Developing an EU Member State’s e-Passport, Biometrics, and Border Control Program

Biometrics Consortium Conference

David Coleman
September 23-25, 2008
Agenda

- IBG overview

- Credentials
  - E-Passports and Schengen Visas
    - Documents
    - Enrolment processes
  - European Citizen Card

- Operational Scenarios
  - Consular Operations
  - Border Control

- Conclusions

- Questions
## International Biometric Group

<table>
<thead>
<tr>
<th>Integration</th>
<th>Consulting</th>
<th>Research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flexibility to Choose</strong></td>
<td><strong>Feasibility Assessments</strong></td>
<td><strong>Government Grants</strong></td>
</tr>
<tr>
<td><strong>Proven Expertise</strong></td>
<td><strong>Privacy Impact Analysis</strong></td>
<td><strong>Comparative Testing</strong></td>
</tr>
<tr>
<td><strong>True Multimodal and Fused Systems</strong></td>
<td><strong>Standards Compliance</strong></td>
<td><strong>Bio1.com</strong></td>
</tr>
<tr>
<td><strong>Biometric Management System</strong></td>
<td><strong>Legal &amp; Regulatory Analysis</strong></td>
<td><strong>Market Analytics</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defense Research &amp; Development Canada</th>
<th>California DMV</th>
<th>U.S. Dept of Homeland Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric fusion program with fingerprint &amp; voice</td>
<td>business requirements and RFP development for 30 million fingerprint/face system</td>
<td>Iris interoperability testing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Government Customers</th>
<th>U.S. Transportation Security Administration</th>
<th>U.S. Department of Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large scale multimodal face, finger &amp; iris biometric processing and management systems</td>
<td>Evaluation of biometrics in air travel applications</td>
<td>High confidence fusion techniques and analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Department of State</th>
<th>White House Office of Science &amp; Technology Policy</th>
<th>U.S. Department of Justice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Largest ever facial recognition technology system for visa issuance programs (with Identix &amp; SAIC)</td>
<td>Evaluation of 1:1 &amp; 1:N use of biometrics in U.S. visa issuance &amp; at U.S. ports of entry</td>
<td>Multi-modal biometric system development</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ChoicePoint</th>
<th>Space and Naval Warfare Systems Command</th>
<th>U.S. National Institute of Justice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized infrastructure for transactional biometric authentication, with image processing and large-scale matching requirements</td>
<td>Biometric device evaluation, including technical and operational assessment, IT and access control systems, standardized and non-standardized functions, user and administrator functions, and multiple biometric technologies</td>
<td>Level III fingerprint analysis</td>
</tr>
</tbody>
</table>
E-Passports and Schengen Visas

- Council Regulation (EC) No 2252/2004 specifies ICAO 9303 as the technical specification

- ICAO 9309 defines the requirements for a Machine Readable Travel Document
  - Part 1 – Machine Readable Passports
    - Volume 1 – Visual and Machine Readable Zones
    - Volume 2 – e-Passports and Biometrics
  - Part 2 – Machine Readable Visas
  - Part 3 – Size-1 and Size-2 MRTDs
    - ISO 7810 ID-1 – standard bank card size
    - ISO 7810 ID-2 – standard A7 size

- US Visa Waiver Program
  - Provides guidelines for passport issuance,
  - Case-by-case evaluation by Department of Homeland Security
E-Passports and Schengen Visas, cont.

- E-Passport Physical Document Considerations
  - Biometrics embedded in document, accessed by ISO 14443 contactless interface
  - Sleeve or Cover prevents transmission, reducing sniffing
  - Secured by:
    - Basic Access Control (Initially)
      - Key to data is printed on e-Passport
      - Prevents sniffing from decrypting data
      - Electronic Photograph
    - Extended Access Control (June 28, 2009)
      - E-Passport authenticates itself to passport station
      - Passport station authenticates itself to e-Passport, using certificate chain whose root is the passport issuer itself
      - Electronic Photograph and Fingerprints

- Schengen Visa Physical Document Considerations
  - Sticker affixed in passport
  - Biometrics stored centrally in C-VIS
  - Traveler identified by number on sticker
E-Passports and Schengen Visas, cont.

