International Civil Aviation Organization

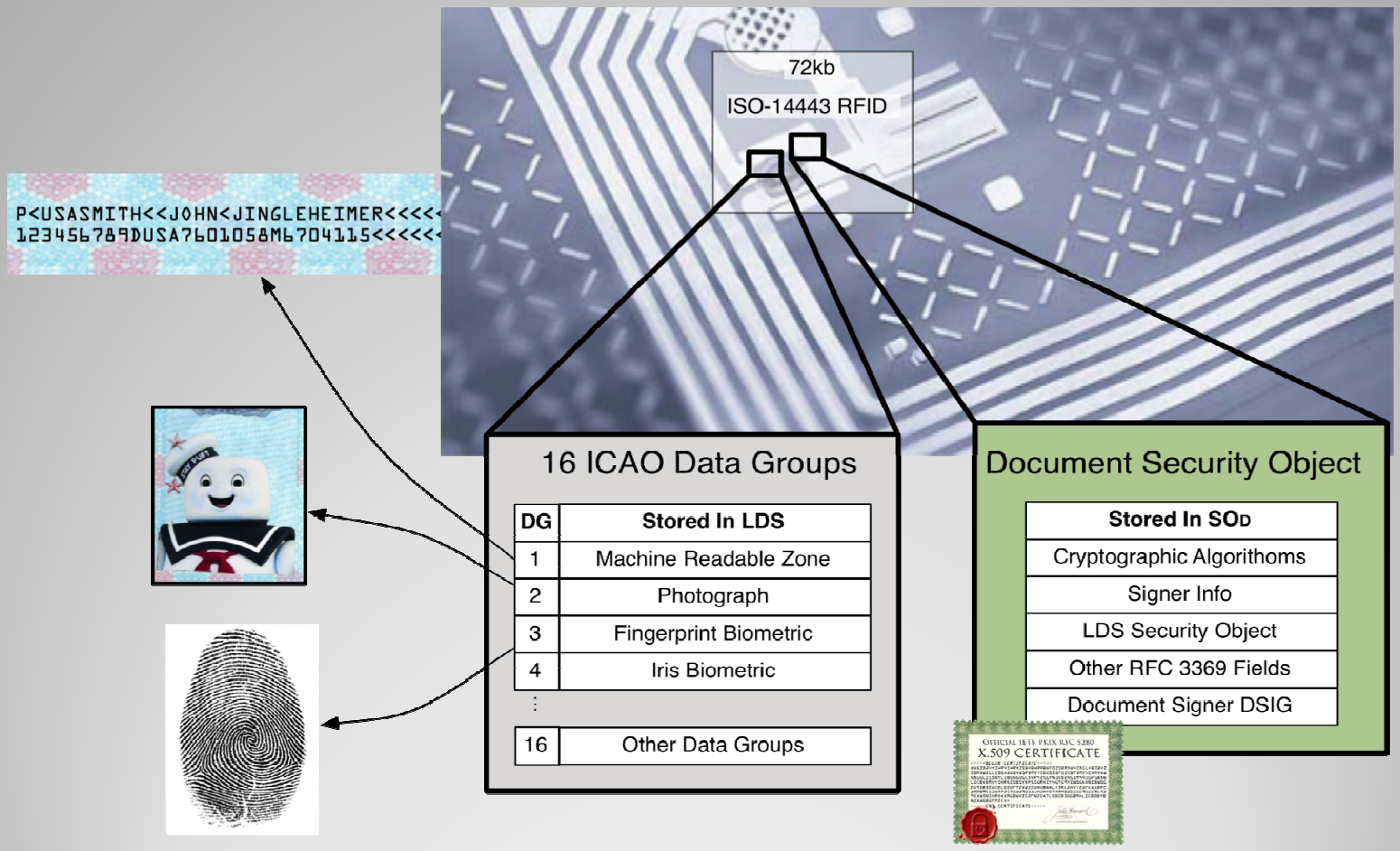
Seventh Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards

ICAO Headquarters, Montréal, Canada
12 - 15 September 2011

Authenticating Travel Documents: Challenges and Good Practices

Bill Russell
Vice President, Mount Airey Group, USA

What's on the Chip?



Doc 9303 Context of MRTD Validation

Over 90 States now use Public Key Infrastructure (PKI) data elements to protect MRTDs.

Section IV, "PKI for Machine Readable Travel Documents", in Vol. 2 of Doc 9303

What is needed to validate MRTD authenticity?

- The Document Security Object (SO_D)
- Country Signing Certification Authority Certificates (C_{CSCA})
- Document Signer Certificates (C_{DS})
- Certificate Revocation Lists (CRLs)
- Master Certificate Lists
- ICAO PKD and access to other country repositories
- Policies governing each State

Why are so few States validating MRTDs?

- Must already have C_{CSCA} for State, C_{DS}, and CRLs
- Systems to validate PKI data must be able to process multiple algorithms
- Data must be obtained from all around the world
- PKI data changes continually, which requires live updates
- Collection systems must protect against bad PKI data
- Border inspection systems should not connect to the internet
- Inspection of PKI authenticity must be fast
- Policies vary widely from State to State
- Validating Doc 9303 components includes:
  - Verifying data groups using SO_D and C_{DS} from MRTD
  - Constructing certificate chain from C_{DS} to a trusted C_{CSCA}
  - Checking revocation status for C_{DS} using CRL
  - Performing X.509 certificate checks based on RFC 3280/5280

Issuer Responsibility Recommendations

- Ensure that publication of travel documents conform to Doc 9303
- Establish known intervals for publishing PKI data elements
  - Certificate Revocation Lists
  - Document Signer Certificates
  - Master Certificate Lists (coordinated between groups)
- Publish all PKI data elements in a publically available LDAP directory
  - ICAO PKD
  - State border directory
  - Commercial border directory
- Identify points of contact that can be notified if there are technical problems with published PKI data elements

