
MONET+
THE MEMBER OF THE SMART WORLD
Hybridní čipové karty
Využití kontaktního čipu
(nejen v projektech studentských karet)
UNINFOS 2010, 3.- 4.11. Trnava
www.monetplus.cz
1


MONET+
Kdo jsme a co umíme …
Specialista na distribuované systémy s čipovou technologií
Transakční systémy
systémy akceptace bankovních platebních karet, aplikace pro platební terminály
bezpečná řešení k provozování nejrůznějších typů platebních a věrnostních systémů
Elektronická identifikace a autentizace
systémy bezpečné identifikace a autentizace v elektronických komunikačních kanálech
využití elektronických certifikátů ve vnitrofiremním prostředí (PKI)
eGovernment řešení
speciální řešení pro oblast státní správy, biometrika, mýtný systém
Personalizační systémy & Speciální řešení
řešení umožňující vydávání karet a moderních identifikačních průkazů
služby personalizační laboratoře
více než 70 zaměstnanců
sídlo Zlín
založení v roce 1996
významný hráč oboru
na středoevropském trhu
Kanceláře v Praze a v Bratislavě
www.monetplus.cz
2

Reference
... aneb kde jsme po sobě zanechali stopu

Česká republika

STC - Cestovní doklad s biometrickými prvky
- Systém pro personalizaci všech typů elektronických cestovních dokladů (e-pasů), bezpečnostní a kryptografická podpora systému vydávání e-pasů

ČSOB
- Dodávka aplikačního vybavení platebních terminálů a centrálního systému pro akceptaci bankovních karet

Česká správa sociálního zabezpečení
- Implementace PKI, řešení životní cyklu hybridní čipové karty
- Autentizovaný přístup všech zaměstnanců do interních IT systémů

Komerční banka
- Dodávka komponent pro vzdálenou autentizaci klienta internetového bankovnictví pomocí čipové karty

Další reference:
NKÚ, ČSÚ, NBÚ, Česká Pošta , Česká spořitelna, Benzina, Čepro, Ahold, Tipsport, Erpet, SynotTip, Telefonica O2, Sazka, AGEL, …

Slovensko

Slovnaft
- platební systém KREDIT, věrnostní systém BONUS, akceptace bankovních platebních karet, akceptace MOL karet a dalších mezinárodních fleet karet
- dodávky karet a personalizačních služby, dodávky platebních terminálů včetně všech aplikací

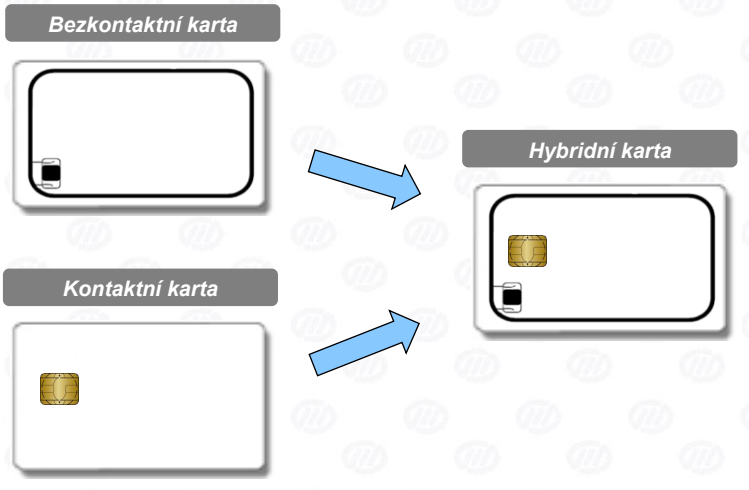
Elektronické mýto
- Aplikační vybavení distribuovaných míst akceptujících bankovní platební karty, centrální systém pro podporu autorizace bankovních platebních karet
- akceptace fleet karet, centrální systém pro podporu autorizace fleet karet

VÚB
- Dodávka klientských komponent pro zabezpečení internetového bankovnictví - karty, middleware, čtečky, …

Další reference:
Kancelária NR SR, Prvá stavebná sporiteľňa, Spoločná zdravotná poisťovňa, Orange, Tatra Banka, Poštová banka, EMtest-SK, Disig, Žilinská univerzita v Žilině, …

www.monetplus.cz 3

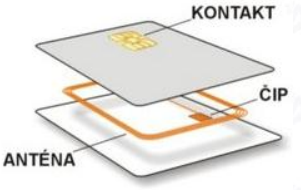
Co je hybridní čipová karta?



www.monetplus.cz 4

Základní vlastnosti hybridní čipové karty

- **Tělo karty**
  - ISO 7810, 7813
  - Materiál - PVC, PET, PC, …
  - Grafický design, bezpečnostní prvky, personální data
- **Bezkontaktní čip**
  - Dominantně ISO 14443 (Mifare, DESFire, DESFire EV1)
- **Kontaktní čip**
  - ISO 7816
  - FIPS 140, CC EAL 4+
  - Java Card 2.2.1, Global Platform 2.1.1



Proč hybridní čipová karta?

