

MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



# *MINISTERSTVO VNITRA*

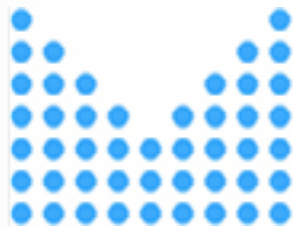
## *Projekt vydávání e-cestovních dokladů*

**Internet ve státní správě a samosprávě  
Hradec Králové, duben 2008**



# Agenda

- Vydávání e-cestovních dokladů – aktuální stav
  - rozsah projektu
  - příklady realizace na úřadech
  - aktuální změny v systému CDBP (vydávání e-cestovních dokladů pro děti do 5 let)
  - ochrana dat v CDBP
- Přípravy a zavedení otisků prstů do e-cestovních dokladů v ČR
  - plánované přípravy
  - testy SW
  - testy kvality
  - návrh EAC PKI



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



# ***VYDÁVÁNÍ E-CESTOVNÍCH DOKLADŮ – AKTUÁLNÍ STAV***

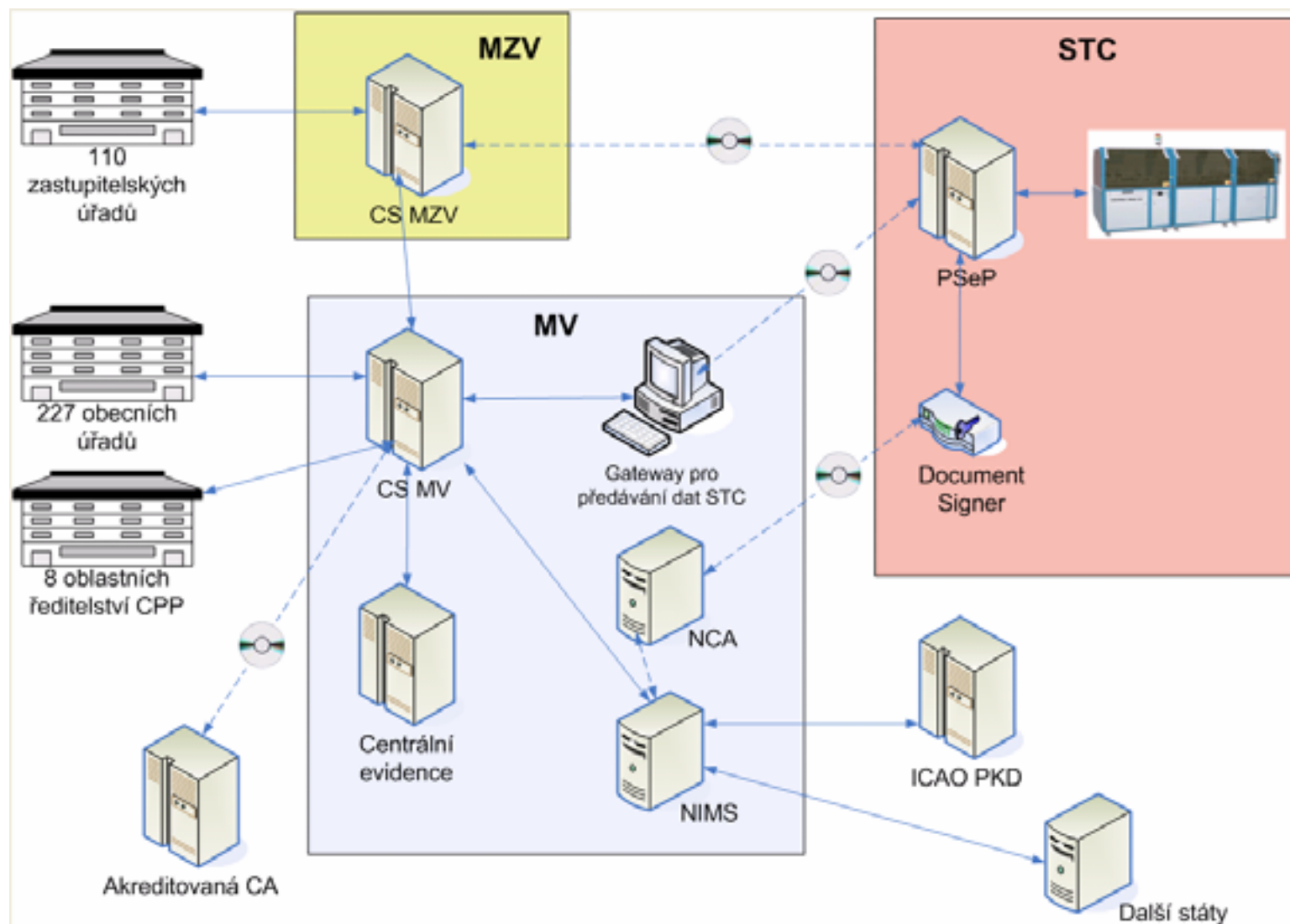


# *Rozsah projektu CDBP*

- Získání osobních a biometrických údajů
- Vydávané e-cestovní doklady
  - e-pas
  - cizinecký a uprchlický e-pas
  - diplomatický a služební e-pas
  - e-pas pro děti do 5 let (cca od poloviny dubna 2008)
- Hraniční systém pro kontrolu e-cestovních dokladů není zahrnut do projektu cestovních dokladů s biometrickými prvky (CDBP)



# Vydávání e-cestovních dokladů – architektura





# Rozsah projektu CDBP

- 227 úřadů (obecních úřadů obcí s rozšířenou působností)
  - cca 400 fotokabin, cca 200 výdejových pracovišť
- 8 pracovišť cizinecké policie
- Systém pro vydávání na obcích
  - centrální systém provozovaný MV, stanice on-line
  - fotografování žadatele na místě
- PKI (infrastruktura veřejných klíčů)
  - NCA, NIMS – provozováno MV; DS – provozováno STC
  - využíváno interně pro ochranu dat při přenosu, uložení a autentizaci subjektů (kvalifikované certifikáty pro tvorbu podpisu)
- Výroba a personalizace e-cestovních dokladů
  - STC
- Hotline CDBP
  - centrální místo podpory všech uživatelů v rámci systému CDBP

