

2nd Symposium on ICAO-Standard MRTDs, Biometrics and Security

MRP Security Features and Privacy

Dr. Uwe Seidel
Senior Scientist
Bundeskriminalamt
Germany

Tom Kinneging
Senior Project Manager
Sdu Identification
Netherlands

MRTD Symposium
ICAO Headquarters, Montréal
6 – 7 September 2006

Contents

☀ Introduction

- document security basics
- cryptography basics

☀ Protection against data alteration

- data page
- chip contents

☀ Protection against copying

- data page
- chip contents

☀ Privacy protection

- skimming
- eavesdropping

Security Requirements as part of international standards

✿ ICAO Doc 9303 Part 1 (MRPs)

- 5th ed. 2003, Annex to Section III
- 6th ed. 2006, Vol 1, Section III, Appendix 1
- 6th ed. 2006, Vol 2, Section III & IV

✿ Council Regulation (EC) No 2252/2004

Standards for security features and biometrics in passports and travel documents

The e-MRTD: a dual document

☀ Physical Document

- Data page
- MRZ
- Physical security features

☀ Digital Document

- RF-Chip
- MRZ and biometrics
- Digital (cryptographic) security features



Major Security Threats

- ☀ Reproduced documents
should be avoided and forgeries should become more easily recognisable.
- ☀ Attempted falsifications
should destroy the document or leave easily detectable traces.
- ☀ Any illegal issuance
using authentic blanks should be avoided.

Physical Security Measures according to Doc 9303

- ✿ Integrating authenticity features in the document material
- ✿ Protecting the document components with security printing
- ✿ Applying optically variable features to thwart reproduction and copying
- ✿ Using secure issuing techniques to integrate data into the document

Physical Security Measures

Document Material

Passport paper

- ☀ UV dull paper
- ☀ dual tone watermark
- ☀ chemical sensitizers
- ☀ Optional:
security threads
fluorescent fibres



Physical Security Measures according to Doc 9303

- ✿ Integrating authenticity features in the document material
- ✿ Protecting the document components with security printing
- ✿ Applying optically variable features to thwart reproduction and copying
- ✿ Using secure issuing techniques to integrate data into the document

Physical Security Measures

Security Printing

Background and Text

- ☀ two-colour guilloche background pattern
- ☀ rainbow printing
- ☀ UV fluorescent ink
- ☀ security design
- ☀ microprint



Physical Security Measures according to Doc 9303

- ✱ Integrating authenticity features in the document material
- ✱ Protecting the document components with security printing
- ✱ Applying optically variable features to thwart reproduction and copying
- ✱ Using secure issuing techniques to integrate data into the document

Physical Security Measures

Copy Protection

Incorporation of OVDs

- ☀ diffractive optically variable image devices (DOVID)
- ☀ integrated in the laminate
- ☀ or as metallised hot stamping element
- ☀ or equivalent protection



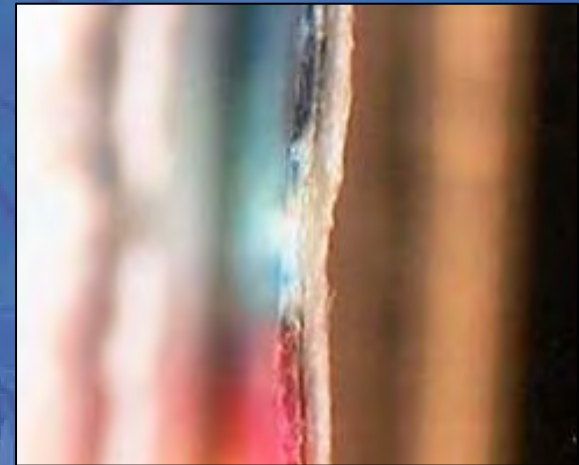
Physical Security Measures according to Doc 9303

- ✿ Integrating authenticity features in the document material
- ✿ Protecting the document components with security printing
- ✿ Applying optically variable features to thwart reproduction and copying
- ✿ Using secure issuing techniques to integrate data into the document

Physical Security Measures

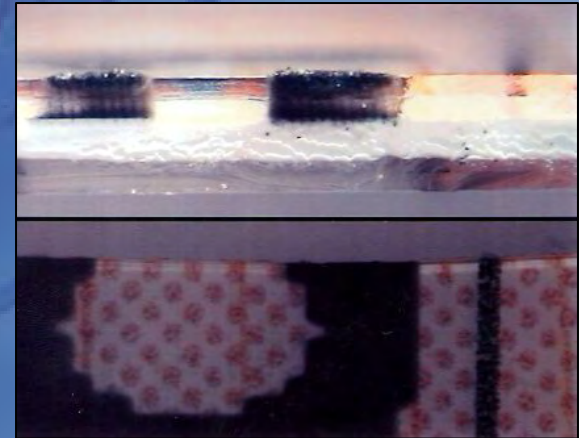
Secure Issuing Techniques

- ☀ Portrait and biographical data integrated in the basic material
- ☀ Secure Personalization techniques
 - electro-photographic
 - thermal transfer
 - ink jet
 - Photographic
 - laser engraving



ink jet data integration

Laser engraving integration



Digital Security Measures

Basic cryptography

- ✱ Hashing for integrity
- ✱ Encryption for confidentiality
- ✱ Signing for authenticity
- ✱ Digital signature

