Document Authentication

Todd Kealey

The world turns to 3M for identification solutions
3M Credentials

- Identification and Authentication business of 3M is a unit of the Security Systems Division
  - Initial focus on document materials and secure laminates
  - Added Canada-based document issuance and border management business in 2002 (AiT)
  - 2006 saw the addition of secure printer (SPSL – UK)
  - Acquired Rochford Thompson, document reader vendor, in 2007
3M Projects

- **Document Issuance**
  - Consular issuance of UK ePassport
  - Manufacture and domestic personalization of UK ePassport
  - Caricom Visa in support of Cricket World Cup
  - ILO Seafarer ID in Nigeria and Indonesia

- **Border Management**
  - KMAR – The Netherlands

- **Document Data Capture or Authentication**
  - Multiple airlines and national governments
Document Authentication

- Identity Documents are secured in layers
  - Materials: chips, laminates, inks, overt & covert attributes
  - Personnel and facilities
  - Process: controlled work flow, audit trails, reporting

- In today’s world, the detection of counterfeit ID documents requires:
  - Optical document authentication
  - Electronic document authentication
Optical Document Authentication

- Document data capture
  - *Multiple illuminations: visible, infra-red, ultra-violet, others*

- Document identification
  - *Data extraction: find text objects, barcodes and graphical patterns*
  - *Determine type: passport, visa, driver’s license, national ID, other*
  - *Determine if known: is reference data available for comparisons?*

- Optical Authentication
  - *Compare document attributes to those of known references*
  - *Is there evidence of tampering?*
Optical Document Authentication
Electronic Document Authentication

- ePassports and SmartCards include microchips
- Data is secured using two mechanisms:
  - Authentication: encoded information that is used to ensure that the content is original and unmodified
  - Access Control: only a knowledgeable or approved system may gain access to the electronic data
Authentication Mechanisms:

- **Passive Authentication**
  - A mandatory requirement of the ICAO specification
  - Verification of digital signature on the document’s data groups (face, MRZ text, etc.)
  - Security Object can also be verified via PKD

- **Active Authentication**
  - Certificate stored in DG15
  - Inspection system challenges the chip
  - Chip uses a secret key to sign challenge data
  - Matching data proves that chip is not a clone
Access Control

- **Basic Access Control**
  - Requires reader to provide text from MRZ to gain access to electronic data

- **Extended Access Control**
  - Additional security for sensitive biometric data
  - Complements, does not replace BAC
  - Mutual validation of credentials: Chip Authentication & Terminal Authentication
  - Increase security of session keys
  - Limit access to Inspection Systems that can prove to the chip the right of access to 2nd biometric data
EAC Components: Chip Authentication

- What it does
  - Verifies that the chip is genuine, not cloned
  - Provides new, more secure session keys used to encrypt messages between chip and inspection system (prevents eavesdropping)
  - Must be executed after BAC

- What it doesn’t do
  - Prove the contents of the chip are unaltered (use passive authentication)
  - Prove that the terminal has any right to access ‘sensitive’ data
  - Alter the security status on the chip
EAC Components: Terminal Authentication

- **Terminal Authentication**
  - *Onus on now Inspection System to prove it is entitled to access ‘sensitive’ biometric data*

- **What it does**
  - *Prevents unauthorized access to sensitive data including fingerprints and iris scan if available*
  - *Must previously have performed Chip Authentication*

- **What it doesn’t do**
  - *Prevent a stolen inspection system from gaining access to sensitive data groups*
  - *Prevent an inspection system being compromised*
Extended Access Control Issues

- Secure certificate storage and key management is required
  - Each country is required to set-up and maintain a certificate infrastructure to issue and distribute certificates
  - Need bilateral relationships with each issuer
  - Constantly needs to be updated and maintained
  - Large number of certificates need to be managed

- Location of key store
  - Local: Timely access but must be secured and protected
  - Central: Reduced risk of “theft” but providing access to all inspection sites is an IT & telecom burden

- What is the time impact on inspections?
Extended Access Control Issues

- Chips need to updated
  - With date/time and new Country Verifier Certificate Authority Certificates to prevent access with ‘old’ certificates
- No specification how the Inspection System interfaces with Document Verifier Certificate Authority or DVCA and CVCA
- Managing many inspection authorities with one country
  - Over 30 different DVs in the Netherlands alone
- Chips still in development
- Conformity specification in development
- Certificate policy document not implemented
- No PKI infrastructure in place
Wrap-up

- Document Authentication continues to mature
  - Optical & Electronic authentication offer the highest levels of security assurance
- Document Authentication is the next critical phase in validating travelers
- Full page readers and automation are fundamental tools for validation of documents
Please enjoy the reception!