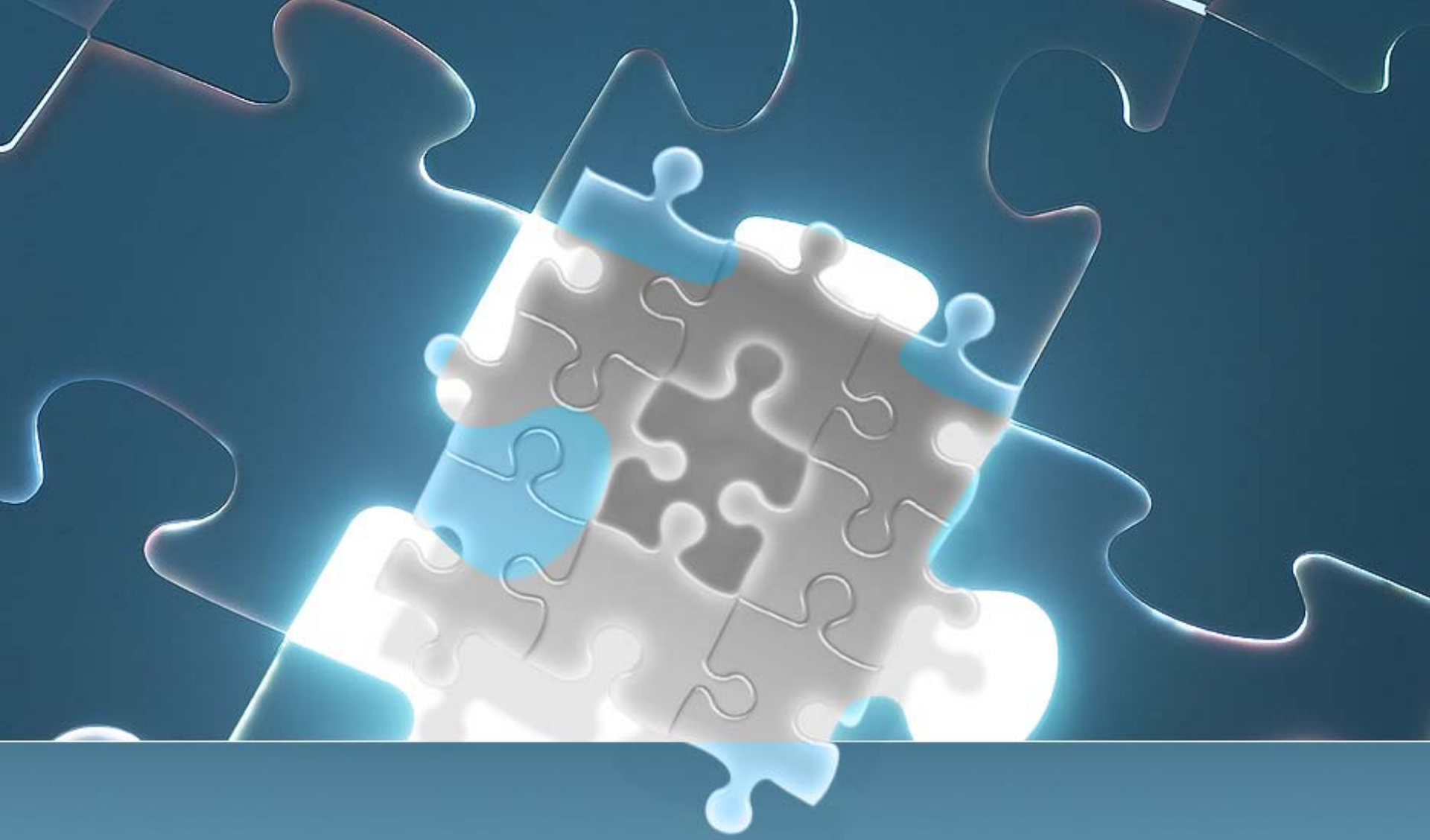


Elektronické pasy v praxi

Zdeněk Říha

Co je elektronický pas

- Klasická knížečka plus
  - Bezkontaktní čip
  - Anténa
- Komunikace podle ISO 14443
  - 0-10cm, 106 až 848 kbps
- Soubory DG1 až DG16
  - Textová data, foto obličeje, otisky prstů
- Digitální podpis dat povinný
- Řízení přístupu
  - BAC, EACv1, EACv2, SAC

ePas - logo


EUROPEISKA UNIONEN
SVERIGE
PASS
EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS

