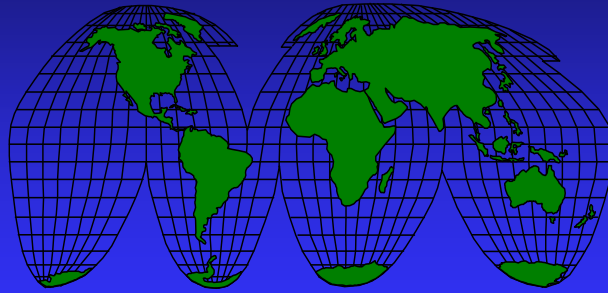


The Use of New Identity Technologies Globally: The Case of Travel Documents



Barry J. Kefauver
Digital Identity Forum
October 25, 2005

International Civil Aviation Organization (ICAO)

- United Nations organization
- Established in 1946 by Chicago Convention
- Headquarters in Montreal
- Regional Offices in 7 Countries
- ICAO Assembly (189 Nation States)
- ICAO Council (33 Nation States)
- Members other than Nations
- ICAO Bureaus comprise the structure (e.g., Air Transport Bureau)
- Technical Advisory Group (TAG)
- Very close relationship with ISO

ICAO Biometrics Selection Technical Report

- Developed over five years
- 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 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

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*)

Co-existing Technologies: Contactless Chips

- Extensive interaction of ISO and ICAO
- ISO 14443 compliant; TR Annex K
- 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

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

Key Considerations: ICAO Technical Report on Biometric Deployment

- Global Interoperability
- Uniformity
- Technical Reliability and Performance
- Practicality
- Future-proofing
- Durability
- Timeliness

Biometrics Deployment Technical Report – Implementation Framework

- Brings together ALL specifications
- Optimal Storage Sizes Research
- Interoperability Specifications
 - Face
 - Iris
 - Fingerprint: Image, Minutiae
- Annexes designed to provide implementation guidance; SC37 compliant
- The successor just underway; Interoperability Implementation

Testing to Date

- Canberra, Australia
- Morgantown, West Virginia, USA
- Sydney, Australia
- Baltimore-Washington International Airport, USA
- Tsukuba, Japan

Post-BWI Expectations

- An Ad Hoc ICAO/NTWG group was formed during the Auckland meetings
- This group met in Berlin on January 10-11, attended by representatives of industry and government
- Intentions were to identify and define the “core” expectations for chip/readers and to provide a common frame of reference for testing.
- That resulted in issuance of a “Guide to Interfacing e-MRTD’s and Inspection Systems”

Tsukuba Testing

- 22 countries total, 16 governments
- Some PCDs read approximately 90% of e-MRPs including BAC and AA (48/51)
- Some e-MRPs can be read with approximately 100% of PCDs (15/16 type B, 15/15 type A)
- Very few errors were encountered using BAC
- Reading time with BAC varied from 3 to 30 seconds
- Total reads of 599/816: 73%
- Focused 20k and 34k Tsukuba data set for DG1 and DG2
- Chose 43 e-MRPs and 8 ICAO reference e-MRPs
- Official e-MRPs from Governments and unofficial from vendors
- Maximum communication distances were 24mm to 50mm
- 848kbps was sometimes elusive
- Some combinations had RF dead zone
- Misinterpretation of Select EF.com after Mutual Authentication

The Wave of the Present: Travel Document Enhancements

- Inks
- OVD's of many hues and flavors
- Paper and accompanying measures to protect
- Watermarks of various technologies
- Security printing
- Many others
- Contactless chips-ISO 14443
- Biometrics-face, finger, iris
- Cryptography-data security and integrity
- Data Sharing-bilateral, multilateral, special-purpose, commercial and government
 - ◆ Bilateral and multilateral data sharing
 - ◆ Law enforcement interfaces
 - ◆ Civil records systems-birth, death, marriage, tax, real estate
 - ◆ Commercial services-document features, background checking, etc.

Primary Challenge: Issuance Systems
A Gun Awaiting to Smoke
~Now the Threats~

- Counterfeit documents
- Theft of blank documents
- Malfeasance, nonfeasance, corruption
- False identity—using genuine evidence obtained improperly to obtain a genuine document
- False identity—using manufactured evidence of support to obtain a genuine document
- False identity—using lost or stolen already-issued genuine documents
- Multiple issuance/multiple identities

Pivotal Factors Affecting system
Integrity

- Procedures and conditions for internal control
- Human resources—greatest strength and weakest vulnerability
- Document issuance and personalization systems
- Legal framework surrounding document abuse

Application and Entitlement Processes Establishing and Verifying Identity

- Breeder documents-over 7,000 differing kinds of US document of birth
- Documentation-establish and prove
- Variables by country-birth, death, marriage, etc.
- Access to official records-databases, commercial services, watch lists, biometric comparisons
- Social footprint-societal interactions
- Training-never ending
- Standards of performance and indices of variances-expectations and a framework so employees know the rules
- Online database linkages-of a wide nature with real time access

Best Practices

- Insure that all aspects of the biometric system(s) are thoroughly understood by all involved, especially the staff on the line and those affected by its administration
- Standards define requirements that must be addressed as minimum specifications both for technical soundness as well as adherence to quality control
- A fundamental first step for system integrity is to conduct a comprehensive risk analysis and THEN construct a risk management profile
- Overseas issuance-inherent differences of culture, infrastructure, external pressures
- Fraud prevention programs-detection, deterrence, follow-up, information sharing
- Monitoring and auditing-border crossings as well as document issuance and entitlement authorizations
- Database linkages and data sharing are multiplicative in impact

Near Term Prospects

- The testing in Japan has been another significant milestone for the direction of deployments and demonstrates the proof of concepts
- TF and WG 3 held meetings in Ottawa in May and Minneapolis in July, NTWG met in Lyon in June, Supplement 9303 issued to update specifications
- Pilot deployment programs and testing will continue, Singapore in November
- Many countries are proceeding toward implementation—over 40 have indicated they will develop programs for e-passports before end of 2006
- This soon-to-be next generation of machine readable travel documents will be the most secure globally interoperable forms of identity determination possible

QUESTIONS?



Barry J. Kefauver
Jetlag10@earthlink.net