RFID II - Machine Readable Travel Documents and Electronic Passports

Basic Access Control (BAC) and Extended Access Control (EAC)

Bernd Waschneck

Sommerakademie II – AG 4 (Applied Cryptography and Security Engineering)

1. Oktober 2009

Outline

1. Introduction/Overview

2. Public Key Infrastructure (PKI)

3. Passive Authentication

4. Active Authentication

5. Access Control
    - 5.1 Basic Access Control
    - 5.2 Extended Access Control

6. Conclusion

Outline

1. Introduction/Overview

2. Public Key Infrastructure (PKI)

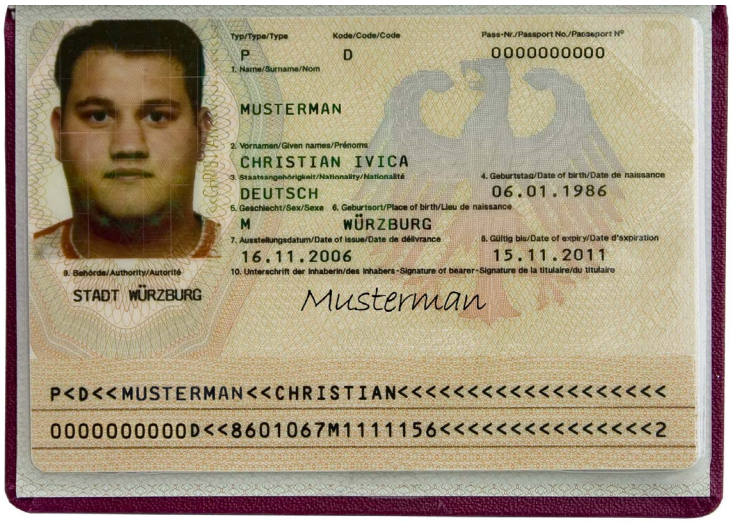
3. Passive Authentication

4. Active Authentication

5. Access Control
    - 5.1 Basic Access Control
    - 5.2 Extended Access Control

6. Conclusion

1. Introduction/Overview



← Machine Readable Zone (MRZ)

2001 9/11 Attacks on WTC

2004 International Civil Aviation Organisation (ICAO) publishes guidelines for the introduction of electronic passports (ePassports)

2005 Germany: RFID chip with facial image, mandatory

2007 Germany: fingerprint, optional

1. Introduction/Overview

Reasons for adoption of RFID chips:

- protection against passport frauds and manipulations of passports
- authenticity of data
- automation of passport control
- stronger connection between passport and holder by biometrics (no look-alike fraud)

The **counter-arguments** focus on data security. The main concerns are tracking and skimming (reading out information without permission of passport holder).

Radio Frequency Identification Chips in ePassports

- contactless chipcard
- ISO 14443 transmission protocol
- no internal power supply (inductive coupling)
- non-volatile memory
- maximal read out distance 25 cm
- eavesdropping from about 2 m (experimentally tested by c‘t and BSI)
- c‘t estimated that up to 10 m would be possible (2004)

Logical Data Structure (LDS) containing the following 16 data groups (DG)

Data Group	**German passports since**	**Content**	**Mandatory / Optional**
DG1	2005	same content as machine readable zone	m
DG2	2005	Biometrics: Face	m
DG3	2007	Biometrics: Finger	o
DG4	---	Biometrics: Iris	o
...	---		o
DG14	2007	Chip Authentication Public Key	o
DG15	2005	Active Authentication Public Key	o
DG16	---	Persons to Notify	o
Document Security Object	2005	Hash of data groups 1-15	m

1. Introduction/Overview

Passive Authentication
ICAO mandatory; Authenticity of chipcard data is secured by a digital signature (two level PKI), chip is passive

Active Authentication
Not used in Germany; Identity and freshness verified by Challenge-Response Protocol; Tag authenticates to Terminal

Basic Access Control (BAC)
Optional for ICAO, mandatory for EU; Privacy (unauthorized reading of biometric data) is secured by symmetric cryptography (DES); establishment of Secure Messaging keys

Extended Acess Control (EAC)
Mandatory for Germany; Privacy of especially sensitive data (fingerprint)/ authenticity of chip is additionaly secured by asymmetric cryptography

