International Civil Aviation Organization

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

ICAO Headquarters, Montréal, Canada
10 - 12 October 2012

PKI Deployment & International Trust

Mark A. Joynes
Director, Product Management
Entrust Inc.

OUTLINE

Role of PKI in eMRTD application

National PKI deployment

International Trust

Summary

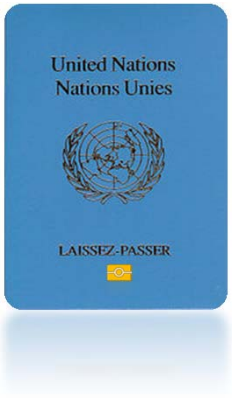
PASSIVE AUTHENTICATION

Security mechanism for eMRTDs

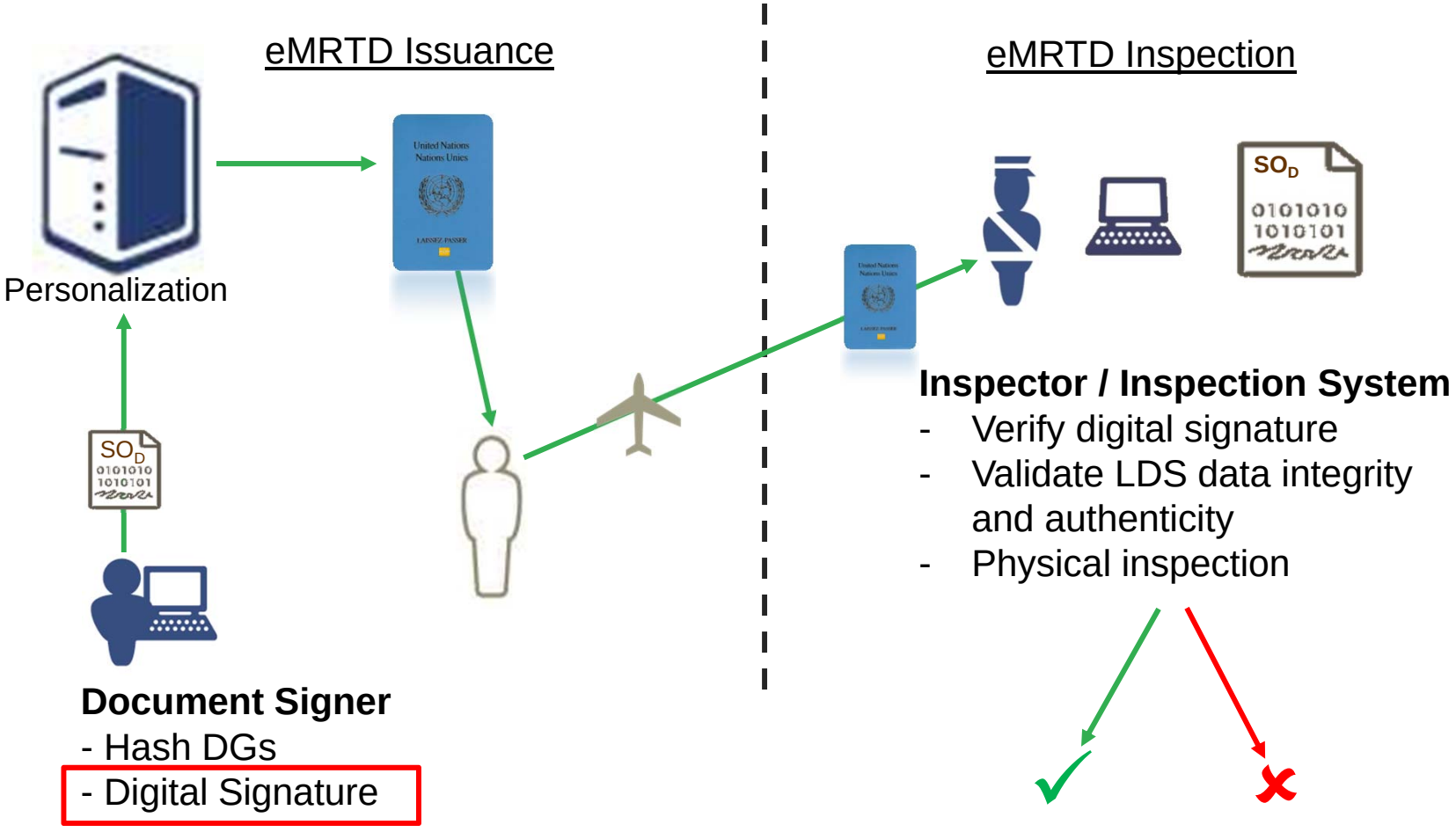
- Verify integrity and authenticity of LDS data
- Assist in detection of forged data
- Uses digital signature technique and PKI

