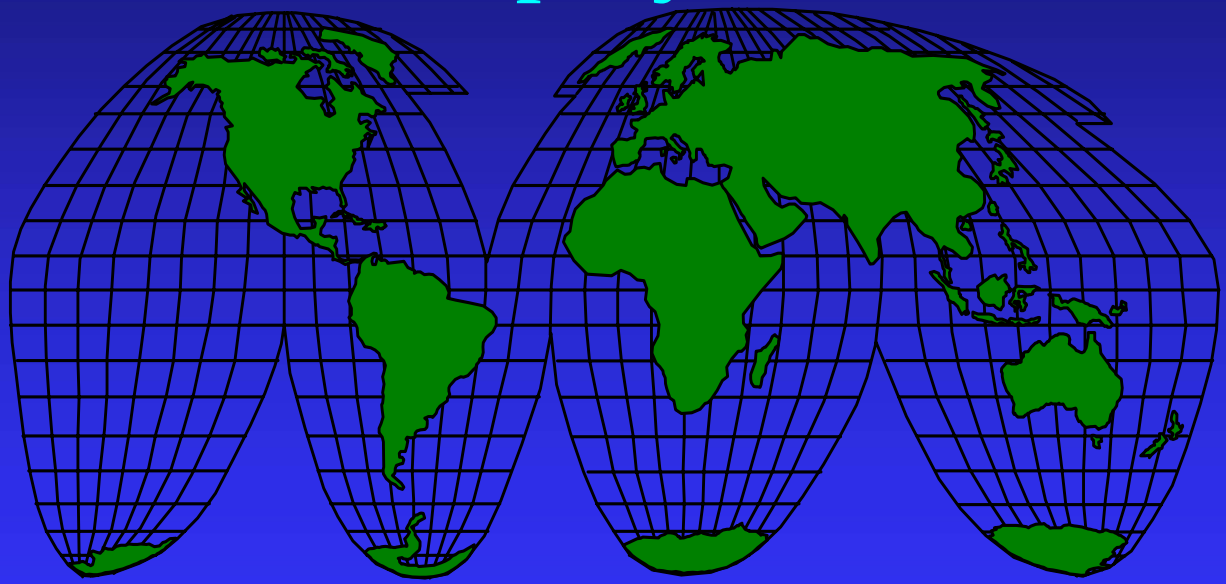
# Machine Readable Travel Documents: Biometrics Deployment



Barry J. Kefauver

Smart Card Alliance

March 10, 2004

# *International Civil Aviation Organization (ICAO)*

- United Nations organization
- Established in 1946 by Chicago Convention
- Headquarters in Montreal
- Regional Offices in 7 Countries
- ICAO Assembly (188 Nation States)
- ICAO Council (33 Nation States)
- ICAO Bureaus comprise the structure (e.g. Air Transport Bureau)

# *International Standards Organization (ISO)*

- Association of various national standards bodies (e.g. SCC, BSI, INCITS/ANSI, DIN)
- Establishes technical standards requiring international cooperation
- Develops test methods
- Membership is voluntary, dues paying and both government and non-governmental (the latter for travel document meetings)
- Serves as official forum for new technologies
- Complex structure for committees and voting
- SC 17 and SC 37 cooperation

# *Documents of ICAO*

- ICAO Doc 9303 when endorsed becomes ISO Standard 7501
- Doc 9303 Parts 1 (Passports) and 2 (Visas) are endorsed by ISO as Std 7501 Parts 1 & 2
- Doc 9303 Part 3 (Other Travel Documents/Cards) endorsed by ISO as Standard 7501 Part 3
- Doc 9303 Part 4, Crew Member Certificates, abolished; survives as Annex J to Part 3
- ICAO document approvals are generally carried out within one year, TR's issued by Work Group responsible

# *ICAO Technical Reports*

- Produced by the Work Groups under the TAG auspices
- The Original TAG/MRTD Biometrics Selection Report
- The Logical Data Structure LDS Technical Report
- The PKI (Security of Electronic Data) Technical Report
- The Contactless IC Chip Technical Report
- The Minimum MRTD Issuance Security Standards Technical Report
- The Minimum MRTD Security Standards/Features Technical Report

