TRIP2017

Traveller Identification Programme

Regional Seminar Montego Bay

Public Key Infrastructure – Basis of trust in eMRTDs

R Rajeshkumar

International Organization for Standardization (ISO)

ICAO TRIP: Making the Air Travel more Secure and Efficient

TOWARDS A BETTER TRAVELLER IDENTIFICATION MANAGEMENT

FOR ENHANCED BORDER CONTROL INTEGRITY

Core Concepts

- Hashing
  - A Mathematical process applied to the process
  - Output is called a Message Digest
  - Input cannot be recreated from the output – hence one way function
  - Same input always gives the same output
  - Any change in input changes the output
  - Ensures that message is not tampered

Core Concepts

- Digital Signature
  - A process of asymmetric encryption
  - Message cannot be decrypted using the key used for encryption
  - The two keys have a mathematical relationship with each other and form a unique pair
  - You keep one part of the key with you – private key
  - You distribute the other key to others – public key
  - You encrypt message with private key and send the message to others
  - If they can decrypt with your public key, then the message originated from you and has not been modified – Digital Signature

Core Concepts

- Message signing
  - First hash the message using a well known hashing algorithm to create a message digest
  - Encrypt the hash using your private key
  - Send the message and the encrypted hash to recipient
- Signature Verification
  - Decrypt the encrypted hash using the public key of the sender. This gives you the message digest.
  - Hash the received message to create a new message digest.
  - If the two match, then the message is from the sender and has not been modified
  - If the decryption of the encrypted hash fails or the message digests do not match, then the message has been modified in transit

Core Concepts

- Public key
  - key pair used to sign messages (Document Signer) must be renewed regularly to avoid compromise
  - To avoid having to distribute these keys every time you renew them, you use a Master Key pair(Country Signer) to sign the Document Signer
  - Distribute Country Signer to recipients
  - Include the Document Signer with your message

Core Concepts

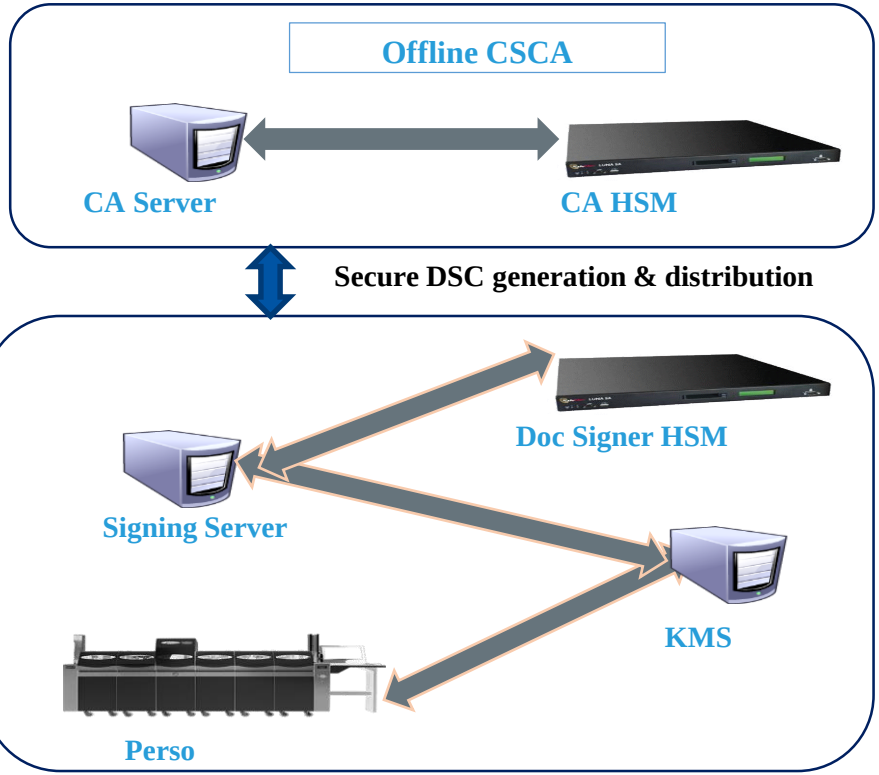
- Certificate Revocation List (CRL)
  - Any certificate that cannot be trusted must be published in CRL
  - Trust may be lost because of:
    - Suspected Compromise
    - Wrong issuance or issuance for different purpose
    - Weakness of keys

Core Concepts

- E-Passport
  - Data groups defined to hold messages
    - DG1 is a copy of the MRZ
    - DG2 holds the image of the passport holder
    - 16 such data groups for different pieces of information
  - Store the Data Groups on chip – “Logical Data Structure (LDS)”
  - Hash each datagroup
  - Encrypt all the hashes with your private key (Document Signer Certificate (DSC)) and store in the “Document Security Object (SOD)” – Store the SOD on the chip along with DSC

Core Concepts

- Issuance system
  - CSCA generation
  - DSC generation and distribution to Personalisation system



Understanding E-Passport validation

- Trust is established by proper verification of the e-Passport
  - Verify SOD against DSC
  - Verify DSC against CSCA
  - Verify DSC not in CRL
  - Check that DG hash values matches the hash values stored in SOD
  - Compare DG1 with MRZ
  - Compare DG2 with printed photo
  - Compare photo to holder of passport

SOD is valid

LDS is valid

eMRTD is valid

Traveller is valid

Security Considerations

- Five phases for security considerations
  - Security in Generation
  - Security in Transport to Personalisation systems
  - Proof of control over usage of Document Signer
  - Secure destruction of private key at end of lifetime
  - Monitoring of compromise and reporting

Proof of control

- CSCA generation and usage
- DSC generation and usage
- Passport issuance

Border Control

- eMRTD not automatically trusted
- Trust depends on
  - Confidence in process of issuance of the document
  - Confidence in control over signing credentials
- Asserted by published Certificate Practise Statement (CPS) and Certificate Policy (CP) – backed by independent audit
- Data analysis acts as a surveillance and ensures continued trust

Contact Details

Name: R Rajeshkumar
Email:
r.rajeshkumar@auctorizium.com