Segurança em Passaportes Eletrônicos

Ivo de Carvalho Peixinho
Perito Criminal Federal

Agenda

1. Introdução
2. Passaportes eletrônicos
3. Aplicações
4. Vulnerabilidades conhecidas
5. Passaporte eletrônico brasileiro
6. Conclusão

Introdução

- Passaporte
  - Documento de identidade
  - Permissão para cruzar fronteiras
  - Diplomacia
  - Padronizado pela OACI (ICAO)

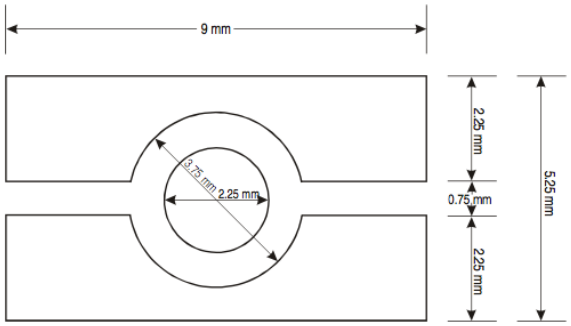
Introdução

- ICAO (OACI)
  - International Civil Aviation Organization
  - Agência especializada das nações unidas (ONU)
  - Desenvolvimento da nagevação aérea internacional
  - MRTD – Machine Readable Travel Documents (ICAO 9303)
    - ePassports