- E-Passport Enrolment Considerations
  - US Visa Waiver Program
    - Security of application, production and delivery processes;
    - Security of passports and incidence of fraud or misuse
  - ICAO 9303
    - Compliant photographs require either:
      - On-site photographing at enrolment centres
      - Proper use of image quality software at off-site photographers
    - Fingerprint capture requires single finger fingerprint sensors

- Schengen Visa Enrolment Considerations
  - Ten Flat Fingerprints for duplicate check, and later verification
  - Electronic Photograph for later verification
European Citizen’s Card - Biometrics

- For E-Government
  - Defined by CEN/TSA 15480
  - Match on Card as an alternative VERIFY function
  - Fingerprint Templates

- As a Machine Readable Travel Document
  - CEN/TSA 15480 refers to ICAO 9303
  - Store on Card
  - Fingerprint Images
  - Secured by Country’s PKI
  - Required for Residence Permit
Consular Operations

- e-Passport applications
  - For Citizens
  - 1 ICAO compliant face image
  - 2 ICAO compliant flat fingerprint images
    - Possibly 10 if an AFIS duplicate check is used

- Schengen Visa applications
  - For non-visa waiver foreign nationals
  - 1 ICAO compliant face image
  - 10 flat fingerprint images for VIS duplicate check and verification

- Equipment
  - A 4-finger scanner can be used for both enrolments
    - Two enrolment applications must use same scanner, or
    - Custom enrolment software covering both credentials
  - Consular staff may be physically separated from enrollees.
Consular Operations, cont.

- Interfaces
  - VIS for Schengen Visa enrolments
  - Central Passport Office
  - If Central Office does not handle all further workflow, SIS and local watchlist as appropriate

- Data must be securely transmitted internationally

- Biometric Data should not be stored locally

- Enrolment workflow may differ from standard due to
  - Physical space available
  - Security concerns
Border Control

- **Schengen Origin**
  - No mandatory border control
  - Some Border Control stations may be in place for spot checks

- **Non-Schengen Origin**
  - Citizens and Residents
    - Document Authentication
  - Visa-Waiver Nationals
    - Document Authentication
      - **Fingerprint Check depends on issuing country’s PKI**
    - SIS Check
  - 3rd-Country Nationals
    - Document Authentication
      - **Fingerprint Check depends on issuing country’s PKI**
    - SIS Check
    - Biometric VIS Check
Border Control, cont.

- **Interfaces**
  - SIS/SIS II
    - Provides name-based watchlist
    - SIS II allows for download of biometrics for verification
  - C-VIS
    - Provides id number based lookup
    - Enrollees have already passed duplicate check
    - Provides biometric verification
  - National Stoplist
    - Country specific
    - May be textual, biometric, or both
    - May include individuals who do not qualify for upload to SIS
    - Prum Treaty
Conclusions

- Consulate and Embassy operations encourage a common e-Passport and Visa enrolment system for both peripheral devices and the user interface used by enrolment operators.

- Both the Process and Documents should be sufficiently secure to pass US Visa Waiver Program evaluation.

- Border Control interface should handle all possible usage cases, ideally in a single GUI-based application.

- Border Control stations must gracefully handle VIS and SIS interfaces, along with biometric collection for VIS and e-Passport verification.
Conclusions, cont.

- Fingerprint-based document authentication cannot occur without diplomatic and technical agreements with each issuing country, which may lag behind EAC date
  - Border Control operations will evolve over several iterations
  - A fully functional system should be in place initially, but issues may arise as BAC, EAC, and Schengen Visa checks go live

- Wherever possible, common hardware should be used for all biometric processes
  - At the Passport Office, for both enrolment and pickup verification
  - At Border Control, for both Passport and Visa verification
  - At Consulates and Embassies, for both Passport and Visa enrolments
Contact Information

International Biometric Group
One Battery Park Plaza
New York, NY 10004
(212) 809-9491
www.biometricgroup.com