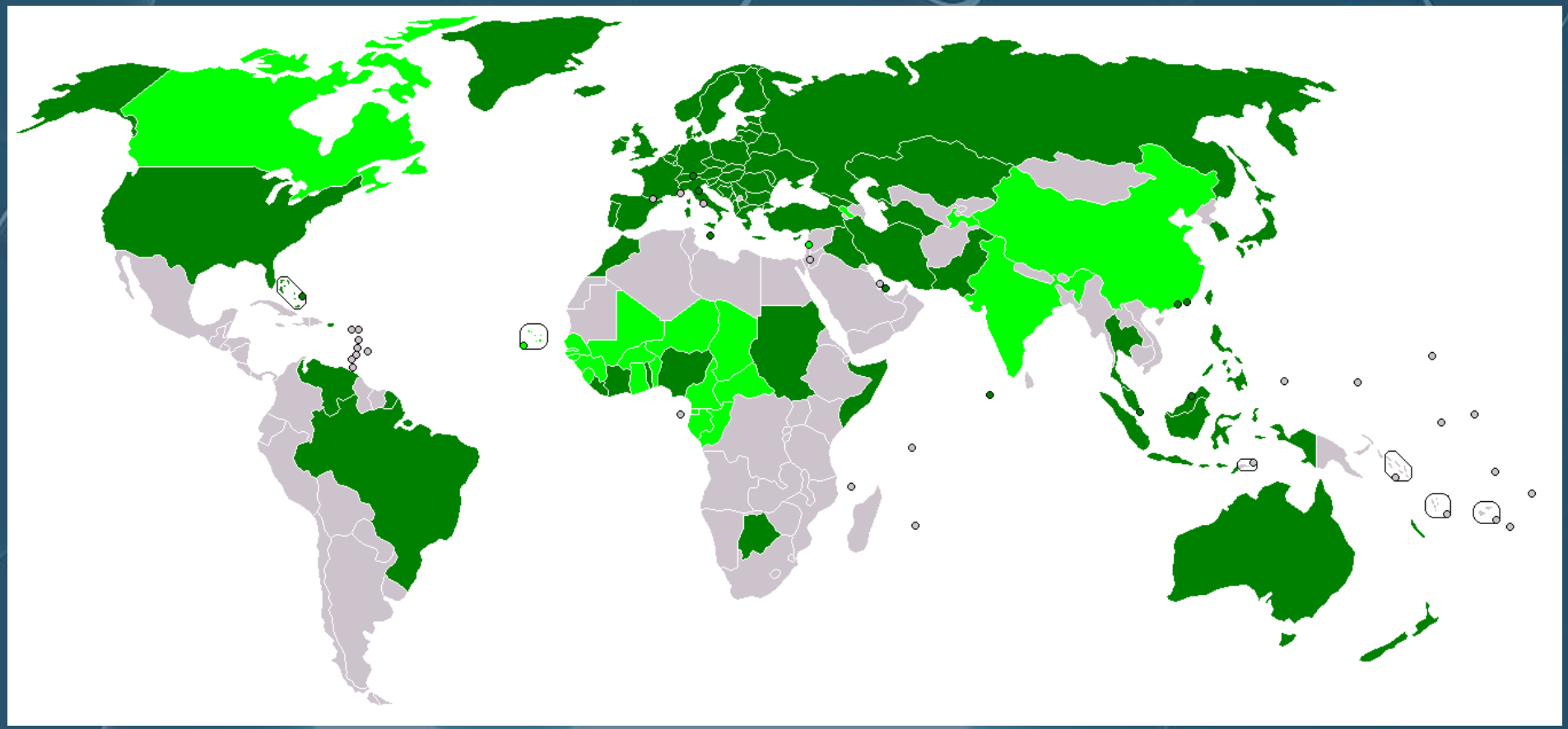
Čip a anténa I

Čip a anténa II

Historie

- Malajsie 1998
- 11/9/2001
- Visa Waiver Program (VWP)
- Nařízení Rady (ES) č. 2252/2004
  - Rozhodnutí K(2005) 409 z 28 února 2005
    - deadline: 28 srpen 2006
  - Rozhodnutí K(2006) 2909 z 28 června 2006
    - deadline: 28 červen 2009
- ICAO Doc 9303, 6. vydání, 2006
- Německé elektronické občanky, 10/2010

Kdo vydává pasy?