http://www.icao.int

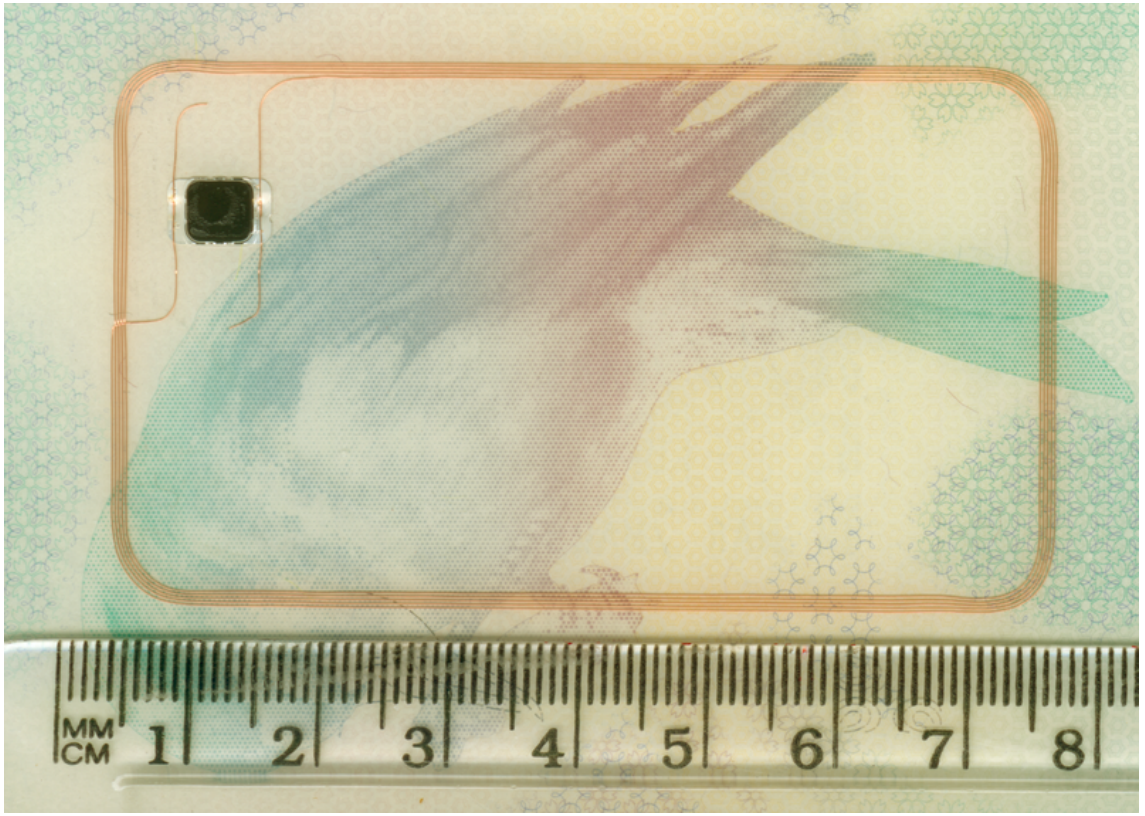
Motivação

- Porque ePassports?
  - Evolução dos recursos anti-fraude
  - Possibilidade de criação de aplicações
    - Imigração automática
    - Visto eletrônico
  - Autenticação do portador
    - Biometria
  - Segurança do documento