Digital Security Measures

Basic cryptography

Hash function

- ✿ Unique representation
- ✿ Irreversible
- ✿ Public algorithms

Hashing for integrity

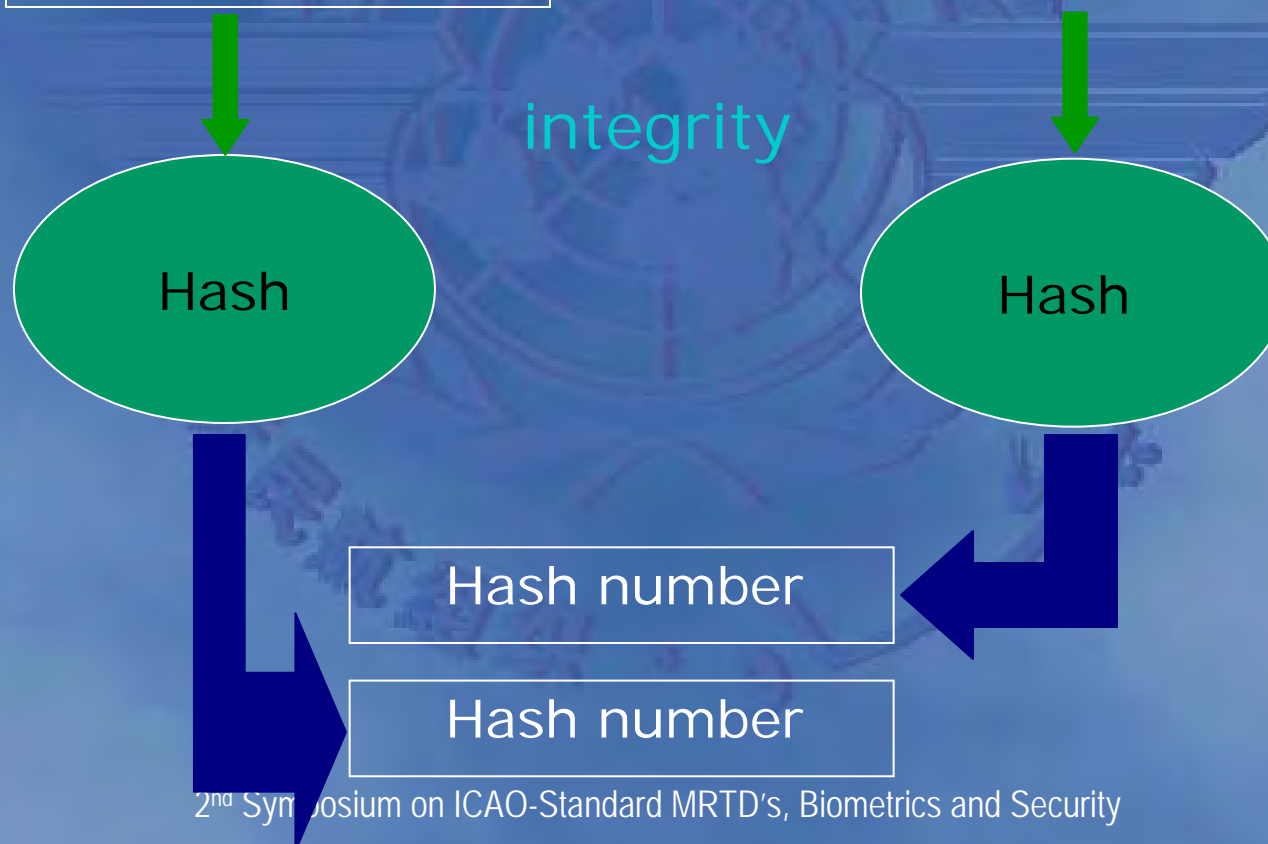


Uwe

"This is an integer message"