  *(The above as input for the Biometric Deployment TR)*

# *ICAO Biometrics Selection Technical Report*

- Developed in 1997- 2002
- Centered around a set of multilateral criteria
- Evaluated factors associated with enrollment as well as inspection
- Considers the compatibility and ranking of the available biometric technologies with the complete set of unique requirements imposed on machine-assisted identity confirmation with MRTD's
- Endorsed by TAG 13 in Feb 2002
- Concluding with the “New Orleans Resolution” in which Facial recognition is THE biometric for global interoperability; fingerprint and/or iris can be used as additional options if countries so choose

# *ICAO Technical Report: Logical Data Structure*

- **What data to store ?**
- **What format to store it in ?**
- **How do you access the data and in what order?**
- **Essentially the rules for making global interoperability possible**

# *ICAO Technical Report: Contactless Chips*

- • Data Storage Technologies Types
- • Which Data Storage Technology ?
- • What Minimum Data Capacity ?
- • Future- proofing & Flexibility
- • “Absolute Minimum” wording
- • Image or Template ?
- • Cropping and storage issues
- • Supporting Research – 12K, 10K, 30K

# *ICAO Technical Report: PKI Enhanced Digital Signatures*

- Risk management
- Data protection, data security and data integrity
- Privacy
- Vulnerability of compromise
- Encryption for protection

# *Ratings Methodology*

- **Compatibility with MRTD enrolment requirements** *(walk-in,mail-in,electronic,outsourced)*
- **Compatibility with MRTD renewal requirements** *(walk-in,mail-in,electronic,outsourced)*
- **Compatibility with MRTD machine-assisted identity verification requirements** *(walk-in,mail-in,electronic,self-service)*
- **Redundancy** *(availability of displayed feature and backup verification method)*
- **Global public perception** *(privacy,health risk,incentive,threat,acceptance,stigma)*
- **Storage requirements** *(template size,compatibility with database,document storage)*
- **Performance** (*speed,accuracy,susceptibility,compatibility,maturity,operational efficiency)*

# *Results:The New Orleans Resolution*

- Face is THE biometric for global interoperability
- Issuers may optionally use fingerprint and/or iris as additions to facial recognition
- Contactless chips are the data storage medium of choice

# *Biometrics Deployment Technical Report – Implementation Framework*

- **Photograph Taking Guidelines**
- **Optimal Storage Sizes Research**
- **Interoperability Specifications**
  - **Face**
  - **Iris**
  - **Fingerprint: Image, Minutiae and Pattern**
- **Annexes designed to provide implementation guidance**

## *Key Considerations: ICAO Technical Report on Biometric Deployment*

- **Global Interoperability**
- **Uniformity**
- **Technical Reliability**
- **Practicality**
- **Future-proofing**
- **Durability**
- **Timeliness**

# *Face—Perception vs. Reality*

- **Traditional Applications**
  - **Access Control (live capture by user)**
  - **Surveillance –poor results**
  - **Third party developers**
- **The above all inhibit obtaining reliable metrics on Facial Recognition**
- **MRP distinguishing traits**
  - **High quality Images**
  - **Constrained images with legacy-year database**
  - **Personally vetted, passport print level quality**
  - **Scanned images**

# *Common Face Traits*

- Already captured and verified now
- No change to the enrolment process
- Immediate deployment –if you already scan and store
- “Watch list matching” capability e.g. terrorism, child abduction
- Always acquired
- Human Verification possible against the photograph
- Children still do not need to appear in person

## *Fingerprint and Iris*

- ID card systems already in place vs. enrollment infrastructure
- Capture and informed consent
- Watch-list availability
- Need to apply in person
- Failure to Acquire

# *Contactless Chips*

- ISO 14443 compliant
- Readable at less than 10cm
- High capacity of at least 32 K
- Data stored for interoperability in accordance with LDS
- Security critical—decision to use PKI-enabled digital signatures