Zdroj: Wikipedie

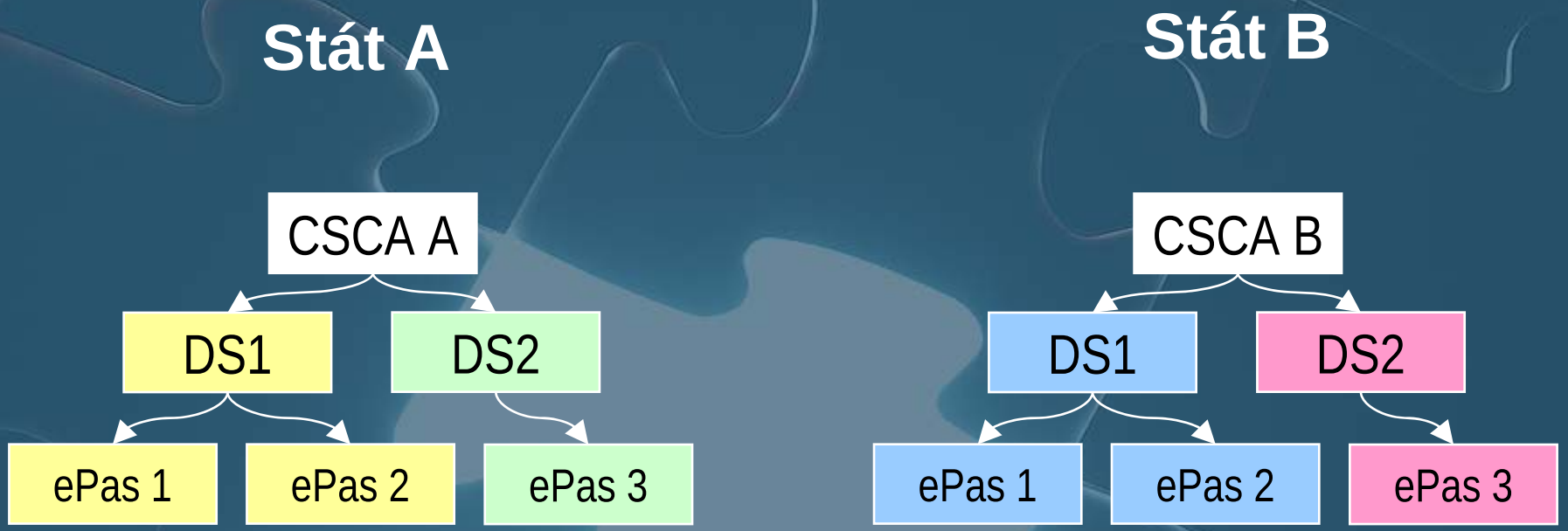
Vydávání pasů dle ICAO

- Zpráva ICAO z léta 2011:
  - 93 zemí vydává elektronické pasy
    - 34 zemí ukládá pouze fotografie držitelů
    - 14 zemí ukládá pouze fotografie, ale plánuje ukládat i otisky prstů
    - 45 zemí ukládá fotografie držitelů a otisky prstů
  - Odhad počtu vydaných elektronických pasů: 345 039 000
  - Vše dle 9303 kromě Pákistánu, Moldávie a Iráku
    - Malajsie od roku 2010

Digitální podpisy

- Jediný povinný bezpečnostní prvek
- Podpis dat v pase (CMS) včetně certifikátu podepisovatele dat (DS)
- Pro ověření je třeba kořenový certifikát CSCA vydávající země