Passaportes eletrônicos

- Tecnologia RFID



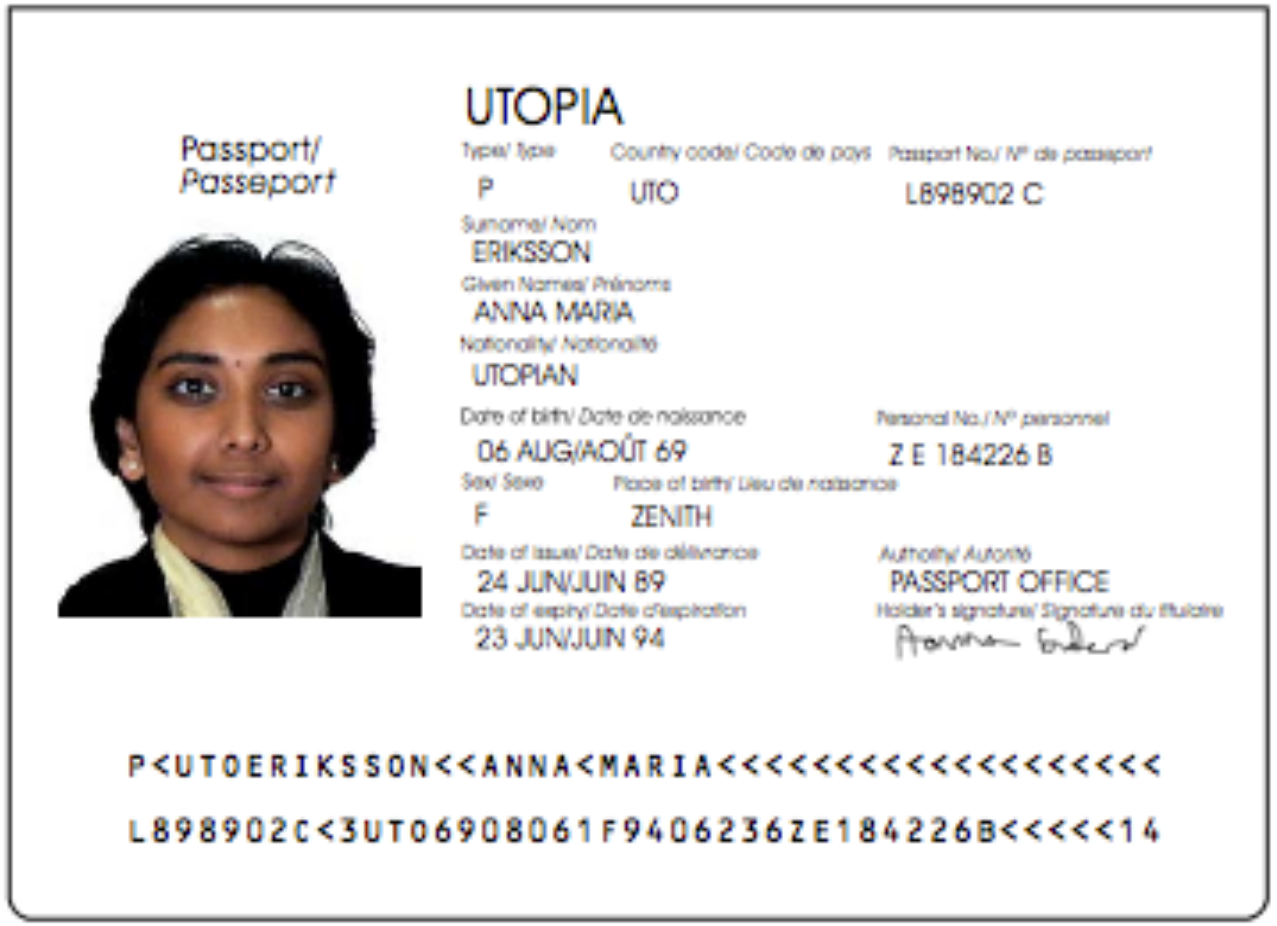
Passaportes eletrônicos

- Documento ICAO 9303
  - Part 1 Vol1 – Elementos de segurança físicos
  - Part 1 Vol2 – Especificações do IC (RFID)
  - Part 2 – Machine Readable Visas
  - Part 3 – Documentos oficiais
- Elementos de segurança físicos
  - MRZ – Machine Readable Zone
  - Suporte (papel), UV, marca d'água, intaglio, guilhochês, etc.

