

Prezentace projektu ePas pro odbornou konferenci iDEME

Bratislava 19. června 2008

přednáší

**Ing. Tomáš Holenda,
ředitel odboru realizace projektů eGovernment MV**

Vytknuto před závorkou

Projekt ePas (projekt CDBP) je výsledkem práce zhruba 10ti odborných útvarů Ministerstva vnitra a je výsledkem úsilí cca 20ti odborných firem, koordinovaných Státní tiskárnou cenin, s. p.

Považuji si za čest
zde tento projekt za všechny zainteresované představit.

V prezentaci jsou použity některé slidy převzaté od řešitelů.

Osnova prezentace

- 1) Geneze problematiky biometrie
- 2) Výchozí právní situace, milníky
- 3) Zadání
- 4) Řešitelé
- 5) Řešení
- 6) Implementace
- 7) Provoz
- 8) Pohledem spoluřešitele
- 9) Pohledem uživatele
- 10) Zajištění bezpečnosti
- 11) Silné a slabé stránky projektu
- 12) Závěr

1) Geneze problematiky biometrie (I.)

- Celosvětová priorita pro víza, složité hledání konsensu
- Po útocích na New York v roce 2001 eskalace naléhavosti řešení
- Celosvětovou koordinaci sjednocení cestovních dokladů zajišťuje s mandátem OSN od roku 1947 ICAO (mezinárodní organizace civilního letectví)

Geneze problematiky biometrie (II.)

- Úspěchy ICAO v oblasti celosvětového sjednocování cestovních dokladů
 - Sjednocení položek na datové stránce
 - Zavedení strojově čitelné zóny
 - Doporučení pro biometrické prvky
- hlavní důvody pro biometrii: snaha odhalovat nelegální migraci, ztížit padělání dokladů, prokazovat případné změny totožnosti
- Dodatečné efekty:
 - 1) váš cestovní doklad nikdo nemůže zneužít,
 - 2) vaším jménem nikdo nemůže vystupovat.

Geneze problematiky biometrie (III.)

- Biometrický prvek:
 - Je zejména universální, jedinečný a stálý
 - Umožňuje jednoznačnou identifikaci osoby
 - Biometrickým prvkem je například:
 - Otisk prstu
 - Otisk dlaně
 - Sítnice oka
 - DNA
 - Pach
 - Styl chůze
 - ...

2) Výchozí právní situace, milníky

- 20. 6. 2003 v reakci na 11. září 2001 potvrzují členské státy EU v Soluni jednotný přístup EU k zavedení biometrie
- 13. 12. 2004 Rada ES vydává Nařízení č. 2252/2004 o normách pro bezpečnost a biometrické prvky v cestovních pasech a cestovních dokladech
- 28. 2. 2005 Komise vydává Rozhodnutí, kterým se stanoví technické specifikace norem pro biometrii v cestovních pasech
- 15. 6. 2005 Vláda ČR vydává Usnesení č. 740, kterým schvaluje Plán postupu ČR při implementaci Nařízení Rady
- 23. 12. 2005 podpis smlouvy s poskytovatelem služby
- 31. 3. 2006 prezident podepsal novelu zákona o cestovních dokladech, zákon č. 136/2006 Sb.
- 25. 8. 2006 vstupuje v platnost prováděcí vyhláška k novele zákona o cestovních dokladech (č. 415/2006 Sb.)
- 1. 9. 2006 **zahájení provozu služby I**
(tzv. zkušební provoz nad ostrými daty, tj. zahájení pořizování a zpracovávání žádostí o cestovní doklady s nosičem dat s biometrickými údaji, zkušební provoz potrvá až do nasazení otisků prstů, tedy do dubna 2009)

Intermezzo - obecná poznámka

- I když jsou celosvětové normy ISO, doporučení ICAO a směrnice EU velmi přísné z pohledu technologického (tedy co systém musí umožnit), řešení, která se vejdou do stanoveného rámce, je mnoho.
- Každý stát hledá v daném rámci obtížně vlastní řešení, které bude nejvíce vyhovovat jeho legislativním zvyklostem a technickým možnostem.
- Při přípravě celého projektu se naši pracovníci seznámili s řešeními v některých státech EU, každé je jiné, žádné z nich nelze kompletně převzít, vždy je třeba řešení upravit podle místních podmínek.
- Jedná se o úkol mimořádně náročný organizačně, legislativně, technicky i finančně.

3) Zadání

- Zadání bylo vypracováno na základě:
 - Znalosti doporučení ICAO, norem ISO, směrnic a doporučení EU
 - Členství v pracovní skupině ICAO
 - Členství v pracovní skupině EU pro víza
 - Rozborů a analýz
 - Konzultací s odbornými firmami
 - Poznatků z pracovních cest (včetně Slovenska)
- Situace byla výjimečná i v tom, že zákon se chystal souběžně a koordinovaně s tvorbou zadání služby
- Příprava zadání trvala cca 1,5 roku (od r. 2004)