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

Key Pairs – Private/Public

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

OUTLINE

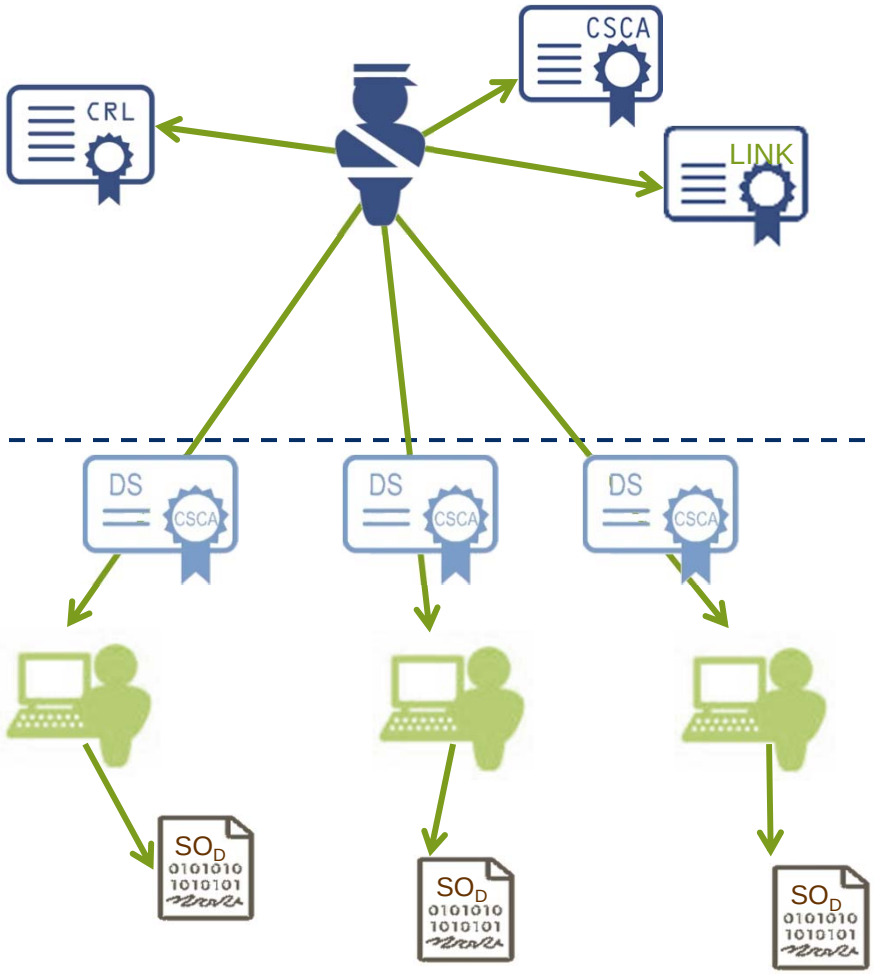
Role of PKI in eMRTD application

National PKI deployment - Issuance

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

CSCA CERTIFICATES

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

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

LINK CERTIFICATE

DS CERTIFICATES

Issuer	United Nations CSCA
Subject	United Nations DS1
Certificate Signed by	UN CSCA Key 1
Public Key	UN 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 & Validation

