Elektronické doklady a eGovernment

Konference Internet ve státní správě a samosprávě 2007

KC Aldis, Hradec Králové, 2.-3.dubna 2007

Filip Hajník

Senior Business Consultant

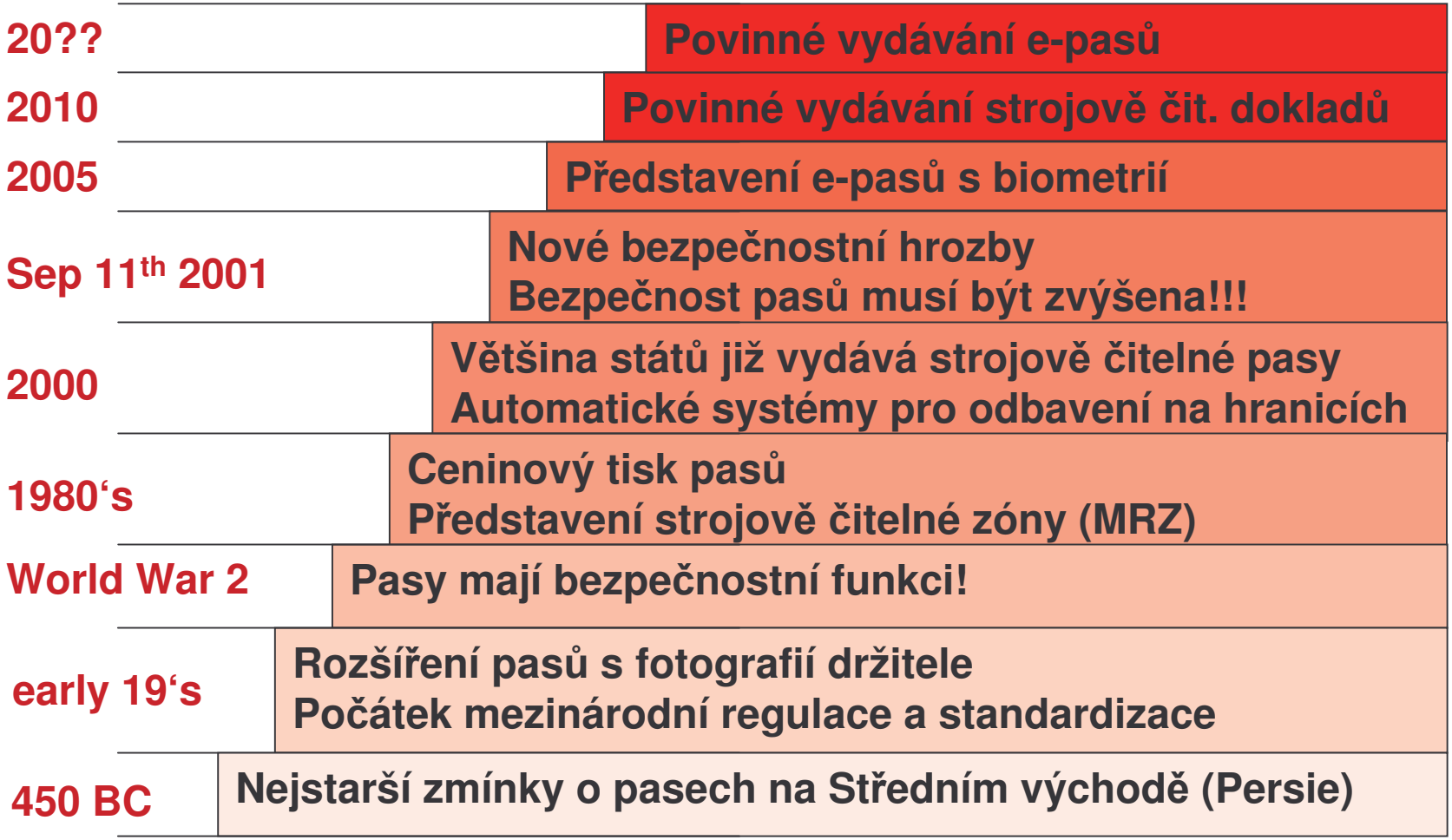
IT Security

Agenda

1. Úvod - historie
2. E-pas – první elektronický doklad pro občany ČR
   - Technologie, Datový obsah, Zabezpečení
   - Budoucí využití na hranicích
3. Možnosti vzdáleného prokazování identity
4. Ideální e-ID – vize elektronického osobního průkazu