Pasivní autentizace



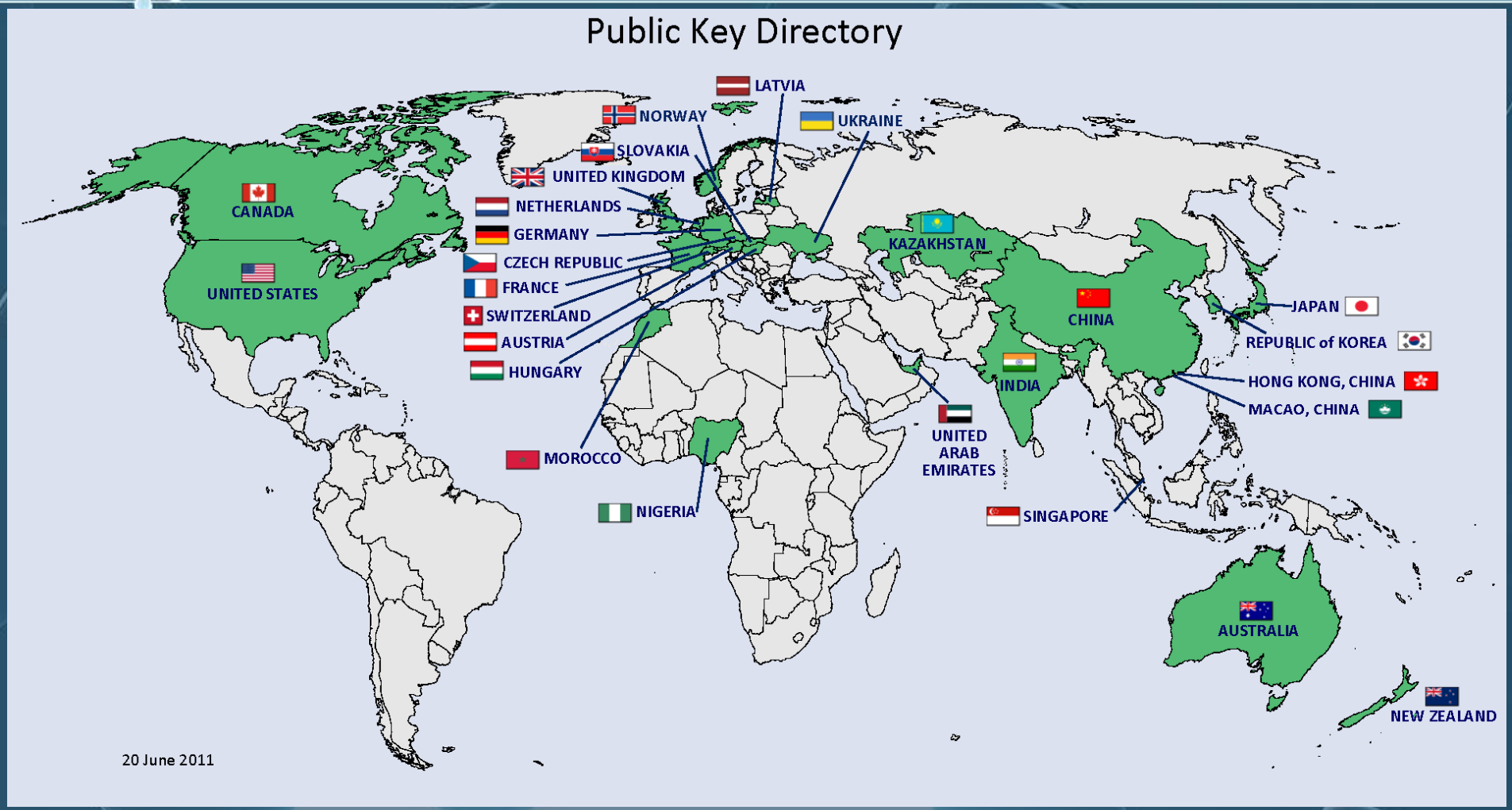
Pasivní autentizace

- DS certifikáty, překlenovací CSCA certifikáty a CRL mohu stáhnout odkudkoliv
  - DS certifikáty přímo v pasu
  - CRL typicky z webu
- Diplomatická výměna CSCA certifikátů
  - DVD/CD skončí kdovíkde
  - Australský experiment…
  - Důvěrnost vs. Integrita
    - Zákonná omezení ☺
- CRL zatím prázdné …
- ICAO PKD