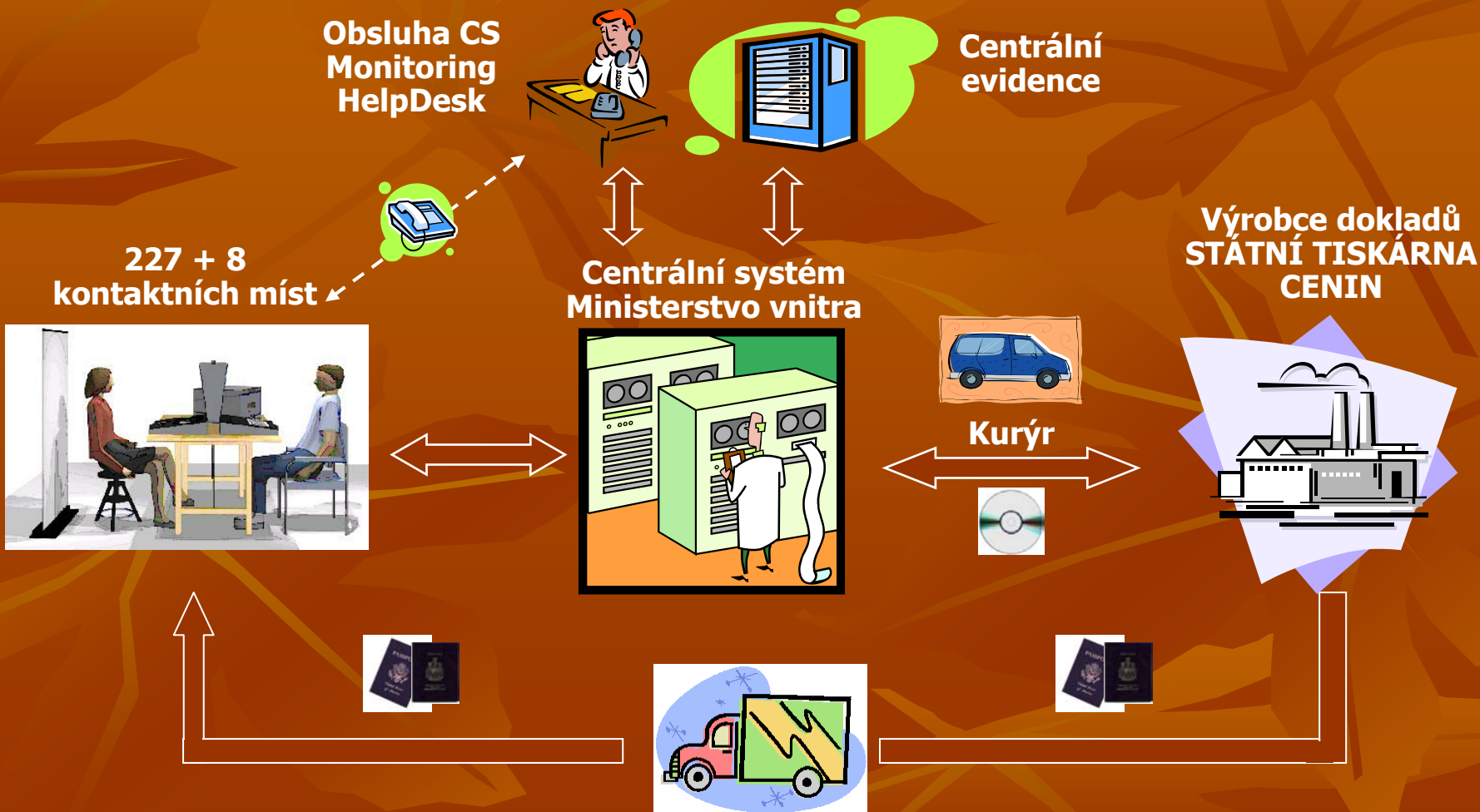
4) Řešitelé

- Generální dodavatel je **Státní tiskárna cenin, s. p.** byl osloven na základě zákona o zadávání veřejných zakázek (výjimka pro státní podnik zřízený za poptávaným účelem, utajované informace, § 4, odstavec 1, písmeno a) a k) zákona)
- Všechny subdodavatele již si vybíral generální dodavatel na základě jeho poptávek
- Hlavními subdodavateli jsou:
 - Logica CMG (projektová kancelář)
 - Siemens IT Solutions
 - Monet Plus
 - Secunet

5) Řešení

- Bylo detailně dopracováno již s řešitelem (obdoba nyní možného soutěžního dialogu)
- Před rozhodnutím o některých variantách byla prováděna měření na prototypch (například vyladění postupu úředníka při snímání podoby žadatele)
- Jako zadavatelé jsme měli velkou podporu vedení (řešení se muselo v termínu nalézt)