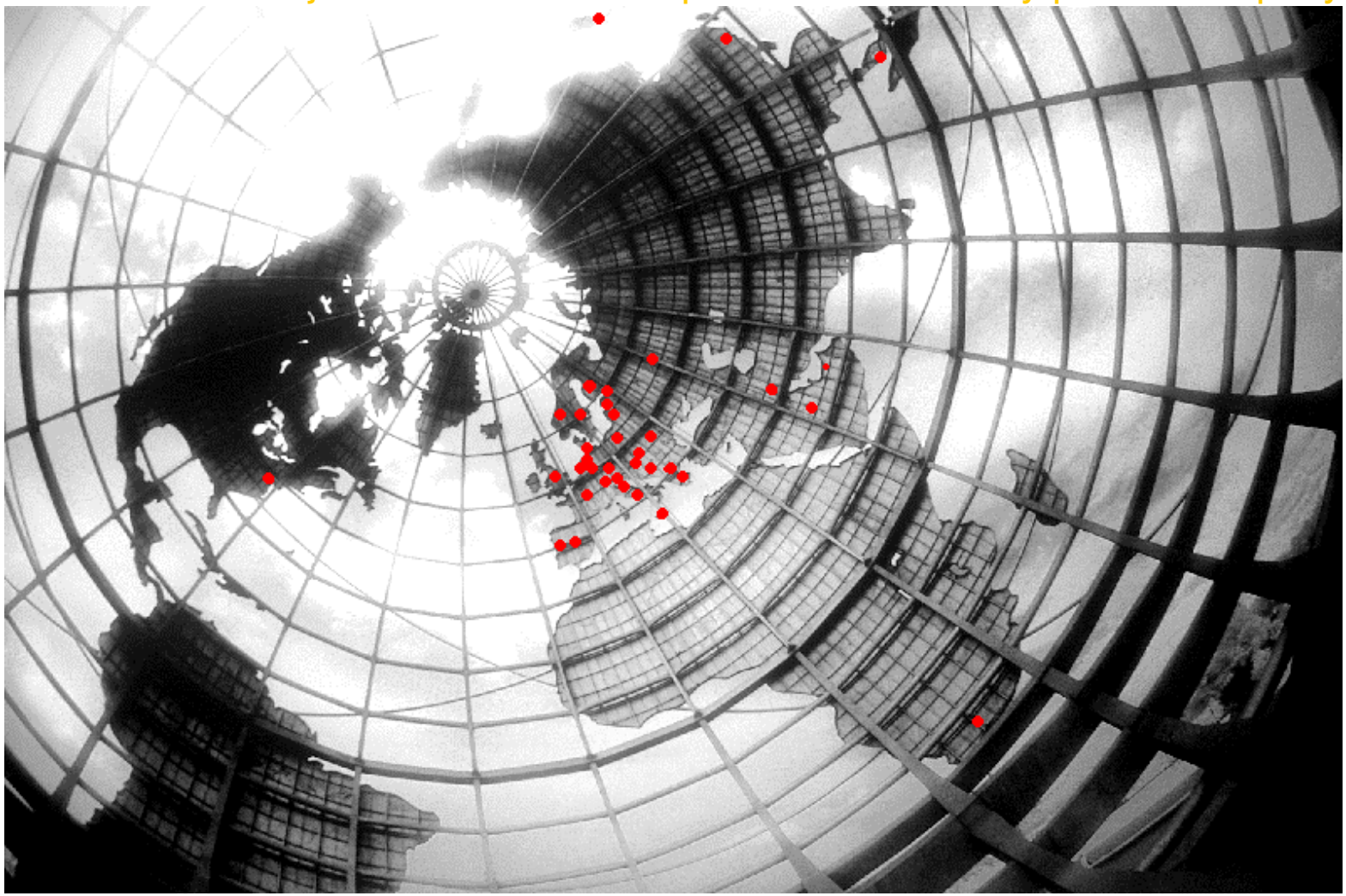
Historie cestovních dokladů - od papíru k čipům a biometrii