Tom



Digital Security Measures

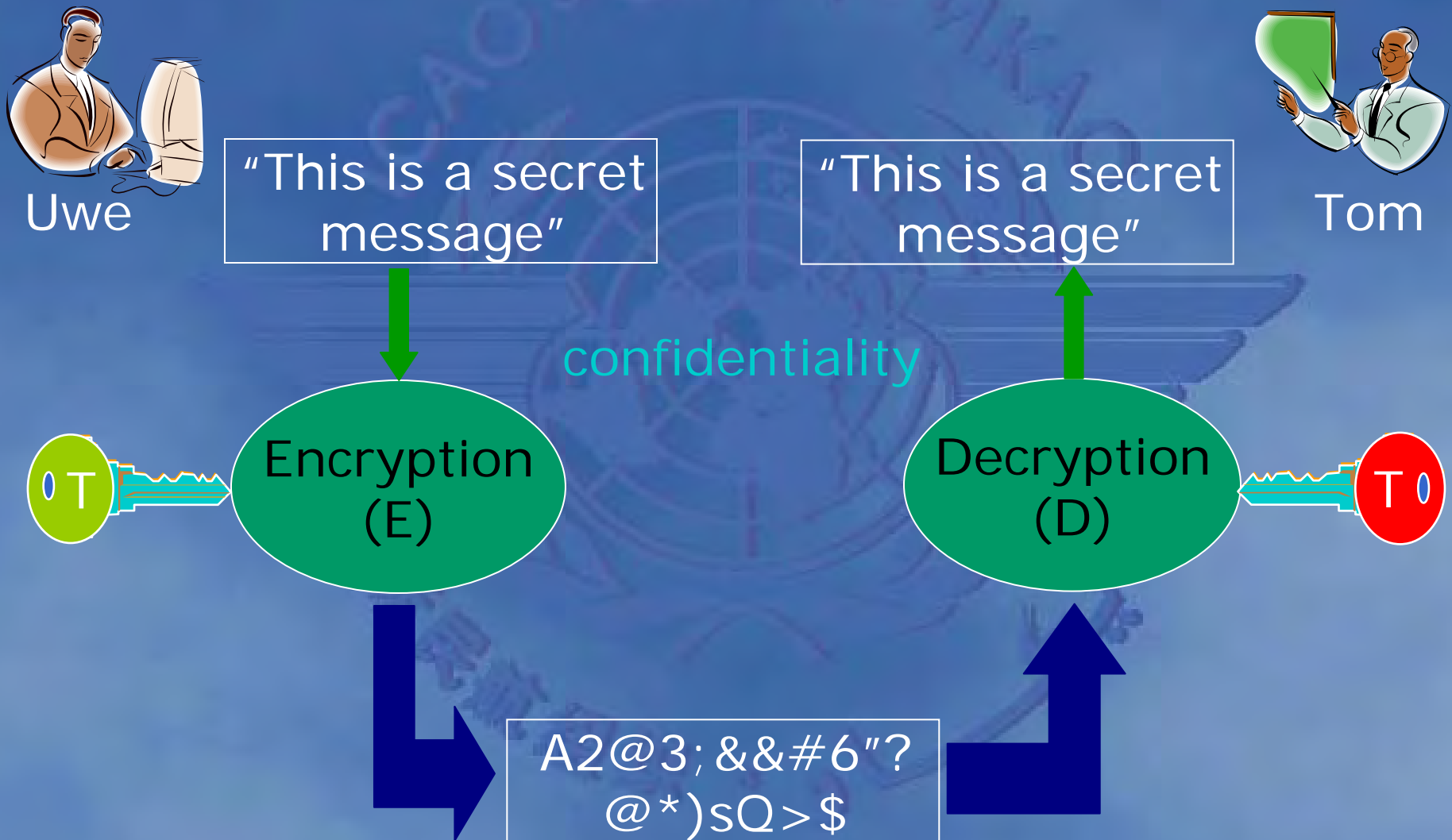
Basic cryptography

A-symmetric encryption/decryption

- ✱ Private/Public key pair
- ✱ Confidentiality
- ✱ Authenticity



Encryption for confidentiality



Signing for authenticity



Uwe

"This is an authentic message"



Tom

"This is an authentic message"