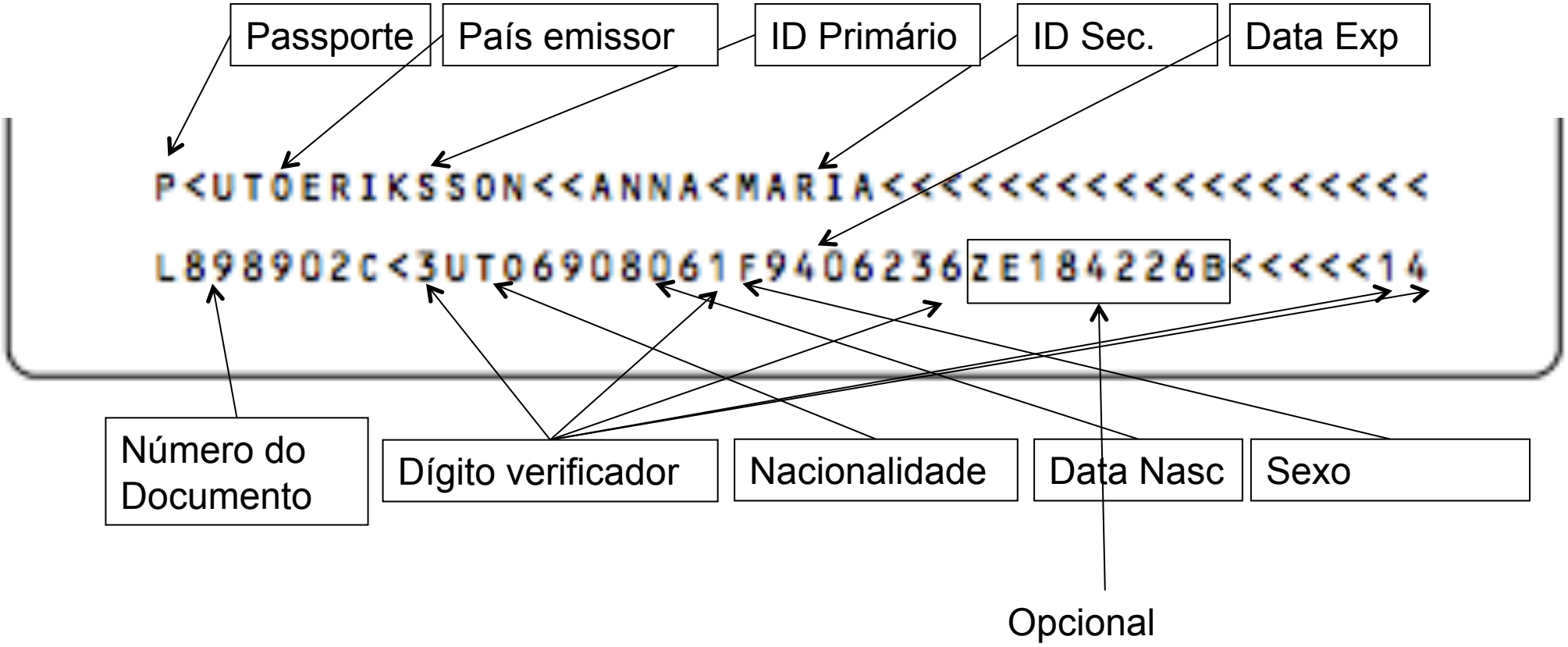
Passaportes eletrônicos

- MRZ
  - Machine Readable Zone
  - Informações utilizadas pela leitora OCR dos postos de imigração.
  - Presente na página de dados do passaporte
  - Possui códigos de verificação (CRC)
  - Utilizado como chave para leitura do IC RFID (BAC)

Passaportes eletrônicos

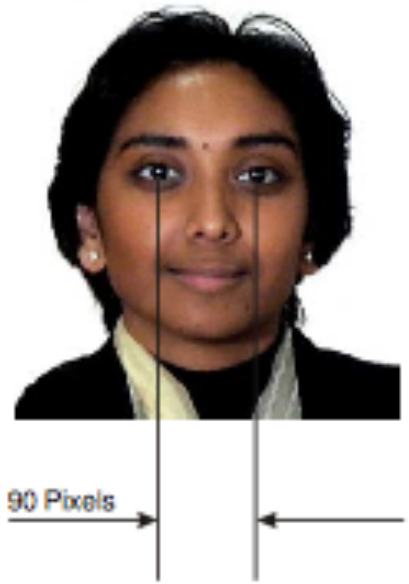


Passaportes eletrônicos



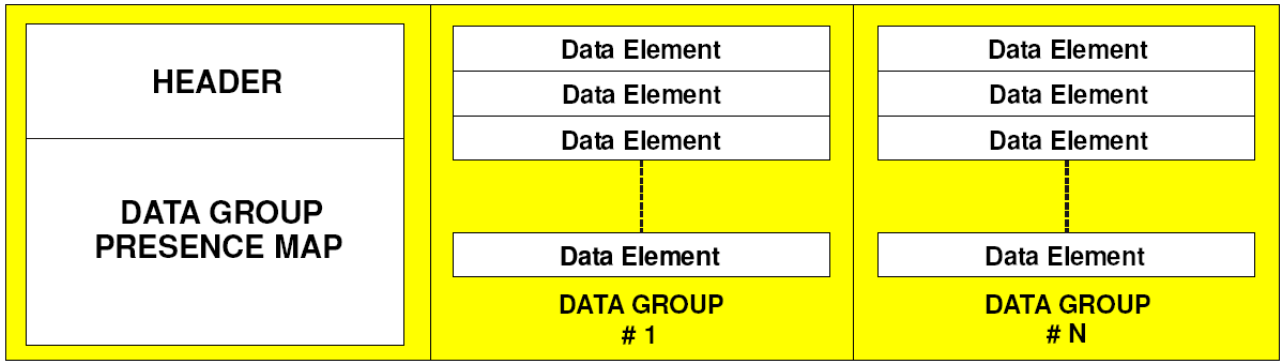
Passaportes eletrônicos

- RFID ePassport
  - Identificação biométrica
    - Face (obrigatório)
    - Impressão digital (opcional)
    - Reconhecimento da íris (opcional)
  - ISO/IEC 14443 (RFID) – 13,56MHz
  - Sistema operacional embarcado
    - Criptografia e Certificação digital
    - Leitura e gravação de dados (Write Once/Read Many)