Řešení - architektura systému



Transport dokladů z STC na MV a z MV na kontaktní místa

6) Implementace

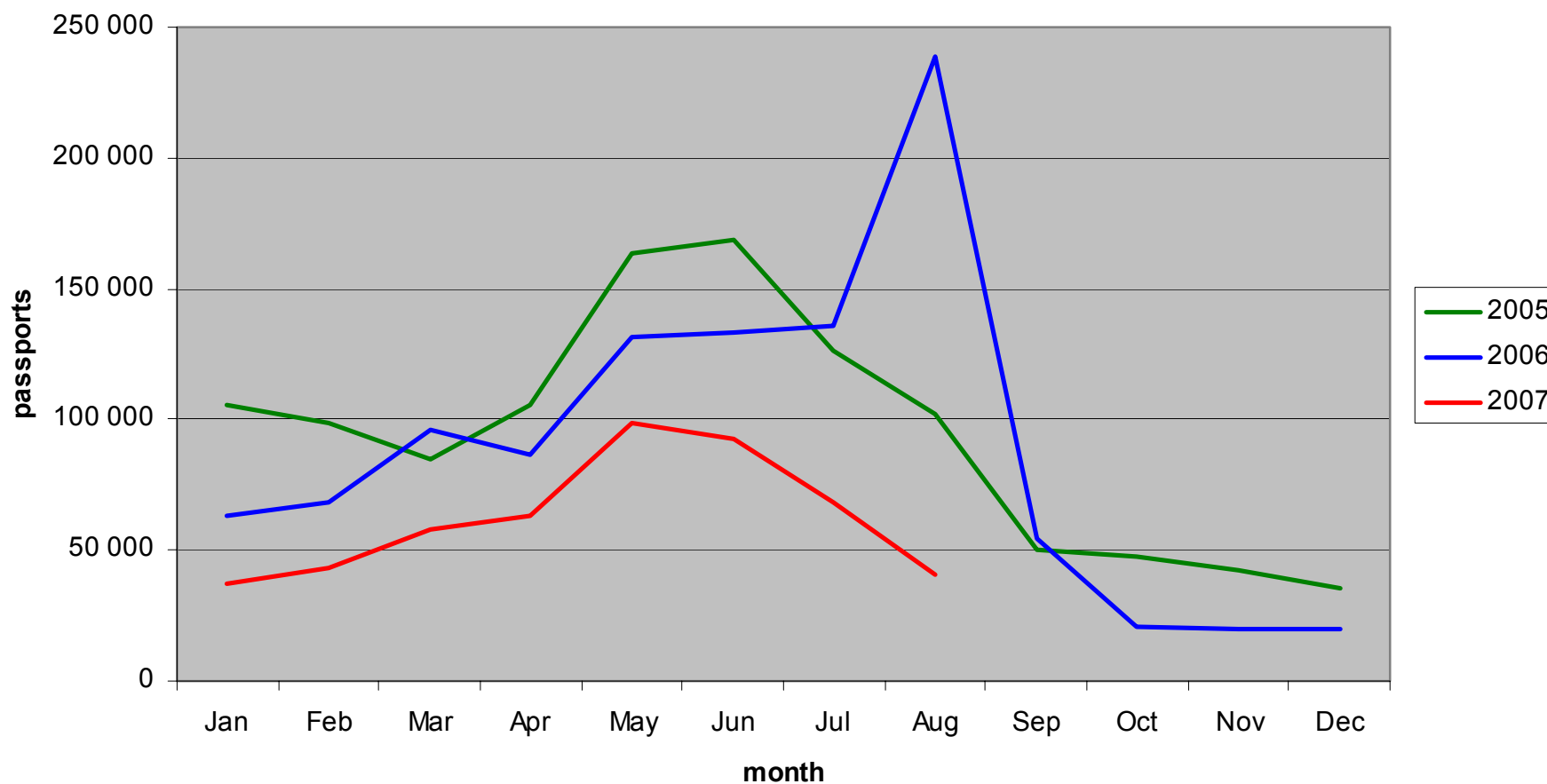
- Bylo potřeba k centrálnímu systému v celé České republice připojit:
 - 205 obcí s rozšířenou působností
 - 22 úřadů městských částí hl. m. Prahy
 - 8 pracovišť cizinecké policie
 - (jedná se o připojení vyhrazenou komunikační infrastrukturou, nikoli internetem)
- Konzultace s obcemi byly zahájeny ještě před schválením zákona i před podpisem smlouvy, v naprosté většině míst se jednalo o rozsáhlé stavební zásahy do budov (rozdílné vlastnické vztahy!!!), obce obdržely od státu příspěvek na tyto úpravy

7) Provoz (I.)

- Provoz byl zahájen jednorázově v celé ČR v pátek 1. září 2006, prakticky bez problémů (dílčí nedostatky Železný Brod a Praha 4)
- Od pondělí 4. září 2006 je systém v testovacím provozu s ostrými daty (tak tomu bude až do rozšíření systému o práci s otisky prstů, tedy do dubna 2009)

Provoz (II.)

2005 - Q3/2007



8) Pohledem spoluřešitele

- OIVS měl odpovědnost za:
 - Vyjednávání s obcemi o stavebních úpravách
 - Elektronickou část ePasu
 - Provoz NCA a NIMS
- Jednalo se o nejrozsáhlejší projekt, který náš civilní úsek na MV kdy realizoval
- Bylo vynikající zkušeností se podílet na práci týmů řízených profesionální projektovou kanceláří

9) Pohledem uživatele

- Systém jako takový je mimořádně spolehlivý, dílčí problémy v provozu jsou způsobeny zejména nedostatky v evidenci obyvatel, se kterou je systém on-line propojen
- Nejsou starosti s Help Deskem (smluvní služba)
- Je vynikající nemít starost ani o hlavní systém (vyladěná SLA), ani o koncová zařízení na obcích (smlouvy mezi poskytovatelem služby a obcemi, na rozdíl od našich dalších systémů)

10) Zajištění bezpečnosti (I.)