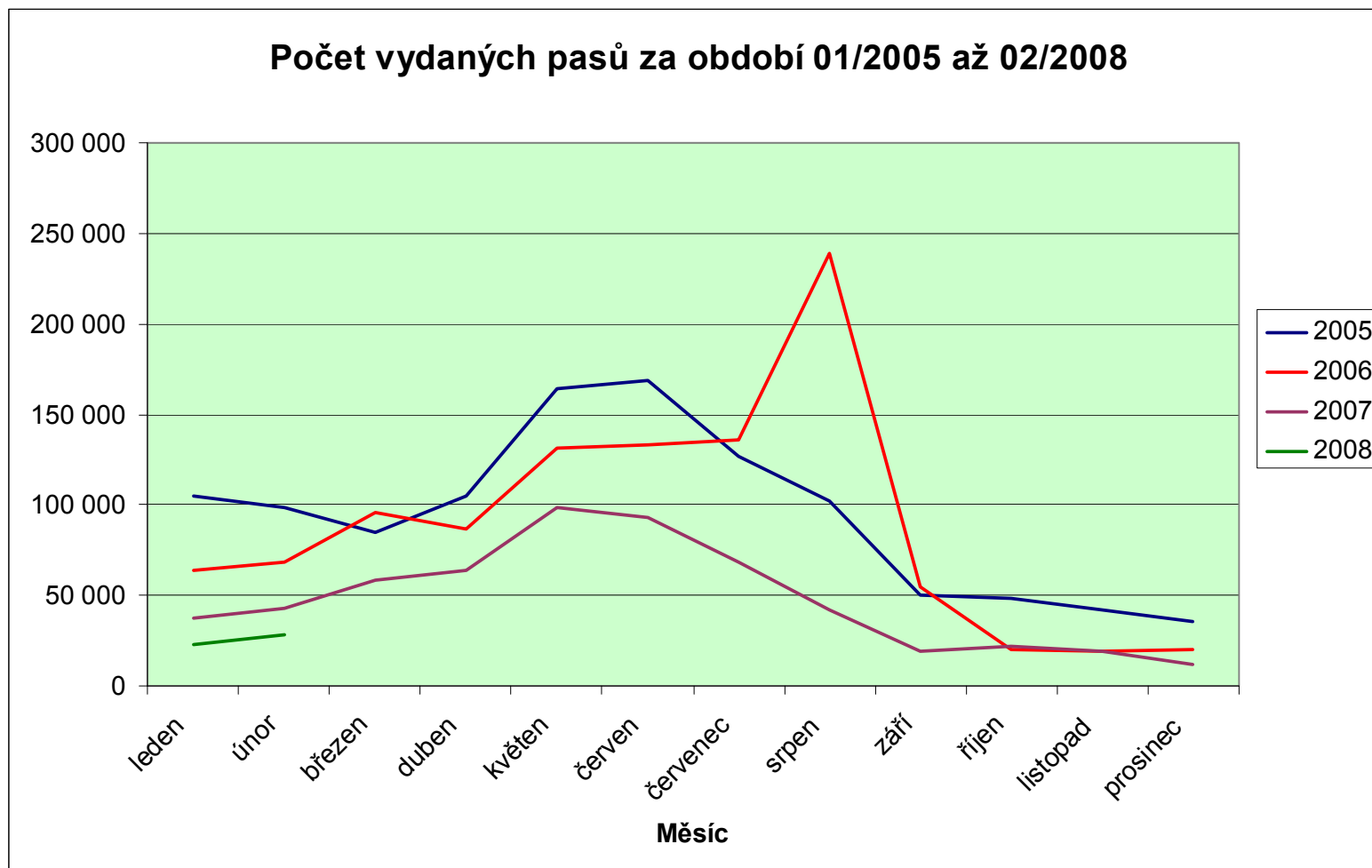


# *Celkový počet vydaných pasů*

<b>Rok</b>	<b>Vydané pasy</b>
2000	39 879
2001	417 518
2002	479 535
2003	642 477
2004	1 092 867
2005	1 131 085
01-08/2006	990 156

<b>Rok</b>	<b>Vydané e-pasy</b>
09-12/2006	78 531
2007	575 362
01-02/2008	44 339

# Vydané pasy (e-pasy)







# *Realizace na OÚ - Příklad 1*





# *Realizace na OÚ - Příklad 2*





# *Realizace na OÚ - Příklad 3*





# *Aktuální změny v systému CDBP*

## *e-cestovní doklady pro děti do 5 let*

- Vydávání e-cestovních dokladů pro děti do 5 let bude umožněno od nabytí účinnosti novely zákona o cestovních dokladech (cca polovina dubna 2008)
- Rozdělení dětí do 3 základních kategorií:
  - děti do cca 1 roku
  - děti ve věku cca 1 – 3 roky  
(do hmotnosti 15 kg)
  - děti ve věku cca 3 – 5 let

# *Pomůcky pro fotografování malých dětí*

- Dětský stupínek
- Pratelná podložka pro fotografování
- Dětská židlička





# *Některé možné postupy pro fotografování malých dětí ve fotokabině*

- V kabině může být přítomna včetně dítěte i doprovodná osoba, musí být mimo záběr fotoaparátu a nesmí zastiňovat žádné světelné těleso (mimo fotografování dítěte do 1 roku)
- Výsledná podoba žadatele nemusí zcela splňovat některé parametry určené pro fotografování žadatelů nad 5 let
- Konečné rozhodnutí o kvalitě pořízené fotografie je na úředníkovi (SW má jen podpůrnou funkci)
- Úřad si může stanovit vlastní postup fotografování dětí

# *Některé možné postupy pro fotografování dětí do cca 1 roku*

- Dítě na rameni doprovodné osoby
- Postup fotografování:
  - sednout si na otočnou židličku zády k fotoaparátu,
  - odhrnout si vlasy z ramena, na kterém bude držet dítě,
  - přehodit přes rameno pratelnou podložku pro fotografování tak, aby nebyla pokrčená a zakryla ty části těla doprovodné osoby, které jsou v oblasti budoucí fotografie dítěte,
  - bezpečně držet dítě na rameni tak, aby byla vidět jeho horní třetina (od prsou).