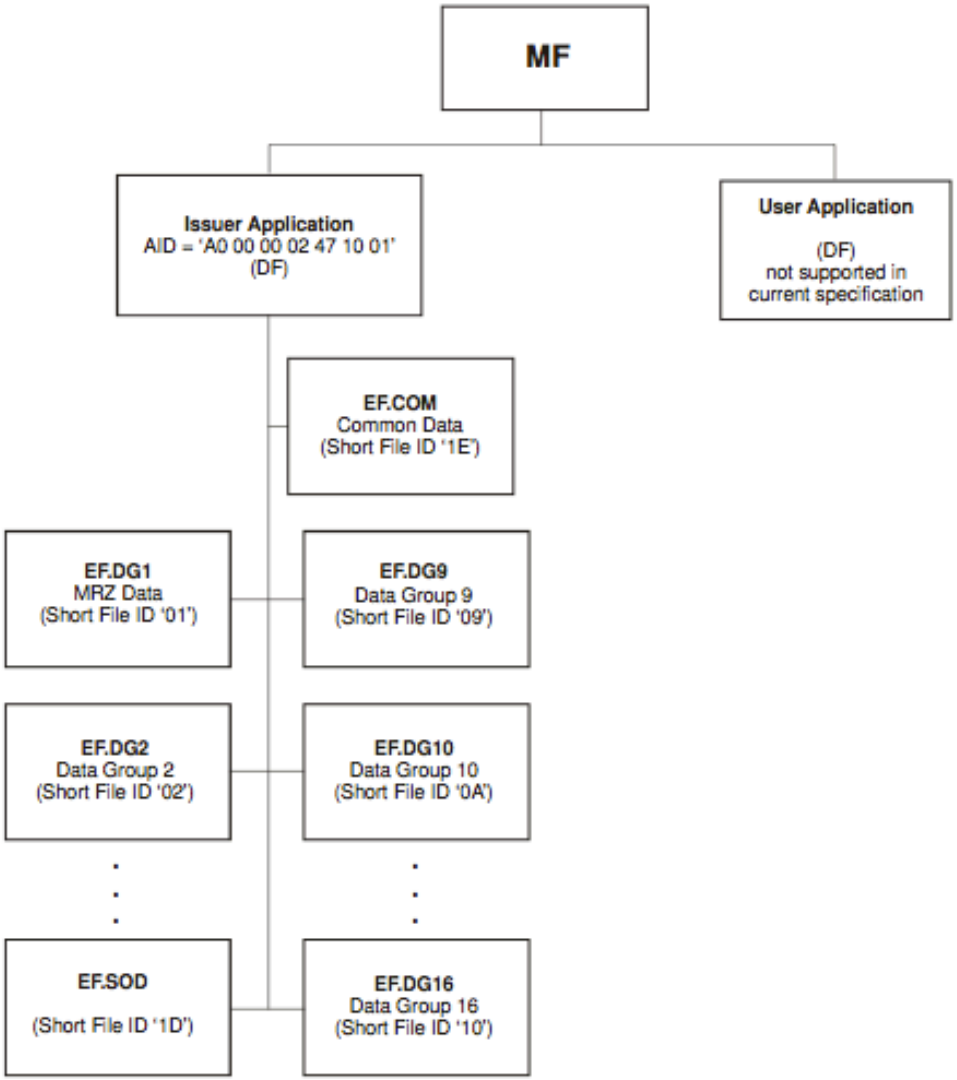
Passaportes eletrônicos

- LDS – Logical data Structure
  - Estrutura de dados padronizada pelo ICAO 9303
  - Data Groups
    - 16 DG's + 3 (versão futura)
  - Data items
    - Itens dos Data Groups