Historie a vývoj cestovních dokladů, klíčové impulsy a činitelé



Svět e-pasů

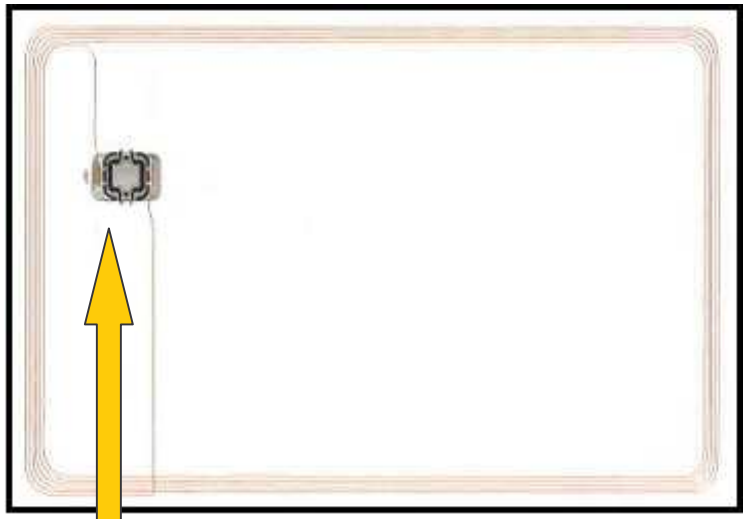
V současnosti již více než 50 států používá / bude brzy používat e-pasy

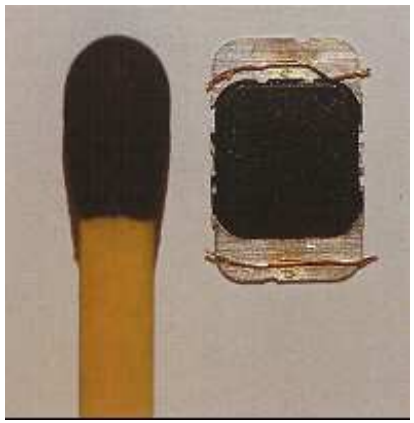


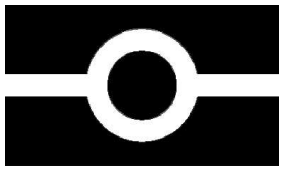
Strojově čitelný cestovní doklad s biometrickými údaji uloženými v nosiči dat s biometrickými údaji

(elektronický pas – e-pas)

