Machine Readable Passports: Evolution of ICAO Standards

Barry J. Kefauver

ICAO Sixth Symposium

Montreal, Canada

Summary

- The work on “co-existing technologies” began 10 years ago.
- A number of countries have devoted tremendous work and funds to implement, or are planning to implement, advanced machine readable and electronic passport programs.
- Nearly all countries are now issuing MRP’s; 89 have chips.
- These initiatives are paying dividends with respect to the integrity of the passport as a highly secure travel document.
- That same success is accompanied by increased pressures and recognition of these pressures on all attending systems and activities that issue and inspect these documents.
- There is a growing awareness that conscious and determined efforts are required to identify the risks in issuing and inspecting travel documents, particularly passports, and then defining ways in which those risks might be mitigated and managed.
- It is crucial that the validation tools of integrity and security be used in passport inspection and examination.
- This presentation will discuss decisions of the past as well as focus on the challenges of the future.

ICAO MRTD Program

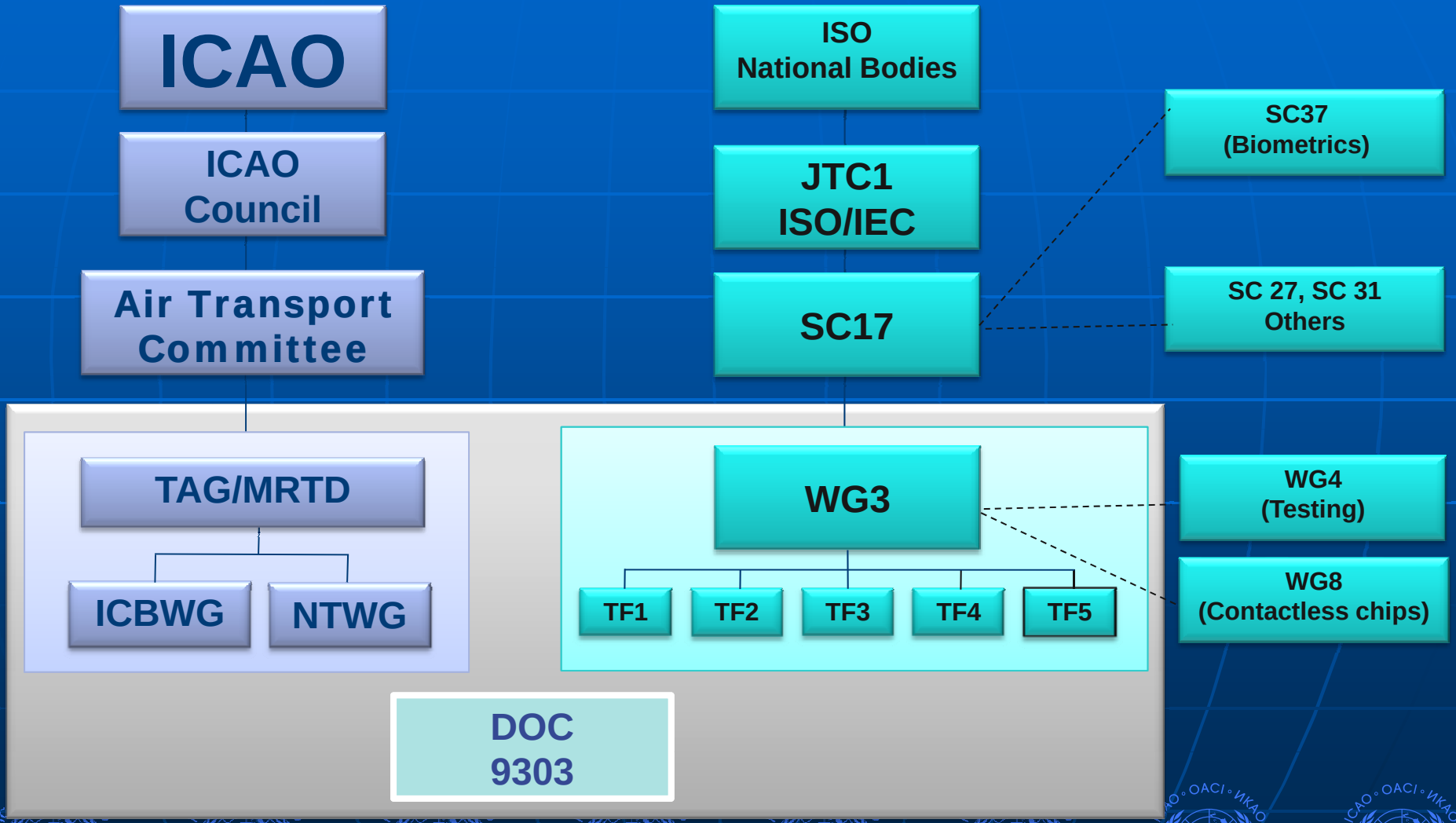
- **ICAO MRTD Program - Critical tasks of Operational Plan 2009-10—A First-- The Business Plan: Security and Facilitation**
  - **Provide assistance to States related to MRTDs upon request**
  - **Conduct workshops on MRTDs and biometrics**
  - **Organize the annual MRTD Symposium and Exhibition**
  - **Publish the MRTD Reports**
  - **Update and maintain the MRTD Website**
  - **Plan training programs for MRTD**
  - **Maintain up-to-date specifications to issue modern, secure travel and identity documents**
  - **Refine the ICAO 2020 vision as the global fulcrum**