Outline

1. Introduction/Overview

2. Public Key Infrastructure (PKI)

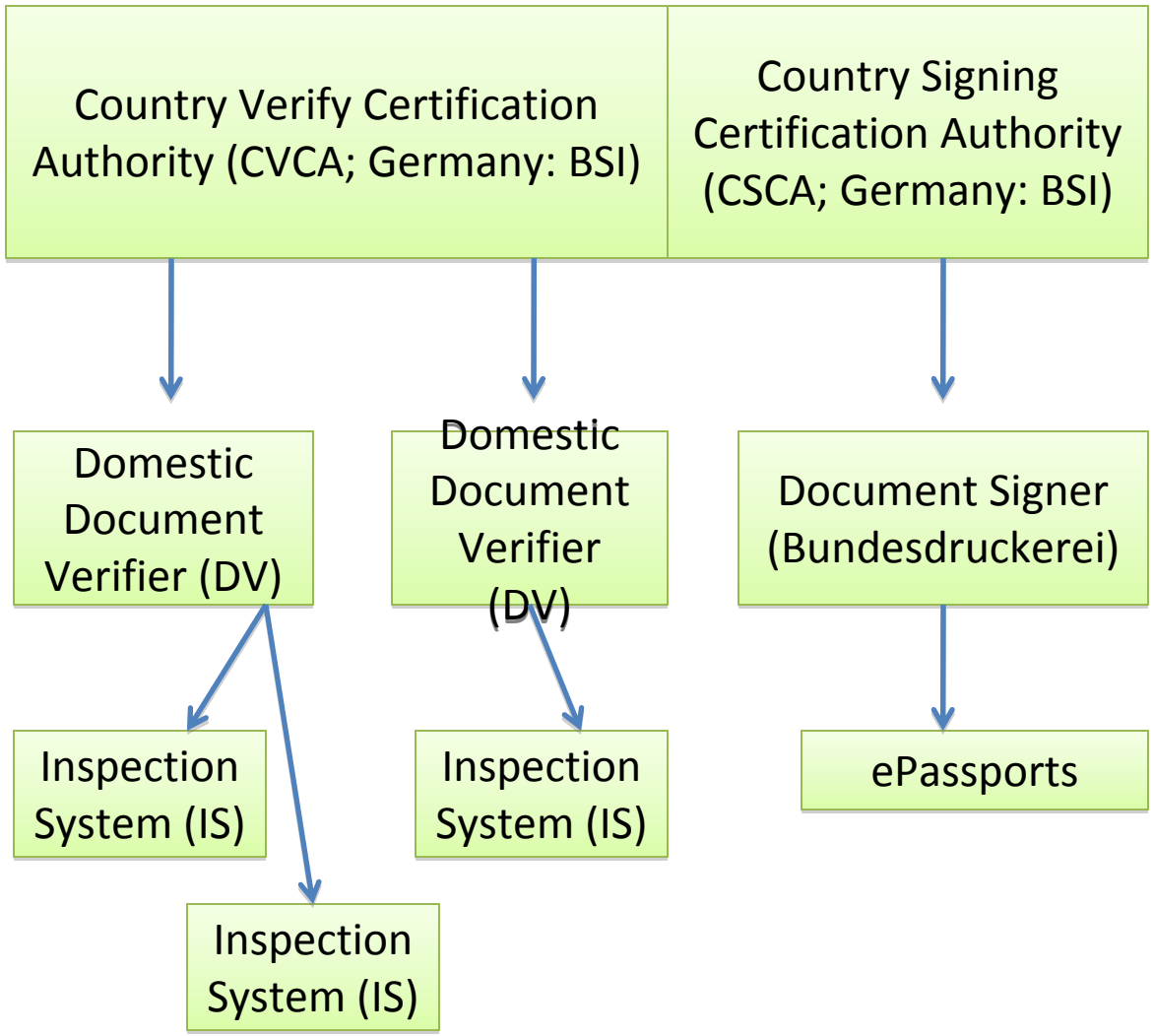
3. Passive Authentication

4. Active Authentication

5. Access Control
    - 5.1 Basic Access Control
    - 5.2 Extended Access Control

6. Conclusion

2. Public Key Infrastructure (PKI) for EAC and PA

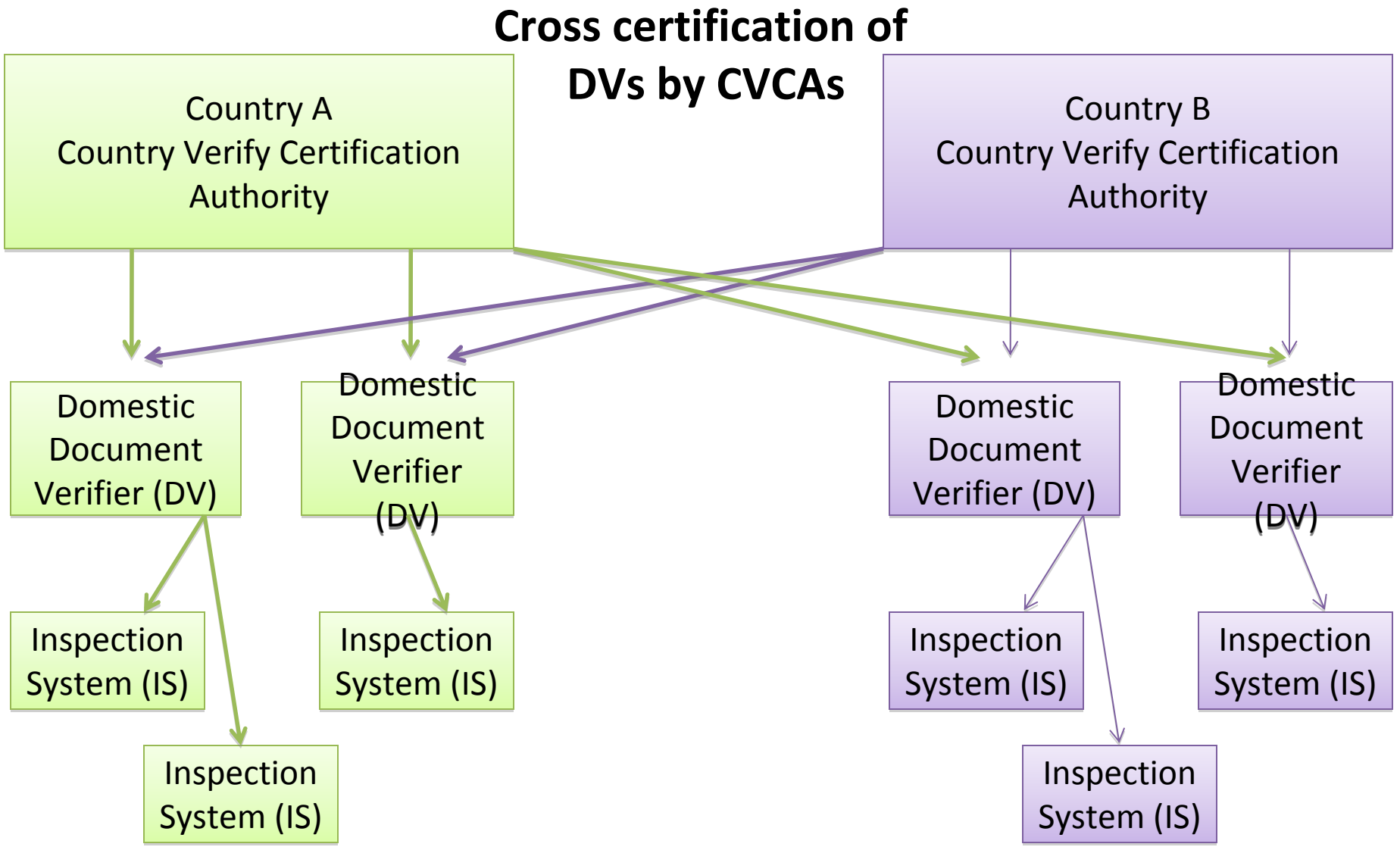


Root of PKI
Typically a government task

DV: Restricts validity period and access rights

Terminals: Obtain access rights via IS certificates

2. Public Key Infrastructure (PKI) for EAC and PA



2. Public Key Infrastructure (PKI) for EAC and PA

- normally chipcards use X509.3 certificates (ASN.1 structure)
- chipcards itself can not parse ASN.1 → use TLV format → Card Verifiable Certificates