authenticity



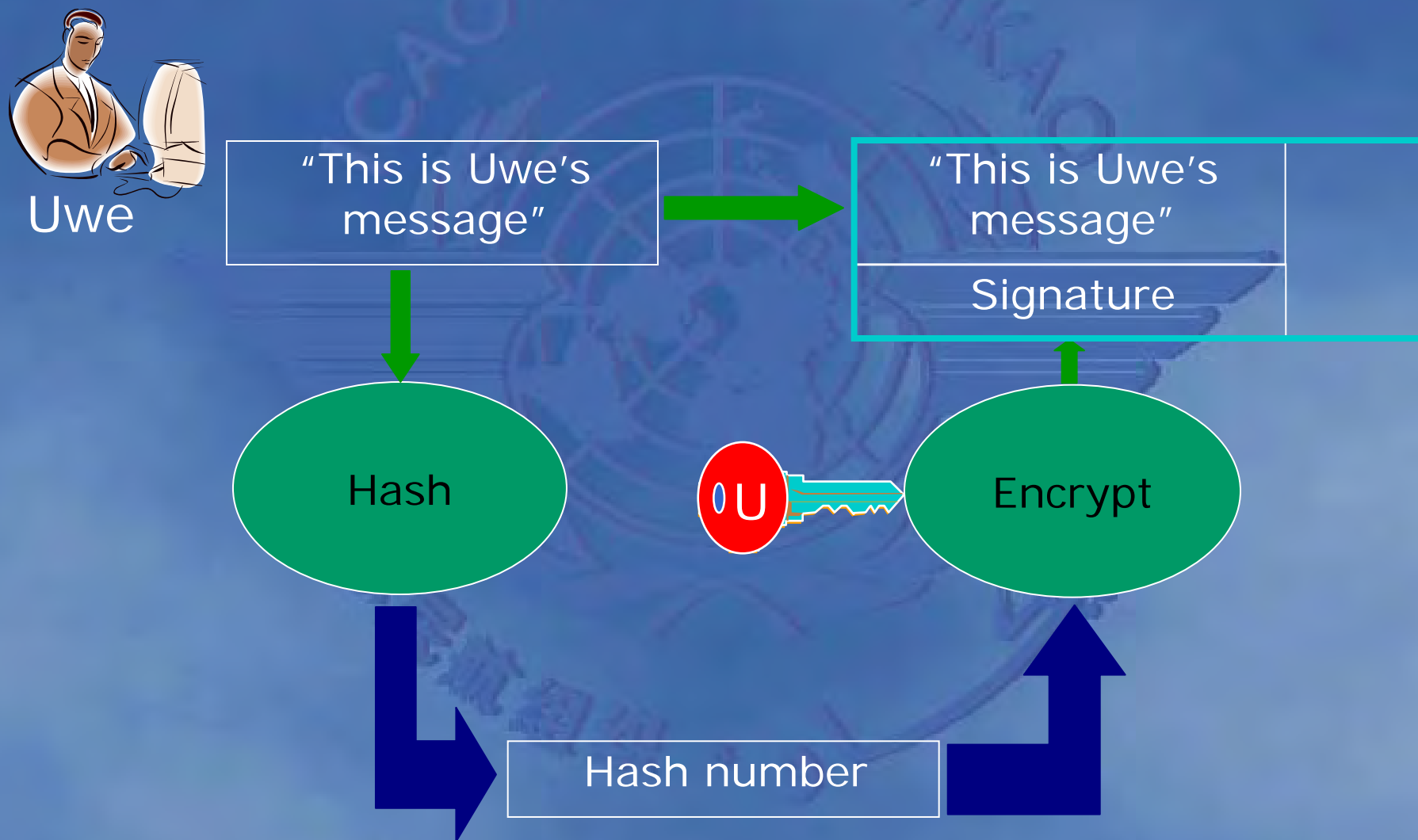
Encryption
(E)

Decryption
(D)



A2@3; &"?
@*)sQ>\$

Digital signature



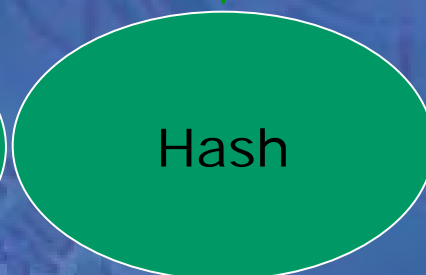
Digital signature



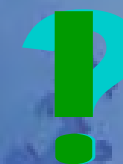
Tom



Hash number



Hash number



authenticity
and
integrity

From theory into practice

- ☀ Physical document security
 - Detected falsifications and counterfeits
- ☀ Digital security features
 - Live Demonstration

