKPF bude do HSM zaveden zašifrovaný klíčem TKCMUKPF a algoritmem 3DES. V HSM bude CMUKPF dešifrován pomocí TKCMUKPF.

Šifrovaný CMUKPF = 3DES[TKCMUKPF](CMUKPF).

Pro kontrolu úspěšného zavedení HSM vypočte a zobrazí kontrolní sumu klíče CMUKPF:
Kontrolní suma = 3 MSB z 3DES[CMUKPF](00 00 00 00 00 00 00 00)

Poznámka: 3 MSB jsou horní 3 byte z vygenerovaného kryptogramu (*Most Significant Bytes*).

1.15.4.5 Transport Key – Card Manager – UKP Family (TKCMUKPF)

Klíč CMUKPF bude zaváděn do HSM jako zašifrovaný. Před zavedením CMUKPF bude nutno zavést do HSM transportní klíč TKCMUKPF.

TKCMUKPF do HSM zavedou 3 bezpečnostní úředníci, každý bezpečnostní úředník zavede pouze jeden fragment TKCMUKPF 1, TKCMUKPF 2 a TKCMUKPF 3. V HSM bude z fragmentů sestaven kompletní TKCMUKPF = TKCMUKPF1 XOR TKCMUKPF2 XOR TKCMUKPF3.

Pro kontrolu úspěšného zavedení HSM vypočte a zobrazí kontrolní sumu klíče TKCMUKPF:
Kontrolní suma = 3 MSB z 3DES[TKCMUKPF](00 00 00 00 00 00 00 00)

1.15.5 Výměna klíčů pro zápis appletů

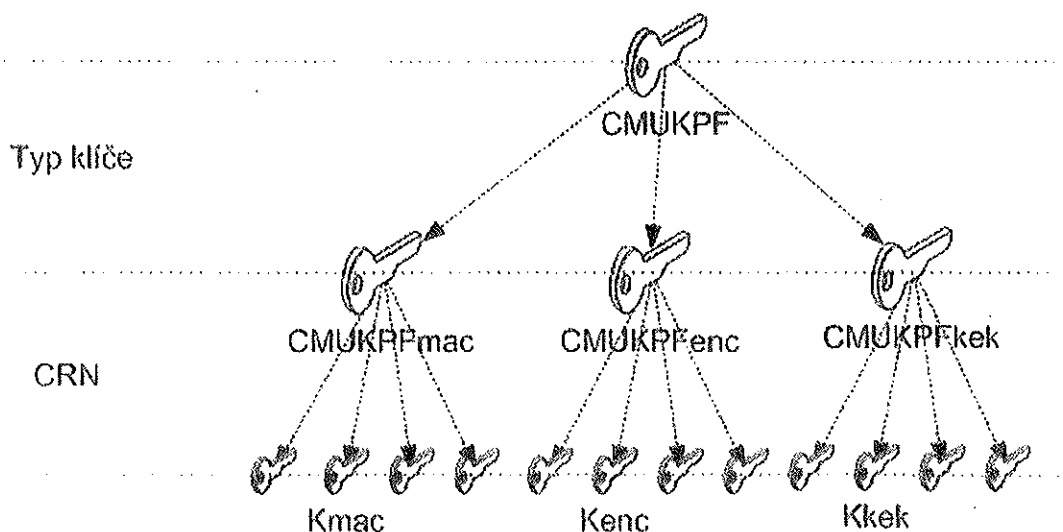
V průběhu zápisu PKI appletu bude klíč CMCV nahrazen klíčem, odvozeným od CMUKPF.

Správce karty používá 3 klíče:

- klíč *Kmac* pro zajištění integrity,
- klíč *Kenc* pro utajení (šifrování) a
- klíč *Kkek* pro výměnu klíčů.

Platí, že všechny klíče karet budou odvozeny z jediného rodinného klíče CMUKPF podle

- typu klíče a
- unikátního čísla kontaktního čipu karty (*Card Reference Number, CRN*).



Obrázek 11: Schéma výměny klíčů pro zápis appletů

Klíče *Správce karty*, které budou do čipu zapsány, budou generovány následovně:

- $K_{enc} = \text{divkey} (CMUKPF, CRN, TYP_ENC)$
- $K_{mac} = \text{divkey} (CMUKPF, CRN, TYP_MAC)$
- $K_{kek} = \text{divkey} (CMUKPF, CRN, TYP_KEK)$

Funkce *divkey* provede nejprve diverzifikaci rodinného klíče CMUKPF podle typu klíče, následně teprve provede diverzifikaci podle konkrétního čísla karty.