# *Některé možné postupy pro fotografování dětí do cca 1 roku*

- Dítě na rukou doprovodné osoby
- Postup fotografování:
  - sednout si na otočnou židličku čelem k fotoaparátu,
  - odhrnout si vlasy z ramena, u kterého bude držet dítě,
  - přehodit přes toto rameno pratelnou podložku pro fotografování tak, aby nebyla pokrčená a zakryla ty části těla doprovodné osoby, které jsou v oblasti budoucí fotografie dítěte,
  - bezpečně držet dítě tak, aby byl jeho obličej ve výšce fotoaparátu.





# *Některé možné postupy pro foto- grafování dětí ve věku 1–3 let (do 15 kg)*

## ■ Postup fotografování:

- přehodit přes opěrku židličky prateľnou podložku pro fotografování tak, aby nebyla pokrčená a zakryla všechny části židličky, které by mohly být v oblasti fotografie,
- posadit dítě do židličky a zapnout mu bezpečnostní upínací popruhy.



# *Některé možné postupy pro foto- grafování dětí ve věku 3–5 let (nad 15 kg)*

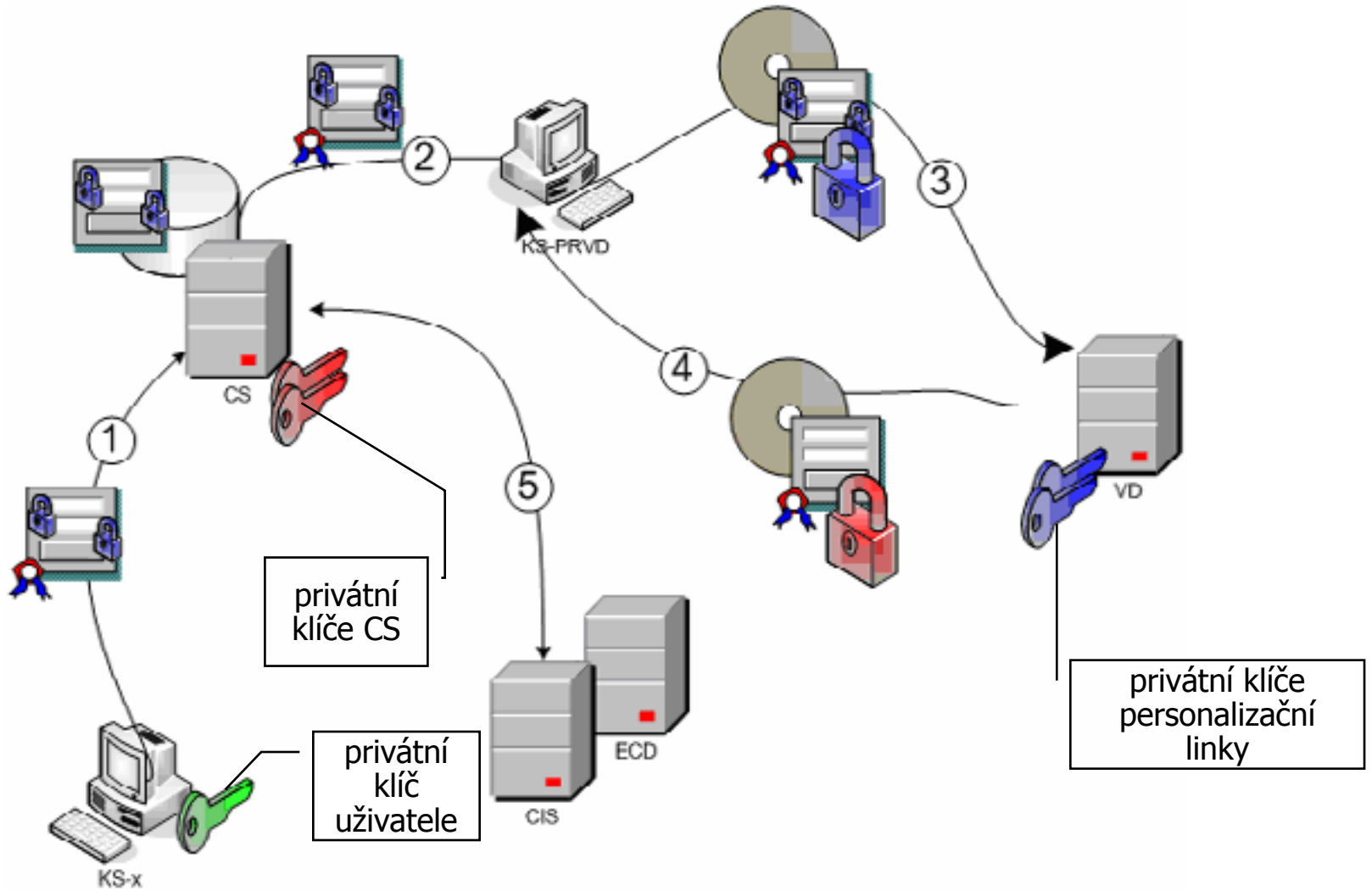
## ■ Postup fotografování:

