ePassport…Really?

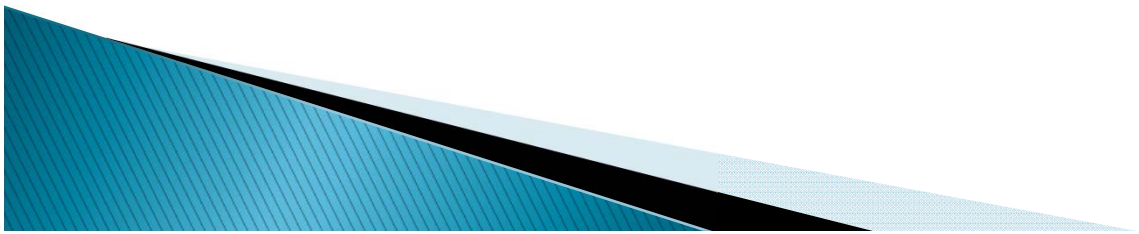
Barry J. Kefauver
ISO/USA

Summary

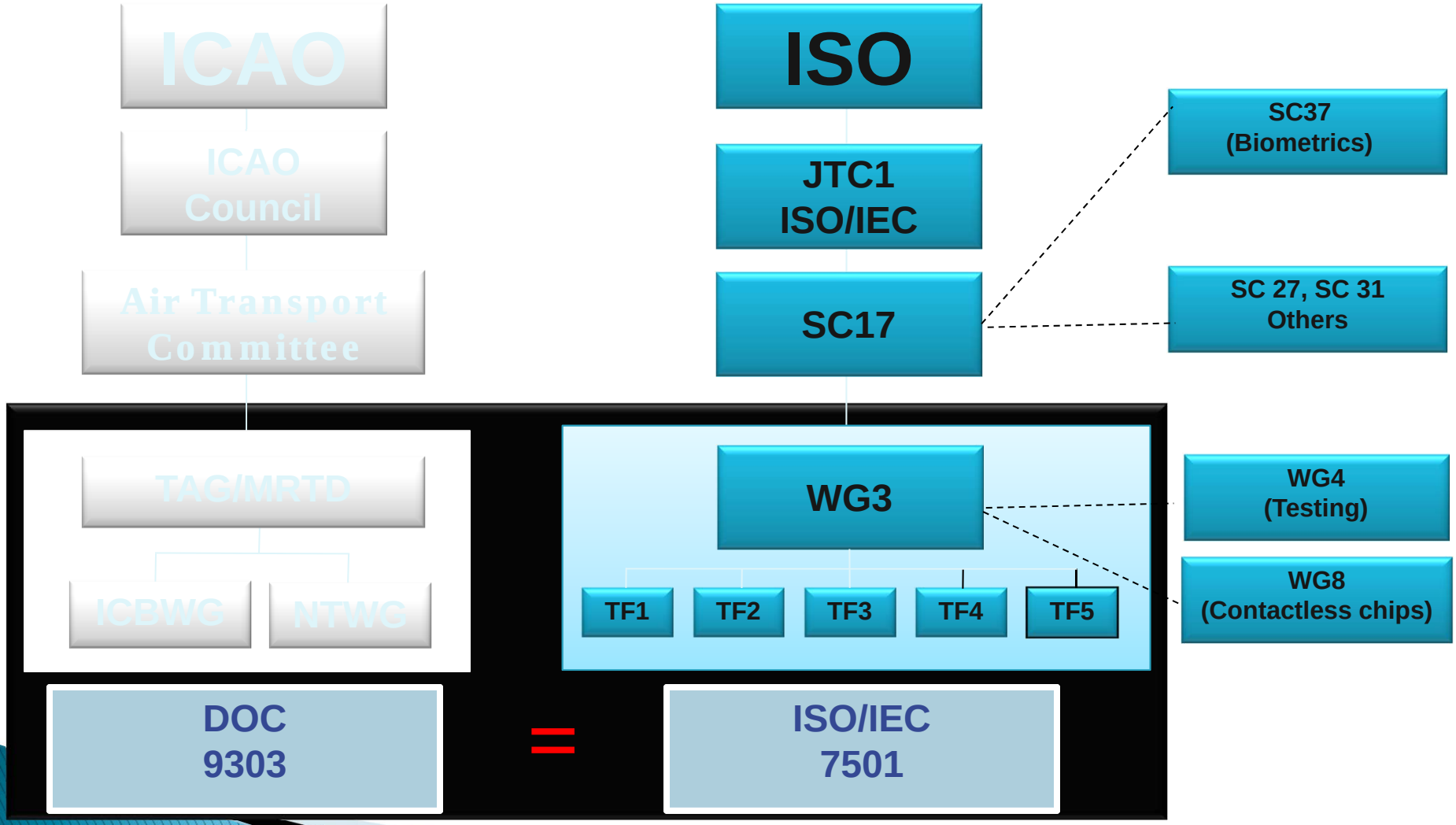
- **There have been enormous strides made over the past decade in researching, designing, developing and deploying today's generations of travel documents.**
- **Building on the fundamental specifications of ICAO Document 9303, the most recent results of these efforts have been the incorporation of RF chips and biometrics in passports and other documents.**
- **This presentation will describe these efforts, provide an understanding of how we have gotten where we are and provide some insight into the work now underway on the next generation of travel documents.**
- **The fundamental message of this presentation is to convey the benefits of ePassport implementation as well as the requirements that are needed to insure that the "e" is carried out in ways that will USE the capabilities of the technologies.**