- Procesní bezpečnost (proces od počátku stavěn podle pravidel bezpečného systému)
- Objektová bezpečnost (obce, MV, STC)
- Mechanické a optické bezpečnostní prvky e-pasu
- Infrastruktura elektronických certifikátů (PKI)
- Mezinárodní standardy
- Šifrování elektronické komunikace
- Biometrické údaje z cestovních dokladů nejsou v ČR ukládány v databázích

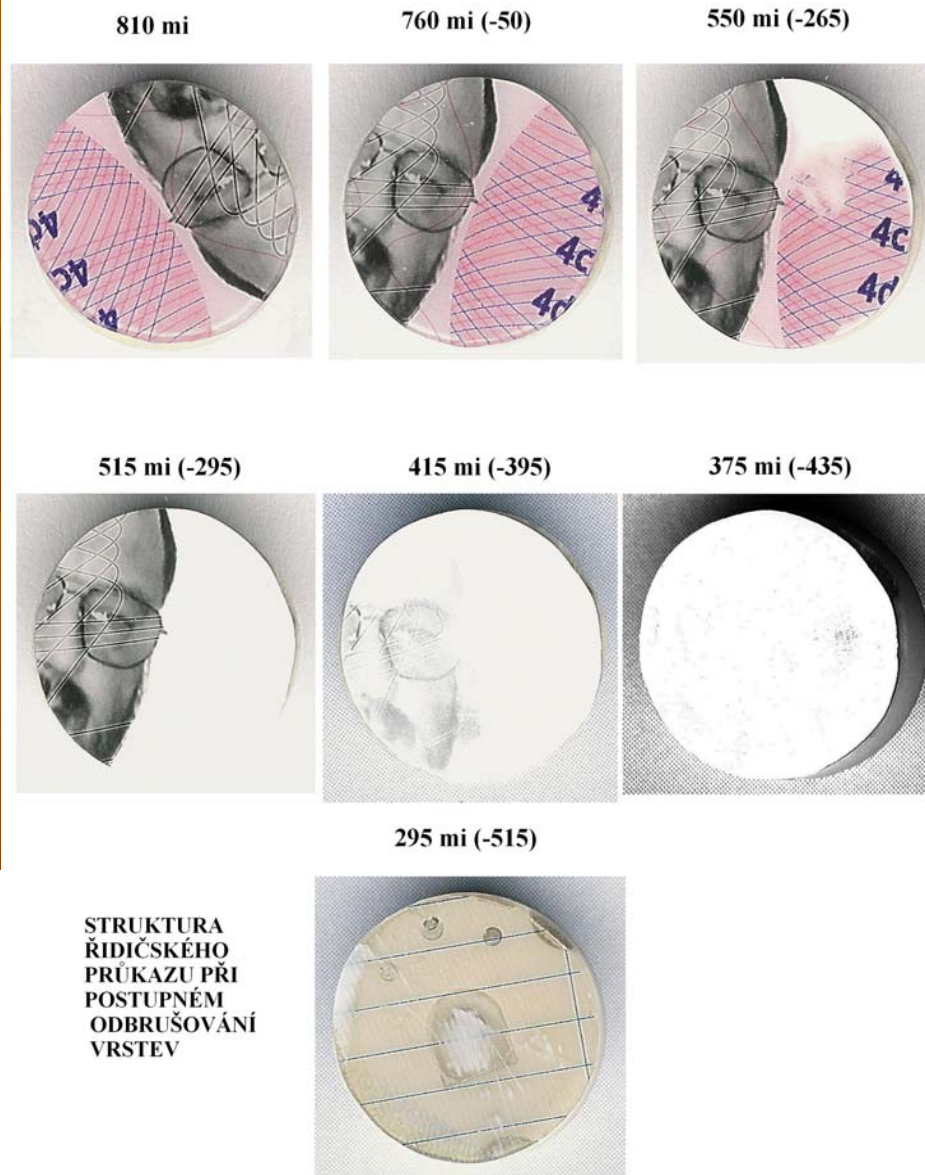


reliévní ražba



Zajištění bezpečnosti (III.)