Physical: Successful protection against data alteration

Attempted falsifications leave recognizable traces



ink jet personalization



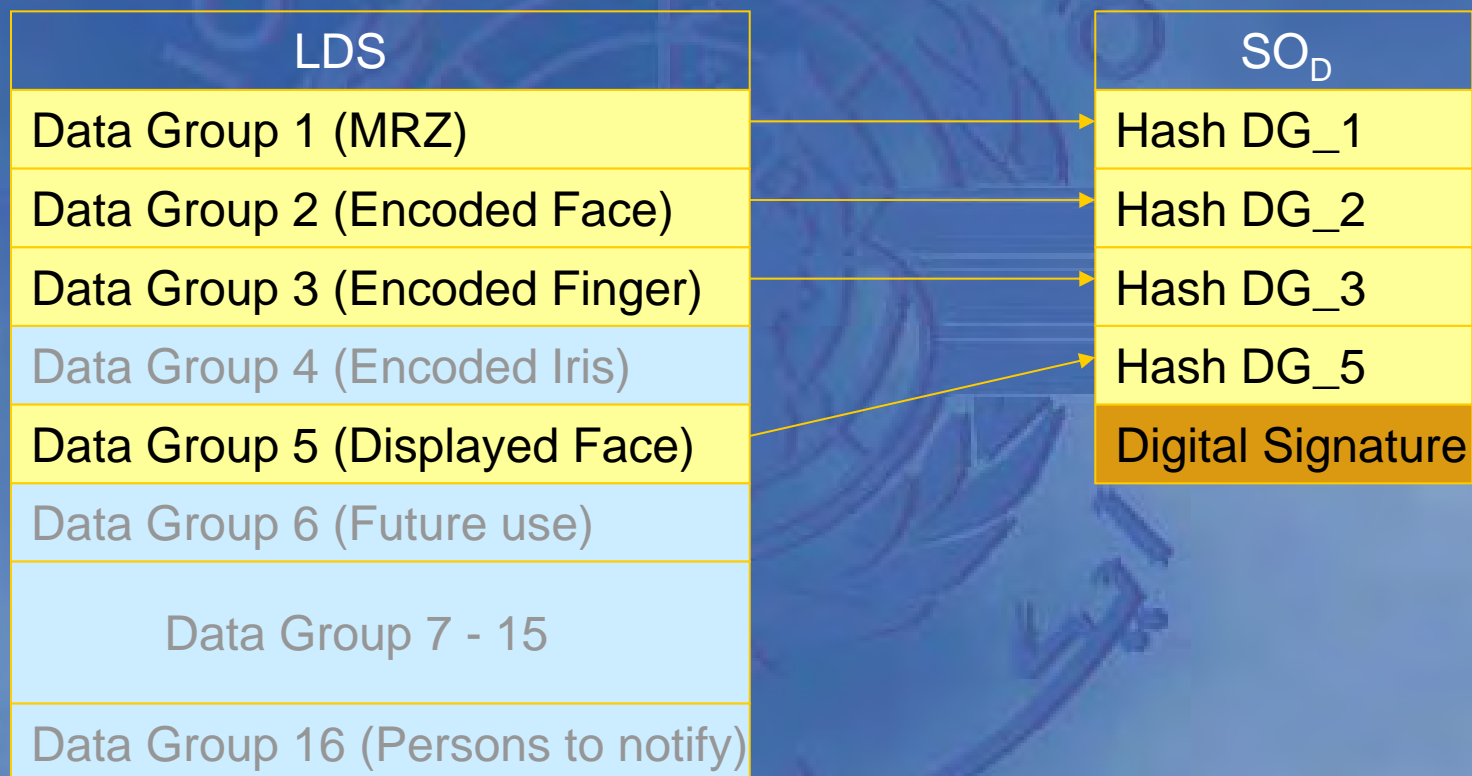
laser engraving

Digital: Successful Protection against data alteration