Z klíče CMUKPF je tedy možné vypočítat tři podřízené rodinné klíče: *CMUKPFenc*, *CMUKPFmac* a *CMUKPFkek* a ty používat podle druhého způsobu odvození klíčů pro klíče karty. Toto řešení umožňuje např. předat třetí straně klíče, které umožní šifrovaný zápis appletu na kartu (klíče *CMUKPFenc* a *CMUKPFmac*), ale neumožní změnu klíče, protože HSM nebude mít k dispozici klíč *CMUKPFkek* ani výchozí rodinný klíč CMUKPF (ze kterého by bylo možné odvodit *CMUKPFkek*).

Detailní popis diverzifikace klíčů bude uveden v dokumentaci, která bude součástí dodávky Dodavatele.

1.15.6 Podrobný popis procesu zápisu appletu

Proces zápisu appletu je řízen programem *MRZAK*, resp. obsluhou programu *MRZAK*.

Proces zápisu appletu do čipové karty se skládá z posloupnosti několika kroků:

- *MRZAK* požádá obsluhu o vložení další (prázdné) karty.
- Obsluha vloží kartu do čtečky, na čip karty jsou připojeny elektrické kontakty.
- *MRZAK* detekuje přítomnost karty ve čtečce. Oznámí obsluze zahájení procesu zápisu appletu, zaznamená událost do auditního deníku a spustí proces zápisu.
- Kontaktnímu čipu se zapne napájení, zkontroluje se ATR karty a podle možností se urychlí komunikace s kartou pro zajištění maximální možné rychlosti zápisu appletu.
- *MRZAK* z bezkontaktního čipu karty přečte logické číslo a dobu platnosti karty. Tyto údaje pošle do *HSM service*, spolu s výzvou k zahájení procesu zápisu appletu do karty.
- Proběhne autentizace *MRZAK* k *HSM service*. Naváže se spojení, které přenáší data mezi HSM a kontaktním čipem karty.

- *MRZAK* požádá *HSM* o výpočet kryptogramu pro autentizaci ke kartě.
- *HSM* vygeneruje kryptogram na základě údajů od *MRZAK* a klíče CMCV. Kromě autentizačního kryptogramu vytvoří *HSM* také sekvenci dat pro zápis PKI appletu a sekvenci dat pro výměnu klíče karty (z CMCV na CMUKPF).
- *HSM service* odešle připravená data z *HSM* do *MRZAK*.
- *MRZAK* se autentizuje ke kartě.
- *MRZAK* postupně zapisuje a provádí sekvenci dat pro zápis appletu do karty. Zápis sekvence probíhá s využitím ustanoveného bezpečného spojení, s využitím šifrování. Po dokončení sekvence je v kartě zapsán PKI applet a je změněno ATR karty pro možnost snadného rozpoznání typu karty.
- *MRZAK* postupně zapisuje a provádí sekvenci dat pro výměnu klíče karty. Zápis sekvence probíhá s využitím ustanoveného bezpečného spojení, s využitím šifrování. Po dokončení sekvence je v kartě uložen (derivát) klíč CMUKPF.
- *MRZAK* odešle do *HSM service* informaci o tom, že applet byl úspěšně instalován a že byl změněn klíč karty. Zároveň požádá o data pro zápis struktury a dat karty.
- *HSM service* požádá *HSM* o vygenerování klíče a certifikátu C.509 pro kartu.
- *HSM service* požádá *HSM* o vygenerování sekvence dat pro zápis do karty.
- *HSM* vytvoří sekvenci dat pro zápis struktury dat pro kartu. Součástí datové sekvence je také změna CLN karty, nastavení PIN a PUK, zápis certifikátu C.509 (včetně klíče). Sekvence dat je konstruována podle akceptovaného customizačního protokolu.
- *HSM service* odešle vytvořenou sekvenci dat do *MRZAK*.
- *MRZAK* postupně zapisuje a provádí sekvenci dat pro vytvoření logické struktury karty (prostor pro klíče, certifikáty, root certifikáty, data, nastavení přístupových podmínek pro operace). Kartě se v průběhu této operace přidělí CLN (*Card Logical Number*). Do čipu se bezpečným způsobem zavede klíč, odvozený od CPLUSFK, nastaví se PIN a PUK, zapíše se C.509 (včetně klíče). Vytvořená struktura se uzamkne proti možnosti následných změn.
- *MRZAK* informuje *HSM service* o úspěšném dokončení zpracování karty.
- Je ukončena komunikace s kartou a je vypnuto napájení.
- Zpracování (zápis PKI appletu) karty je u konce. *MRZAK* tuto událost zaznamená do auditního deníku.
- *MRZAK* oznámí obsluze dokončení procesu zápisu appletu. Požádá o vyjmutí karty ze čtečky.
- Zpracování pokračuje zápisem appletu do další karty – viz bod 1.