- při tomto způsobu fotografování dětí se postupuje již standardně jako při pořizování žádosti pro osoby starší 5 let jen s tou podmínkou, že dítě stojí na stupínku.





# Ochrana dat v CBDP





## Ochrana dat v CDBP - legenda

Autentizace uživatele KS-x (1)	SSL s klientskou autentizací (čipová karta s privátním klíčem/certifikátem)
Integrita a autenticita dat (1,2,3)	Elektronické podpisy kvalifikovaným certifikátem <ul style="list-style-type: none"><li>■ uživatel podepisuje data žádosti za využití čipové karty</li><li>■ každá výměna dat mezi servery je zabezpečena elektronickou značkou (priv. klíč uložen v HSM)</li></ul>
Ochrana přenosového kanálu (1,2,5)	SSL s klientskou autentizací je nasazeno na všech komunikačních linkách (klient-server i server-server)
Důvěrnost dat – biometrie (1,2,3)	Jakmile jsou vytvořena biodata, jsou zašifrována s využitím veřejného klíče personalizační linky (MV nemá během přenosu přístup k biodatům)
Důvěrnost dat - dávky(3,4)	DVD obsahuje šifrované soubory
Vyhrazená síť	Veškeré on-line komunikace využívají interní dedikované síť MV



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



# *PŘÍPRAVA A ZAVEDENÍ OTISKŮ PRSTŮ DO E-CESTOVNÍCH DOKLADŮ*

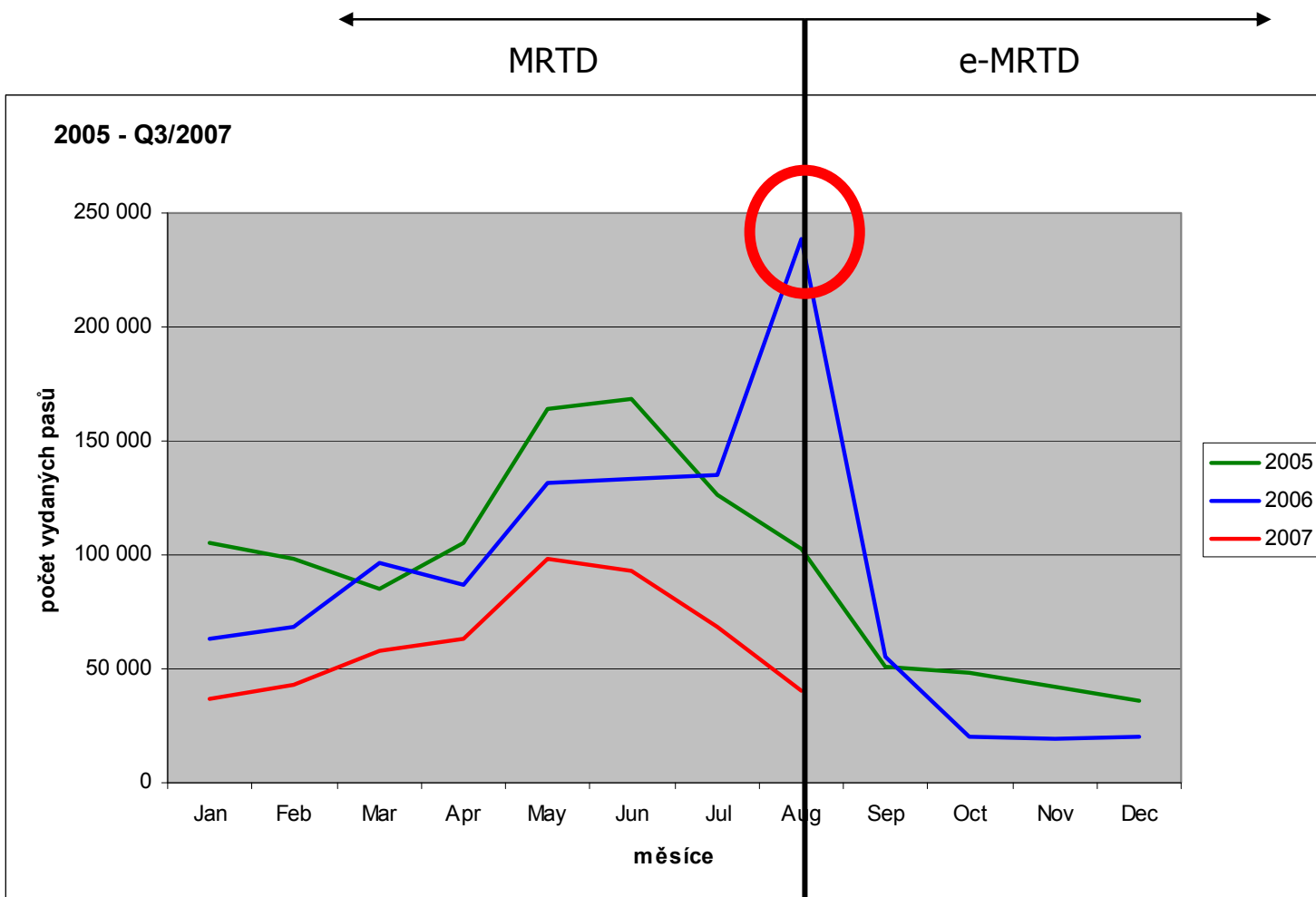