Current Status

- There are more than 100 countries issuing chip-based passports
- There are over 420 million ePassports in circulation
- There remain a very small number of countries that need to develop machine-readable passport programs to comply with the ICAO April 2010 requirement
- The deadline of 24 November 2015 is of current concern
- Work continues to refine and enhance, but implementations go quite well
- The inspection of these documents lags far behind the issuance programs

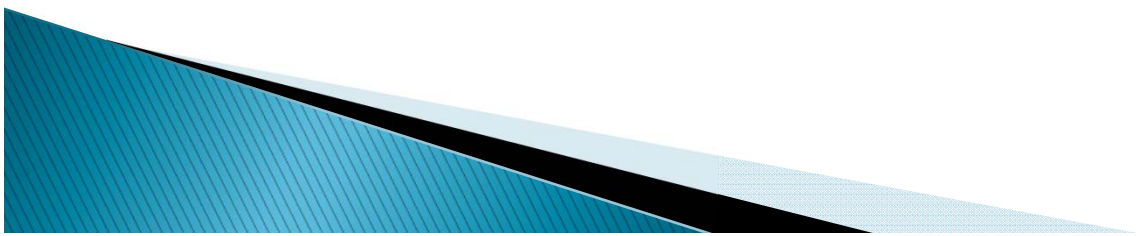


Partnership ICAO/ISO



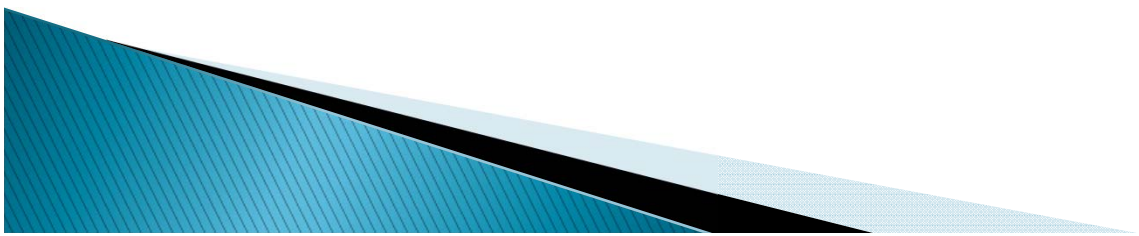
Threshold Questions

- Do I want an ePassport system?
- Do I need an ePassport system?
- Am I prepared to USE an ePassport system?
- Is the integrity of my current process consistent with and complementary to the technological advances of an ePassport program?
- “Make everything as simple as possible, but not simpler.” – Albert Einstein



Do You Want an ePassport System?

- Have you done a comprehensive risk identification and management analysis of your present system?
- Are you confident that your vulnerabilities will be identified and corrected to take advantage of the ePassport?
- Why is an ePassport useful to your country?

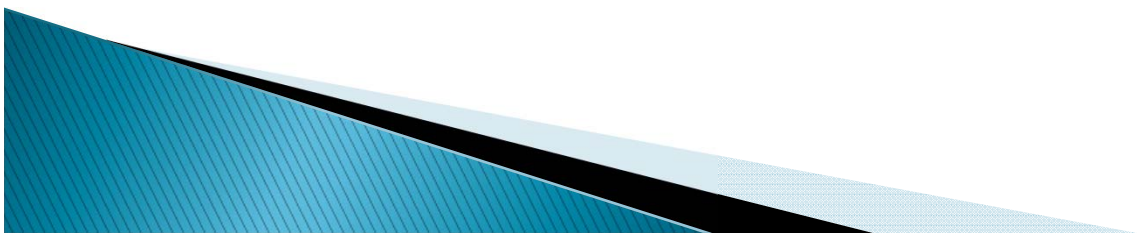


Do You Need an ePassport System?