Pokud v průběhu zpracování nastane chyba, je:

- Událost zaznamenána do auditního deníku.
- Ukončen proces zápisu appletu.
- Obsluze zobrazeno chybové hlášení s popisem a kódem chyby.

Operace zápisu appletu nezačne (resp. bude ukončena před započítáním zápisu) pokud:

- Má vložená karta nesprávnou hodnotu ATR.
- Nelze zapsat záznam o startu operace do auditního deníku.
- Není dostupné *HSM service*, resp. služby *HSM*.
- Se zjistí, že karta s daným CLN (přečteným z bezkontaktního čipu) již systémem byla v minulosti zpracována.

1.15.7 Autentizace k HSM

Pro běžnou práci s modulem HSM je prováděna standardní autentizace heslem, pro citlivé operace (například vkládání klíčů na lokální konzole HSM) je zapotřebí kooperace více osob, např. jedna osoba má heslo pro přihlášení do systému a následně HSM vyžaduje dvě hesla osob pro autorizaci vložení klíče.

1.15.8 Autentizace do OPZA

Autentizace a řízení přístupu do počítače *Obslužného pracoviště zápisu appletů (OPZA)* je realizováno prostředky operačního systému, na němž *OPZA* běží.

Obsluha *OPZA* i správce *Serveru HSM* se budou do počítačů autentizovat jménem a heslem. Obsluha *OPZA* nebude mít přístup (možnost autentizovat se) na *Server HSM*.

Předpokládá se, že MHMP deleguje pracovníka pověřeného správou uživatelských účtů pro *OPZA* i *SZA server*. Tento pracovník musí být držitelem oprávnění správce domény *SZA*.

1.16 Doba odezvy zápisu appletu

Systém zápisu appletů bude dostatečně dimenzován, aby byl schopen v krátké době uložit PKI applet do velkého množství karet.

Na pracovišti *OPZA* bude možno zapsat PKI applet do kontaktního čipu za 90 sekund (v čase je započítána cca 20s manipulační rezerva). Jedno *OPZA* tedy bude schopno za 1 hodinu zapsat applety do 40 karet.

Zápis 1 appletu do 1 karty:	90 s
• Počet appletů, zapsaných na 1 <i>OPZA</i> za 1 hodinu:	40
• Počet appletů, zapsaných na 1 <i>OPZA</i> za den (8 hodin):	320
• Počet appletů, zapsaných na 1 <i>OPZA</i> za měsíc (20 prac. dní):	6400

Budou dodána 4 pracoviště *OPZA*. Výkon celého systému charakterizují následující údaje:

• Počet appletů, zapsaných na 1 <i>OPZA</i> za 1 hodinu:	160
• Počet appletů, zapsaných na 1 <i>OPZA</i> za den (8 hodin):	1280
• Počet appletů, zapsaných na 1 <i>OPZA</i> za měsíc (20 prac. dní):	25600

Dodané technické řešení bude schopno při jednosměnném provozu kompletně zpracovat dávku 50.000 čipových karet v průběhu 2 měsíců.

Pozn.: Kompletním zpracováním dávky karet se rozumí zápis PKI appletů do všech dodaných karet. Doba zpracování dávky je časový interval od převzetí „prázdných“ karet do předání karet s PKI appletem. Předpokládá se, že klíče a konfigurace potřebné pro zápis appletů budou do *SZA*, resp. *SZA Serveru* zavedeny před převzetím karet.

Pokud by bylo třeba proces zápisu appletu urychlit, lze to provést těmito způsoby:

- Zavedením vicesměnného provozu na pracovištích *OPZA*.
- Zvýšení počtu pracovišť *OPZA*. Systém *SZA* lze škálovat v rozsahu od stávajících 4 *OPZA* až do 200 *OPZA*. Při dalším zvětšování počtu *OPZA* by bylo vhodné implementovat do systému výkonnější HSM.

Specifikace ověřovacích testů

Akceptace dodávek ze strany MHMP je podmíněna provedením a úspěšným dokončením ověřovacích testů.

V následujících podkapitolách jsou uvedeny jednotlivé ověřovací scénáře. Ověřovací procedura bude realizovat scénáře v uvedeném pořadí.

