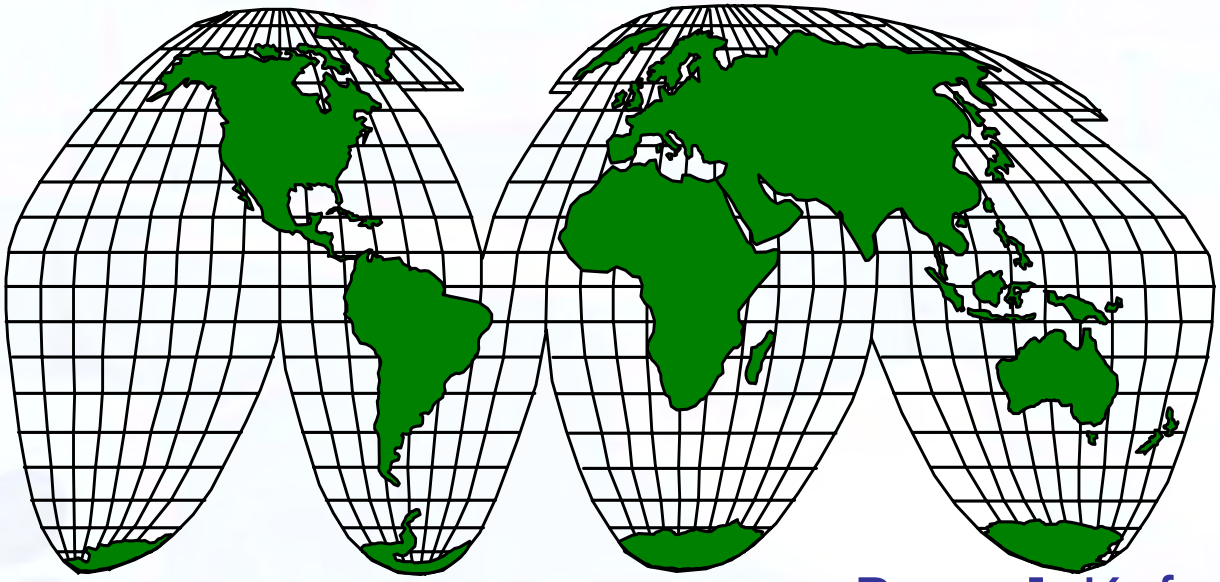
Improving The Integrity of Identity Management Programs



Barry J. Kefauver

3rd ICAO Symposium

October 2, 2007

Summary

- To describe the measures that have been taken to standardize and enhance the security of travel documents. While the documents themselves are becoming near-bullet-proof in terms of security, the systems on which entitlement decisions rely are vulnerable and demand immediate attention.
- To suggest a holistic perspective on the end-to-end travel document adjudication, issuance and inspection processes. This broad view includes organizational structure, facilities, internal controls, risk analysis and management, civil registry database sharing, effective and efficient biometric utilization and automated tools to improve security, productivity and quality.
- To provide a comprehensive review of the areas of vulnerability and weakness which are subject to today's threats. Offer some recommendations and suggestions for shoring up the foundations on which these enhanced travel documents reside, with a particular emphasis on identity verification, breeder documents and human resources.

The Partnership

- ICAO is the fulcrum around which the travel document standards deliberations revolve
- As well, ISO, the International Standards Organization, and ICAO have forged a highly effective working relationship
- ISO SC17, Cards and Personal Identification, where WG3 and WG8 reside, is THE center of ICAO interests
- Additionally, ISO SC37, the Biometrics standards-making body is also important

Summary of 9303 Development

- London November 2000—Contactless chips
- Biometrics Selection TR 2001
- London July 2003--Joint ICAO/ISO meeting
- LDS TR 2003
- PKI TR 2003
- Biometrics Deployment TR 2003
- Canberra, February 2004
- 9303 Supplement—Kyoto, September 2004
- NTWG—Auckland, December 2004
- Berlin, February 2005—the “Guide”
- Montreal, September 2005—TAG acceptance of Edition Six Draft Part 1
- Berlin, May-June 2006—Testing and TF/WG3 meetings
- Supplements, Editions Four and Five, published as posted
- Supplement Edition Six submitted for posting
- Part 3 drafted, readying for publication before the end of this year

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 other physical features
- 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

Measures For Internal Control

- Human systems-zero tolerance
- Work atmosphere and environment
- Spoiled documents
- Blank document controls
- In-house auditing
- Penalties-legal judicial system as well as administrative