Elektronický pas



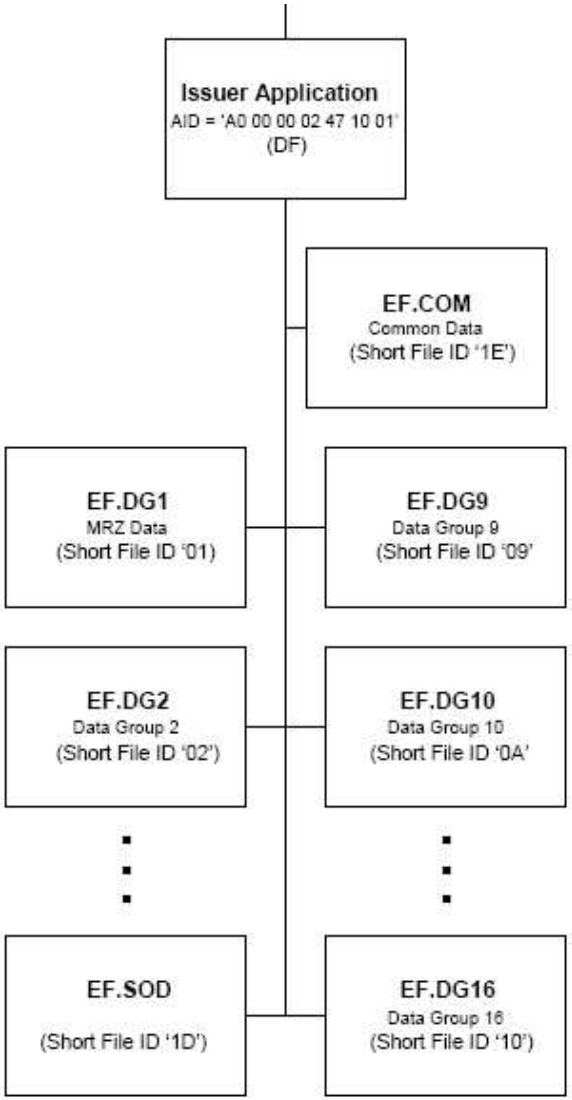


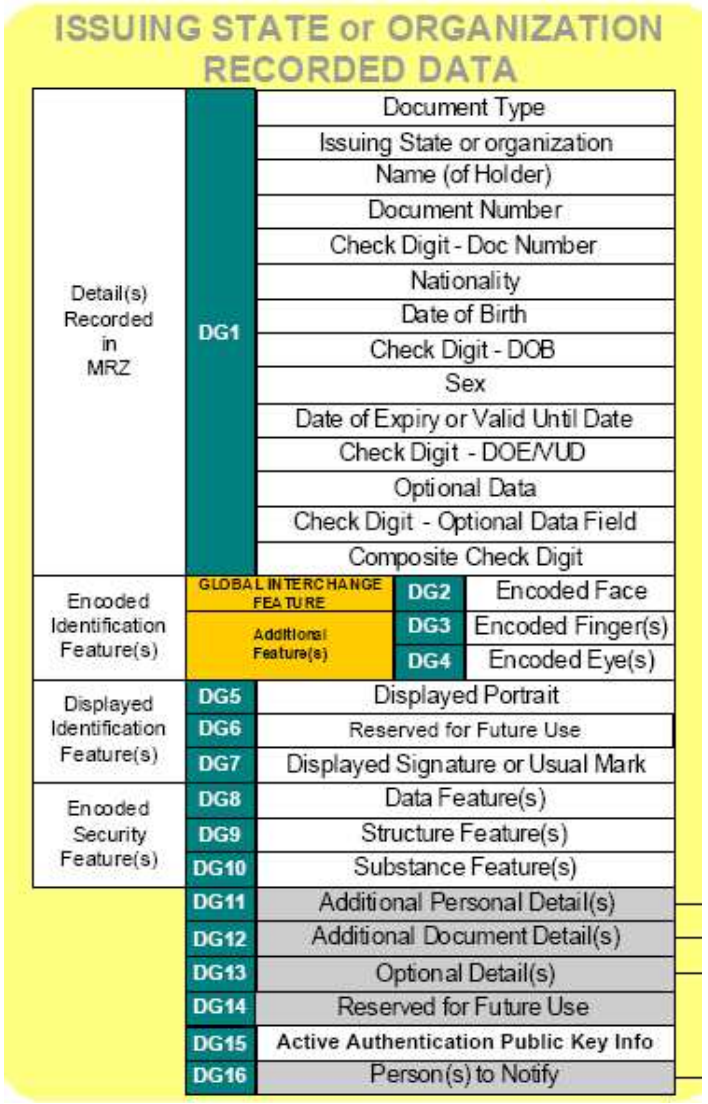


RFID čip - technologie

- RFID čip
  - Vlastní operační systém
  - Paměť EEPROM 72 kB,
  - RF komunikace dle ISO/IEC 14443 typ A
  - UID nezbytné pro fungování bezkolizního mechanismu generováno náhodně při každém čtení
  - Max. rychlost komunikace 424 kbps
  - Certifikace dle CC na EAL5+

RFID čip – datový obsah





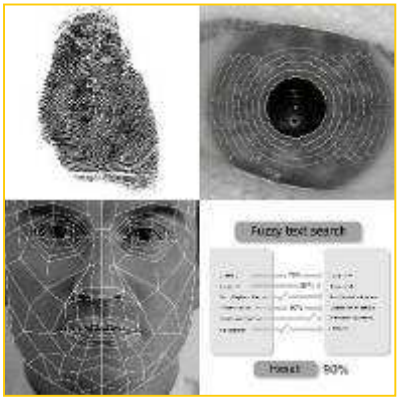
- Basic Access Control (BAC)
  - Terminál se autentizuje klíčem, který vypočetl na základě údajů ze strojově čitelné zóny – ochrana proti „skimmingu“
  - Komunikace mezi terminálem a čipem je šifrována – ochrana proti „eavesdroppingu“
  - Známé nedostatky – kryptograficky slabý klíč
  - Pro účel, pro jaký je používán, je BAC dostatečný

RFID čip – bezpečnost údajů 2

- Integrita dat v čipu
  - Využívá se asymetrická kryptografie (PKI)
  - Všechna osobní data a biometrické údaje v čipu jsou elektronicky podepsány – Document Signer
  - Důvěryhodnost garantuje Národní certifikační autorita
  - Sdílení certifikátů mezi státy
- Aktivní autentizace (AA)
  - Důkaz, že e-pas nebyl zkopírován
  - Čip s pomocí podpisu výzvy prokáže, že je schopen použít privátní klíč
  - Nepovinná bezpečnostní technika