ICAO PKD

- Public Key Directory
  - DS certifikáty a CRL
  - S CSCA nemůže pomoci přímo
    - Zavádí se „Master List"
    - Německo podepisuje CSCA certifikáty **45** zemí
    - Austrálie podepisuje CSCA certifikáty 3 zemí
  - https://pkddownloadsg.icao.int
- Poplatky:
  - 1x 56 000 USD
  - 43 000 USD za rok 2011

ICAO PKD mapa



Zdroj: ICAO

Nedostatečnost BAC

- Základní řízení přístupu
  - Založeno na čísle dokumentu, datu narození, datu exspirace pasu
  - Vytištěno v pase (i jako součást MRZ)
  - Nedostatečná entropie -> možné útoky
- Změna výpočtu klíče odmítnuta
- Náhodná čísla dokumentů
  - Německo (entropie klíče 35 -> 45 bitů)

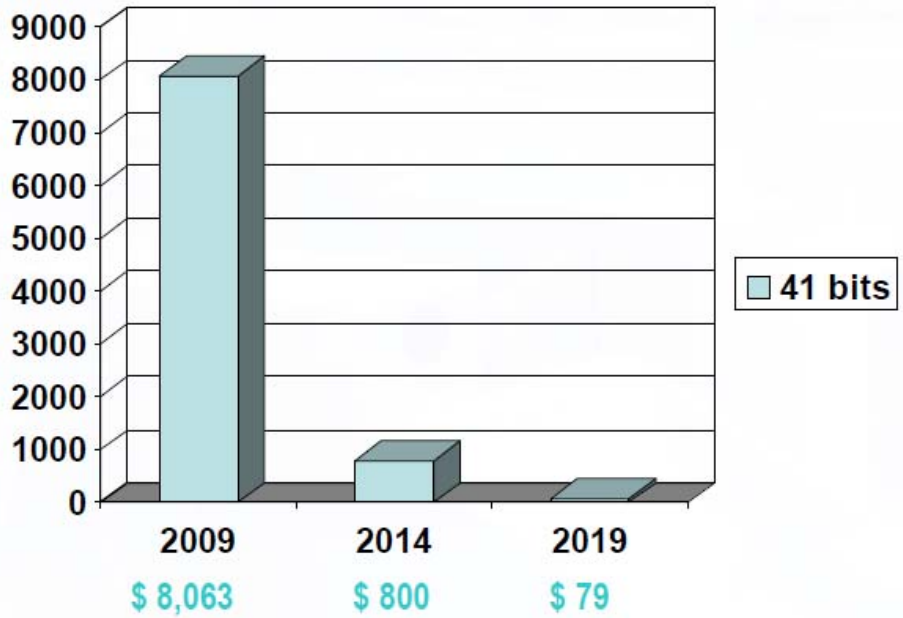
Výpočet klíče pro BAC

Zdroj:
MV ČR

Nedostatečnost BAC

Moore's Law and BAC

- 1 hour



- Cena útoku na BAC pro pas s entropií BAC klíče 41 bitů

Zdroj: TAG on MRTD

Řešení: SAC

- Supplementary access control (SAC)
  - Dodatečné řízení přístupu
- Založeno na protokolu PACE
  - Password authenticated Connection Establishment
- Užívá stejná data pro klíč
  - Číslo dokladu, datum narození, datum exspirace
- Bezpečnost PACE však nezávisí (tak významně) na entropii klíče

Technikálie SAC

- 1. Pas generuje náhodné číslo a odesílá čtecímu systému šifrovaně
- 2.Čtečka dešifruje a obě strany použijí číslo pro odvození náhodného generátoru grupy (DH/ECDH)
- 3. Nad takto získanou grupou proběhne klasický anonymní (DH/ECDH)
- 4. Generování a ověření autentizačních tokenů

Protokoly a verze

- 0. generace pasů
  - Žádné řízení přístupu
- 1. generace pasů
  - BAC
- 2. generace pasů
  - BAC + EACv1 (CA,TA)
- Německé občanky
  - EACv2 (TA, CA, PACEv1)
- 3.generace pasů (od roku **2014**)
  - BAC + PACEv2 (+EACv1)
  - Zpětná kompatibilita – přítomnost BAC !!!