Attempted changes to data leave
recognizable traces

✱ Passive authentication

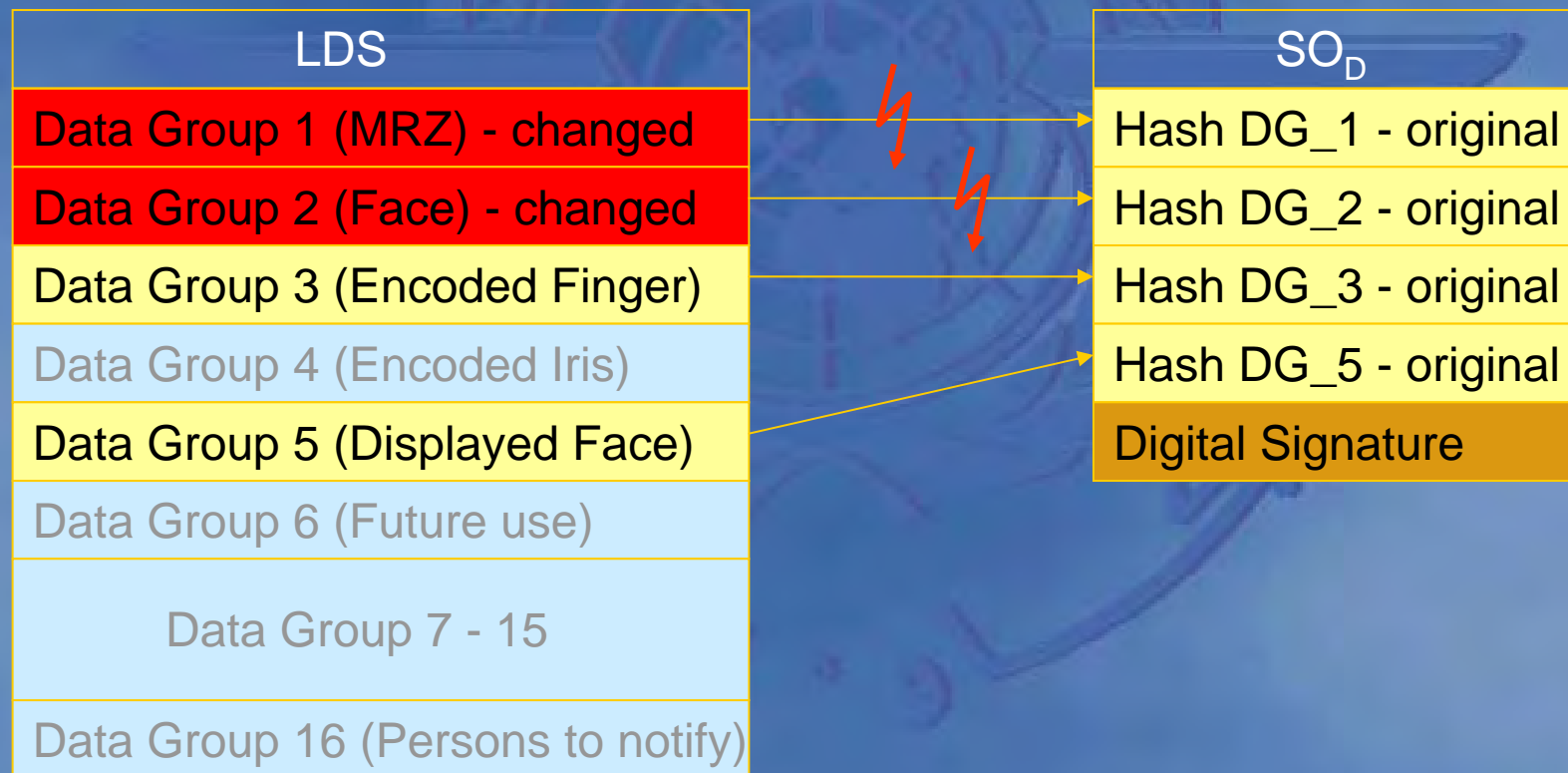
Passive authentication (PA)



Attack 1: Exchange Data Groups

Counterfeiter manipulates
digital personal data
(DG1/DG2)