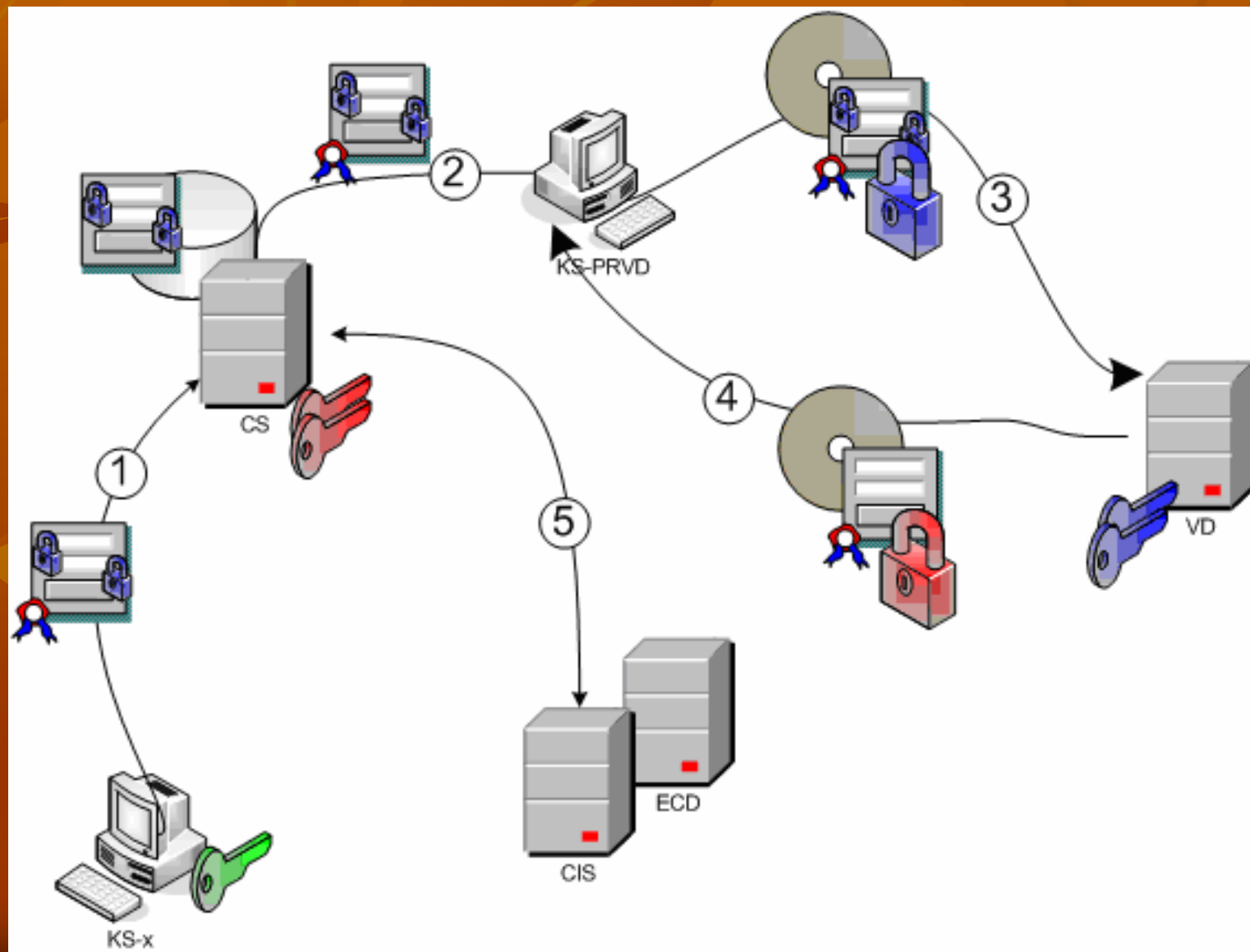
Ukázka postupného odbrušování vrstev polykarbonátu



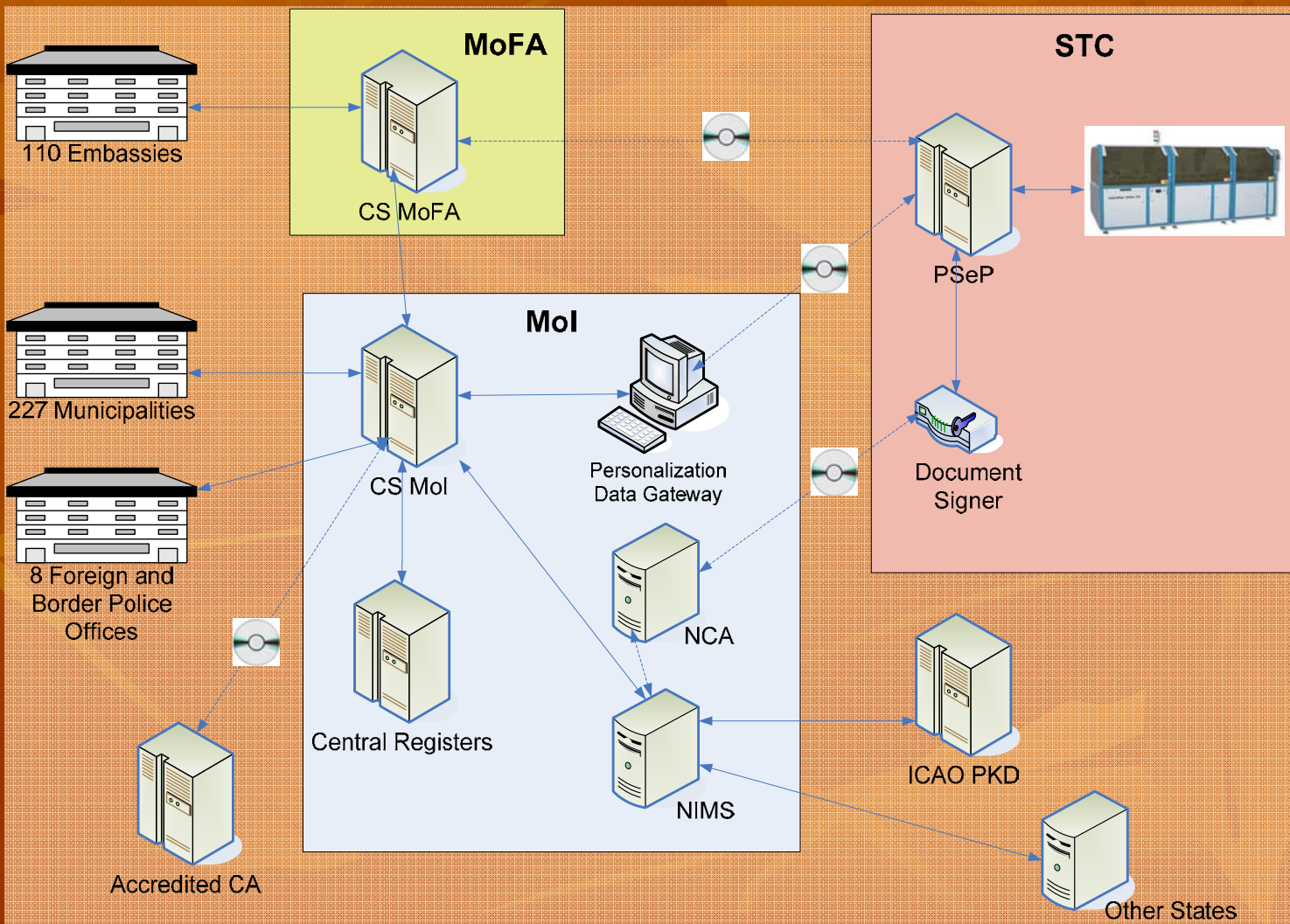
Zajištění bezpečnosti (IV.)

