ePasy - cestovní doklady nově s otisky prstů

Projekt CDBP

ISSS 2009
Hradec Králové, 6. 4. 2009
Ing. Petr Mayer, SI II

Obsah

1. Cíl projektu: Nový biometrický ePas
2. Organizace projektu
3. Harmonogram projektu
4. Základní architektura řešení
5. Koncové pracoviště
6. Biometrická fotografie
7. **Nově od 1. 4. 2009 otisky prstů**
8. Zabezpečení elektronické části
9. Zajímavosti projektu

Cíl projektu: Nový biometrický ePas pro občany ČR

Zavedeno na základě Nařízení Rady EU č. 2252/2004 o normách pro bezpečnostní biometrické prvky v cestovních pasech a na základě návrhů a doplnění Evropského parlamentu a Komise.

Čipový modul s vinutou anténou uložený v polykarbonátové kartě:

Organizace projektu

Zadavatel: Ministerstvo vnitra ČR

Generální dodavatel: STÁTNÍ TISKÁRNA CENIN, státní podnik

Projektová kancelář

Systémový integrátor I: Národní certifikační autorita

Systémový integrátor II: Návrh, výstavba a provoz

1. Centrální systém
2. Dohledové centrum
3. Kontaktní místa
4. Certifikační služby
5. Smluvní připravenost
6. Analýza rizik
7. Hotline CDBP

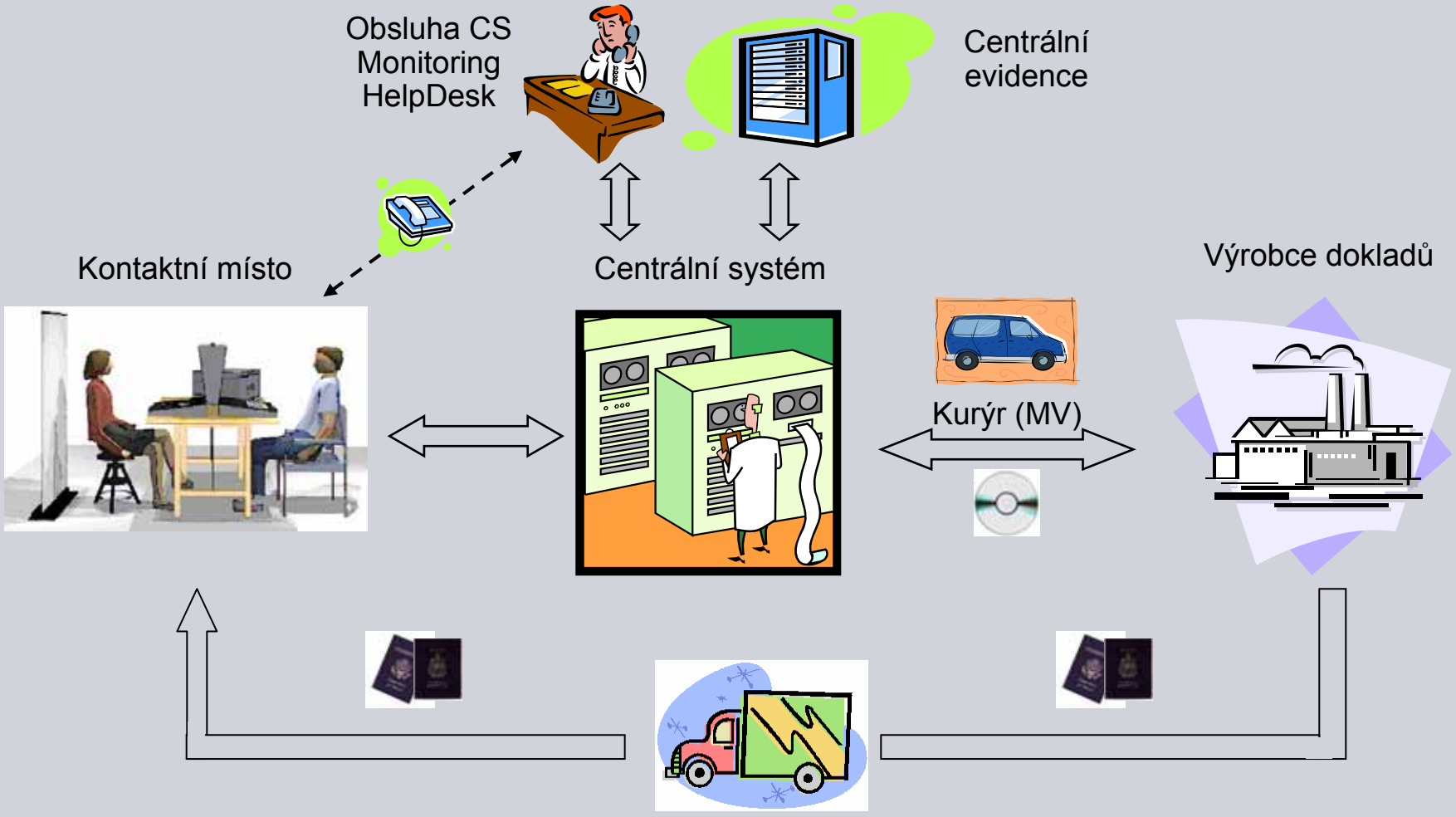
Systémový integrátor III: Personalizační systém

