Trust Management –PKI Deployment & International Trust

Sharon Boeyen
Principal - Advanced Security
Entrust
Canada

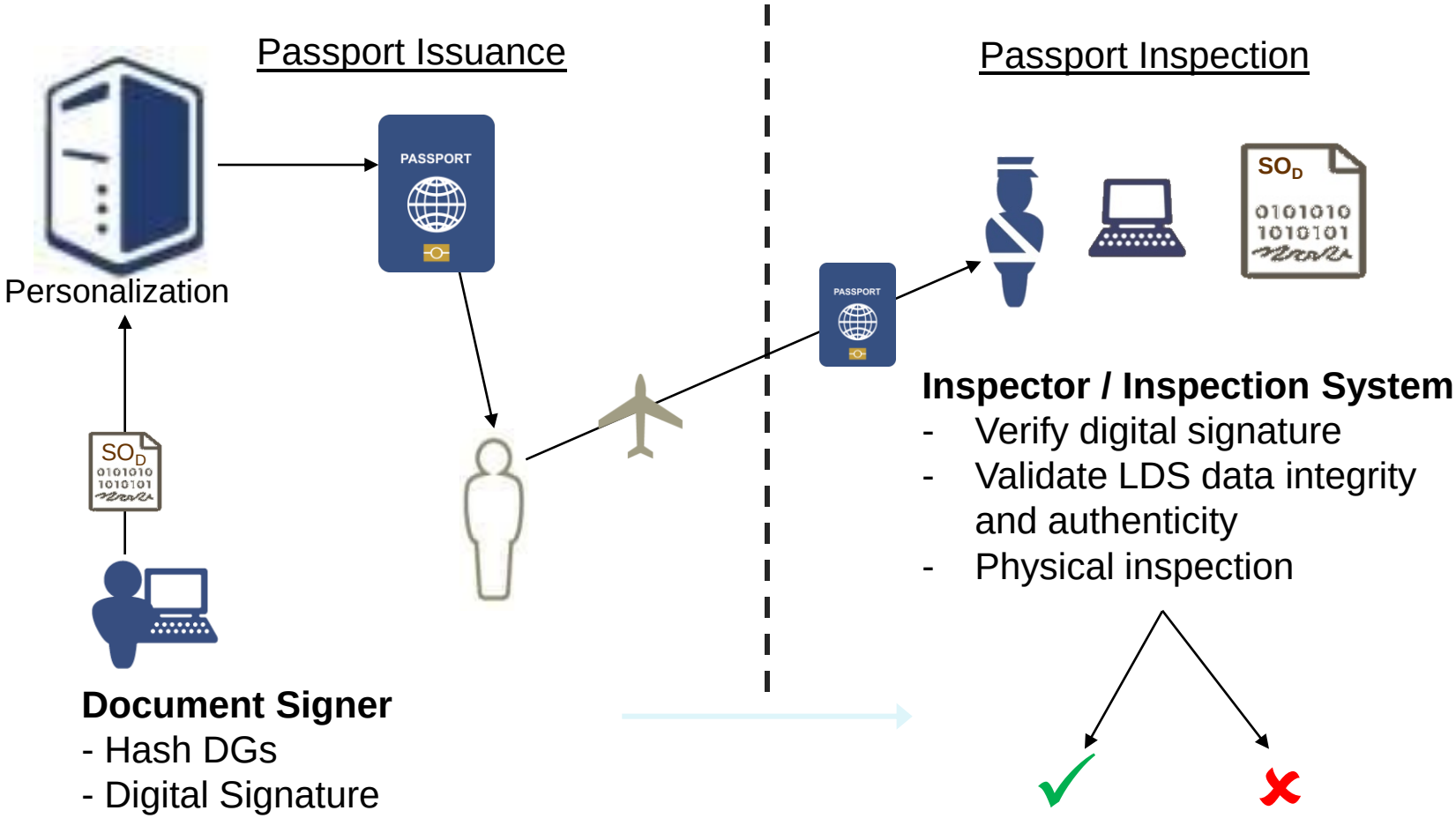
Outline

- **Role of PKI in eMRTD application**
- National PKI deployment
- International Trust
- Summary

Passive Authentication

- Security mechanism for eMRTDs
  - Verify integrity and authenticity of LDS data
  - Assist in detection of forged data
  - Uses digital signature technique and PKI
- Should be used in conjunction with physical inspection of MRTD
  - Does not prevent chip copying or substitution

