



Entrust Solutions for ePassport Issuance & Validation

Kumar Vankalapati, Entrust

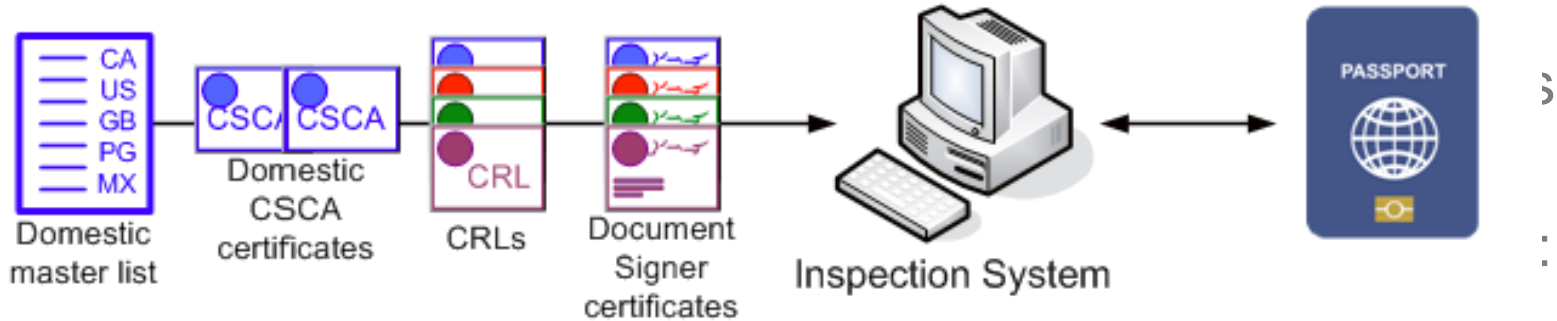
eMRTD

Why electronic ID documents?

- Strong Binding of document to Identity
- Mitigate threats of document forgery
- Mitigate Individual Impersonation
- Integrity and Privacy Protection



1st Generation eMRTD (ICAO BAC)



;

:

ates

Inspection Systems validate e-passports & access their biometric data

Inspection Systems verify the integrity and authenticity of the eMRTD chip using:

- CSCA Certificates

- Master Lists



- CSCA Publishes to ICAO PKD:

- DS Certificates
- CRLs
- Master Lists

Entrust BAC Solution

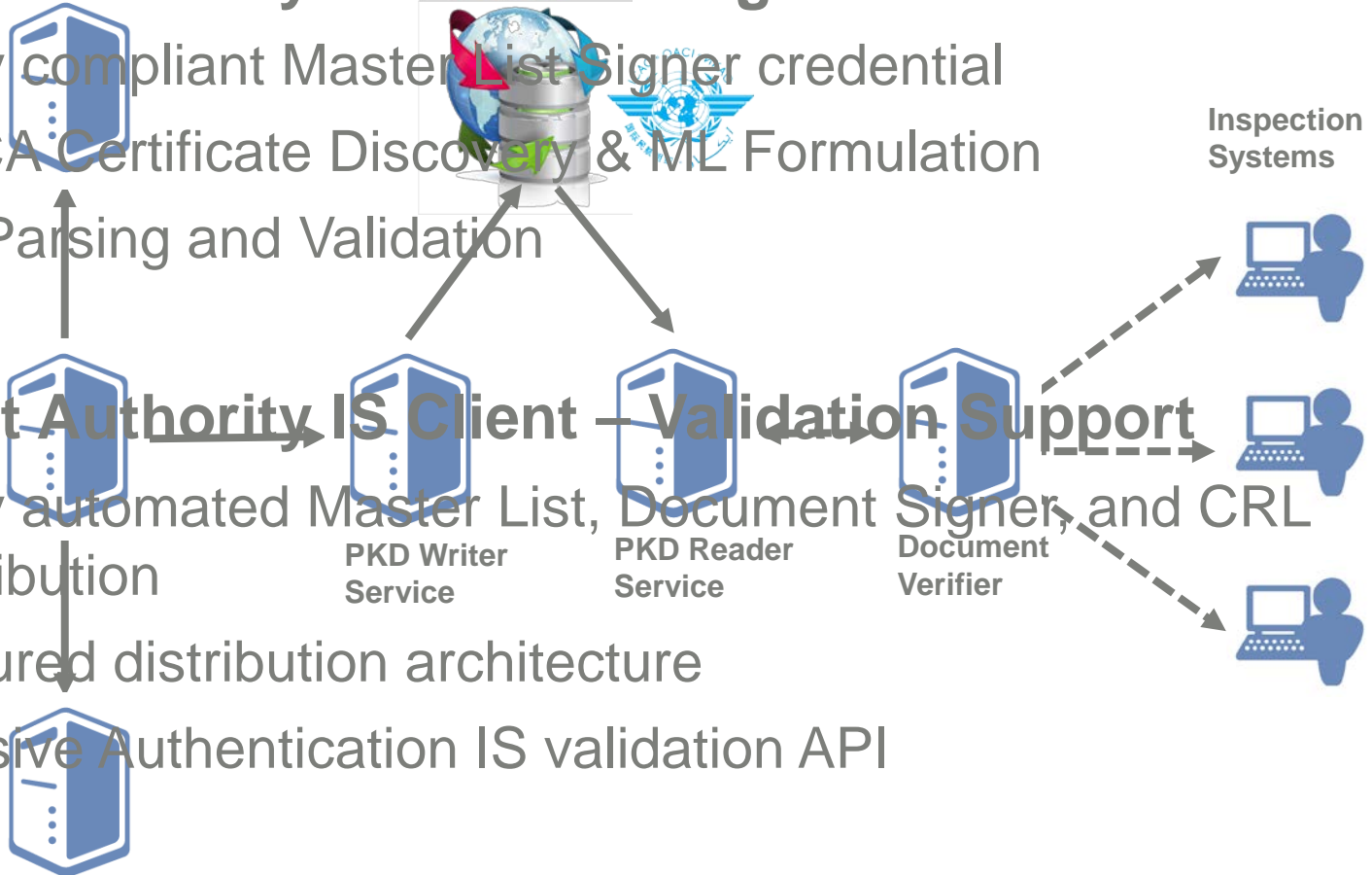
- Entrust Authority Master List Signer**