- What will the “e” do that a traditional MRP will not?
- Are you prepared to take advantage of the extensive economies of scale (centralization) often accompanying ePassport implementation?
- Have you considered the impact on overseas issuance?
- Is your border management procedure and process equipped to deal with inspecting ePassports?

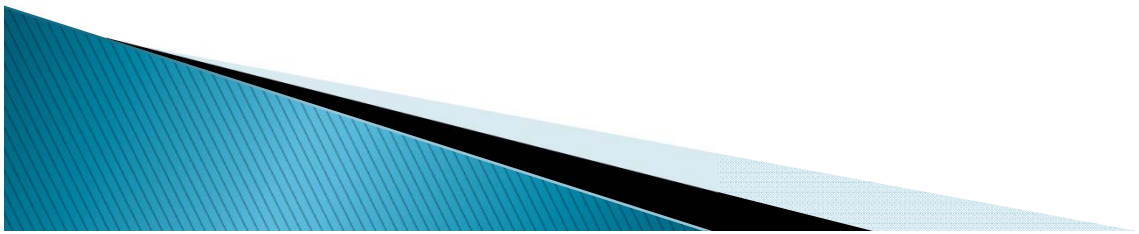
Are You Prepared to USE an ePassport System?

- Are your inspection processes ready to use the cryptographic keys in ePassport?
- Are you going to join the PKD prior to ePassport implementation; have you taken appropriate budgeting precautions?
- Have you prepared your traveling public for the changes that biometric capture and use will bring about?



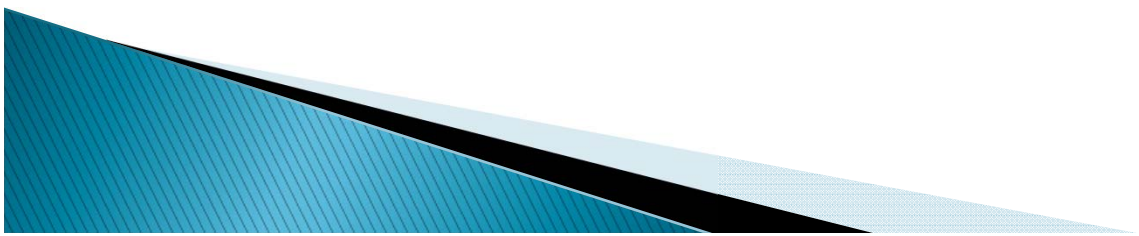
Overall System Integrity: Is Yours Enough?

- Is the integrity of the current issuance and handling process consistent with and complementary to the technological advances of an ePassport program?
- Are evidence of identity procedures and safeguards as strong as the document that you issue that alleges identity?
- Have you effected changes to insure to respect personal privacy of biometric and other data?
- Have your human resource issues been thoroughly addressed?
- Do you comply with both the letter as well as the ***spirit*** of 9303?
- Have you examined overseas issuance considering inherent differences of culture, infrastructure, external pressures?
- Will emergency travel documents be a fraudster loophole?



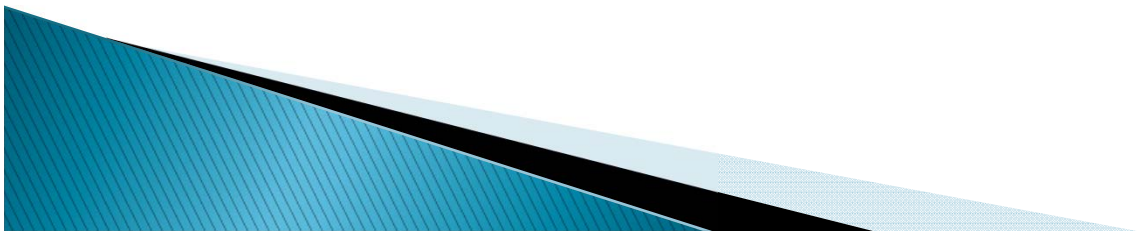
Measures of Integrity

- Human systems-zero tolerance
- Work atmosphere and environment
- Evidence of identification
- Spoiled document handling
- Blank document controls
- In-house auditing
- Penalties-legal/judicial system as well as administrative



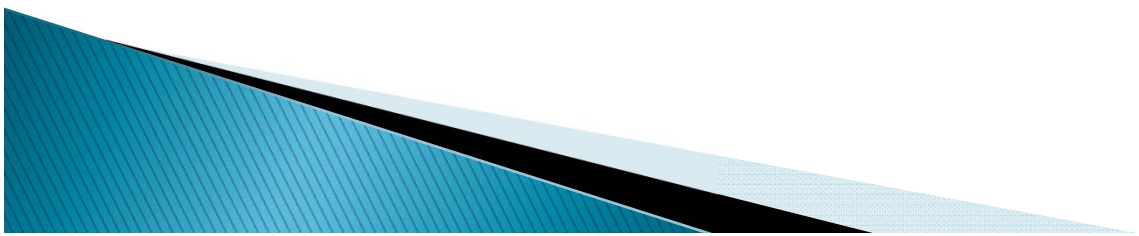
Application and Entitlement Processes: Evidence of Identification