Operational View



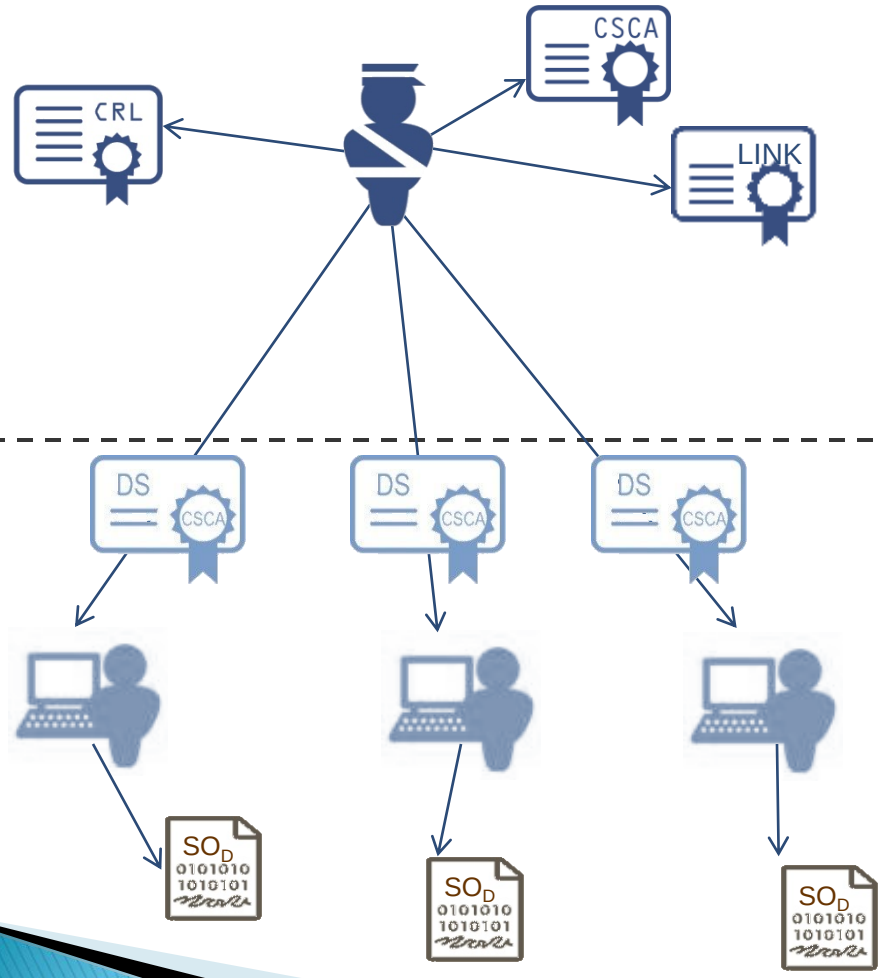
Role of PKI

- Keys and certificates support digital signatures
- Private key used to generate signature
  - Kept private by holder
  - Cannot be derived from public key
- Public key used to verify signature
  - Assures signature created by corresponding private key
  - Published in certificate and distributed widely
- Infrastructure supports international trust
  - Simple direct trust model between states
  - Distribution of certificates and revocation lists
  - Flexible scheme tailored to needs of individual state

Outline

- Role of PKI in eMRTD application
- **National PKI deployment**
- International Trust
- Summary

National PKI Components



CSCA

- Trust point for national PKI
- One per country
- Issues all certificates
- Issues CRL

DS

- One or more per country
- Signs eMRTD data
- Generates SO_D

CSCA Certificates

Issuer	Canada CSCA
Subject	Canada CSCA
Key Usage	Certificate and CRL signing exclusively
Public Key	CA CSCA Key 1
Certificate Signed by	CA CSCA Private Key 1
Certificate Validity	Typically 10-15 years
Private Key Period	Typically 3-5 years
Etc.	

Self-Signed Certificate

Issuer	Canada CSCA
Subject	Canada CSCA
Key Usage	Certificate and CRL signing exclusively
Public Key	**CA CSCA Key 2**
Certificate Signed by	CA CSCA Private Key 1
Certificate Validity	Typically 10-15 years
Private Key Period	Typically 3-5 years
Etc.	

