Joint Research Centre (JRC)

The European Commission’s
Research-Based Policy Support Organisation

Biometrics in Border Management –
Grand Challenges for Security, Identity and Privacy

AAAS Annual Meeting 2008 Boston
17 February 2008
Biometric Passports at European Border Controls

Pravir Chawdhry

Institute for the Protection and Security of the Citizen

Joint Research Centre – European Commission

AAAS Annual Meeting - Boston - 17 February 2008
About JRC and IPSC

• Joint Research Centre:
  – Scientific and technical support to the European Commission
  – Conception, development, implementation and monitoring of EU policies
  – Reference centre of science and technology for the EU

• Institute for the *Protection and Security* of the Citizen (IPSC)

• *Border Security*
  - Identification and detection technologies
  - Privacy and identity management
  - Support successful rollout of **ePassports in the EU**
About JRC and IPSC
Outline

• Motivation & Background
• ePassport
• Challenges
• Conclusions
Motivation – Global Security

• **U.S. Visa Waiver Program – in 2004**

• **Securing external borders of the EU**
  – 11,400km land border + 75,000 km coastline
  – 1,792 external border crossings
  – 300 million crossings per year

• Keep the bad guys out!

• Let the citizens and genuine visitors pass
  – Convenience
  – Speed
  – Accuracy

• *Reduce the risk of impersonation*
  – Strongly link the *passport* to the *real person*
Passport – a brief history

• First introduced in 1414 (Henry V)

• Commonly required for international travel since WW-I

• After WW-II, ICAO introduced worldwide standardization of passports

• 1980s: machine readable passport

• 2004: Biometrics in travel documents
Passport – A Personal Asset of Global Value

- **Identity**
  - Unique official document for the citizen’s *identity* recognized worldwide

- **Privacy**
  - Personal data

- **Security**
  - Tamper-proof
  - Non-transferable
Identity and Biometrics

Three ways to establish identity

1. Something you have
   - Passport / id card
2. Something you know
   - Secret password
3. Something you are
   - Personal traits / characteristics
   = Biometrics
Biometrics – something you are

- Personal traits
- Unique, distinguishable

- Physical (face, finger, iris)
- Behavioural (handwriting, voice, gait)

- Soft v. hard biometrics
Biometric Passport

• **Something you are**
  + **Something you have**

• All European Union countries since August 2007

• Legacy features
  – Printed Page (biodata and photo)
  – Machine readable zone

• Can be read by human as before
Biometric Passport – now & tomorrow

• New Features:
  – Embedded RFID Chip and antenna
  – Facial image
  – Fingerprint images (in EU from 2009)

• Security
  – Improved security markings (infra-red, ultraviolet, watermarks)
  – Access control mechanisms to read the chip
  – Additional protection for sensitive data
Biometrics Passports in the EU – Three Principles

1. **FULLY** readable at all EU borders by authorized readers (biodata, photo, fingerprint)

2. **BASIC** readability at all border controls **worldwide** with the holder’s consent (biodata and photo)

3. Resistant to Eavesdropping
Biometric Passport: Three-way verification

1. **Immigration officer**: Does the person in front of me look like the one on the printed page?

2. **Immigration officer + chip reader**: Do the data on the printed page match with the data stored on the chip?

3. **Biometric matcher**: Do the biometrics of the person match with those stored on the chip?
Security and Privacy in ePassport

• Access control mechanisms – who can read the data on the chip and how much?
• Holder’s consent required
• Basic Access Control
  – Allows reading of chip data same as on printed page
  – Border control authorities worldwide
• Extended Access Control
  – Allows reading of all biometric data
  – Only the EU border control authorities
Basic Access Control (Worldwide)

1. Holder presents the passport
2. Printed page on the passport is scanned (Machine-readable zone)
3. Reader generates a cryptographic key based on the passport data
4. Passport allows the reader to read the basic data using the cryptographic key
Extended Access Control (EU Only)

European Innovation in Security

Chip Authentication

strong session encryption

Terminal Authentication

Access restricted to authorized reading terminals

Digital certificates from 30+ passport issuing authorities

Complex PKI infrastructure
## Overview of Security Features

<table>
<thead>
<tr>
<th>Risks mitigated Security features</th>
<th>Skimming</th>
<th>Eavesdropping</th>
<th>Tampering</th>
<th>Cloning</th>
<th>Tracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shielding</td>
<td>☺☺</td>
<td></td>
<td></td>
<td></td>
<td>☺☺</td>
</tr>
<tr>
<td>Basic access control + Random UID</td>
<td>☺☺</td>
<td>☺</td>
<td></td>
<td>☺☺</td>
<td>☺☺</td>
</tr>
<tr>
<td>BAC + Passive Authentication</td>
<td></td>
<td>☺☺</td>
<td>☺</td>
<td>☺☺</td>
<td>☺☺</td>
</tr>
<tr>
<td>BAC + Active Authentication</td>
<td></td>
<td></td>
<td>☺☺</td>
<td>☺☺☺</td>
<td>☺☺☺☺</td>
</tr>
<tr>
<td>Chip Authentication</td>
<td>☺☺</td>
<td>☺☺</td>
<td>☺</td>
<td>☺</td>
<td>☺☺</td>
</tr>
<tr>
<td>Terminal Authentication</td>
<td>☺</td>
<td>☺</td>
<td>☺</td>
<td>☺</td>
<td>☺</td>
</tr>
</tbody>
</table>
Political Challenges at EU Borders

- Internal borders removed

- Common standard
  - for passports
  - for visa (Schengen area)

- Several implementations
  - 30+ European countries
  - Issuing passports
  - Managing border control

- 30+ National border control agencies
  - Securely read all the EU Passports
  - Read all non-EU passports
ePassport – Operational Challenges

• Trust and Security of the passport issuing process
• Interoperability

• Future technical evolutions in ePassport
  – Electronic visa
  – Immigration endorsement
  – Travel records

• Further demands
  – Automated border clearance
  – Large-scale, distributed infrastructure
  – Trusted traveller and cross-border processes
Identity, Privacy and Security Challenges

• **Identity challenges**
  – How to acquire new identity
  – Managing partial / multiple identities

• **Privacy challenges**
  – *Proliferation of biometrics beyond national borders*
  – *Losing control on own biometrics*

• **Security challenges**
  – Continuously moving target
  – Counter new threats and vulnerabilities
Biometrics at JRC

• Working with EU Member States and technology providers
• Interoperability testing of ePassport protocols – harmonization
• Support to standardization
• Scientific R&D
  – Multi-modal biometrics
  – Biometric security
  – Bio-Crypto convergence
  – Privacy enhancing technologies
  – Distributed identity management
A) Same biometric and different sensors

B) Same biometric, different sensors and multiple views

C) Temporal variation of the same biometric with the same sensor.
Conclusions

• Passport is just one element of border management
• The biometric genie is out of the bottle
• Scientific and technical challenges are just beginning to emerge
• Aim for a positive sum game between security, privacy and convenience
• International collaboration is paramount for success