.... but leaves the SO_D
unchanged



Attack 1 Detected

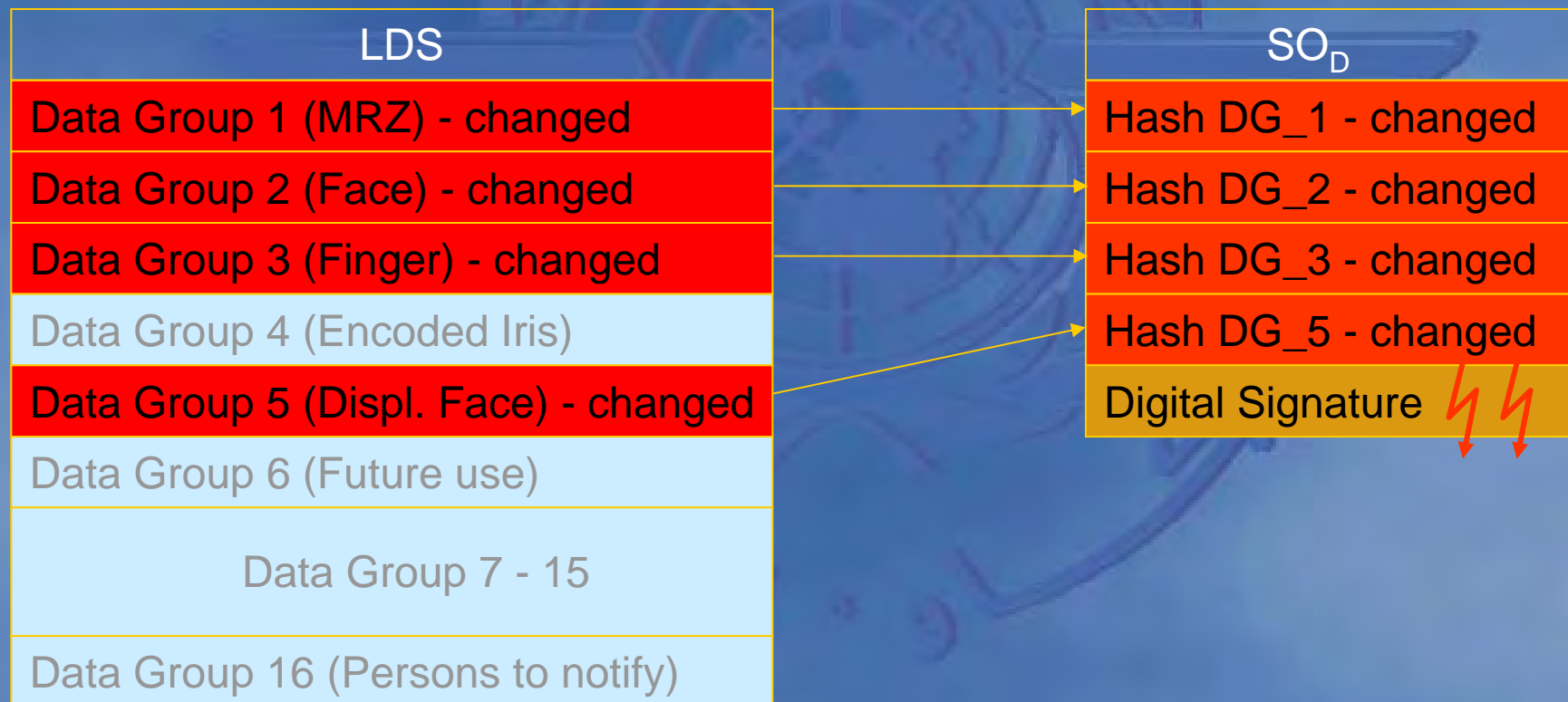
Passive Authentication

- ✱ Wrong hash values

Attack 2: Hash your own data

Counterfeiter manipulates
digital personal data
(DG1/DG2)

.... and changes the hashes
in the SO_D accordingly



Attack 2 Detected

Passive Authentication

- ✱ Digital Signature verification fails

Passive Authentication

Provides protection against data alteration, but...

only if inspection systems perform this ICAO
mandatory security protocol !

Always!

The authors wish to thank K. Nguyen (Bundesdruckerei) for preparing the samples

Physical: Successful protection against copying

Reproduced Documents are easily reconizable by Optically Variable Devices (OVDs)

