PKI and Digital Watermark based Biometric Passports

Facts sheet

ICAO security specifications can be fulfilled without RFID deployment

Applied fundaments

- Based on ISO and ANSI security standards
- Applied by different national governments (US)
- Applied cryptographic techniques approved by BSI in Germany
- Compliant with ICAO specifications
- No security by obscurity approach
- Provided security level for the document has no impact on the document holder's privacy

Technology

- First worldwide application of asymmetric cryptographic technologies for passport protection in analogue layout
- Ciphering of biometric data with strong cryptographic key stored in 2D barcode or RFID
- Digital watermark: Invisible security feature for binary digital signature data
- Machine readable (fast and reliable)
- Combination of digital watermarking and PKI schemes creates new barriers against forgery

Advantages

- No need of RFID's or in combination with RFID's
- Extremely cost-saving as actual production process can be reused (figures for Germany: 12% of RFID initial costs, 8% of RFID recurring costs)
- Actual passport layout can be reused
- Independence of third parties (RFID suppliers)
- Very short time for implementation
- Non-sensitive to mechanical or electromagnetic stress
- Usage of existing reading devices
- Digital watermarking with coloured or black/white facial images
- Privacy protection of passport holder is higher than current ICAO solutions
- Backup solution for RFID solutions if chip is damaged

"The Border Security Act stipulated only that biometric identifiers and documents meet ICAO standards, and that the passport be 'machine-readable,'" Sensenbrenner said. "That the EU should choose an elaborate and expensive path to meet the requirement has led to consequences that are regrettable, but not insurmountable."

Wired News, Rep. James Sensenbrenner (R-Wisconsin), Chairman of the House Judiciary Committee, Reporter Kim Zetter, 2005-05-04.

xsmart
swiss security technology

xsmart AG
Allmendstrasse 19
CH – 8320 Fehraltorf
T +41 44 956 51 22
www.xsmart.ch
info@xsmart.ch

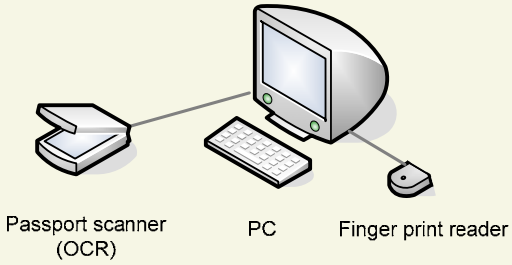
xsmart AG
An der Zeil 17
D – 74906 Bad Rappenau
T +49 7268 960 950
www.xsmart.de
info@xsmart.de

Verification examples

Successful digital watermark and signature verification for genuine identification document.

Signature verification failure for a modified MRZ field.

Faked image data results in watermark and signature verification failure.



Verification system

Product Development

Joint development effort of MediaSec Technologies (Germany and US) and xsmart (Switzerland and Germany).
MediaSec is a subsidiary company of Thomson.

Technical References

- A new low-resolution and robust digital watermarking technique for the personalization of travel documents, A. Herrigel, S. Voloshynovskiy, and Y. Rytsar, Optical Security and Counterfeit Deterrence Techniques VI, 20–22 January 2004, San Jose, California, USA.
- smartID: A new Approach for the Integrity Verification of Analogue and Digital Documents, A. Herrigel, Optical Security and Counterfeit Deterrence Techniques VI, 20–22 January 2004, San Jose, California, USA.
- RFID Identity Theft and Countermeasures, A. Herrigel and J. Zhao, Optical Security and Counterfeit Deterrence Techniques VI,15–19 January 2006, San Jose, California, USA.

xsmart
swiss security technology

xsmart AG
Allmendstrasse 19
CH – 8320 Fehraltorf
T +41 44 956 51 22
www.xsmart.ch
info@xsmart.ch

xsmart AG
An der Zeil 17
D – 74906 Bad Rappenau
T +49 7268 960 950
www.xsmart.de
info@xsmart.de