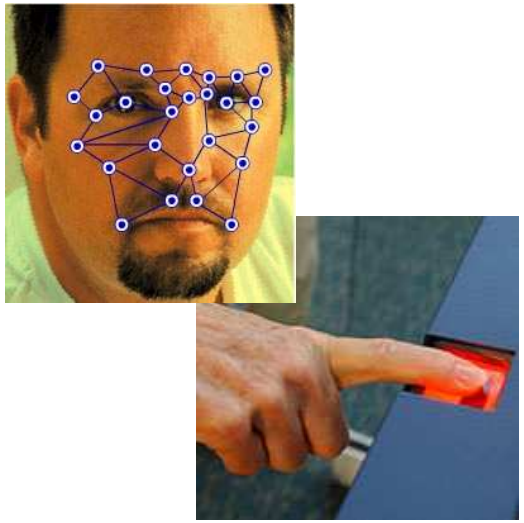
- Extended Access Control (EAC)
  - Bude zaveden se zavedením otisků prstů – umožňuje řídit přístup k citlivým údajům v e-pasu
  - Skládá se ze dvou komponent
    - Chip Authentication (CA) – nahrazuje AA, vytváří silně zabezpečený kanál mezi čipem a terminálem
    - Terminal Authentication (TA) – terminál se prokazuje certifikátem a čip podle totožnosti terminálu řídí přístup k datům
  - Vyžaduje novou, oddělenou PKI infrastrukturu

Prokázání identity pomocí e-ID

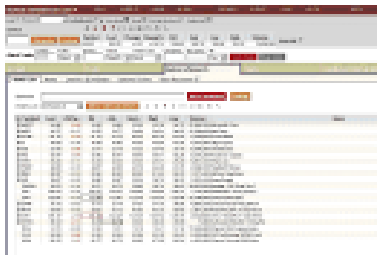


Využití e-pasu - scénář hraniční kontroly

Ověření identity



Identifikace



Jiné využití e-pasu

Je možné prokázat identitu pomocí e-pasu i jinde???

- Pasová knížka **ANO**
- Údaje v čipu **NE**

Důvody

- Současný zákon č.329/1999 Sb. o cestovních dokladech ve znění pozdějších předpisů (především novela č.136/2006 Sb.) ZAKAZUJE jiné zpracování dat z čipu, než jak stanoví zákon.
- Po zavedení otisků prstů do e-pasů bude pro jejich čtení potřeba autorizovaný terminál!!!
- Cena RFID čtečky

Jak jinak vzdáleně prokázat identitu?

Kvalifikovaný certifikát - jediné řešení

- Podporováno legislativou
- V současnosti v ČR 3 akreditované CA
- Ceny kvalifikovaného certifikátu od 190,- do 752,- Kč/rok
- Pouze 1 CA nabízí kvalifikovaný certifikát na čipovou kartu
- Kolikrát za rok použije certifikát běžný občan???
- Počet uživatelů kvalifikovaného certifikátu ? Tendence?

Jak podpořit rychlejší rozšíření?

Elektronická identita by se měla stát součástí osobního ID průkazu občana => e-ID

Ideální e-ID doklad z pohledu občana

- Personalizovaná kontaktní čipová karta
- Na čipu jsou uloženy
  - Osobní údaje občana
  - Komerční certifikát – autentizace ke službám eGovernmentu
  - Kvalifikovaný certifikát (elektronická identita občana)
  - Biometrické údaje (vazba mezi osobou a dokladem)
- Volitelně může obsahovat další informace, např.
  - Řidičský průkaz – získané skupiny oprávnění, zůstatek bodů pro bodový systém, …
  - Lékařské záznamy – očkování, krevní skupina, alergie,...