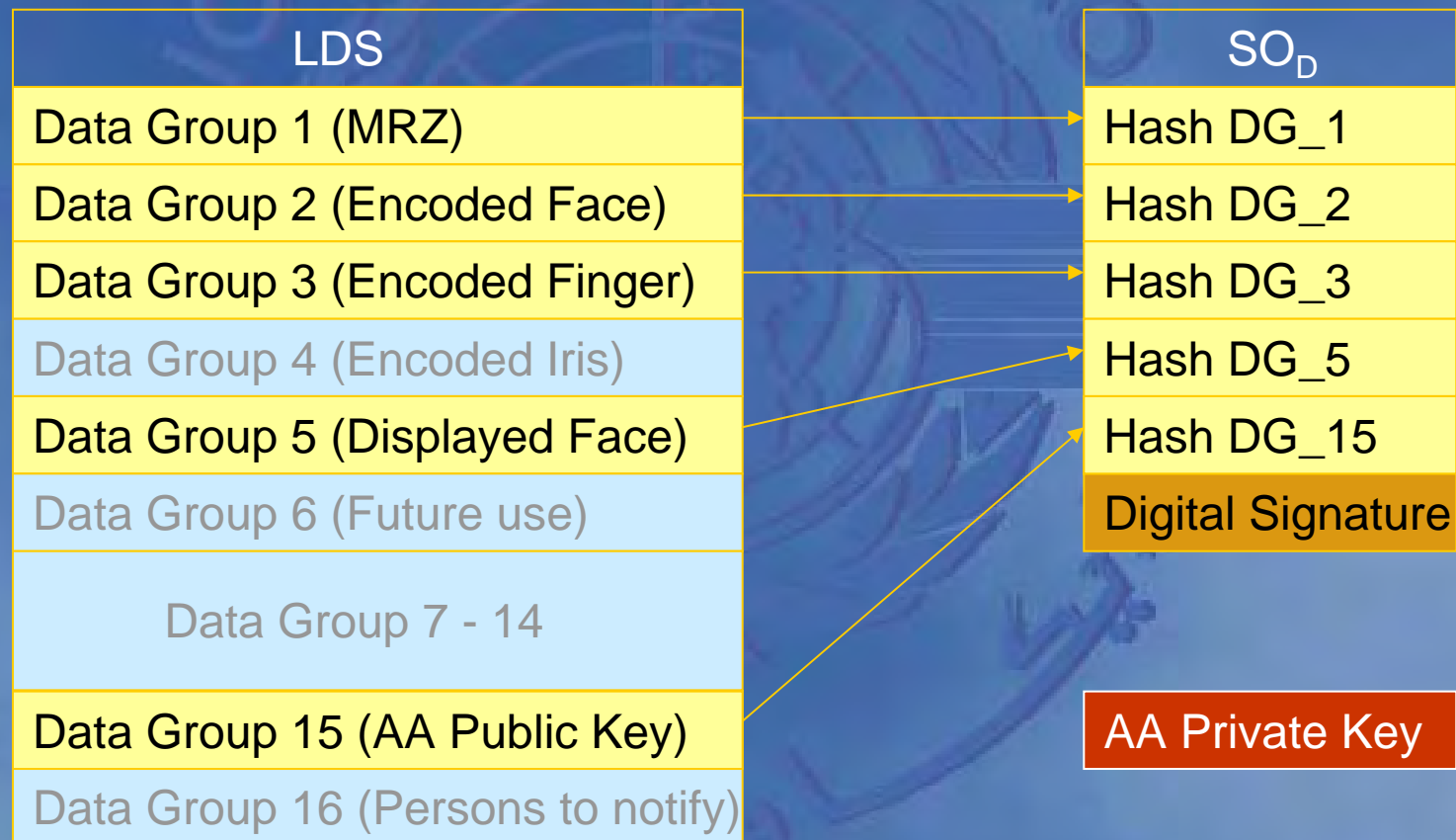


Digital: Successful protection against data copying

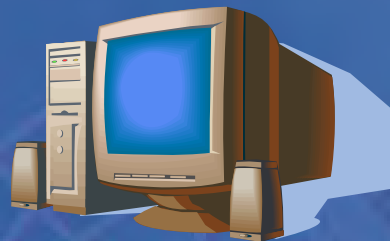
A demonstration

- ✿ Original chip contents
- ✿ Copy
- ✿ Copied contents

Active authentication



Active authentication



14739A239A2

Data Group 15 (AA Public Key)



e-MRTD and Privacy Protection

No problem for “non-e” MRTDs

- ☀ You can't read a closed book!

Problems introduced by RF chips

- ☀ Skimming:
Actively read out data stored on a RF chip
- ☀ Eavesdropping:
passively reading along an existing communication



Skimming and Eavesdropping

Legitimate reading device



e-MRTD with RF chip



Energy →

← Data →

reading distance
0-10 cm



Eavesdropping

Illegal listening into an existing communication between reader and RF chip

Several meters!

Skimming

Illegal use of a concealed reading device, unnoticed by the document bearer

Up to a few centimeters.



Skimming

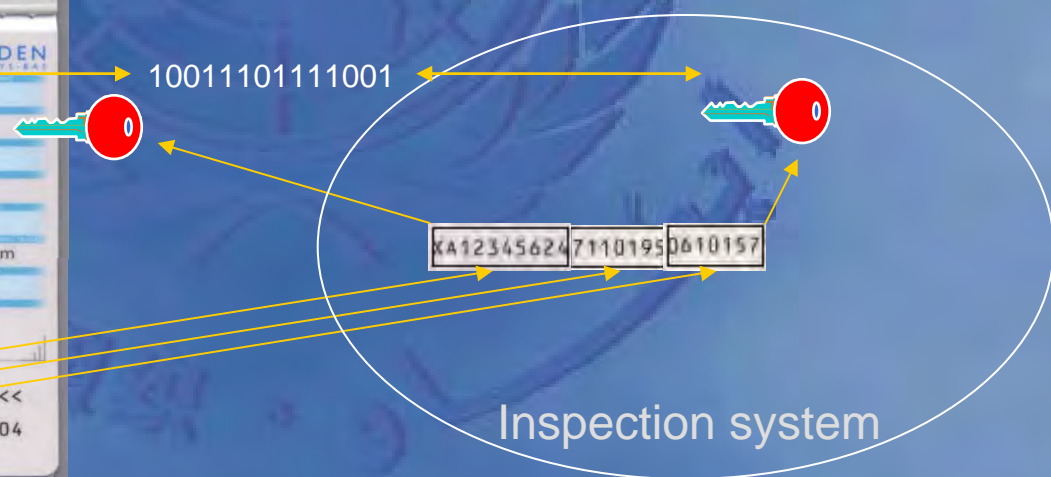
A demonstration

☀ Skimmer

Basic Access Control



Basic Access Control



Basic Access Control

A demonstration

✶ Skimmer

Establishing Trust in e-MRTDs

✱ Physical Security Features

establishing trust in the physical document

✱ Digital Security Features

establishing trust in digital data

✱ Privacy Protecting Features

establishing confidence in the legal and conscious use of personal data

Summary

Physical and digital security measures complement each other to form a modern, machine verifiable document which can be trusted by travelers and control authorities alike.

Thank you for your attention.

Contact information:

Tom Kinneging

Senior Project Manager

Sdu Identification

The Netherlands

Tel: +31 23 7995 218

e-mail: tom.kinneging@sdu-identification.nl

Dr. Uwe Seidel

Senior Scientist

Bundeskriminalamt, Forensic Science Institute

Germany

Tel: +49 611 55 13909

e-mail: uwe.seidel04@bka.bund.de