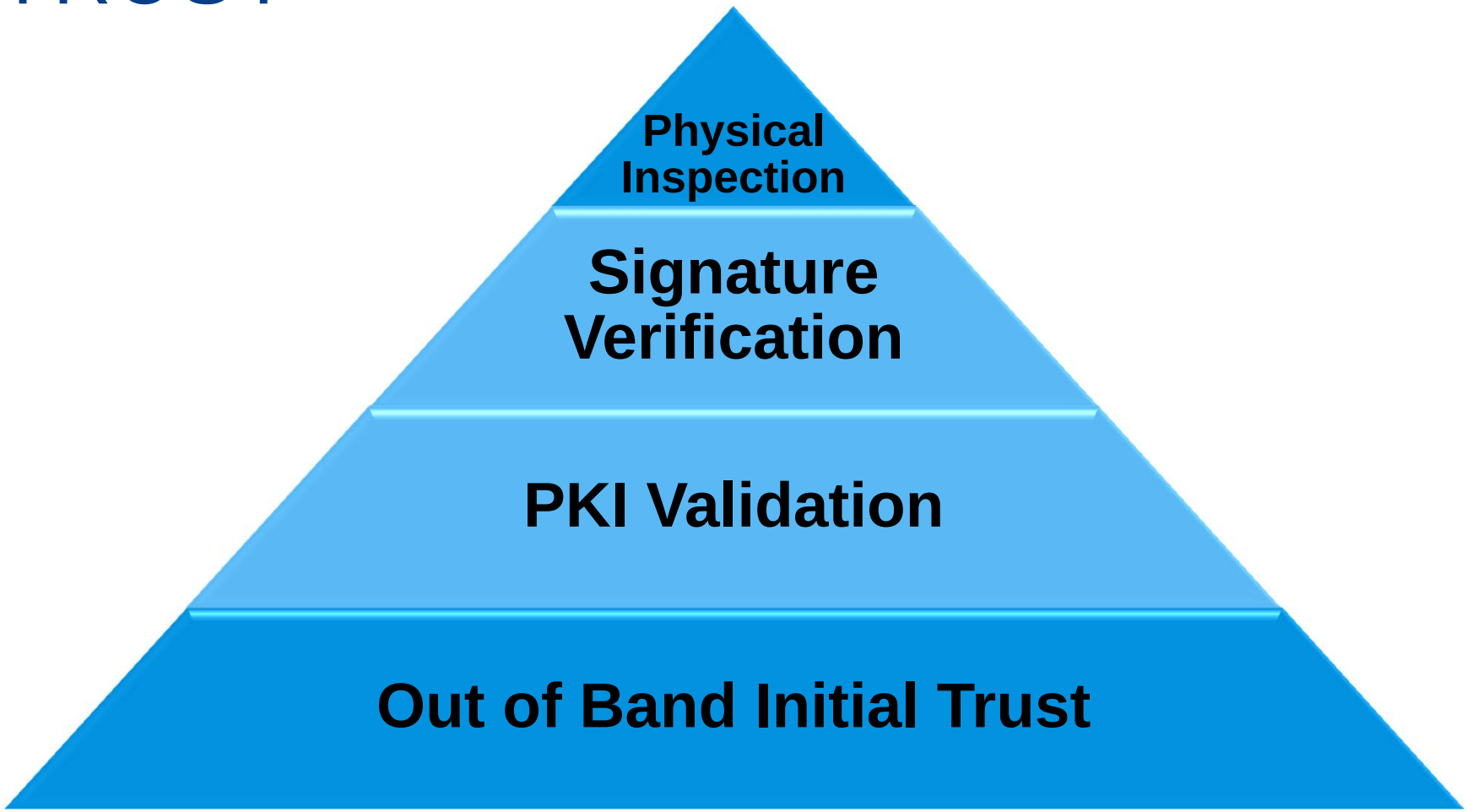
Summary

INTERNATIONAL eMRTD TRUST

UN LAISSEZ PASSER HOLDER

Canadian 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)