- Fully compliant Master List Signer credential
- CSCA Certificate Discovery & ML Formulation
- ML Parsing and Validation

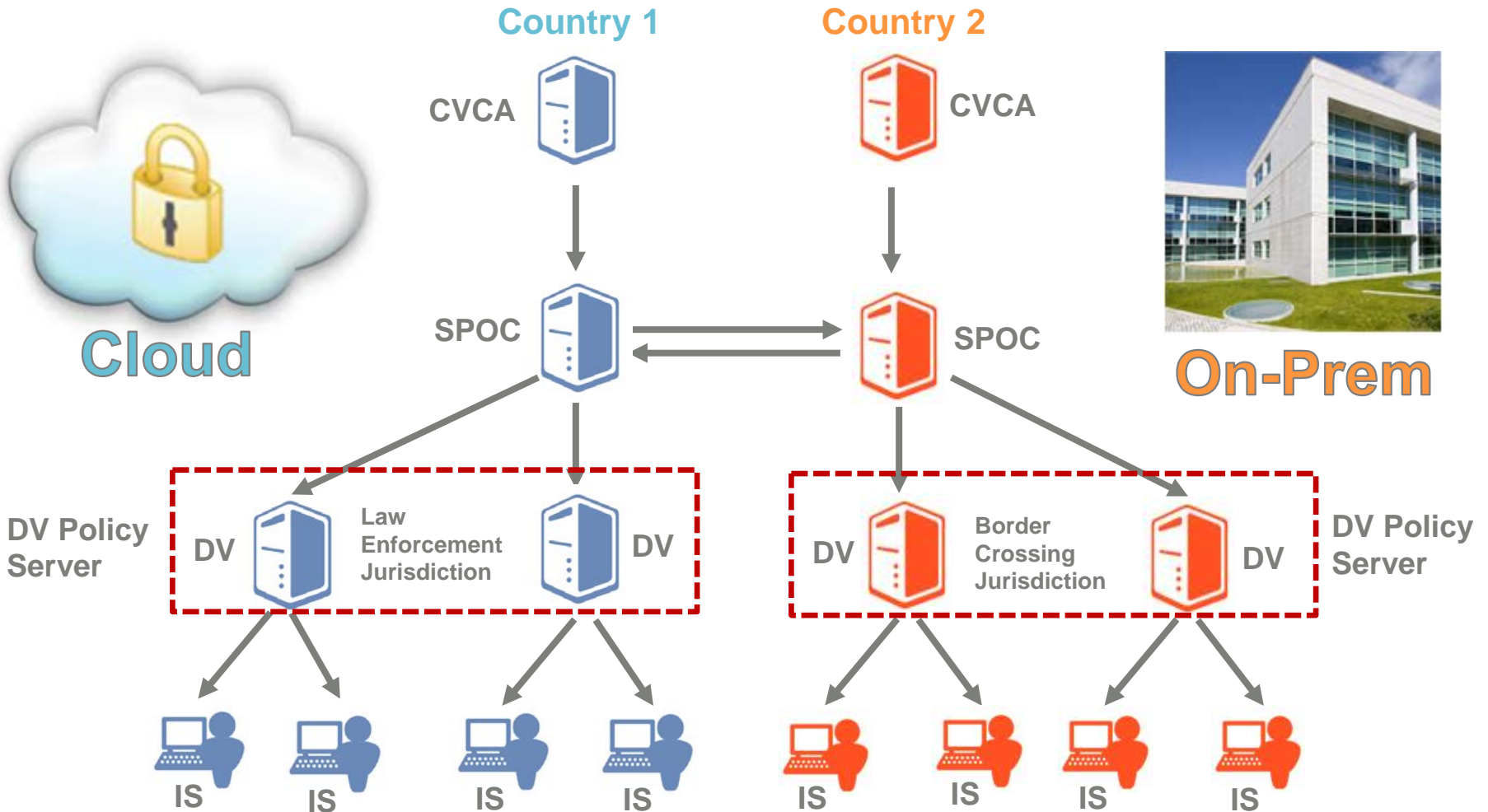
- Entrust Authority IS Client – Validation Support**