Application and Entitlement Processes

- Breeder documents-over 7,000 differing kinds of US document of birth
- 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

Procedures For Applicant Throughput

- Applicant flow
- Conflicts of interest-friends, family, financial obligations
- Staff rotation-variety of assignments
- Provide independent levels of approval and shared responsibilities; no single staffer able to issue a document

Establishing and Verifying Identity

- Documentation-establish and prove
- Variables by country-birth, death, marriage, etc.
- Access to official records-databases, commercial services, watch lists
- Utilize person-centric databases that will link the application to prior records
- Use biometrics in one-to-many context
- Social footprint-societal interactions, a compendium of that comprises the individual and that individual's "true" identity

Document Issuance and Personalization Systems

- Blessing and curse of technology
- Desk top publishing revolution
- Off the shelf capability
- Authorizations of those who effect decisions in the system
- Physical security of the manufacturing as well as personalization facilities

Human Resources—The Greatest Strength/Weakest Vulnerability

- Background investigations and stringent selection processes
- Periodic updates of credentials and adherence to standards of conduct
- Training
- Splitting of functions-no single individual can have unilateral “approval” authority
- Morale (e.g., some airlines)

The Legal Framework of Document Abuse

- Penalties-appropriate measures for infractions and more serious offenses
- Prosecution-must be teeth in the law through meaningful penalties; and those penalties must be sought
- Administrative remedies-suspensions and related on-job sanctions
- Define breaches and table of infractions-staff must know expectations up-front
- Work environment and atmosphere

Lost and Stolen Documents

- Identity theft now accounts for over $5 billion in fraud losses in the US alone (FTC, 2006 report, reported losses to FIX what theft measures took away, not inclusive of the $50 billion in the thefts themselves)
- Photo substitution
- Imposters
- Look alikes
- Interpol system for passports

The Structure

- Central vs. decentral organization
- In particular, overseas issuance-inherent differences of culture, infrastructure, external pressures
- Must balance security and the quest for customer service
- One person/one document doctrine

Generic Nature of the Threats

- Customer Related
- Information
- Secure Materials and Supply Chain
- Physical Intrusion
- Human Resources
- Disaster Planning for Recovery

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
- Increasing trend to use of passports for non-travel Identity purposes

Security Detection and Updating (Noted from REAL ID)

Detection of security features can be at any or all of the following three levels of inspection:

- Level 1 – Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features)
- Level 2 – Examination by trained inspectors with simple equipment
- Level 3 – Inspection by forensic specialists

To maintain security and integrity of document security, annual reviews of card design should be conducted to certify the document's ability to resist compromise and document fraud activity attempts

- Photo substitution
- Delamination or other effects of deconstruction
- Reverse engineering of chip as well as other components
- Modification of any data element
- Erasure or modification of other information
- Duplication, reproduction or facsimile creation
- Effectiveness of security features at all three levels: cursory examination, trained examiners with simple equipment and inspection by forensic specialists
- Confidence and ease of second level authentication

Risk Analysis Framework

- For example, Frontex, an EU organization specifically intended to conduct risk management analyses
- To identify key threats and risks to border security
- To provide the Member States' border guard services with systematic and immediate early warnings
- To identify the most appropriate potential locations for the positioning of technical border control equipment
- To identify the need for joint operations
- To assess the most effective focus for Border guard training programs

Best Practices

- The fundamental first step for system integrity is to conduct a comprehensive risk analysis and THEN construct a risk management profile; this is particularly critical for assessment of the biometric data collected and its uses.
- Use standards to define requirements that must be addressed as minimum specifications both for technical soundness as well as adherence to quality control
- 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
- Make extensive use of the tools of technology, e.g., rules-based adjudication software
- Overseas issuance is higher risk with inherent differences of culture, infrastructure, external pressures
- Fraud prevention programs-detection, deterrence, follow-up, information sharing
- Database linkages and data sharing are multiplicative in impact and become especially powerful tools when combined with biometric data
- Monitor and audit document inspection processes as well as document issuance and entitlement authorizations

Smart Card Alliance RFID Best Practices

- 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
- Notify the user about what information is used, how and when it is accessed and by whom and provide a redress mechanism to correct information and to resolve disputes

Issues Facing Border Control Today

- Biometrics
- Enrollment and other systems
- Profiling
- Information sharing
- Privacy and data integrity
- New visions

The Worldwide Prognosis

- Chips
- Enrollment systems
- Biometrics
- Inspection systems

Thank you for your attention
QUESTIONS?

Barry J. Kefauver

Jetlag10@earthlink.net