Data contained in Card Verifiable Certificates

– Certification Authority Reference

– Public Key

– Certificate Holder Reference

– Certificate Holder Authorization

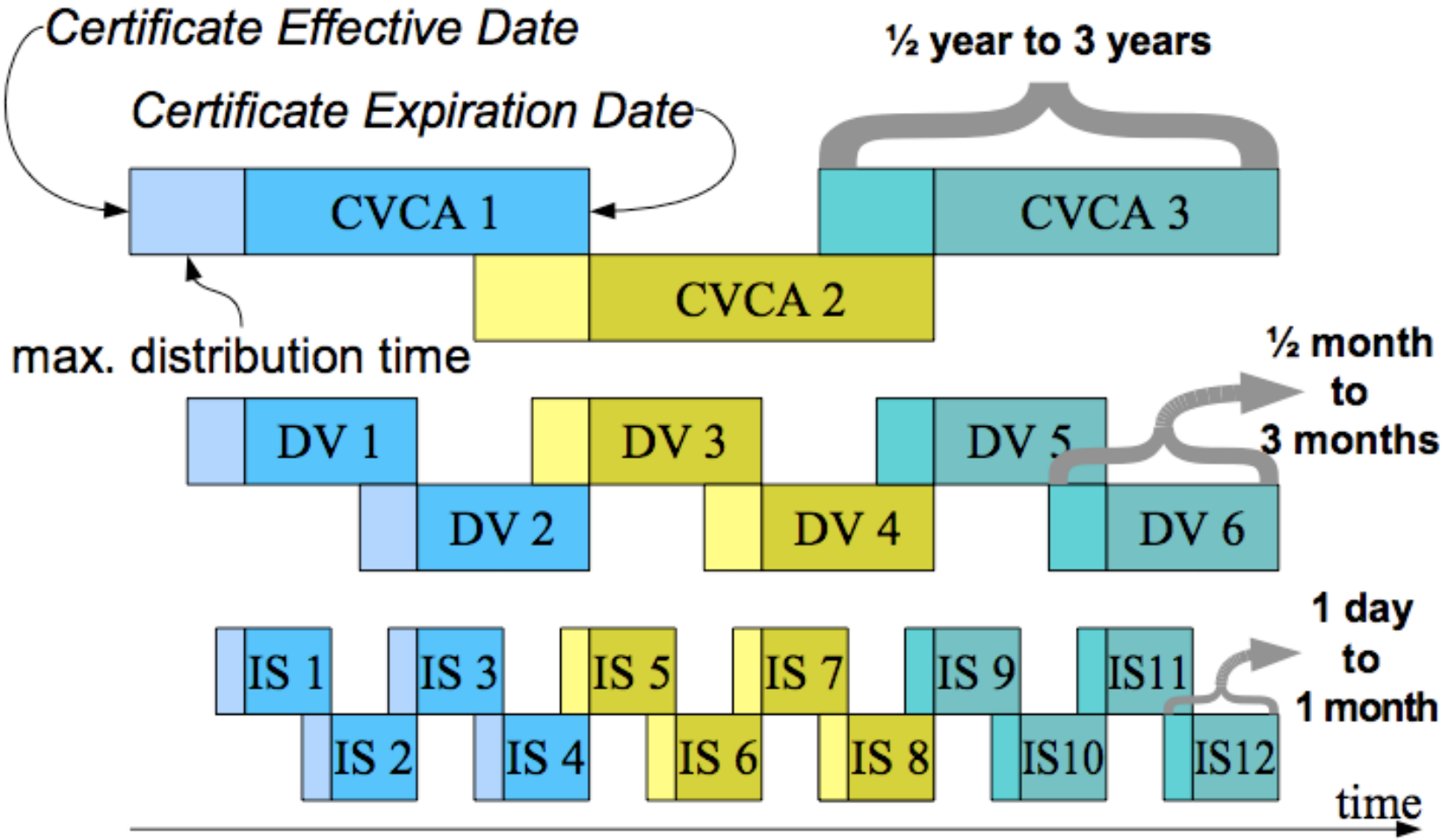
– Certificate Effective Date

– Certificate Expiration Date

– ...

– Signature

Certificate validity



source: Dennis Kügler. Extended access control: Infrastructure and protocol. Talk at Interop-Test Berlin, 2006-06-01, Slides, 2006.

passports are valid for ten years → the CVCA / DV keys have to be secure for 13 / 10 years

Certificate validity

- root public key of the national CVCA is stored on chip

- Problem: RFID has no internal power supply → no internal clock
- Internal date of MRTD is set, when the MRTD has successfully verified the IS certificate
- Certificates are rejected if their expiry date lies before the MRTD‘s internal date

➔ IS certificates have to be changed frequently

Outline

1. Introduction/Overview

2. Public Key Infrastructure (PKI)

3. Passive Authentication

4. Active Authentication

5. Access Control
    - 5.1 Basic Access Control
    - 5.2 Extended Access Control

6. Conclusion

3. Passive Authentication

- the only mandatory security mechanism for the ICAO
- secures authenticity of document