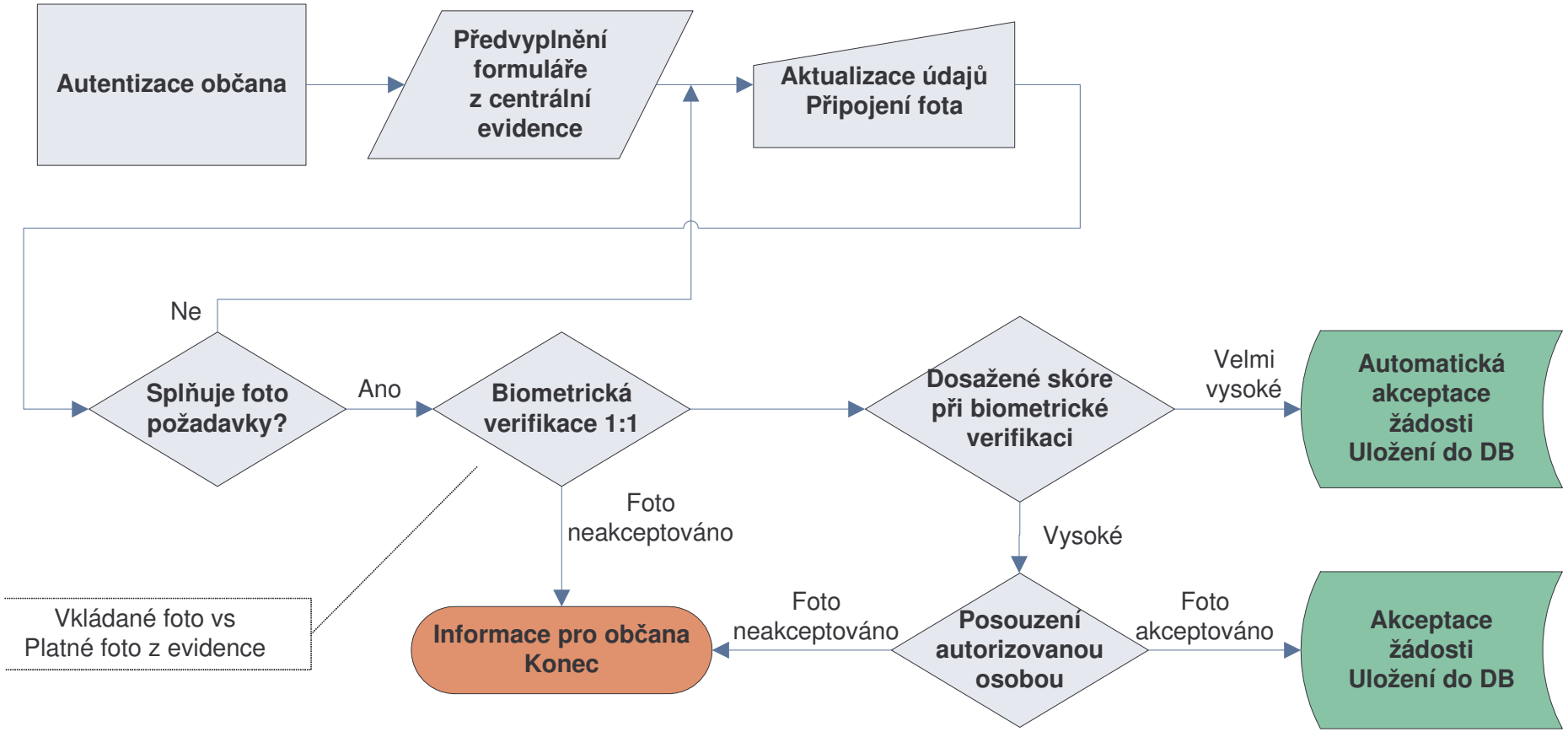
Výhody e-ID

- Na základě speciálního oprávnění (certifikát) lze aktualizovat vybrané osobní údaje (adresa apod.)
- Každou skupinu údajů může spravovat jiný subjekt na základě svého vlastního certifikátu
  - Řidičský průkaz - Ministerstvo dopravy
  - Lékařské záznamy – Ministerstvo zdravotnictví
- Snadné využití i v komerční sféře

Taková řešení se v jiných zemích již implementují!!!

Bude s nimi EU / ČR držet krok???

Příklad použití – vzdálená žádost o nový e-ID / e-pas



Diskuse & Otázky

Děkuji za pozornost!

Filip Hajník
Senior Business Consultant
LogicaCMG

Na okraji 335/42
162 00 Praha 6
Česká republika
http://www.logicacmg.cz/

Tel: +420 284 020 111
E-mail: filip.hajnik@logicacmg.com