Link Certificate

DS Certificates

Issuer	Canada CSCA
Subject	Canada DS1
Certificate Signed by	CA CSCA Key 1
Public Key	CA DS1 Key 1
Certificate Validity	Typically 10 years + 3 months
Private Key Sign Period	Typically 3 months
Key Usage	Digital Signature
Document Type	“P” (as per MRZ for passports)
Etc.	

CRL

- List of certificate revocation notices
  - All revoked certificates that have not expired
- One CRL per CSCA
- Updated at least every 90 days
- Signed with current CSCA private key

Distribution Mechanisms

- Bilateral exchange with other states
- ICAO Public Key Directory (PKD)
- eMRTD SO_D

	CSCA Certificates	Master Lists	DS Certificates	CRL
Primary	Bilateral	PKD	eMRTD SO_D	Bilateral
Secondary	Master Lists	Bilateral	PKD	PKD

Bilateral: Diplomatic courier, website, ldap etc
Master List: Signed list of verified CSCA certificates

Outline

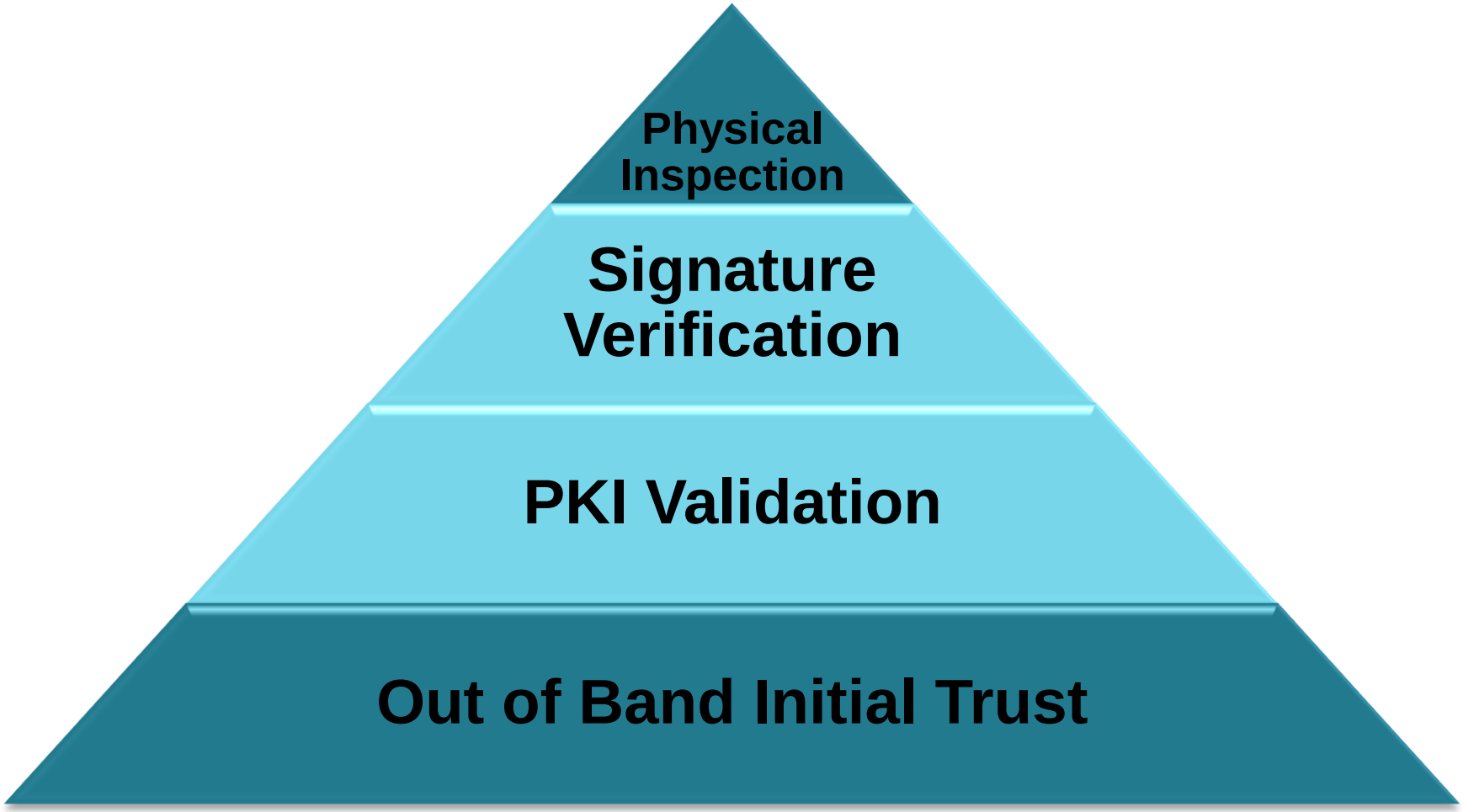
- Role of PKI in eMRTD application
- National PKI deployment
- **International Trust**
- Summary