- Systém ePasu zajišťuje velmi vysokou ochranu osobních údajů na několika úrovních
- A) Basic Access Control (BAC)
 - Data nelze načíst bez znalosti algoritmu a bez znalosti MRZ
 - Čip v ePasu ČR nelze klonovat, aniž by se to u klonu zjistilo (na rozdíl například od SRN je v ČR u BAC použita ještě AA)
 - V případě neoprávněného načtení dat se jejich příjemce dozví stejně pouze informace, které lze získat z otevřeného pasu z datové stránky (stránka s fotografií a základními údaji)
- B) Extended Access Control (EAC)
 - Nejvyspělejší ochrana, kterou budou mít otisky prstů

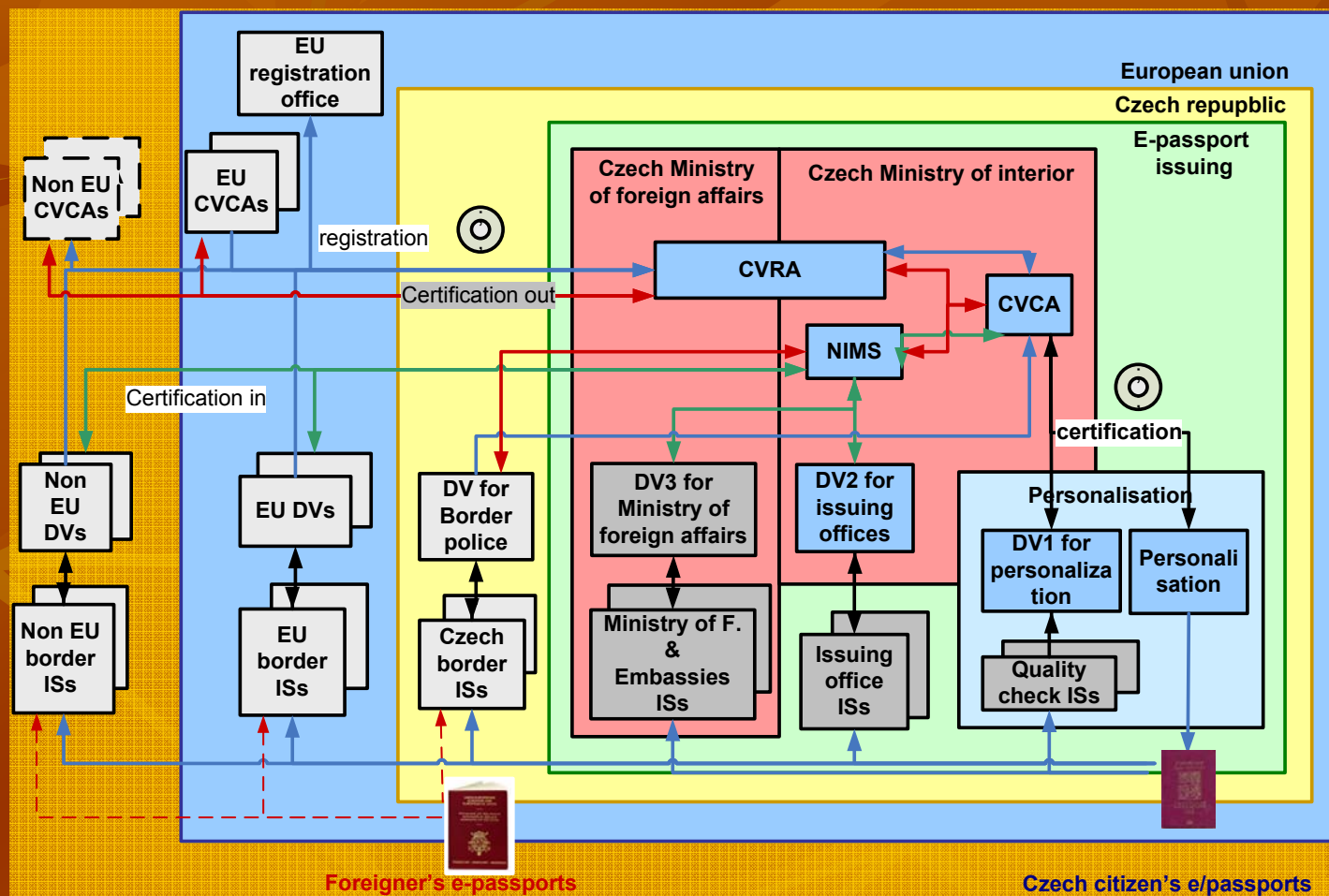
Zajištění bezpečnosti (V.)



Zajištění bezpečnosti (VI.)



Zajištění bezpečnosti (VII.)



Zajištění bezpečnosti (VIII.)