1.17 Zápis appletu do karty

Vstupy:

- Prázdná karta (bez PKI appletu a objektů)
- Systém zápisu appletů (SZA)

Výstupy:

- Karta s PKI appletem a certifikátem karty (C.509)

Postup:

- Autentizace uživatele do systému SZA
- Spuštění aplikace pro zápis appletu do karty
- Vložení karty do čtečky
- Provedení zápisu appletu do karty
- Vyjmutí karty ze čtečky
- Odhlášení uživatele

1.18 Ověření funkčnosti PKI karty a middleware

Vstupy:

- Karta s PKI appletem a certifikátem C.509 (výstup předchozího scénáře)
- Instalační balíček PKI middleware (na CD)
- Klientské PC s OS MS Windows, CD mechanikou a funkční PC/SC čtečkou čipových karet

Výstupy:

- Informace o datech na kartě
- Číslo karty
- Informace o certifikátu C.509 z karty

Postup:

- Autentizace uživatele do PC (k provedení instalace middleware musí být uživatel vybaven oprávněním lokálního administrátora)
- Vložení instalačního CD a spuštění instalace
- Provedení instalačních kroků podle pokynů instalačního průvodce
- Spuštění aplikace Správce karty
- Vložení karty do čtečky a načtení obsahu (dat) karty
- Zobrazení dat na kartě, vč. čísla karty a certifikátu C.509
- Test integrity klíče (Testovací kryptografická operace s RSA klíčem a certifikátem C.509. V průběhu operace uživatel musí zadat platný PIN karty.)

1.19 Použití karty s C.509 při autentizaci na web server

Vstup:

- PC s instalovaným webserverem a testovací stránkou. WWW server je konfigurován pro akceptaci autentizace uživatele pomocí PKI certifikátu C.509.
- PC s instalovaným PKI middleware (výstup předchozího scénáře) a MS Internet Explorer (verze 5.0 anebo vyšší)
- Propojení obou PC sítí TCP/IP (Test lze provést také na jednom PC s instalovaným klientem i serverem.)
- Karta s certifikátem C.509 (výstup předchozích scénářů)

Výstup:

- HTTPS autentizace držitele karty pomocí C.509 z karty, vč. zobrazení autentizačních údajů

Postup:

- Spuštění webového prohlížeče a zadání URL testovací stránky
- Navázání bezpečného (HTTPS) a oboustranně autentizovaného spojení klienta se serverem (v průběhu autentizace uživatel zadá platný PIN karty)
- Zobrazení testovací stránky s informacemi o parametrech zabezpečeného spojení, vč. vlastností certifikátu C.509, jímž se uživatel autentizoval. Srovnání informace s vlastnostmi C.509. zjištěnými v předchozím scénáři.

1.20 Požadavky na součinnost ze strany MHMP

Pro provedení ověření funkčnosti řešení zápisu PKI appletů do kontaktních čipů vyžaduje součinnost Dodavatele a SKC (resp. MHMP) v těchto oblastech:

- MHMP zajistí hybridní čipové karty dle specifikace v Zadávací dokumentaci.
- MHMP zajistí od dodavatele karet klíč CMCV pro zápis appletů do čipu.
- Při podpisu smlouvy MHMP Dodavateli sdělí přesný typ použitých karet, způsob předání klíčů CMCV a způsob diverzifikace klíčů pro jednotlivé karty. Bez těchto údajů není Dodavatel schopen zahájit přípravu implementace
- MHMP zajistí místo v rack-u pro uložení SZA Serveru
- MHMP zajistí síťové prvky (IP adresy, kabely, switche, routery) k propojení počítačů SZA. MHMP zajistí oddělení LAN SZA od okolních informačních systémů.
- MHMP zajistí prostory pro instalaci SZA, včetně elektrických sítí. Do těchto prostor musí být umožněn přístup pracovníkům Dodavatele – alespoň k provedení implementace řešení.
- MHMP deleguje pracovníky pro ceremonii zavedení / převzetí klíčů HSM.
- MHMP zajistí správu lokálních uživatelských účtů na počítačích SZA. Vyhradí uživatelské účty pro přístup pracovníků Dodavatele. Alespoň pro implementaci řešení musí mít Dodavatel oprávnění administrátora do počítačů OPZA i SZA Serveru.
- MHMP zajistí obsluhu počítačů OPZA pro provádění zápisu appletů.
- MHMP předá definovaný personalizační profil PKI appletu a customizaci middleware

Bez splnění výše uvedené součinnosti není možné provést ověřovací implementaci ani její přípravu.