# Plánované přípravy

- ČR zahájí vydávání e-cestovních dokladů s otisky prstů od **1.4.2009**
  - nový termín určen na základě novely zákona o cestovních dokladech
  - původní termín 1.5.2008 byl posunut kvůli chybějícím technickým specifikacím EU pro ochranu uložených otisků prstů
- Velký dopad do současného systému
  - Nová verifikační infrastruktura – CVCA, DV
  - Nový čip a OS čipu
  - Nový HW/SW – HW snímání otisků, SW pro snímání otisků a upgrade centrálního systému
- Krátká doba
  - na implementaci projektu
  - pro dodavatele
- Přejít systému na e-cestovní doklady s otisky prstů proběhne během týdenní odstávky systému
  - po dobu odstávky nelze přijímat žádosti ani **vydat vyrobené e-cestovní doklady**



# Produkce pasů v období 2005 – Q3/2007 – ukázka špičky před přechodem na e-cestovní doklady





# *Testy kvality software, ověření proveditelnosti*

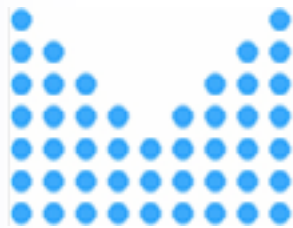
- Bylo provedeno testování kvality SW zamýšleného pro snímání otisků prstů
- Bude provedeno ověření proveditelnosti za účelem:
  - ověření funkčnosti HW & SW
  - získání zkušeností pro navržení procesu snímání
  - poskytnutí zdrojových dat pro úpravy právních požadavků na implementaci