- „Vyprávené schéma“ komunikace ePasu a čtečky pro BAC (pro případ, kdy ePas není v pouzdru):
 - Komunikace není šifrována
 - Čtečka vysílá signály vhodné frekvence, ePas se ozve
 - Čtečka je schopna rozpoznat, že se jedná o ePas
 - Čtečka vyzve ePas, aby jí dal data:
 - Když nezná „heslo“, ePas mlčí, data nevydá
 - Když čtečka zná „heslo“ (je odvozeno známým algoritmem ze strojově čitelné zóny), pas data (z DG 1 a z DG 2) čtečce vydá
 - Je třeba mít na paměti:
 - ePas vydá pouze data, která stejně obsahuje datová stránka
 - V ČR použitá aktivní autentizace (AA) umožňuje poznat „klon“

Zajištění bezpečnosti (IX.)

- „Vyprávené schéma“ komunikace ePasu a čtečky pro EAC (pro případ, kdy ePas není v pouzdru):
 - Proběhne komunikace jako u BAC
 - ePas data z datové stránky vydá (ne otisky prstů z DG3)
 - Čtečka požádá ePas o další data (nešifrovaně, ale již pošle ePasu klíč, kterým bude očekávat zašifrovanou zpětnou komunikaci, tedy odpověď ePasu čtečce)
 - ePas (zašifrovaně podle předchozí odrážky) požádá čtečku o „heslo2“ (další komunikace je také šifrována)
 - Čtečka spočte aktuální „heslo2“ a pošle ho ePasu

Zajištění bezpečnosti (X.)

- Pokračování „vyprávěného schématu“ komunikace čtečky a ePasu pro EAC:
 - ePas má v paměti, že když se ho někdo zeptá certifikátem „A“, má mu odevzdat data, je ale třeba dále vědět:
 - Root certifikát má platnost 2 roky,
 - Provádí se jednou měsíčně řízená změna (upgrade) certifikátu,
 - Po dvou rocích tzv. „link certifikát“ překlene konec platnosti jednoho root certifikátu (2 roky), aby bylo možno zajistit životnost ePasu (10 let),
 - ePas si při komunikaci „dohraje“ potřebné upgrade certifikátů a aktualizuje si čas (čtečka tím, že upgrade má, dokazuje, že je v systému platně zapojena, že jí stát X dal důvěru a může číst)

Zajištění bezpečnosti (XI.)

- Ochrana proti odevzdání dat otisků prstů z ePasu (ze zóny DG3) neoprávněné čtečce:
 - Nedůvěryhodný stát od nás nedostane certifikát, čtečka v takovém státu data nepřečte (i kdyby byla tato čtečka zapojena v systému platně pro jiný stát, naše data nenačte, nebude mít „náš“ certifikát)

Zajištění bezpečnosti (XII.)

- Ochrana proti načtení dat otisků prstů zcizenou (zneužitou) čtečkou (v oprávněném i v neoprávněném státu):
 - Všechny čtečky jsou jednoznačně v systému identifikovány, při jejich ztrátě je možno každou jednotlivě okamžitě „zablokovat“ (obdobně, jako bankovní kartu u banky při její ztrátě/ztrátě důvěry)
 - Čtečka, která nebude platně zapojena v systému, nedostane měsíční upgrade certifikátů a tedy se nebude moci ePasu prokázat, že je ona ta oprávněná
 - Čtečka, která nedostane upgrade certifikátů sama řízeně „umře“ a lze ji oživit pouze připojením k systému (a v systému zneplatněná čtečka upgrade nedostane)
 - Vybrané čtečky podle „rizikovosti“ jejich umístění budou mít svou řízenou „smrt“ nastaveny rozdílně, od lhůty pouze na jednu směnu, (ruční přenosné), 24 hodin, více dní, týden, maximálně měsíc

11) Silné a slabé stránky projektu (I.)

■ Silné stránky:

- Plný soulad s podmínkami a pravidly ICAO i EU
- Systém „end to end“
- Robustnost
- Bezpečnost
- Vyladěný proces (úředník prakticky nemůže udělat chybu, občan se pouze podepíše, nic nevyplňuje)
- Konečným příjemcem služby je občan, který má vynikající bezpečný cestovní doklad pro celý svět

Silné a slabé stránky projektu (II.)

- Slabé stránky:
 - Nesladěnost se systémem MZV (scany místo fota)
 - Občasné vady v centrální evidenci obyvatel, které občas znemožní odbavit občana napoprvé (jedná se zejména o vady v datech místa narození)
- Sporné stránky:
 - Nutnost osobní návštěvy úřadu při nabírání žádosti i při vydávání dokladu

Závěr

Bylo mi potěšením
Vám tento projekt představit.

BONUSY

Nyní jsem pro Vás připravil nějaké
obrázky z projektu.