Passaportes eletrônicos

- LDS – Logical data Structure
  - Common (EF.COM) – Estrutura do LDS
  - DG1 – MRZ (EF.DG1)
  - DG2 – Face (JPEG 2000) (EF.DG2)
  - DG3 – Fingers (WSQ) (EF.DG3)
  - DG4 – Eyes (EF.DG4)
  - DG5 – Displayed Portrait (EF.DG5)
  - DG7 – Signature (EF.DG6)
  - DG8, DG9, DG10 – Features (EF.DG8, EF.DG9, EF.DG10)
  - DG15 – AA Public Key (EF.DG15)
  - DG16 – Persons to Notify (EF.DG16)
  - Security Data (EF.SOD) – Hashes of LDS Data Groups + Certificate


MF
Issuer Application
AID = 'A0 00 00 02 47 10 01'
(DF)
User Application
(DF)
not supported in
current specification
EF.COM
Common Data
(Short File ID '1E')
EF.DG1
MRZ Data
(Short File ID '01')
EF.DG9
Data Group 9
(Short File ID '09')
EF.DG2
Data Group 2
(Short File ID '02')
EF.DG10
Data Group 10
(Short File ID '0A')
EF.SOD
(Short File ID '1D')
EF.DG16
Data Group 16
(Short File ID '10')

Passaportes eletrônicos

- Protocolos de Segurança
  - Certificação digital (M)
    - Country Signing CA
    - Document Signing CA
    - ICAO PKD
  - Passive Authentication (PA) (M)
  - Active Authentication (AA) (O)
  - Basic Access Control (BAC) (O)
  - Extended Access Control (EAC) (O)