- Fully automated Master List, Document Signer, and CRL distribution
- Secured distribution architecture

- Passive Authentication IS validation API



Entrust EAC Solution



Entrust EAC Architecture

- **CVCA**
 - Dual Rooted for X.509 and ISO 7816
 - Can serve as combined CSCA & CVCA
 - Can support Multiple DVs
 - Intuitive Domestic & International DV Management UI
- **DV Policy Server**
 - UI to manage Inspection Systems in to a chosen DV, and view the current status information about all Inspection Systems across all DVs
 - Capability to group Inspection Systems from the same or other DVs
 - Able to define a policy which can be applied consistently across otherwise disparate servers
- **SPOC**
 - Fully Automated International Certificate Management
 - Interoperable with 3rd party CVCA and/or DV components
 - Integrated SPOC CA
 - Secured SPOC Administration UI

Entrust EAC Architecture

- **Document Verifiers**
 - Fully automated Certificate & Key Management with CVCA, SPOC and Inspection Systems
 - Intuitive UI for Domestic & International Certificate Management
 - Intuitive UI for management of Inspection System Architecture
- **Inspection Systems**
 - Support for IS Concentrator & distributed IS architecture
 - APIs for Passive Authentication & Terminal Authentication
 - Fully automated certificate lifecycle management
 - PKCS#11 support for HSM

COTS Solutions For:

- Country Signing (CA)
- Document Signing
 - Online Management – CMP
 - Offline Management – OTCU
- Master List Signing
- PKD Integration (Reader & Writer)
- Document Validation Distribution Architecture
- Passive Authentication Validation API's for IS integration
- EAC Oriented
 - Country Verifying (CA)
 - Single Point of Contact (SPOC)
 - Document Verifier (CA)
 - IS Concentrator/IS Client
 - Terminal Authentication API's for IS integration



Entrust Solutions – Key Differentiators

Entrust Authority
Country Signing Solution

Entrust Authority
Document Validation Solution

Entrust Authority Security Manager

CSCA

Document
Signer

- Unique Dual-rooted PKI
- 8th Generation Stability
- Out-of-the-box Certificate specifications
- Production deployed for BAC & EAC
- Policy-controlled Intuitive Management Interfaces
- PKD Integration
- Fully Automated Certificate & Key Distribution & Management
- Managed X509 end-entities for SSL (DS & IS)
- Open WS APIs
- Committed to Open Standards
- Common Criteria Evaluation

CVCA

Document
Verifier

Entrust IS Key Value

Entrust Authority Document Validation Solution

Entrust Authority IS Concentrator

- Trusted distribution channel
- Centralized EAC Transaction Processing
- Fully Automated Certificate & Key Mgmt
- Engineered for High Performance, Load & Availability
- Supports Market leading HSM (PKCS#11)
- Access Controlled



Entrust IS Client

- Trusted distribution channel
- Leveraging Domestic Master List
- Passive Authentication
- Terminal Authentication (EAC)
- Distributed or Centralized EAC Processing
- Fully Automated Certificate & IS Key Mgmt
- Open WS Integration API



Global eMRTD Projects

- Root of trust for 1st & 2nd Generation ePassports
- ~50%+ of all ePassports issued
- 50%+ of 2nd Generation ePassport Countries
- 21 Countries
- On Premise & Cloud solutions for ePassport Digital Signing
- Document Validation at Border Control
- Guidance to ICAO on PKI & PKD Trust





Questions?