Governance

- New Technologies Working Group (NTWG)
  - Ongoing research into travel documents' technologies
  - Development of strategies, policies, specifications and guidance material to achieve standardization and interoperability of travel documents
  - Liaison and joint activity with ISO

- Implementation and Capacity Building Working Group (ICBWG)
  - Established in concept at TAG 18 in May 2008
  - Initial priority was Universal Implementation of MRPs by April 2010
  - Capacity building activities, e.g., Armenia, FYROM, Colombia, priority list developed
  - Third international meeting in Dublin in September

Partnership ICAO/ISO



Critical Alliances

- OSCE
- IOM
- Interpol
- EU
- APEC
- OAS
- UN/CTED
- And others

Document 9303 Development

- London November 2000—Contactless chips
- Biometrics Selection TR 2001
- New Orleans Resolution February 2003—face, finger, iris, chips
- London July 2003--Joint ICAO/ISO meeting
- LDS TR 2003
- PKI TR 2003
- Biometrics Deployment TR 2003
- Canberra testing, February 2004
- Berlin, February 2005—the “Guide”
- Montreal, 2005--TAG acceptance of Edition Six Part 1
- Berlin, May-June 2006—many rounds of testing leading to this
- Prague Conformity and Interoperability Testing—EAC
- Part 3 drafted and approved, published
- ICBWG operational April 2009
- Supplement Edition Eight Posted

The Supplement

- Began as a maintenance vehicle for 9303
- There are now Eight editions that have been posted by ICAO
- The Supplements are must-reading since they are the clarifications and amplifications (not changes) for 9303
- Much PKI guidance, Appendix 1 of Part 1, et al
- The full force and effect of 9303 when issued

Testing History

- Canberra, Australia
- Morgantown, West Virginia, USA
  - A very significant event
  - Participants
- Sydney, Australia
  - Improved, but much work to be done
- Laboratory testing at US NIST
- Several other operational tests, e.g. BWI, Tsukuba, Berlin
  - Each one reflected improved interoperability
- Conformity testing in Prague
- While chip oriented, these testing sessions addressed the total document by necessity

Chips: Fundamental Truth vs. Urban Myth

- 14443 and 180006c/Gen 2
- Skimming

  - Reading the electronic data in an IC chip surreptitiously with a reader in the vicinity of the travel document.
- Eavesdropping

  - When data from an IC chip are intercepted by an intruder while it is being read from an authorized reader.
- Cloning

  - Copying the data that has been placed on a chip

  - Although he can clone the tag, (the hacker) says "...it's not possible, as far as he can tell, to change data on the chip, such as the name or birth date, without being detected. That's because the passport uses cryptographic hashes to authenticate the data."
- Shielding and the Faraday cage

Factors to Keep in Mind

- The so-what test—the pragmatics of mischief
  - Distance
  - Power
  - Visibility
  - At what price?
  - And then “what” do you have?
- Not just a Chip
  - The e-passport is everything that non-ePassports have ever been, but in addition, there is a chip
- Need to inspect fully and properly—”Hacks will not work in a properly functioning inspection system” (Dr. Van Beek)

Biometrics

- The only reason why we have a chip
- The early days post 9/11
- Evolution to the present, politically as well as technically
- Countries underway now or soon to be
- Coming challenges

Nature of Specific 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
- NOT inspecting ePassports in the proper manner

THE Emergent Threat Today

- Highly secure and robust document
- Porous foundation of evidence of identity procedure and source
- Evolution from document fraud to identity fraud
- A topic that demands its own set of presentations
- ICAO Evidence of Identity TR work item underway now

Current Status

- There are approximately 90 countries issuing chip-based passports
- There are currently more than 250 million ePassports in circulation
- There remain a “small” number of countries that need to develop machine-readable passport programs, having missed the April 2010 deadline
- Work continues to refine and enhance, but implementations go quite well
- The inspection of these documents lags behind the issuance programs

Current Issues

- Policy judgments are paramount
- LDS considerations
- Visa specifications
- Next generation technologies, including biometrics (RFI)
- Changing nature of identity fraud--evidence of identity, identity management, including privacy, best practices, etc.
- Data and information sharing
- PKI, PKD, EAC, etc.
- Testing protocols
- Capacity building, priority listing, training
- Machine readable security feature(s)
- Need for full and proper inspection

Conclusions

- The story needs to be told—inform the traveling public of measures being taken and why
- What identity management, the “e” in ePassport and biometrics all do FOR you rather than TO you
- Make certain that the “readable” part of “machine readable” is fully carried out
- Take pride in the past, but be vigilant to prepare ourselves for the future

Thank you for your attention…

Barry J. Kefauver

Jetlag10@earthlink.net