# Border Control Considerations

- States are encouraged to use biometrics to establish or validate identity at border control.
- The use of biometric data does not ensure that a person has provided their correct name, citizenship and other information, but when biometric identity has been confirmed, it does help to prevent the person from using another name in their dealings. Biometric identity should be identified at ports of entry and ideally points of exit.
- If the biometric verification is negative, or there are other actions to be taken determined at the primary port of entry, the traveler may be sent to secondary inspection for detailed inspection.
- Primary or Secondary inspection can include a three-way visual comparison of the MRTD holder, the printed portrait image on the Data Page of MRTD and the stored digital record read from the biometric storage medium in their MRTD (passport) or central database (visa).
- Ideal would be a gate/booth that captures those biometrics noted in that holder's passport, e.g.. booth capable of capturing all 3, but only actually captures based on read of the LDS, if passport holder has face biometric only stored, face (image) is captured; if passport holder has fingerprint and face biometrics in their LDS, fingerprint and face are captured.

# Border Control Considerations (Cont.)

- Procedures need to be determined for how inspection officers would handle exceptions such as when the biometrics on the MRTD do not match the person at the border because the document is not working, the storage medium is damaged or not functioning properly, the verification software does not match the person successfully, the document has been physically tampered with, or the traveler is an imposter. Similarly inspection officers need to be aware of, and have procedures in place, with respect to liveness checking and detection of spoofing.
- States need to change the focus of border systems from merely processing entries and exits, to systems that confirm identities through automated systems; and thereby seek to also identify fraudulent identities and fraudulent travel documents.
- One-to-one verification systems (and one-to-few watch list checking systems) are the appropriate ones to implement at primary inspection. These could be supplemented by use of one-to-many systems at borders as appropriate.
- States need to be aware that land borders present unique challenges – many people cross the same land border regularly for commuting purposes and several people may cross in the same vehicle.
- Border Control systems can be complemented by the use of pre-entry systems including API (Advanced Passenger Information) which may also use verification systems as part of their processing.

# *US Border Security Act*

- **Section 303(b)(2)(A): "The Attorney General, in consultation with the Secretary of State, shall install at all ports of entry of the United States , equipment and software to allow biometric comparison and authentication of all United States visas and other travel and entry documents issued to aliens, and passports issued pursuant to subsection (c) (1)."**
- **Section 303(c)(1): Requires that the Visa Waiver Program ". . . shall be available to foreign countries that shall certify, as a condition for designation or continuation of that designation that it has 'a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization'."**

# *Work in Progress*

- **Testing/Reporting on Facial Recognition pilot programs**
- **Other Biometrics and biometric testing**
- **Biometric deployment TR-next version**
- **Electronic government service delivery, electronic visas and policy for new technology use/data sharing**
- **Technical paper (in draft) on system integrity**
- **Refinement and application of PKI principles and use of digital signatures**
- **Strategy/Vision Paper for an integrated Automated Border Clearance System**
- **Analysis of privacy, data protection and related implications**
- **Incorporate Glasgow/The Hague findings into**

# *Current Issues in TAG*

- **Refining the use of biometrics and the enabling technologies (New Orleans Resolution)**
- **Biometric deployment for global interoperability**
- **Privacy, National Legislation, data use/sharing and the role of Biometrics**
- **Balancing technical influences:cost/performance/effectiveness**
- **Geographic Diversity in issuance as well as inspection**
- **Implementing the choice of next generation storage medium, contactless IC**
- **Address system-related issues affecting overall integrity including breeder documents; these issues shall comprise MAJOR focus in the coming years**

# *The Hague NTWG: Action Items*

- PKI
- Chips
- LDS/Interoperability
- Work papers completed for TAG to ratify in May; standards!
- Papers developed/underway for each area of focus; October 26, 2004 timeline driving specifications issuance urgencies

# QUESTIONS?

**Barry J. Kefauver**

**Jetlag10@earthlink.net**