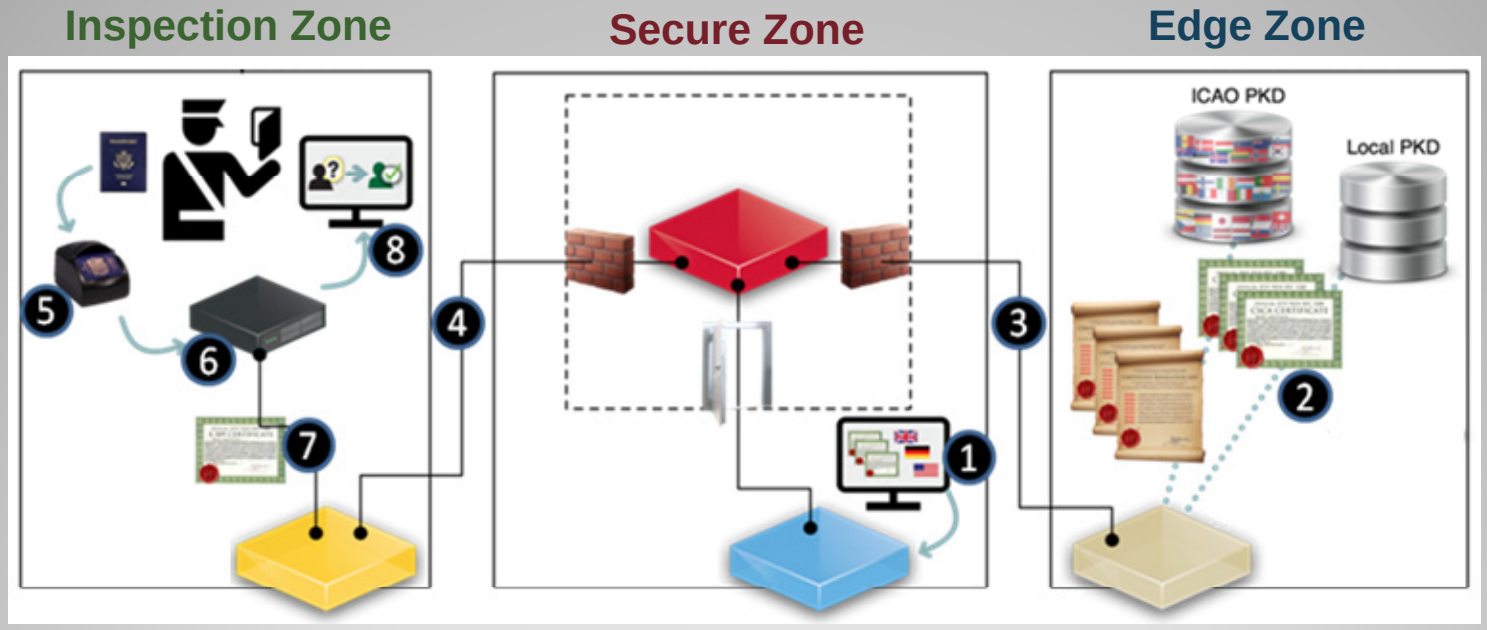
Inspection Design Recommendations

- ICAO Public Key Directory (PKD) interface support
- LDAP directory interface support
- Configurable X.500 directory precedence for data sources
- Centralized service for e-Passport Document Signer Certificates
- Extended algorithm support, unnamed ECDSA curves & RSA-PSS
- ICAO Master Certificate List management support (coordinated)
- Blacklist capability for explicitly untrusted signers
- Ability to configure grace policies specific to each State
- Multi-tier authentication process to maximize security
- Multi-person security controls to avoid single points of failure
- Secure audit trail

Policy & Configuration Options by State

- What root authorities (C_{CSCA}) are allowed for each State?
- Is a Certificate Revocation List (CRL) required?
- Will unanticipated document signers (C_{DS}) be allowed?
- What grace periods will be allowed for revocation lists?
- What certificates have been explicitly blacklisted?
- Where should PKI data be obtained for each State?
- How frequently should data be refreshed for each State?
- Which data sources have priority?
- How frequently will data be updated?
- Who are the primary and secondary points of contact
  - To report an issue such as an expired CRL?
  - To receive update notifications from?

Multi-Tier Authentication Design



1. Securely administrate policies
2. Pre-screen PKI data from internet
3. Pre-authenticate document signers
4. Publish authentication results to border
5. Read travel document
6. Authenticate travel data (SO_D)
7. Authenticate signer (C_{DS})
8. Display results

Robustness & Performance Testing

Authentication of e-Passport data should meet your Border Inspection Peak Load estimates.

Keep in mind:

- With global e-Passport participation the ICAO PKD *might grow to* 20,000 document signer certificates, however there are currently less than 2,000 document signer certificates in the PKD.
- The IATA projects 3.3 billion international air passengers in 2014; or about 100 transactions/second if every international traveler was processed by one server.
- Individual transaction times of 100-200ms can be processed in parallel to other e-Passport checks, making the authentication time negligible.

Questions?

Paul Townsend
Director of Cybersecurity
ptownsend@mountaireygroup.com
(Office) +1 240 285 9596
(Mobile) +1 301 908 0293

Bill Russell
Vice President, Mount Airey Group
brussell@mountaireygroup.com
(Office) +1 703 327 2573
(Mobile) +1 571 334 1671

You can download this presentation on our website:
http://www.mountaireygroup.com/e-passports/