Systémový integrátor IV: Nezávislé testování

Harmonogram projektu

- Etapa 1: příprava projektu 12/2005 – 01/2006
- Etapa 2: implementace „Služba I – fotografie“ 01/2006 – 08/2006
- Etapa 3: provoz „Služba I“ 09/2006 – 03/2009
  implementace „Služba II – otisky prstů“
- Etapa 4: **provoz „Služba II“** **od 1. 4. 2009**

Základní architektura řešení



Koncové pracoviště

- 227 obcí s rozšířenou působností a cca 600 koncových pracovišť.
- On-line propojeno s centrálním systémem.

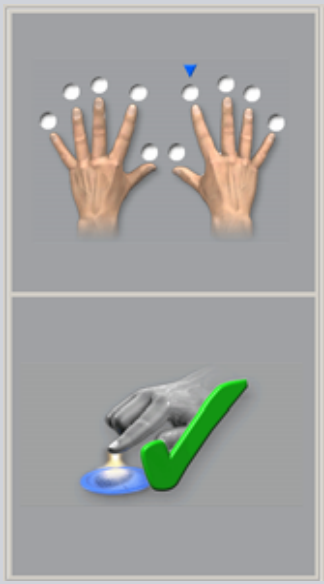
Biometrická fotografie

- Požadavky organizace ICAO definované v normě ISO19794-5 pro uložení zobrazení obličeje na RFID čip.
- Snímání fotografie na úřadě, nepoužívá se skenování donesené fotografie

International Civil Aviation Organization (ICAO)

Otisky prstů

- Doplnění biometrických dat v ePase o otisky prstů (primárně oba ukazováčky)
- Rozšíření zabezpečení dat otisků na čipu o EAC
- Rozšíření technologického a programového vybavení



Cíl: Zabránit neoprávněnému čtení pasu bez vědomí držitele.

Princip: Umožnit dekódovat data z čipu jen těm uživatelům, kteří dobrovolně otevřou doklad na datové stránce (čtení MRZ).

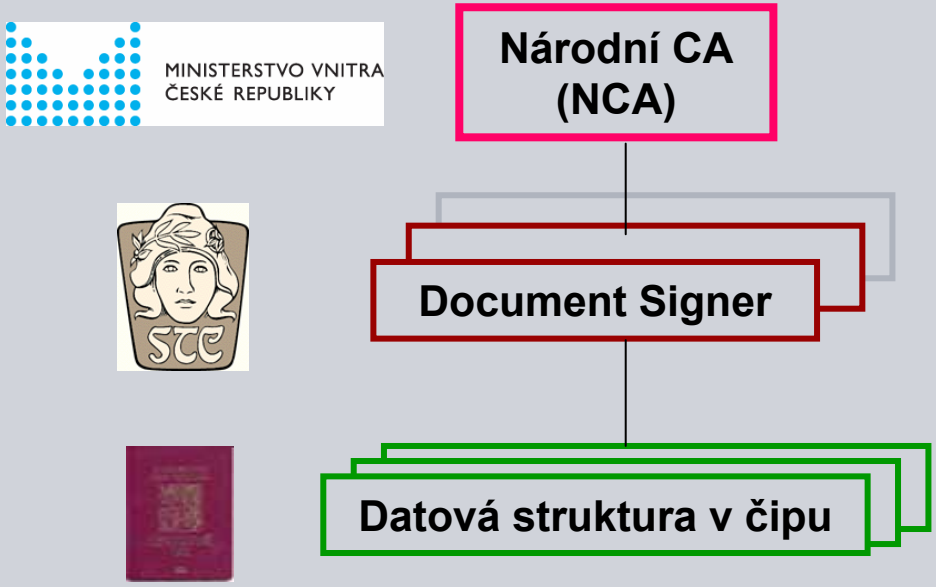
Postup:

