

SEMINÁŘ PKI

Jaromír Svoboda

Svoboda@coprosys.cz

- Možnosti přechodu na nové čipové technologie pro ID-Karty a PKI v prostředí VŠ

- 4.12.2003

Úvod

- Základní funkce čipové karty jsou
 - záznamová (na čipovou kartu je možné zapsat data a z karty je číst)
 - identifikační (čipovou kartu je možné použít k identifikaci jejího držitele)
 - kryptografická (umožňuje bezpečně provádět kryptografické operace, zejména šifrování, autentizaci a elektronický podpis)
 - „programová“ (na čipovou kartu lze umístit aplikace pro vytváření rozšířených funkcí).

Vývoj rozhraní karty

- Čipová karta umožňuje implementovat různé typy rozhraní kontaktních i bezkontaktních (trendy)
- Čipové karty s oběma implementovanými rozhraními (kontakt a bezkontakt) je
 - duální - pokud realizována jedním čipem
 - hybridní – se dvěma čipy

Vyšší nároky na bezpečnost

- Trend – technologický vklad primárně do funkcí, podporujících schopnosti identifikace, autentizace a elektronického podpisu.
- Trend zajištění bezpečnosti operací:
- Citlivé oblasti dat, jako jsou například šifrovací klíče, neopustí nikdy bezpečné prostředí čipu karty, nelze je číst, lze jen provést kryptografické operace přímo na kartě
- Autentizace držitele karty vůči kartě (PIN, biometrie)

Nová generace karet

- Masové nasazení uvedených technologií v posledních letech ve světě
 - Na rezortním principu v různých zemích:
 - Občanské karty
 - Veřejná správa
 - Armáda
 - Bankovníctví
- Trend snižování cen smart karet

- Statistika využití karetních aplikací v ČR
 - pro státní organizace a veřejnou správu (2001)
 - 80% organizací má karetní systém, z toho
 - 40% organizací má přístupový systém
 - 26% docházkový, 19% stravovací, 15% parkoviště, přístup k počítačům, ke kopírkám
 - 79% bezkontaktní čipové karty a karty s mg pruhem (11%).

Harmonizace se standardy

- Zastřešující rámec
 - eEurope Smart Card Charter (eESCC)
 - Cílem je harmonizovat vývoj a využití čipových karet důsledně na bázi standardů
 - Výsledkem Common Specification 2:
 - postupy, standardy, architekturu, modely a technické specifikace pro dosažení interoperabilní infrastruktury „Evropské čipové karty“

Smart karta - požadované funkce

- Identifikace držitele
- Obecně bezpečné řešení přístupů
- Autentizační funkce
- Bezpečný nástroj pro elektronický podpis
- Nástroj pro ochranu dat pomocí šifrování
- Multifunkčnost a implementační otevřenost

Technologické předpoklady

- Jak lze splnit očekávání pomocí technologie nové generace posledních let?

Přínosy současné technologie

- Oblast HW – architektura, kapacita paměti
- Operační systémy
- Komunikace podle ISO 7816, ISO 14443
- Bezpečnost, kryptografické funkce
- Funkcionalita
- Společný jmenovatel: pokrok na poli standardizace

Technické parametry

- Typický čip pro smartcard z r.2003
 - 32-64kB ROM
 - 16kB EEPROM
 - 2,3kB RAM
 - Kryptografický koprocessor (3DES)
 - [Kryptografický koprocessor (RSA)]
 - Rozměry 4,28 x 4,96 mm

Charakteristiky karty

- Rozhraní: kontaktní bezkontaktní/duální
- Varianty OS
- Komunikace podle rozhraní: ISO 14443, ISO 7816
- Kryptografie: 3DES, RSA1024 (RSA 2048)
- Požadavek: Update funkcí/aplikací

Neúplná standardizace

- Souborový systém
- Administrace podle ISO 7816-9
 - Nikoliv proprietární (create/delete file)
 - Porovnání s ISO 7816-4
 - Select, Read / Update Binary
 - Verify, Internal, External, Mutual Authenticate
 - Podpora aplikací MIFARE