Protocol

1.Reader retrieves certificate of Document Verifier
2.Reader uses the public key from the certificate to verify the digital signature of the passport
3.Reader computes the hash value from the Data Groups and compares it to the value stored on the passport

3. Passive Authentication

ICAO Public Key Infrastructure report offers three choices for the signature algorithm:

- RSA
- DSA
- ECDSA

with the following hash functions:

- SHA-1 and SHA-256 for RSA/DSA
- SHA-1 for ECDSA

Key Length recommendations:

Algorithm	**CSCA [bit]**	**DS [bit]**	**Active Authentication**
RSA/DSA	3072	2048	1024
ECDSA	256	224	160

Outline

4. Active Authentication

- optional protocol in the ICAO first generation specification

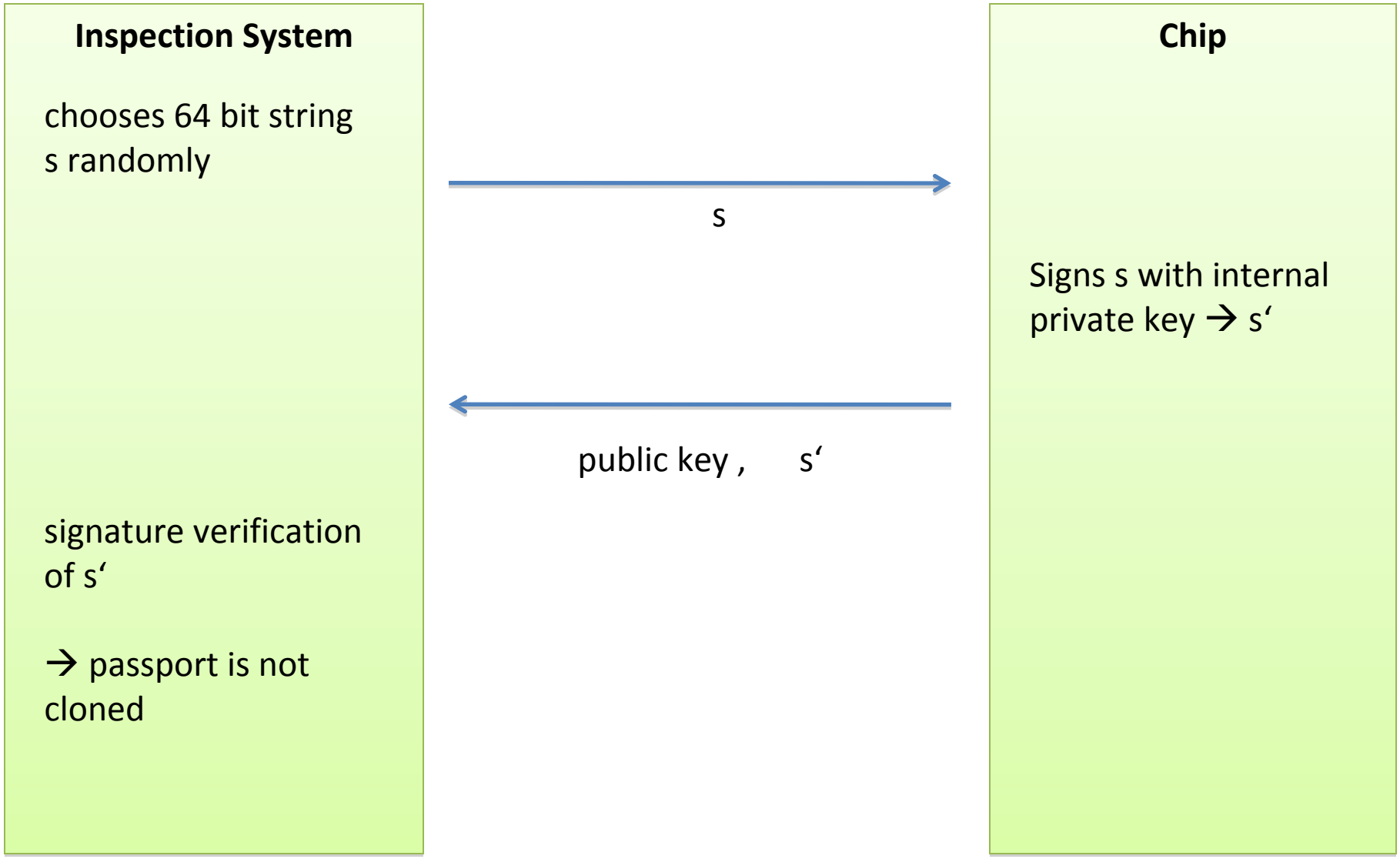
Security Objectives

- secure authenticity of the document
- avoid cloning

Cryptographic mechanism

- Challenge-Response Protocol
- The chip's public key is stored in DG 15; the private key is stored in internal memory

4. Active Authentication



4. Active Authentication

Active Autentication is not used in Germany due to data security concerns. Instead of a randomly chosen string, an information, e.g. a date, could be signed by the chip, so that access to the passport could later be proven and persons could be tracked.