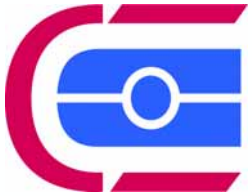
1. vložení otevřeného pasu do čtečky
2. načtení Machine Readable Zone („MRZ“)
3. z obsahu MRZ jednocestnou funkcí se vytvoří pří
   k čipu
4. vypočtené heslo použije k přístupu k datům v čipu

Zabezpečení elektronické části
2. Elektronický podpis dat v čipu

Cíl: Průkaznost pravosti dat v pasu.

Princip: Datová struktura v pasu je elektronicky podepsaná tzv. Document Signerem (výrobcem dokladu).





Zabezpečení elektronické části
3. Aktivní autentizace (AA)

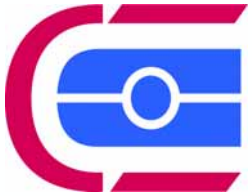
SIEMENS

Cíl: Zabránit kopírování obsahu čipu do jiného čipu (BAC tomu nebrání).

Princip: Při personalizaci čipu se vygeneruje veřejný a soukromý klíč. Soukromý klíč se uloží do nadále nedostupné části čipu, veřejný se uloží do datové struktury čipu.

Postup aktivní autentizace:

1. Čtečka provede čtení datové struktury z dokladu včetně veřejného klíče.
2. Čtečka vygeneruje náhodná data a pošle je do čipu.
3. Čip v pasu tato data elektronicky podepíše s využitím soukromého klíče a podepsaná data odešle do čtečky.
4. Čtečka ověří elektronický podpis dat pomocí veřejného klíče z datové struktury:
   - pokud se podpis podaří ověřit, je doklad v pořádku
   - pokud ne, může se jednat o falzifikát.



Zabezpečení elektronické části
4. Extended Access Control (EAC)