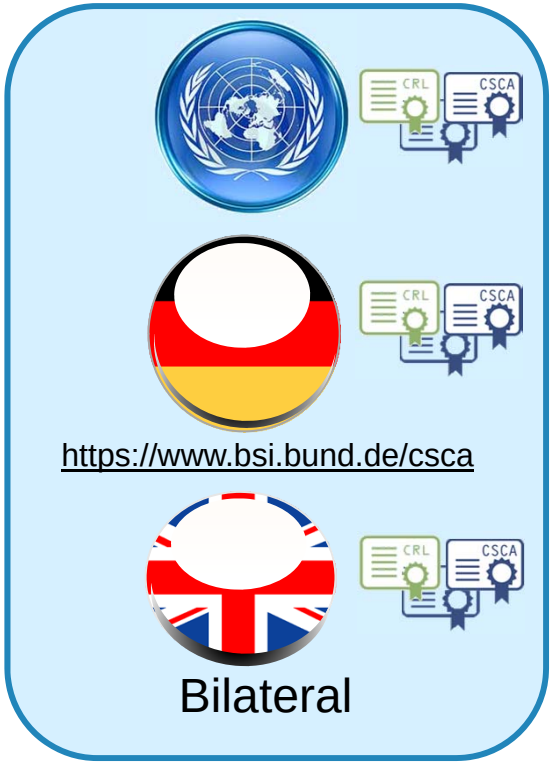
Assess issuer's eMRTD process

- PKI related aspects
  - Systems security & reliability, compliance, policies etc.
- Non-PKI related aspects
  - Existing trust relationship, issuer policies and procedures, etc.
  - Evidence of Identity

Policy decision to trust eMRTD

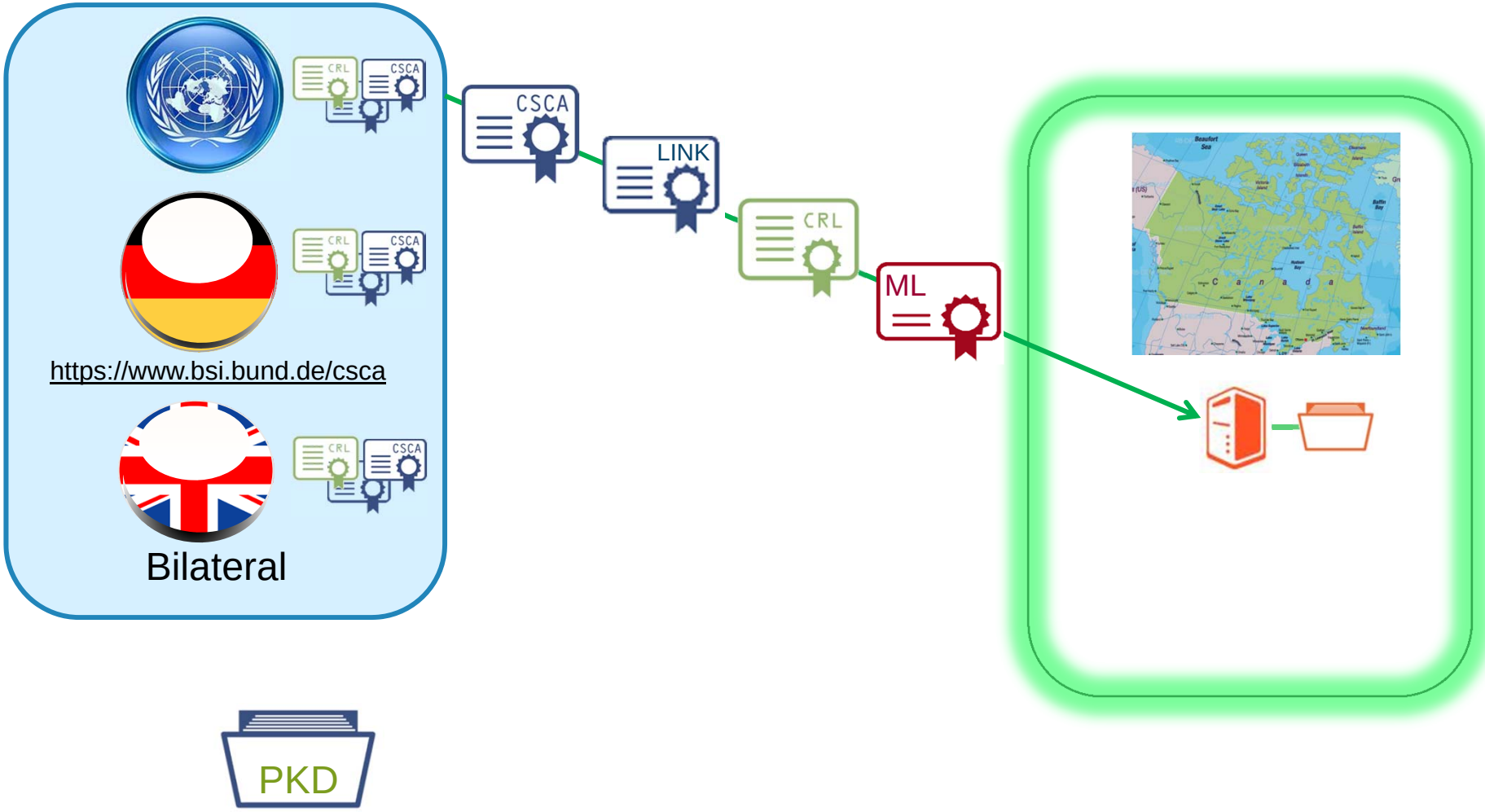
- Validate issuer CSCA self-signed certificate
- Establish trust anchor for CSCA