Outline

1. Introduction/Overview

2. Public Key Infrastructure (PKI)

3. Passive Authentication

4. Active Authentication

5. Access Control
    - 5.1 Basic Access Control
    - 5.2 Extended Access Control

6. Conclusion

5.1 Basic Access Control

Introduction to BAC

- Inspection system has to have physical access to passport
- data can only be read out with permission of holder
- avoids skimming

Cryptographic Mechanisms

- Two-Key Triple DES in CBC mode
- Message Authentication Codes (MAC)
- keys are derived from MRZ

5.1 Basic Access Control

read MRZ optically

Chip

Inspection System

Calculate access keys K_{ENC1} and K_{MAC1}

Calculate access keys K_{ENC1} and K_{MAC1}

The Access Keys are derived from the data on the MRZ containing the passport number (DocNo), the date of birth (DOB), the date of expiry (DOE) and check digits (C):

$$K_{seed1} = SHA{-}1\ (DocNo||DOB||DOE||C)$$

$$K_{ENC1} = SHA{-}1\ (K_{seed1}\ ||1)$$

$$K_{MAC1} = SHA{-}1\ (K_{seed1}\ ||2)$$

key derivation function

K_{ENC1} is used for encryption; K_{MAC1} is used for building Message Authentication Codes (MACs).

5.1 Basic Access Control

read MRZ optically

Inspection System

Calculate access keys K_{ENC1} and K_{MAC1}

Chip

choose 64 bit string r_{Chip} randomly

Challenge r_{Chip}

Choose r_{Reader} and K_{Reader} -> encrypt

Ciphertext

$E_{K\_ENC1}(r_{Chip}||r_{Reader}||K_{Reader})$

decrypt
check r_{Chip}
choose K_{Chip} randomly
encrypt

Ciphertext

$E_{K\_ENC1}(r_{Reader}||r_{Chip}||K_{Chip})$

decrypt
check r_{Reader}

Verification is finished

new session keys are computed by Chip and Reader

$K_{seed2} = K_{Reader} \oplus K_{Chip}$

$K_{ENC2} = SHA\text{-}1(K_{seed2}||1)$

$K_{MAC2} = SHA\text{-}1(K_{seed2}||2)$

Threats to BAC

- The entropy of the BAC key is maximal 56 bits, but the key is derived from the information
  in the MRZ
- entropy can be reduced to 2^{20} by investigations (knowledge about MRZ)
- BUT: Brute Force takes still about 12 days
- passport laws changed → random alpha-numeric passport numbers → greater entropy in
  MRZ