International eMRTD Trust

Canadian Traveler

Brazil Border Control

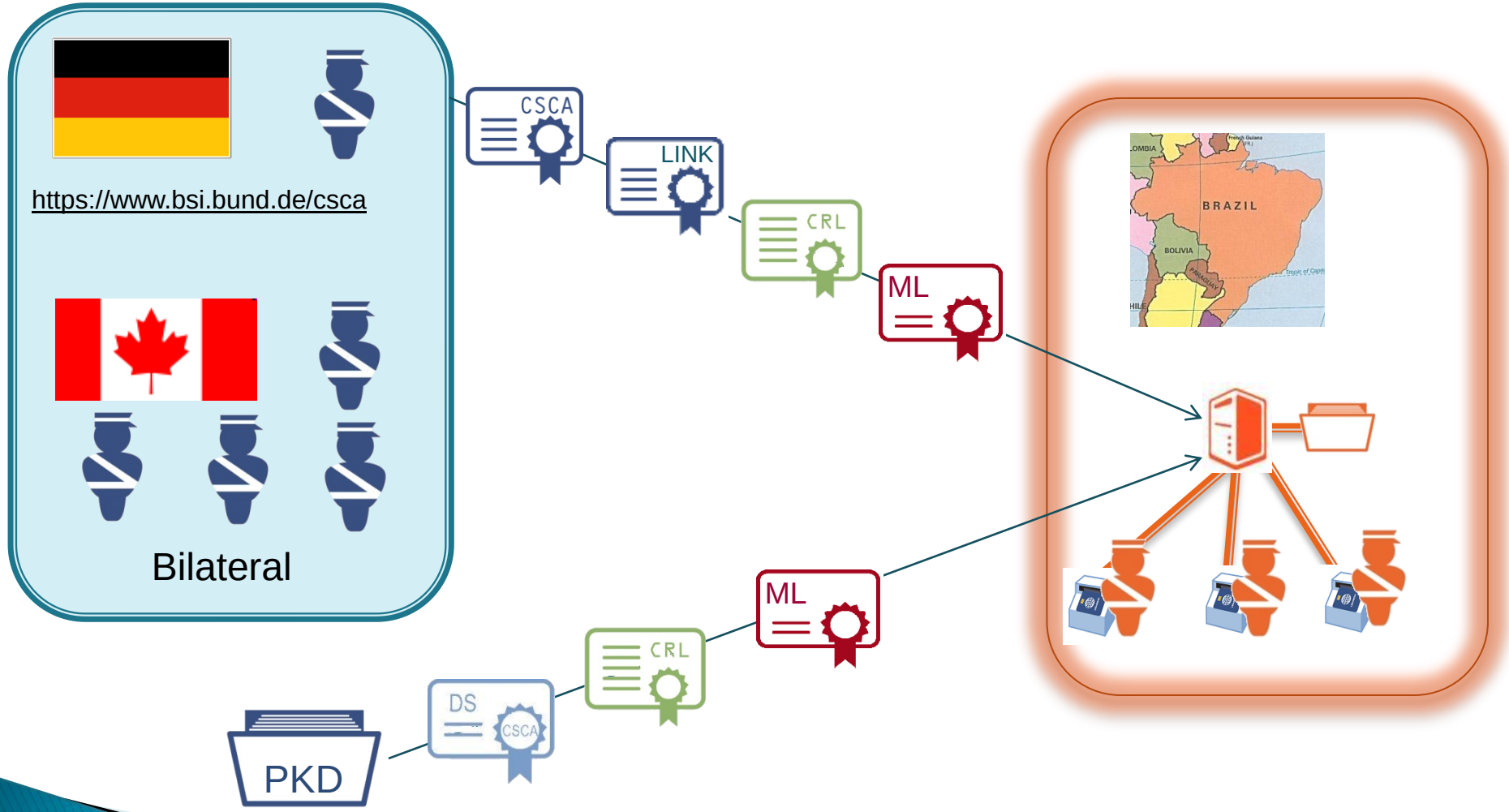
Steps to Building Trust



Out-of-Band Initial Trust

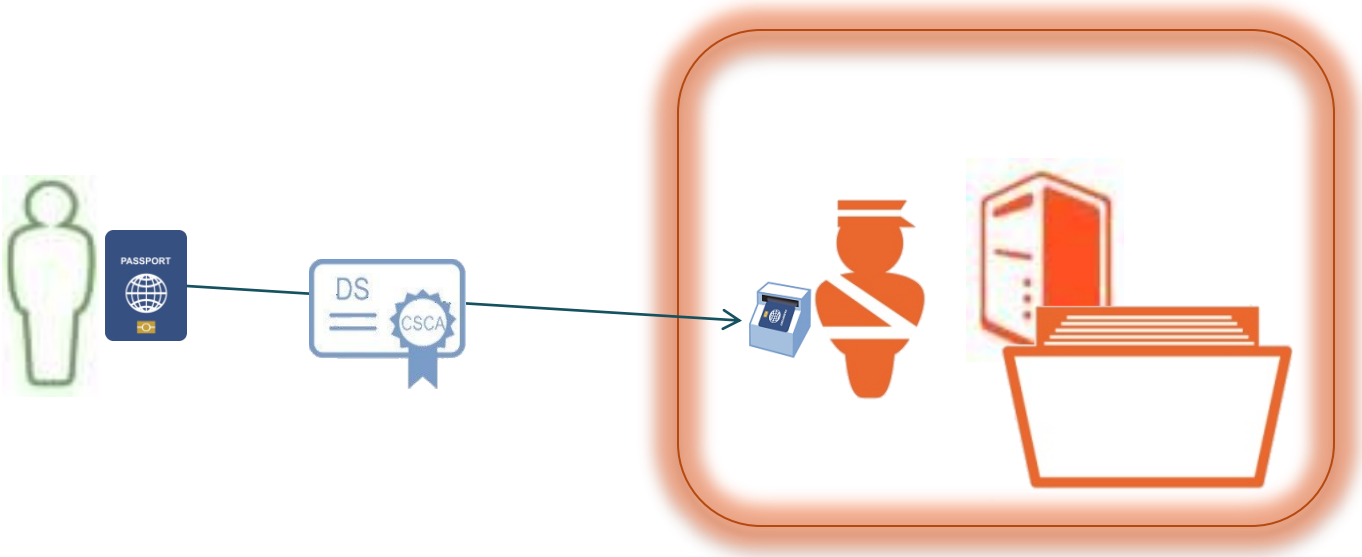
- Trust: Firm belief in the reliability, truth, or ability of someone or something (Oxford Dictionary)
- Assess issuer's eMRTD process
  - PKI related aspects
    - Systems security & reliability, compliance, policies etc.
  - Non-PKI related aspects
    - Existing trust relationship, issuer policies and procedures, etc.
- Policy decision to trust eMRTD
  - Validate issuer CSCA self-signed certificate
  - Establish trust anchor for CSCA

PKI Validation – Plan Ahead



PKI Validation – Inspection

- Retrieve trust anchor DS certificate & CRL
- Path validation (as defined in RFC 5280)
  - Verify certificate signature, validity periods, key usage etc.
- Check certificate revocation status



SO_D Signature Verification

- Retrieve SO_D and LDS data
- Verify digital signature on SO_D
- Create new hash of LDS data
  - Using hash algorithm as indicated in SO_D
- Compare new hash to that in SO_D

Physical Inspection

- Passive authentication ensures
  - Data on chip has not been modified
  - Data signed by authorized DS
- Physical inspection required
  - Ensure paper document and chip contain identical data
  - Additional physical security features

Outline

- Role of PKI in eMRTD application
- National PKI deployment
- International Trust
- **Summary**

Summary

- PKI plays major role in eMRTD security
  - Technology supporting political trust decisions
- National PKI deployment
  - Must be reliable, secure, ICAO 9303 compliant
- International Trust
  - Initial trust establishment out-of-band
  - Compliant electronic processing extends trust
  - Certificates and CRLs must be accessible (PKD/websites)
- Benefits of PKI realized ONLY if issuing and receiving ICAO member states participate

THANK YOU

Contact Information
E-mail: sharon.boeyen@entrust.com
Tel.: +1 613 270 3181