Výrobce karty

Dostupnost technické podpory

Konzultace

Dodání technické specifikace

Pružnost výrobních a obchodních podmínek

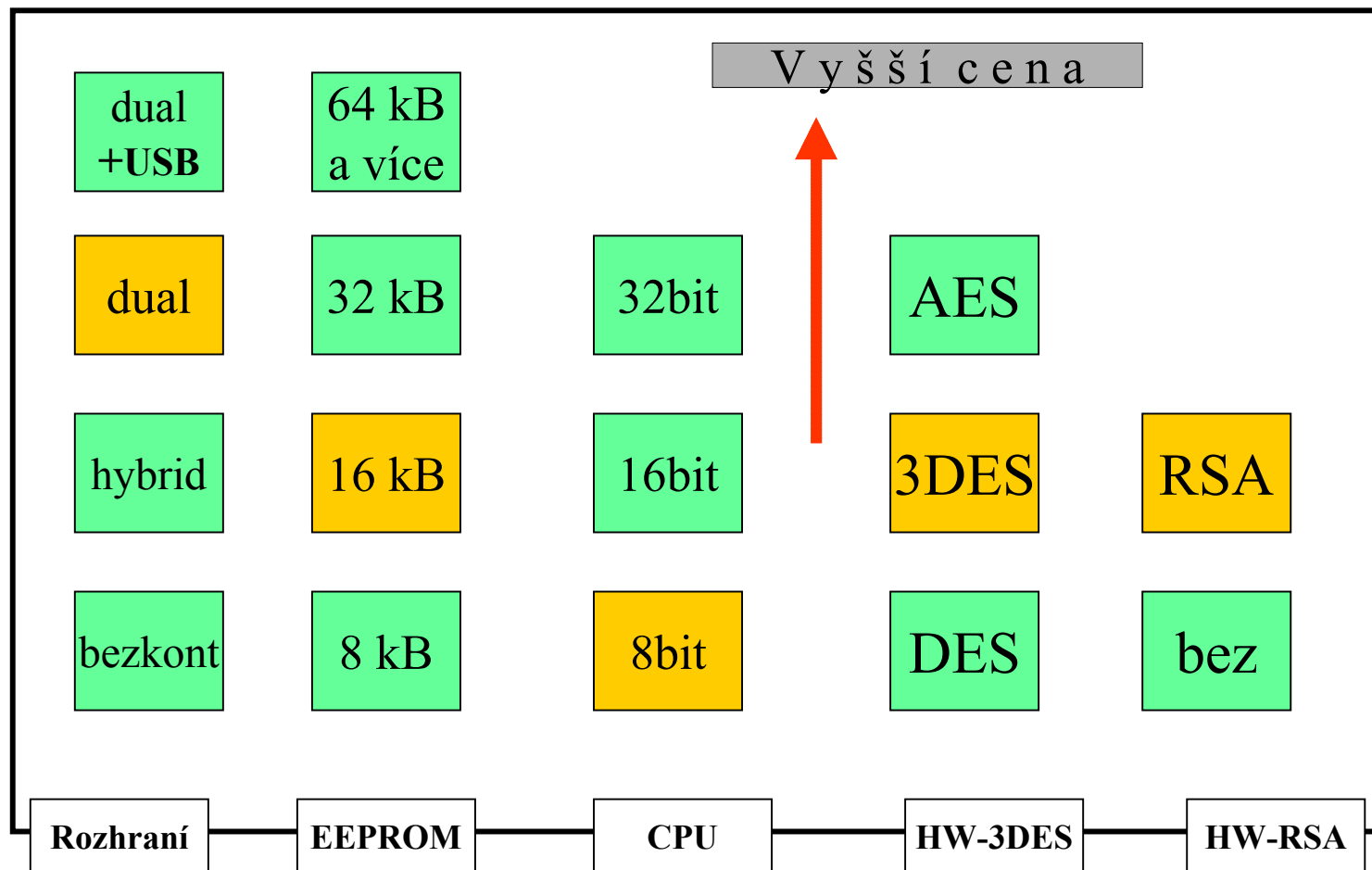
Implementace kryptografie

Algoritmus	Doba	HW/SW
DES	4-8 μ S	HW
3DES	<100 μ S	HW
RSA 1024	80-800ms	HW
SHA-1		SW

Interoperabilita

- Kdy karta a čtečka disponují interoperabilitou
 - Obecně - budou spolu komunikovat nezávisle na tom, od jakého jsou výrobce
 - Konkrétně - Čtečka ve VŠ1 přečte kartu z VŠ2, VŠ3, ...
 - Karta vydaná ve VŠ1 bude použitelná na VŠ2, VŠ3, ...
 - Problém k řešení v rámci pilotních testů pro bezkontaktní čtečky

Výběr ID karty



Širší kritéria výběru

- Přenositelnost funkcí (aplikací)
- Průmyslové standardy a trendy
- Nové funkce během životního cyklu
- Bezpečnost při mobilitě uživatelů
- Ohled nejen na současné provozní a aplikační potřeby – tříletý výhled
- Stupeň kompatibility k běžícím systémům

- Normalizace – výběr základních standardů
 - Postupy a metody vytváření systémů informační bezpečnosti
 - ČSN ISO/IEC TR 13335-(1-4) - Information technology - Guidelines for the management of IT Security
 - ISO/IEC 17799 (BS 7799) – Code of Practice for Information Security Management
 - ISO/IEC 14443
 - ISO/IEC 7816

Normalizace související

- Bezpečnost produktů informačních technologií
 - ČSN ISO/IEC 15408-(1-3) – Evaluation Requirements for IT Security (tzv. Common Criteria)
- Kryptografické moduly
 - FIPS PUB 140-2 : 2000 (Federal Information Processing Standards) – Security Requirements for Cryptographic Modules
- Certifikáty
 - X.509v3, v4 – Public Key Infrastructure