Outline

1. Introduction/Overview

2. Public Key Infrastructure (PKI)

3. Passive Authentication

4. Active Authentication

5. Access Control
    - 5.1 Basic Access Control
    - 5.2 Extended Access Control

6. Conclusion

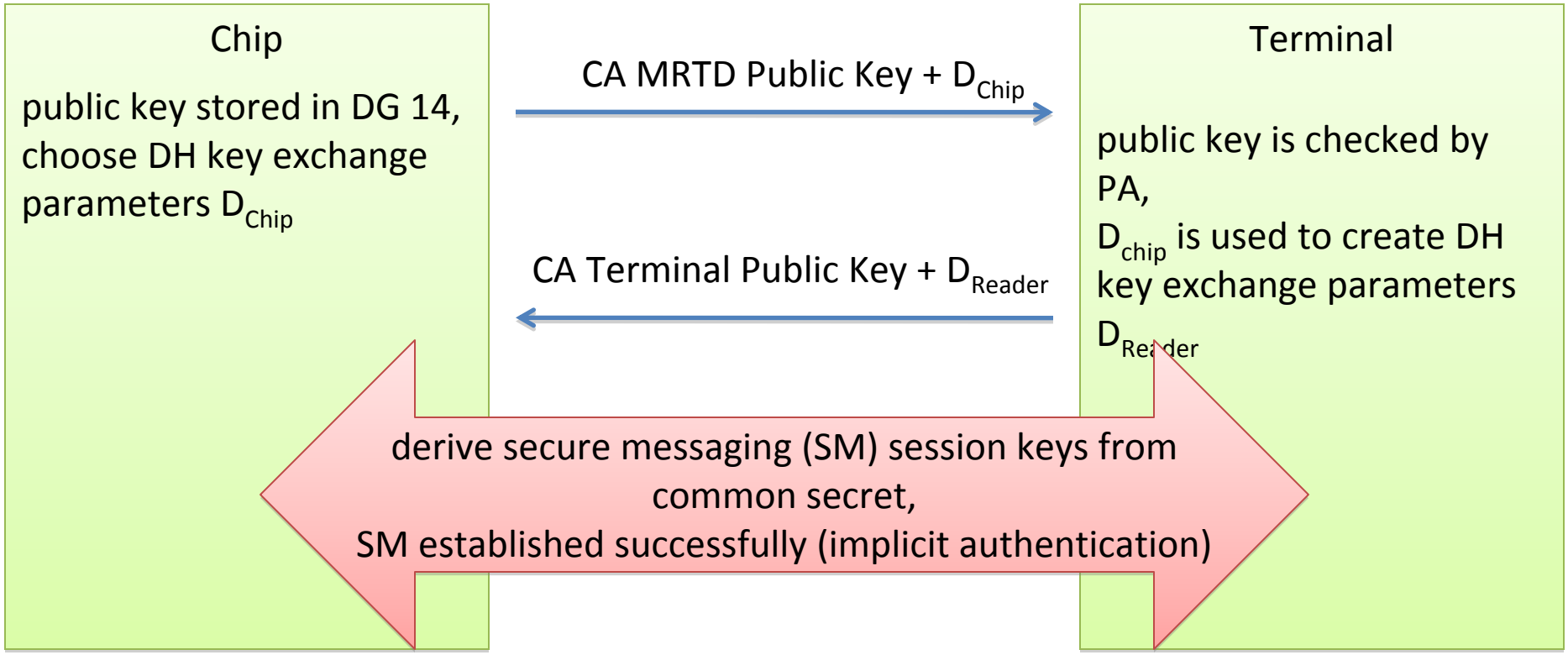
5.2 Extended Access Control

Introduction to EAC

- EU mandatory
- asymmetric protocol
- secure that only authorised readers grant access to sensitive biometrics (DG3: Fingerprint)
- Two components:
    - Chip Authentication (EC Diffie Hellman key agreement)
    - Terminal Authentication (ECDSA or RSA based mechanisms)
- BUT: On-chip asymmetric cryptography computations needed (expensive and slow)