Testovací maketa e-pasu ČR



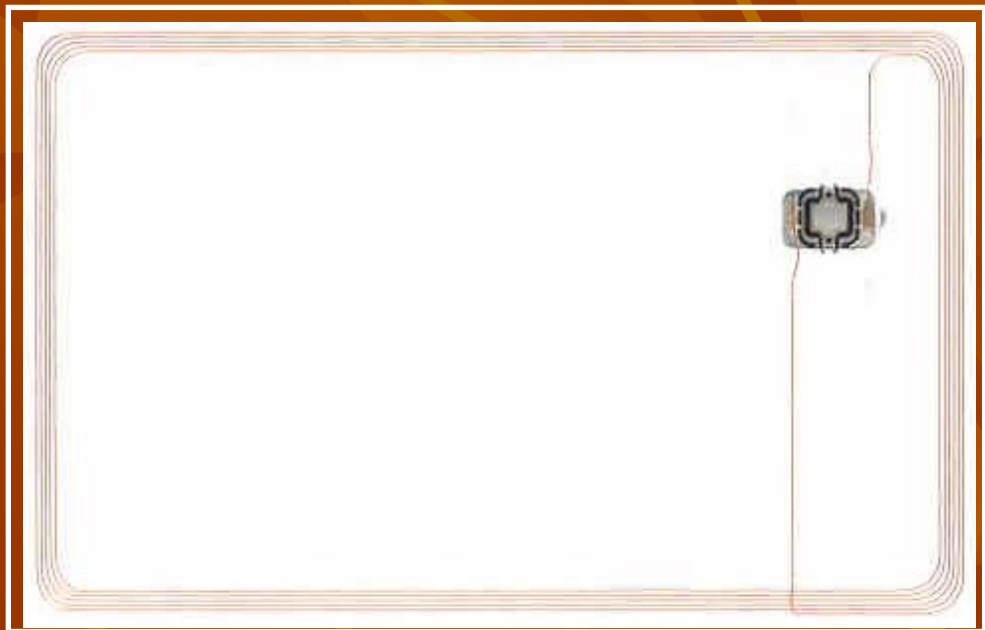
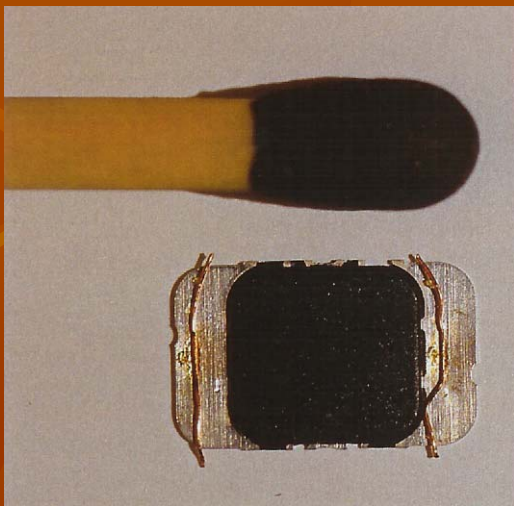
Kontaktní místo na obci - studie



CESTOVNÍ PAS / PASSPORT / PASSEPORT		ČESKÁ REPUBLIKA/CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE	
TYP/TYPE/TYPE P	KÓD/CODE/CODE CZE		ČÍSLO PASU/PASSPORT NO./PASSEPORT NO. 00001362
01 PŘÍJMENÍ/SURNAME/NOM SKOČDOPOLOVÁ			
02 JMÉNO/GIVEN NAMES/PRÉNOM VIKTORIE			
03 STÁTNÍ OBČANSTVÍ/NATIONALITY/NATIONALITÉ ČESKÁ REPUBLIKA / CZECH REPUBLIC		00001362	
04 DATUM NAROZENÍ/DATE OF BIRTH/DATE DE NAISSANCE 08.08.1982	11 RODNÉ ČÍSLO/PERSONAL NO./NO PERSONNEL 825808/8872		
06 MÍSTO NAROZENÍ/PLACE OF BIRTH/LIEU DE NAISSANCE FRÝDEK-MÍSTEK	05 POHLAVÍ/SEX/SEX F		
07 DATUM VYDÁNÍ/DATE OF ISSUE/DATE DE DÉLIVRANCE 18.07.2006	08 PLATNOST DO/DATE OF EXPIRY/DATE D'EXPIRATION 18.07.2016		
09 PAS VYDAL/AUTHORITY/AUTORITÉ BRANDÝS NAD LABEM-STARÁ BOLESLAV	10 PODPIS DRŽITELE HOLDER'S SIGNATURE SIGNATURE DU TITULAIRE 		
P<CZESKOCDOPOLOVA<<VIKTORIE<<<<<<<<<<<<<<<<<<<<<			
00001362<4CZE8208086F16071858258088872<<<<26			

Konstrukce e-pasu

- Čipový modul s vinutou anténou uložený v polykarbonátové kartě



Automatická hraniční kontrola - Austrálie



Automatická hraniční kontrola - Nizozemí



Budoucnost na hranicích – studie



Příklady realizace fotokabin v ČR (I.)



Příklady realizace v praxi (II.)



Příklady realizace v praxi (III.)



Příklady realizace v praxi (IV.)



Příklady realizace v praxi (V.)



Příklady realizace v praxi (VI.)



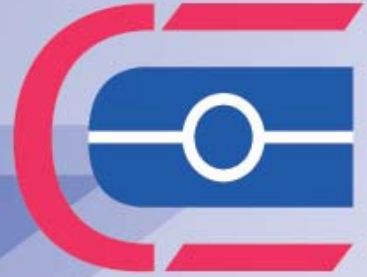
Příklady realizace v praxi (VII.)



Mobilní fotokabina (záložní řešení)



PROJEKT CDBP



Prostor pro vaše dotazy

(pokud je ještě čas ...)

Děkuji za pozornost (dovidenia)

Ing. Tomáš Holenda,
ředitel odboru realizace projektů eGovernment
mail: tholenda@mvcv.cz