Projekty pro PKI karty

- Občanská karta (Itálie, Belgie, Skandinávie)
- PKI karty pro veřejnou správu
- CAC Common Access Card

Bezpečnost

- Algoritmická bezpečnost
 - Založena na standardizaci ověřených algoritmů
- Proprietární bezpečnost
 - Založena na utajené technologii

Smartcards (SC)

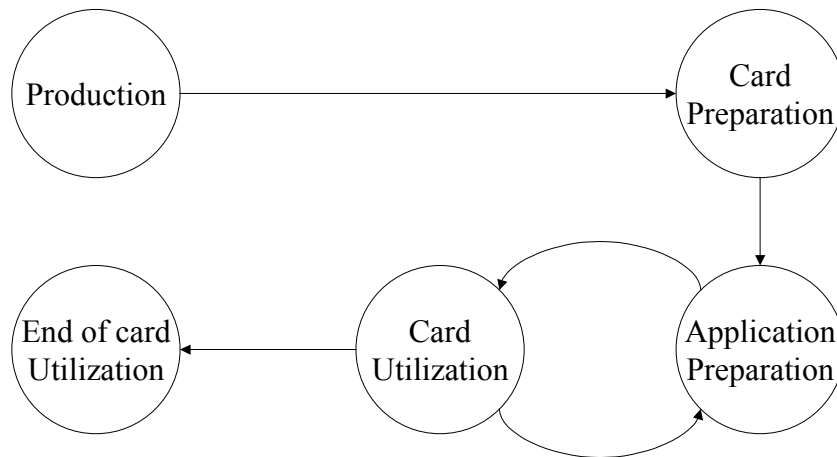
- Funkční charakteristika SC
- autentizace uživatele vzhledem ke kartě – znalost PIN – ochrana před zneužitím privátního klíče (v EEPROM) – po násobném neúspěšném zadání je karta blokována
- identifikační data – privátní a veřejný klíč + certifikát
- kryptografické algoritmy
 - asymetrické (RSA – klíč 512, 768, 1024 bitů)
 - symetrické (DES nebo 3DES)
 - generátor náhodného čísla RNG
 - hash algoritmy (SHA-1, MD5)
- přenosové rozhraní – protokoly T=0 (znakově orientovaný), T=1 (blokově orientovaný), T=CL (bezkontaktní)

Smartcards

- Další fyzické podoby čipový produktů - tokenů
- USB token – výhoda: nemusí se pořizovat čtecí zařízení – nevýhoda: nelze použít pro další aplikace (např. jako identifikační vchodovou kartu), má nižší životnost než SC
- Další kryptografické produkty – kryptografické moduly (HSM) akcelerátory – zásadní zrychlení kryptografických procesů a zvýšení bezpečnosti procesů
FIPS PUB 140-1/2 level 2, 3, 4

- Životní cyklus karty

Životní cyklus karty



Personalizace

- Optická
 - Embossing
 - Laser engraving
 - Printed picture
- Elektrická
 - Magnetic-stripe data
 - Memory chip or microcontroller

4. Fáze – používání karty

- Známa z každodenního života
- Lze přidávat a ubírat celé aplikace

5. Fáze – konec životního cyklu

- Typicky – skartování
- Existují příkazy, po jejichž provedení je čip nepoužitelný (přestane komunikovat)
 - např. TERMINATE CARD USAGE

Diskuse

- Shrňme: Cílem migrace na novou technologii pro ID-kartu VŠ je:
- mít na jedné karte dohromady:
 - a) el. prukaz studenta / zamestnance
 - b) nástroj fyzického přístupu
 - c) podpisové a šifrovací klíče
 - d) klíče jako nástroj přístupu k datum:
autentizace) k PC, intranetu, portálu, aplik.
 - e) místo pro přidávání dalších aplikací

Diskuse bod 2

O celkovém počtu a druhu aplikací nemusí být, díky výberu vhodného systému karty, rozhodnuto od počátku nasazení karty. Karta se chová tak trochu jako počítač u kterého můžeme přidat nebo smazat aplikace.

Diskuse bod 3

Lze používat i jako kartu s jedinečným identifikátorem pro staré aplikace. Teoreticky. Prakticky je nutno teprve overit u VŠ systému s MIFARE.

U některých systému dalších (cip e5560), je nutno upgradovat ctecky na vyšší frekvenci a podporu ISO14443. Toto začneme společne zkoušet v Plzni.

Diskuse bod 4

- Podpora šifrované a podepsané komunikace v rámci VŠ, postupně všude, kam „dohlédne“ PKI propojená s dalšími systémy PKI/CA vhodnou topologií (VŠ v dalších městech, akademická obec, zahraničí napr. přes cross-certifikáty nebo i ve stylu obdobném PGP)