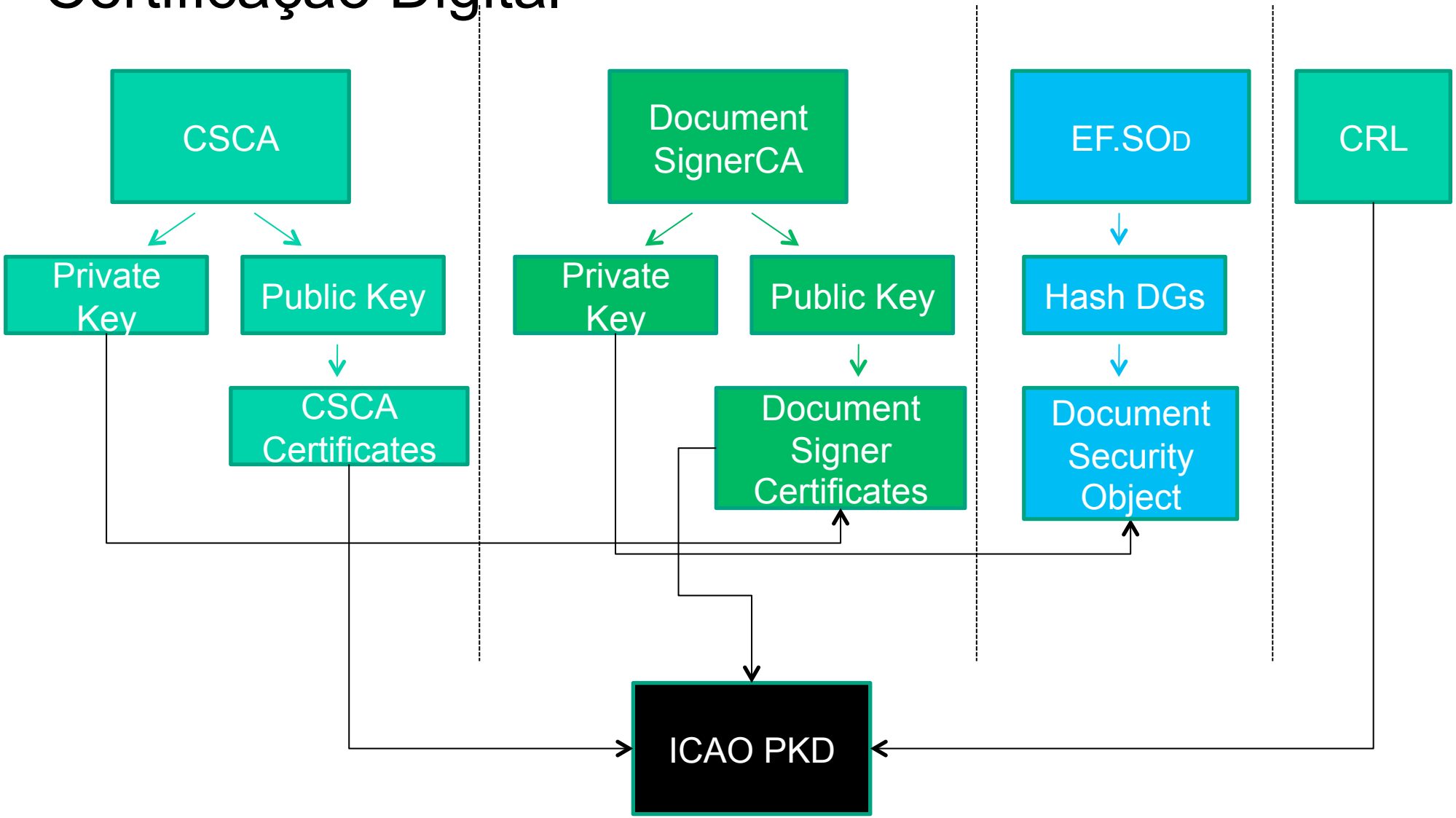
Passaportes eletrônicos

- Certificação digital
  - ICAO PKD
    - Diretório central de certificados digitais (LDAP)
    - Verifica certificados DS com o CSCA
    - Não fornece o CSCA de cada país
  - Country Signing CA
    - CA raiz (auto assinado)
    - Informado ao PKD e aos países com relação diplomática
    - Armazenado na leitora de imigração

Passaportes eletrônicos

- Certificação digital
    - Document Signing CA
        - CA de assinatura de documentos
        - Incluso no PKD
        - Incluso no passaporte (Opcional)
        - Incluso nas leitoras dos pontos de imigração
        - CRL armazenado no PKD

Certificação Digital



Passaportes eletrônicos

- Protocolos de Segurança
  - Passive Authentication (PA)
    - Verificação da assinatura digital do SOD
      - Certificado do DS
    - Verificação dos hashes (EF.SOD)
    - Autenticidade do SOD e integridade do SOD e dos DG's.

Passaportes eletrônicos

- Protocolos de Segurança
  - Active Authentication (AA) (OPCIONAL)
    - Leitura do MRZ no DG1
    - Leitura da chave AA no DG15
    - Desafio-resposta com a chave pública e privada do AA
      - Chave privada armazenada internamente
    - **Autenticidade da página**
    - **Correspondência do chip com a página de dados**
    - **Previne cópia dos dados do chip**

Passaportes eletrônicos

- Protocolos de Segurança
  - Basic Access Control (BAC) (OPCIONAL)
    - Proteção contra leitura indevida
    - Utiliza o MRZ como chave para acesso ao IC
      - Número do documento
      - Data de nascimento
      - Data de expiração
      - Dígitos verificadores
    - Deriva chaves de sessão para comunicação segura

Passaportes eletrônicos

- Protocolos de Segurança
  - Extended Access Control (EAC) (OPCIONAL)
    - Proteção dos dados biométricos
    - Não é padronizado pelo documento ICAO
      - Diferentes implementações
    - Funcionalidades
      - Chip Authentication (CA) – Provar que o chip não foi clonado
      - Terminal Authentication (TA) – Verificar se o leitor tem permissões para ler o chip.