Praktické aspekty EAC

- Přístup k citlivým údajům
  - Otisky prstů a oční duhovky (nevyužíváno)
  - Chráněno pomocí autorizačního certifikátu a patřičného soukromého klíče
- Infrastruktura klíčů (PKI)
  - Státy musí navázat iniciální vazbu důvěry
  - A potom mnohokrát ročně obnovit certifikát…

Vydávání certifikátů

- Emailem !!!
  - Nezabezpečený email s přílohami typu žádost o certifikát a certifikát.
  - Popis původně v technické specifikace EACv1, později přesunuto do certifikační politiky
  - Email je nespolehlivý
    - Nevíme zda se ztratil již požadavek nebo až odpověď
- Při implementaci se ukázalo, že spolehlivější bude nasadit web services
  - 1. Dobrovolná skupina aktivnějších zemí
  - 2. Emailová komunikace zcela nahrazena webem
    - I legislativně ošetřeno

SPOC

- Webové služby založeny na SPOC jednotlivých zemí
  - Single Point of Contact (SPOC)
  - Komunikace chráněna pomocí SSL/TLS
  - Specifikace dle ČSN 369791:2009
- Aktuální situace
  - První úspěšné výměny mezi několika málo zeměmi EU

Využívání ePasů na hranicích

- Červnová zpráva ICAO
  - 10 zemí čte ePasy
    - Co znamená čtení pasů?
  - Austrálie, Kanada, Německo, Indonésie, Japonsko, Nový Zéland, Portugalsko, Singapur, Spojené království, Spojené státy americké
- Povinné využívání v EU zatím není
- Cena zařízení …

ABC systémy

- ABC
  - Automated Border Control
- Starší systémy vyžadovaly registraci
  - PEGASE (Paříž), ABG (Frankfurt), …
- Novější systémy využijí přímo data z pasu
  - Dnes založeno na snímcích tváře
  - V budoucnu i na otiscích prstů
    - Komplikováno certifikáty EAC

První ABC Systémy

- Smart Gate v Austrálii
- RAPID v Portugalsku
- ABC v UK
- ...

RAPID - Portugalsko

ABC systémy

- Bezpečnost
  - Ověření digitálního podpisu
    - Chybějící CSCA certifikáty
  - Aktivní autentizace
    - Další 1-2s při čtení pasu
  - Autentizace čipu
    - Relativně nový protokol
  - Biometrie
    - RAPID (prahová hodnota 40%)
      - zero effort FAR: 0,03 %
      - Test univerzity Algarve (448 párů osob): FAR 1,25 %
    - Německo: ABG (duhovka) -> EasyPass (obličej)

Bezpečnost ABC

The Telegraph

Search - enhanced by Google

HOME NEWS SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL LIFESTYLE FASHION TECH Dating Offers Jobs

Technology News | Technology Companies | Technology Reviews | Video Games | Technology Video | Mobile App Reviews | Blogs

Technology

Facial recognition passport gates shut down

Border gates at Manchester Airport that rely on facial recognition technology had to be shut down after they failed to recognise that a couple had swapped passports.

Photo: CORBIS

By Christopher Williams, Technology Correspondent
10:51AM GMT 17 Feb 2011

Follow 326 followers

7 Comments

Share:

Recommend

Tweet 35

Share 9

+1 0

Technology
Technology News »
Christopher Williams »

Gadgets taken apart

Follow us on... facebook twitter

TECHNOLOGY REVIEWS »

Sony S and P tablets: hands on

Matt Warman tries out Sony's new S and P tablet computers.

★★★★☆

Tag Heuer £16,000 mobile phone

Zdroj:
Telegraph.co.uk

Interoperabilita

- Dnes interoperabilita pasů a čteček není problém
- Čtení EAC pasu za 2,6 s
  - Asi 48kB
  - Včetně CA+TA

Ochrana soukromí

Děkuji za pozornost