5.2 Extended Access Control – Chip Authentication

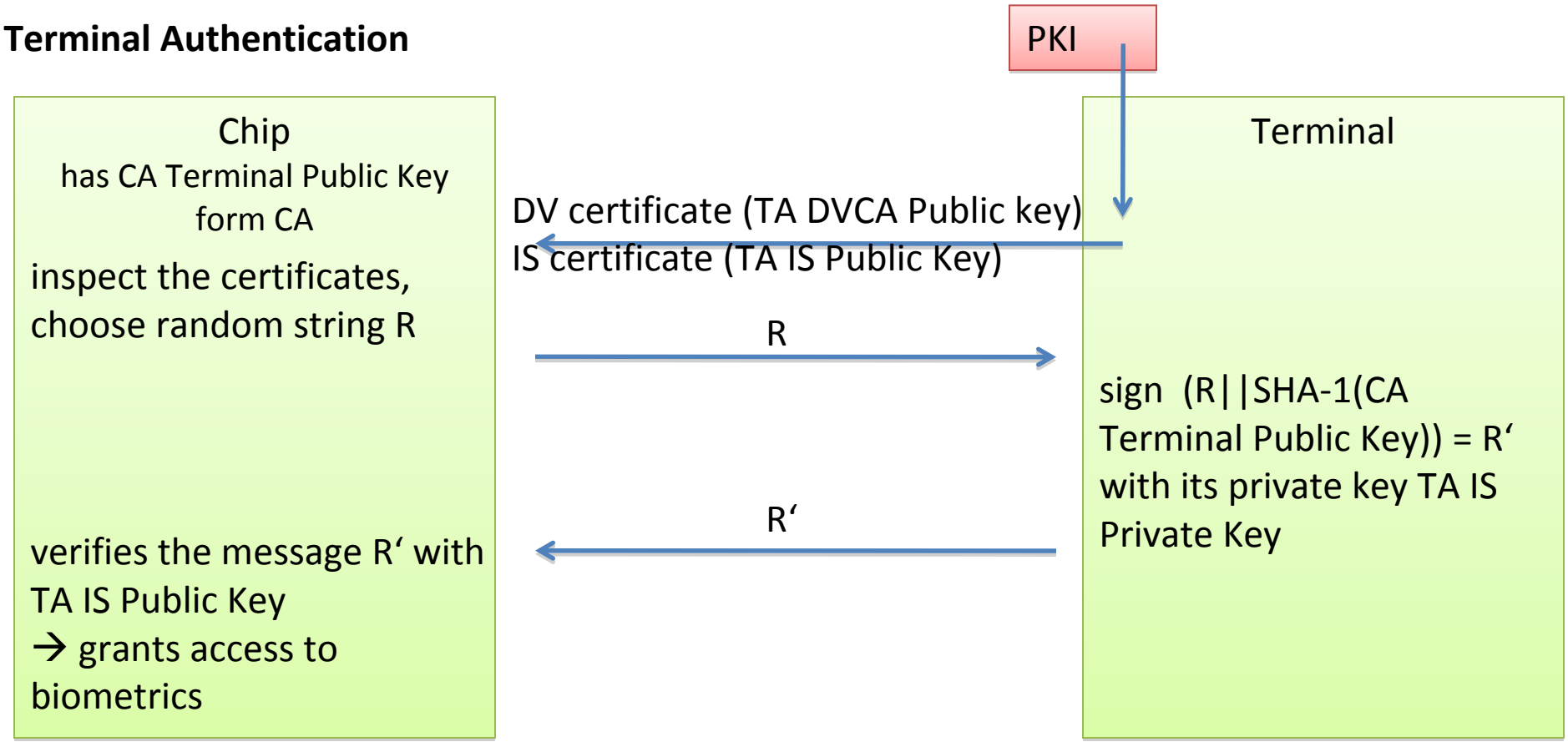
Chip Authentication



From the fact that the chip is able to use these new keys, the terminal concludes that the chip is authentic. The chip does not have to sign the challenge!

5.2 Extended Access Control – Terminal Authentication

Terminal Authentication



Threats to EAC

- The deployed RFID chips are passive, so they have no internal clock. Every time they are activated, their internal date is updated. A Reader with an expired certificate could get access to sensitive data, if the date on the passport has not been updated for a long time.

- As Chip Authentication is performed before Terminal Authentication, the chip could identify itself for non-valid readers.

Outline

1. Introduction/Overview

2. Public Key Infrastructure (PKI)

3. Passive Authentication

4. Active Authentication

5. Access Control
    - 5.1 Basic Access Control
    - 5.2 Extended Access Control

6. Conclusion

6. Conclusion

- new level of security for MRTDs
- counterfeiting of passports very difficult
- connection between passport and holder strong due to biometrics
- skimming and tracking are avoided
- successful authentication cannot be proven afterwards
- BSI did a lot for data security (EAC)

BUT:

- data security concerns due to BAC

➔ BSI developed new cryptographic protocol PACE for german Personal Ausweis (ePA)

Thank you for your attention!

Questions?

References

[1] Kim Nguyen. Contactless authentication protocols for machine readable travel documents (MRTDs). Invited talk at CHES 2007 in Vienna, Slides, 2007.

[2] Dennis Kügler. Extended access control: Infrastructure and protocol. Talk at Interop-Test Berlin, 2006-06-01, Slides, 2006.

[3] Rishab Nithyanand. The Evolution of Cryptographic Protocols in Electronic Passports. IACR Cryptology ePrint Archive 2009/200, 2009.

[4] Dr. Dennis Kügler, Dr. Ingo Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. DuD – Datenschutz und Datensicherheit 31 (2007), 2007.

[5] Dr. Dennis Kügler. Risiko Reisepass? – Schutz der biometrischen Daten im RF-Chip. c't 2005, Heft 5, page 84-89.

[6] Bundesamt für Sicherheit in der Informationstechnik. Technical Guidline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents. Version 1.00 published in 2006, current version 2.01 published in 2009.

[7] Dennis Kügler, Heike Neumann, Sebastian Stappert, Markus Ullmann, Matthias Vögeler. Password Authenticated Key Agreement for Contactless Smart Cards. Slides, 2008.