Passaportes eletrônicos

- Protocolos de Segurança
  - EAC v2
    - Evolução do EAC
    - Não depende de BAC
      - Implementa um protocolo substituto (PACE)
    - Ainda não é normatizado
    - Evolução futura
    - Atualmente em conflito com o documento ICAO

Passaportes Eletrônicos

- Aplicações
  - Imigração automática
    - Sistema RAPID
    - CEF Portugal
  - Visa eletrônico
    - Em fase de estudo
    - DG’s reservados

Passaportes eletrônicos

- Vulnerabilidades conhecidas
  - Skimming
    - Leitura não autorizada do chip
    - Detectar e rastrear passaportes
    - Captura de transações
  - Clonagem de chip
  - Entropia BAC
    - 56 bits reduzido a 25 a 35 bits
  - EAC dependente de BAC
    - Resolvido no EAC v2 (PACE)

Passaportes eletrônicos

- Vulnerabilidades conhecidas

Passaportes eletrônicos

- Vulnerabilidades conhecidas
  - BlackHat 2006
    - Identificação de passaportes pelo RFID
    - Aumento da distância padrão (10 cm) com radios mais potentes
      - 3, 4, 6, 10, 31 ft? (0.9, 1.2, 1.8, 3, 9 metros)
    - Clonagem de RFID em passaportes
      - Não permite alteração
  - Defcon 2009
    - “Portal” de leitura de RFID (Feds)

Passaportes eletrônicos

- Vulnerabilidades conhecidas
    - RFIDIOt (http://rfidiot.org/)
        - Leitura de passaportes com BAC
    - Interferências propositais (jamming)

Passaporte eletrônico Brasileiro

- Evolução
  - Adoção do padrão ICAO a partir de 2007
  - Programa de Modernização, Agilização, Aprimoramento e Segurança da Fiscalização do Tráfego Internacional e do Passaporte Brasileiro (PROMASP)
  - Novos elementos de segurança
  - Novo sistema de tráfego internacional
    - Consultas SINPI, MIND, AFIS
  - Passaporte eletrônico (Mai/2009)

Passaporte eletrônico Brasileiro

- Timeline passaporte eletrônico
    - Maio 2009 - Início dos trabalhos
    - Julho 2009 – Parceria CMB
    - Dezembro 2009 – Projeto Básico
    - Agosto 2010 – Aprovação requisitos
    - Setembro 2010 – Modelo de dados
    - Outubro 2010 – Testes e correções
    - Novembro 2010 – Homologação
    - Dezembro 2010 – Pré-produção
        - Lançamento oficial 08/12/2010
    - Janeiro 2011 - Produção

Passaporte eletrônico Brasileiro

- Características
  - 3 tipos
    - Comum
    - Estrangeiro
    - Laissez-Passer

Passaporte eletrônico Brasileiro

- Características RFID
  - ISO/IEC 14443 – 13,56Mhz
  - Interface tipo “B”
  - Suporte a BAC, EAC, PA e AA
  - PKI (CS, DS, AA)
  - LDS
    - DG1 – MRZ
    - DG2 – Face em JPEG 2000, 300 DPI, 90 pixels
    - DG3 – Fingerprint (WSQ, 500 DPI, duas digitais, EAC)

Passaporte eletrônico Brasileiro

- Características RFID
  - LDS (cont.)
    - DG4 – Iris (vazio)
    - DG7 – Signature (vazio)
    - …
    - DG15 – Active Authentication Public Key
    - DG16 – Persons to notify

Passaporte eletrônico Brasileiro

- Imigração automática no Brasil
  - Sistema RAPID Português
  - Piloto com 2 cabines de imigração (e-gates)
  - Aeroporto de Brasília
  - Dezembro de 2010

Conclusões

- Passaporte em constante evolução
    - Prevenção de fraudes
- Passaporte eletrônico como evolução de segurança
    - Protocolos de segurança em constante evolução
- Passaporte eletrônico permite novas aplicações
    - Imigração automática
    - Visa eletrônico
- Passaporte eletrônico no Brasil em Jan/2011

Ivo de Carvalho Peixinho

Perito Criminal Federal