PKI VALIDATION – PLAN AHEAD

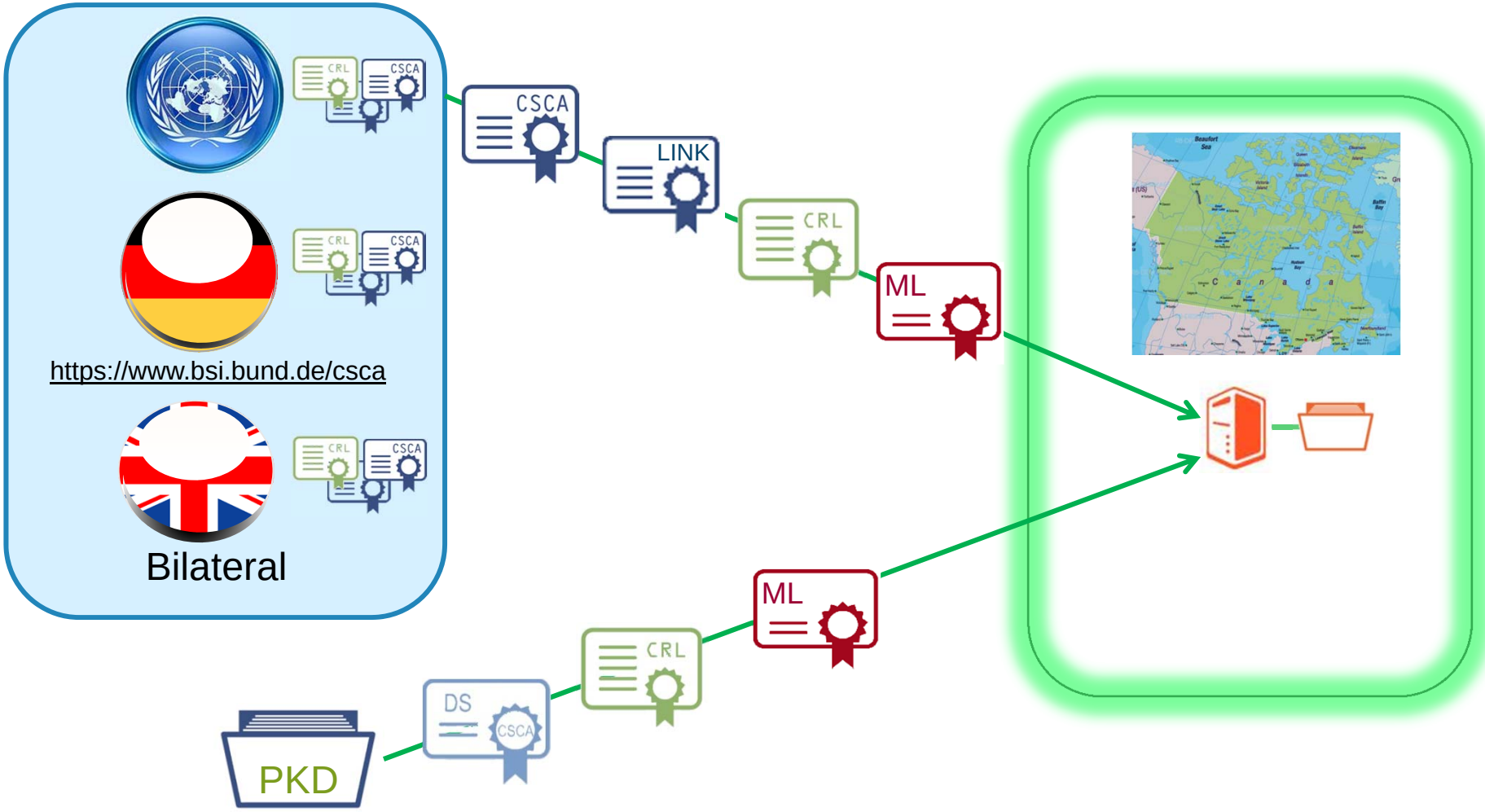


PKD

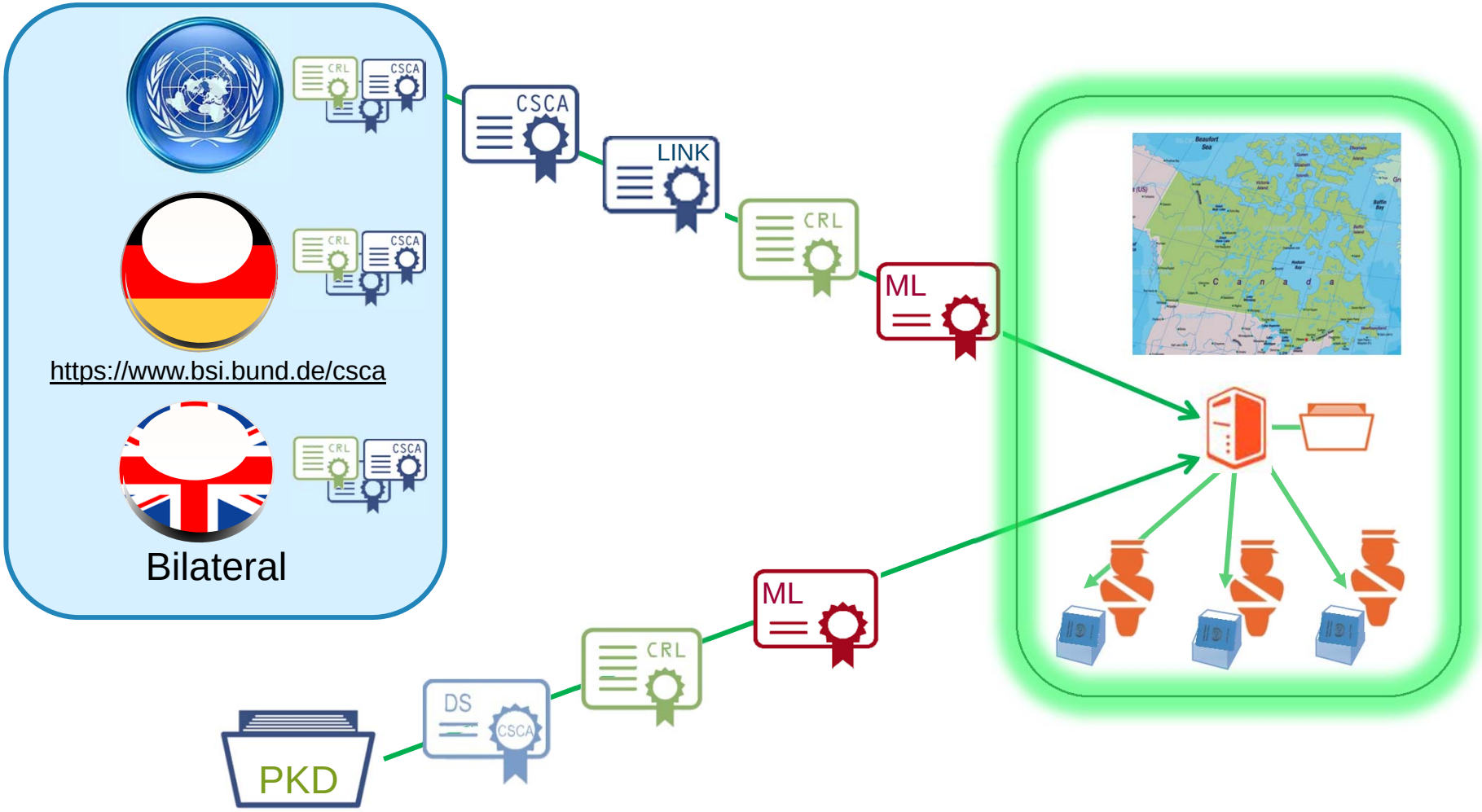
PKI VALIDATION – PLAN AHEAD



PKI VALIDATION – PLAN AHEAD



PKI VALIDATION – PLAN AHEAD



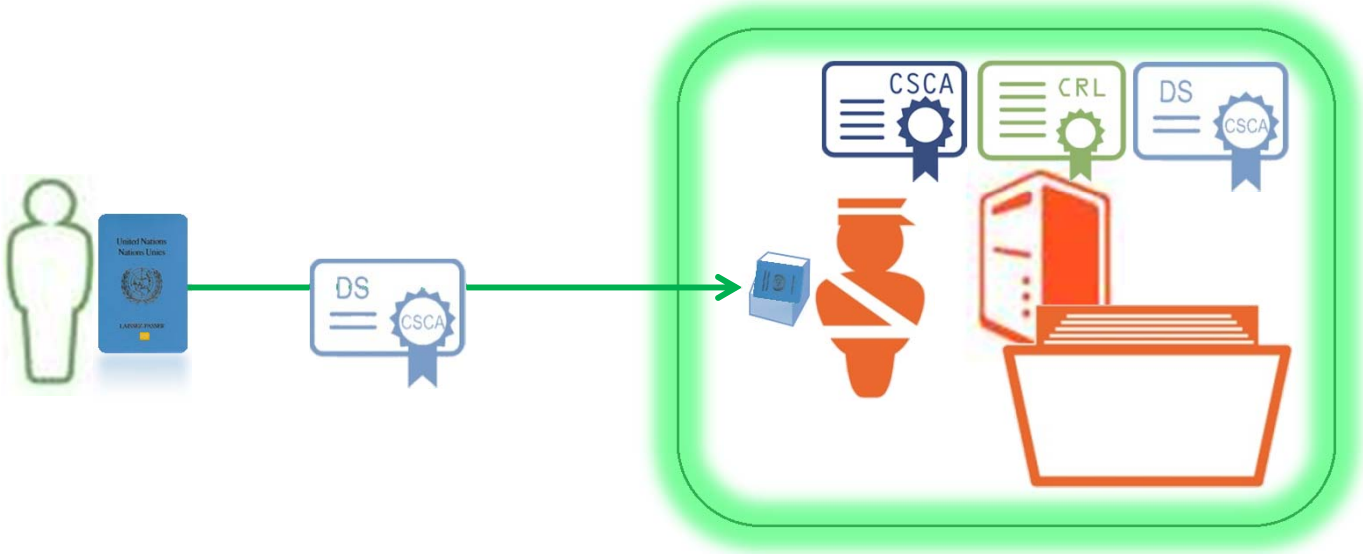
PKI VALIDATION – INSPECTION

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

- Authorized DS signed data
- LDS data is authentic and has integrity

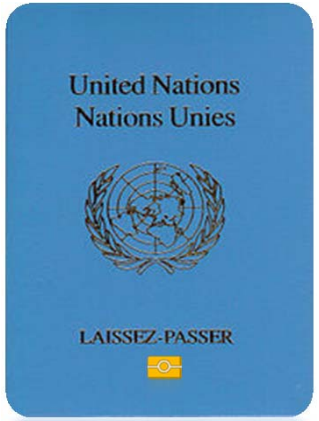
PHYSICAL INSPECTION

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 is critical to eMRTD security

- Technology supporting political trust decisions
- Identity vetting is key

National PKI deployment for eMRTD issuance

- Must be reliable, secure, ICAO 9303 compliant
- Digital Signature

International Trust & Domestic Validation

- Initial trust establishment out-of-band
- Certificates and CRLs must be accessible (PKD/websites)
- Compliant electronic processing extends trust
- Signature Verification

Benefits of PKI realized ONLY if issuing and receiving ICAO member states participate

THANK YOU

Contact Information

E-mail: mark.joynes@entrust.com

Tel.: 613 270-3134