Spojení výhod kontaktní a bezkontaktní technologie v jednom médiu

- **Tělo karty**
  - Vizuální identifikační průkaz (zaměstnanec, ISIC, ITIC), reklamní plocha
- **Bezkontaktní čip**
  - Nástroj pro řízení fyzického přístupu, evidenci docházky, stravování, ubytování, využití v dalších interních systémech
  - Časové jízdenky a ticketing pro MHD
- **Kontaktní čip**
  - Autentizovaný přístup uživatele do IT systému organizace (PC, VPN, …)
  - Elektronický podpis, šifrování
  - Platební a věrnostní funkce

Hybridní karta – typy kontaktního čipu

- **Paměťový čip**
  - Žádná bezpečnost ani kryptografie
  - Jednoduché médium pro čtení/zápis dat

- **Procesorový čip**
  - OS, základní kryptografické nástroje (symetrická kryptografie)
  - Platební a věrnostní funkce

- **Procesorový čip s RSA koprocesorem („PKI čip“)**
  - Vysoce výkonný čip s implementovanou asymetrickou kryptografií
  - PKI funkcionalita (autentizace a elektronický podpis)

www.monetplus.cz 7

Hybridní karta – integrace do systémů a aplikací

- **Bezkontaktní čip**
  - Speciální aplikace do speciálních čtecích zařízení (uzavřené systémy)

- **Jednodušší kontaktní čipy**
  - Speciální aplikace do speciálních čtecích zařízení (např. POS terminály)

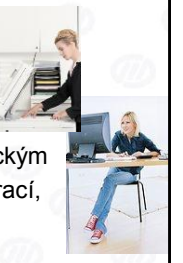
- **Kontaktní PKI čip**
  - Integrace do operačních systémů a aplikací prostřednictvím **MIDDLEWARE** přes definovaná rozhraní CryptoAPI a „Crypto service provider moduly“ (CSP, PKCS#11)
  - čtecí zařízení standardizována dle standardu PC/SC

www.monetplus.cz 8

Příklady využití hybridních čipových karet

- **Průkaz zaměstnance**
  - Průkaz zaměstnance pro vizuální kontrolu
  - Docházka, přístup, stravování, …
  - IT identifikace, autentizace a aplikační log-on

- **Studentská karta**
  - Průkaz studenta (ISIC)
  - Přístup, docházka, jídelna, knihovna, kopírka, parking, …
  - E-peněženka, slevy a věrnostní funkce
  - Autentizovaný přístup k IT zdrojům školy v kombinaci s elektronickým podpisem – zápis, volba přednášek, odevzdávání seminárních prací, písemné testy, …



www.monetplus.cz 9

Hybridní karta – studentská karta

ZKUŠENOSTI ZE SVĚTA

- Definování národního standardu
  - Polsko, Maďarsko, Slovensko, …
- Lokální implementace
  - Německo, Severní Amerika, Izrael, …
- Impulsy k rozvoji studentských karet
  - Interoperabilita a automatizace procesů
  - Rozšíření IT služeb a jejich bezpečnosti
  - Marketing a cross selling
- **Nejčastější technická podoba studentské karty**
  - **Bezkontaktní čip Mifare Classic / DESFire**
  - **Kontaktní PKI čip na platformě JavaCard**

Studentská karta
=
multifunkčnost

www.monetplus.cz 10

Specifika projektů hybridních studentských karet

- **Strategické otázky**
  - Definice priorit a cílů (funkčnost)
  - Interní potřeby univerzity společně s národním standardem
  - Financování (nejen karta, celá infrastruktura)

- **Technická specifika**
  - Personalizace a distribuce karet (bezkontaktní i kontaktní čip, multifunkčnost)
  - PKI infrastruktura (národní, univerzitní, fakultní)
  - Životní cyklus karet (certifikáty, výdej, ztráta, oprava, reklamace, …)
  - Multifunkčnost – aplikační a infrastrukturní rozvoj v čase
  - Projektové vedení a integrace

www.monetplus.cz 11

Děkuji za pozornost

Martin Tischer
martin.tischer@monetplus.cz

We **make** the world a **smarter** and **safer** place

www.monetplus.cz 12