- ***Evidence*** *that the claimed identity is valid,* i.e. that the person was in fact born and, if so, that the owner of that identity is still alive.
- ***Evidence*** *that the presenter links to the claimed identity* – i.e. that the person claiming the identity is who they say they are and that they are the only claimant of the identity.
- ***Evidence*** *that the presenter uses the claimed identity* – i.e. that the claimant is operating under this identity within the community; ***Social Footprint***
- Standards of performance and indices of variances-expectations and a framework so employees know the rules
- Breeder documents-e.g., over 7,000 differing kinds of US document of birth
- Online database linkages of a wide nature with real time access; civil registries, systems of birth, death, marriage, tax, real estate, and related commercial services



Biometrics

- The only reason why we have a chip
- The early days post 9/11
- Evolution to the present
- Germany was first to launch fingerprint, others underway now or soon to be
- Coming challenges, e.g., public education, privacy, facilitation, spoofing, accuracy, etc.



Factors to Keep in Mind

- Pragmatics of mischief with ePassports

  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.

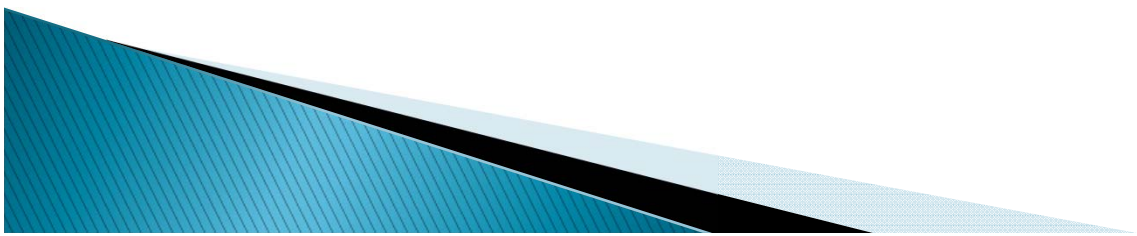
  Cloning

  - 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."

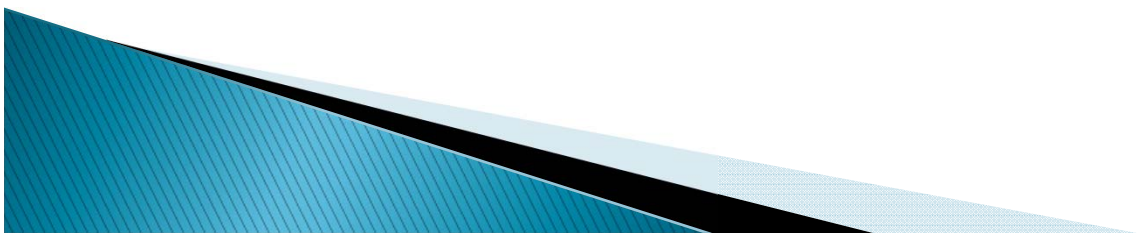
- Distance, power, visibility, at what price? And then "what" do you have?—The So what test!
- Not just a Chip

  - The e-passport is everything that non-ePassports have ever been, but in addition, there is a chip



A Few Best Practices

- Conduct a comprehensive risk analysis and THEN develop a risk management profile
- Adherence to specific guidelines.
- Accept only original documents or copies certified.
- Accept only documents that are currently valid; request evidence of 'use in the community' documents that are less than one year old.
- Require at least one form of trusted photographic identification.
- Require documented evidence of any name change .
- Where the authenticity of a particular document is in any way questionable, verify the authenticity of that document with the source issuing authority.
- Fraud prevention programs-detection, deterrence, follow-up, information sharing
- Monitoring and auditing document inspection processes as well as document issuance and entitlement authorizations
- Implement security techniques, such as mutual authentication, cryptography and verification of message integrity, to protect identity information throughout the application
- Ensure protection of all user and credential information stored in central identity system databases, allowing access to specific information only according to designated access rights
- Notify the user as to the nature and purpose of the personally identifiable information (PII) collected - its usage and length of retention and what information is used, how and when it is accessed and by whom; provide a redress mechanism to correct information and to resolve disputes



Thank you for your attention…

Barry J. Kefauver

Jetlag10@earthlink.net