SIEMENS

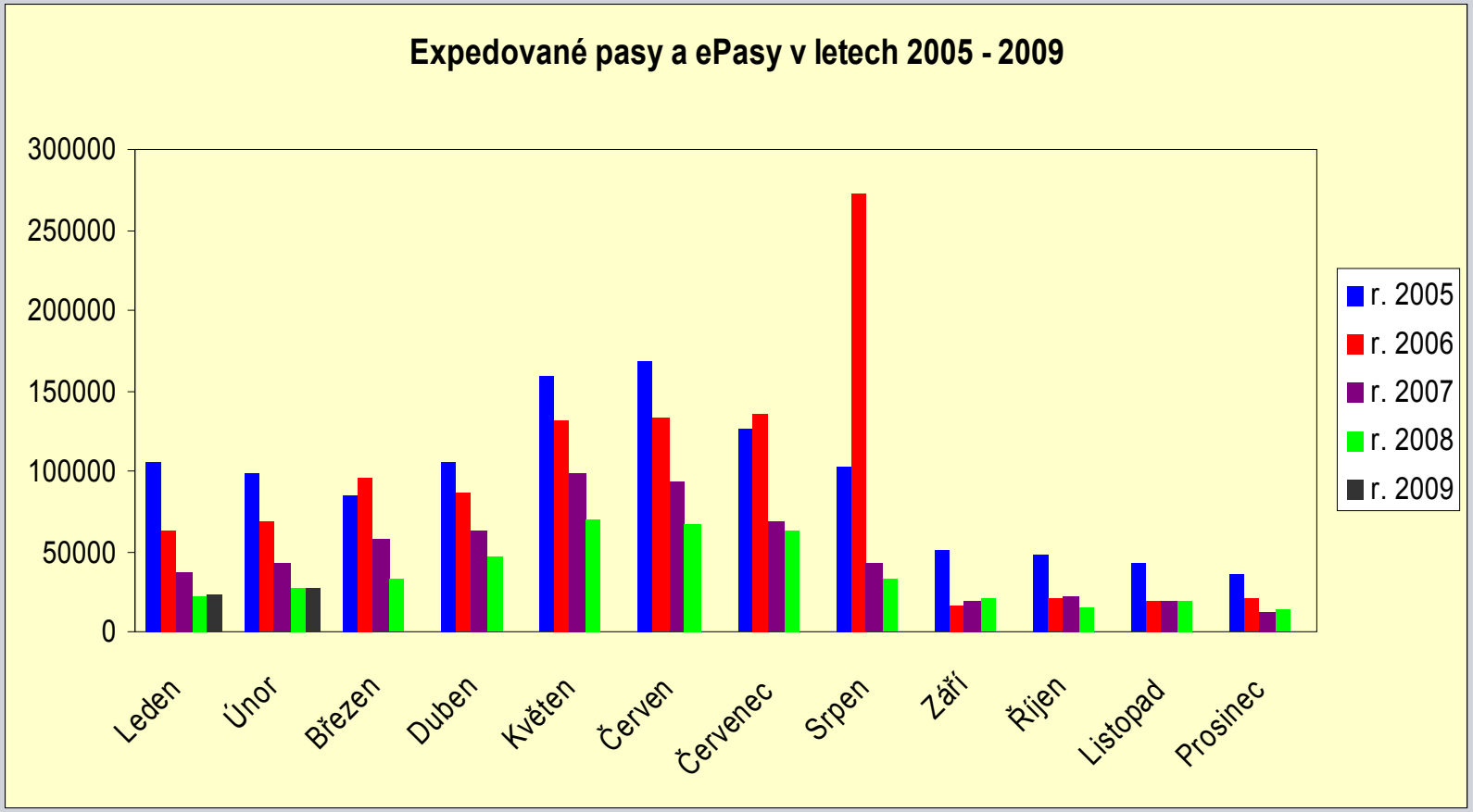
Cíl: Rozšířená ochrana čipu proti kopírování; autorizace inspekčních systémů (čtecích zařízení).

Princip: Rozšířená specifikace EAC v rámci nové legislativy EU zvyšuje zabezpečení ePasu s ohledem na zacházení s „citlivými údaji“ – otisky prstů.

EAC se skládá ze dvou autentizací:

- **Chip authentication (CA)** – ochrana proti kopírování ePasu. Založeno na algoritmu výměny klíčů Diffie-Hellman.
- **Terminal authentication (TA)** – zjištění, zda inspekční systém (čtečka) může či nemůže číst citlivá data z čipu. Nutnost budování další (nové) PKI infrastruktury.

Zajímavosti Projektu CDBP
1. Expedované pasy a ePasy v letech 2005 - 2009



Zajímavosti Projektu CDBP
2. Důraz na bezpečnost

SIEMENS

- Součástí projektu je bezpečnostní dokumentace
- Velký důraz na bezpečnost přístupu do systému a také na bezpečnost a ochranu dat občana:
  - žádná data se neukládají na lokálních pracovištích,
  - žádné biometrické údaje se neukládají do centrálních evidencí; z provozní databáze se mažou po 60 denní reklamační lhůtě,
  - shoda se zákony (os. údaje 101/2000 Sb., ISVS 365/2000 Sb., ...).

Zajímavosti Projektu CDBP
3. Rozsáhlý IT projekt

SIEMENS

- Prakticky první projekt eGovernmentu v ČR, ve kterém se všechna data načítají z ISVS, žadatel pouze podepisuje vygenerovanou žádost
- Velmi rozsáhlý IT projekt s celorepublikovým dopadem (620 pracovišť na 235 lokalitách)
- Plošné školení 1150 úředníků (spec. školící lokality; jednotlivě pro každou etapu projektu)
- Spolupráce s paralelním projektem na MZV (110 ZÚ)
- Implementace technologií v těsném sledu/předstihu s normami EU/ČR
- Plošné použití biometrických technologií
- Široký rozsah integrovaných komponent
- Výrazný mediální zájem, zejména v roce 2006
- Hlavní implementace během 8 měsíců

Děkuji za pozornost

Petr Mayer
vedoucí projektu

Siemens IT Solutions and Services, s.r.o.
Evropská 33a
160 00 Praha 6

e-mail: petr.mayer@siemens.com