# Testování kvality

- Testovací data - 12360 otisků od 515 osob (8 prstů, od každého prstu 3 otisky)
- Ověření, že SW vyhodnocuje korektně/správně kvalitu otisků podle normy NIST (NFIQ)
- Ověření algoritmu pro ztotožnění za účelem stanovení závislosti FAR/FRR na různé výši prahové hodnoty
- Výsledky:
  - vybraný SW pracuje korektně
  - konverze z formátu BMP do WSQ může zhoršit kvalitu otisku na nepřijatelnou úroveň (1%)
  - doporučení pro nastavení provozních parametrů algoritmu pro ztotožnění (prahová hodnota)



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



# *Návrh EAC PKI*

Pro vydávání pasů



# Členění EAC PKI pro dobu vývoje

- Jakmile je jednou e-cestovní doklad personalizován, lze ho číst pouze za použití odpovídajícího řetězce certifikátů
- Pro vývoj a testování budou použity následující varianty PKI
  - Produkční EAC PKI
    - Klíčový materiál v HSM
    - použitelné pro čtení platných e-pasů ČR
  - Testovací EAC PKI
    - Jelikož je využíváno pro testování včetně procedur nastavení HSM, klíče leží v HSM
    - Lze číst testovací pasy personalizované v testovacím prostředí
  - Ověřovací EAC PKI
    - privátní klíč ověřovací CVCA je publikován všem, kdo jej potřebují
    - EAC\_UTIL nástroj pro generování CVCA, DV a IS certifikátů
    - umožňuje čtení pouze vývojových e-pasů
    - bude používáno pro testy konformity
- Všechny výše uvedené typy e-cestovních dokladů jsou personalizovány v STC za využití odpovídajícího certifikátu CVCA





# Česká CVCA

V současnosti probíhají analytické a návrhové práce

- Splňuje požadavky EU a certifikační politiky EU
  - ČR aktivně pracovala na přípravě evropské certifikační politiky
- Implementace musí být dokončena dříve, než ostatní komponenty (kvůli přechodnému období)
- Personální problém
  - Mnoho rolí a současný požadavek na oddělení pravomocí generuje potřebu mnoha pracovníků
  - Není možný režim 24x7 – budou vyhrazena období, kdy budou přijímány žádosti o certifikát
  - Současný režim vydávání certifikátů na NCA (CSCA) bude využit i pro certifikáty CVCA



# *Potřeba DV pro vydávání e-cestovních dokladů*

- Výstupní kontrola při výrobě (DV1)
- Volitelné ztotožnění žadatele při předání e-cestovního dokladu
  - Obecní úřady (DV2)
  - Zastupitelské úřady (DV3)

- 
- CZE DV – pro kontroly Policie ČR

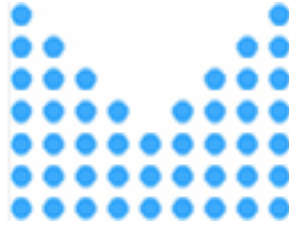
# DV1



## **DV1 - pro provádění výstupní kontroly ve výrobě:**

- Provozováno na personalizačním pracovišti (STC s.p.)
- Neprovádí se žádné zpracování načtených otisků
  - načtené otisky jsou použity pouze pro ověření, že e-cestovní doklad funguje a datové struktury jsou správně naplněné
- Spravuje 5 inspekčních systémů
- Privátní klíč Is je uložen centrálně
  - v téže lokalitě
- Podpora pro čtení pouze e-cestovních dokladů ČR

# DV2



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

## **DV2 – pro vydávání e-pasů v ČR:**

- Provozováno MV jako součást Centrálního systému
- Ztotožnění žadatele při předání e-cestovního dokladu
- Spravuje více jak 800 inspekčních systémů
- On-line přístup k centrálně uloženému privátnímu klíči
- Jeden sdílený privátní klíč pro všechny Is
- Privátní klíč je uložen v HSM
- Využíváno pro čtení e-cestovních dokladů vydaných ČR





# DV3

**DV3 - pro vydávání služebních a diplomatických e-pasů a e-pasů vydávaných na zastupitelských úřadech:**

- provozováno MZV
- ztotožnění při předání e-pasu
- Spravuje cca 110 inspekčních systémů (Is)