Entrust® Securing Digital Identities & Information

Global eMRP PKI: Status

Craig Delmage, CISSP

Director, Entrust Ltd.

Entrust - World leader in Identity Solutions

- Global security solutions provider
- 15 Years
- HQ (US), R&D (Canada), Offices (Lots)
- Pioneer: 1st commercial PKI – 1995
- 1000+ global PKI deployments
- 15 eMRP Projects (US, Canada, UK…)
- PKI Software & Identity Card Solutions
- PKI SaaS PKI & Credentialing Services

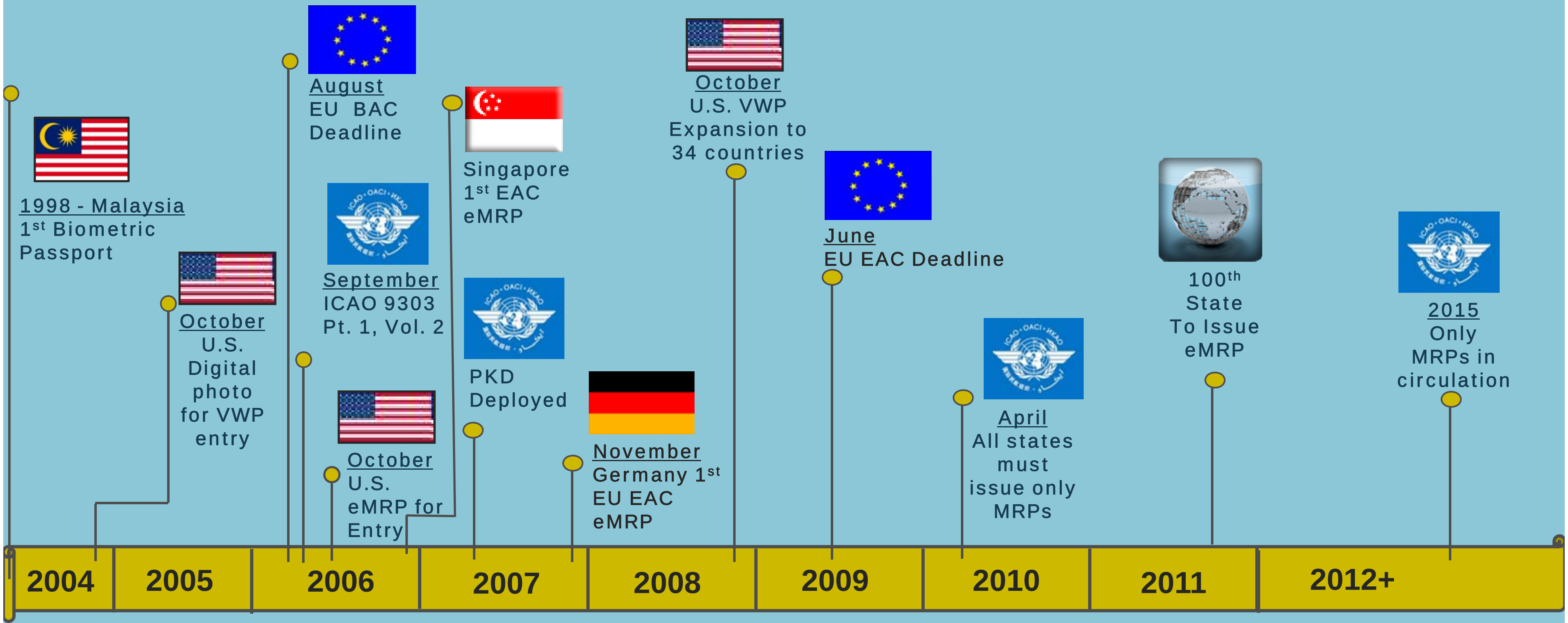
Outline

1. Historical Timeline
2. BAC PKI Progression
3. EAC PKI Progression
4. Related PKI Advancements

Entrust
Securing Digital Identities & Information

The March of ePassports

Major Milestones (1998 – 2015)



1998 - Malaysia
1st Biometric
Passport

October
U.S.
Digital
photo
for VWP
entry

August
EU BAC
Deadline

September
ICAO 9303
Pt. 1, Vol. 2

October
U.S.
eMRP for
Entry

Singapore
1st EAC
eMRP

PKD
Deployed

November
Germany 1st
EU EAC
eMRP

October
U.S. VWP
Expansion to
34 countries

June
EU EAC Deadline

April
All states
must
issue only
MRPs

100th
State
To Issue
eMRP

2015
Only
MRPs in
circulation

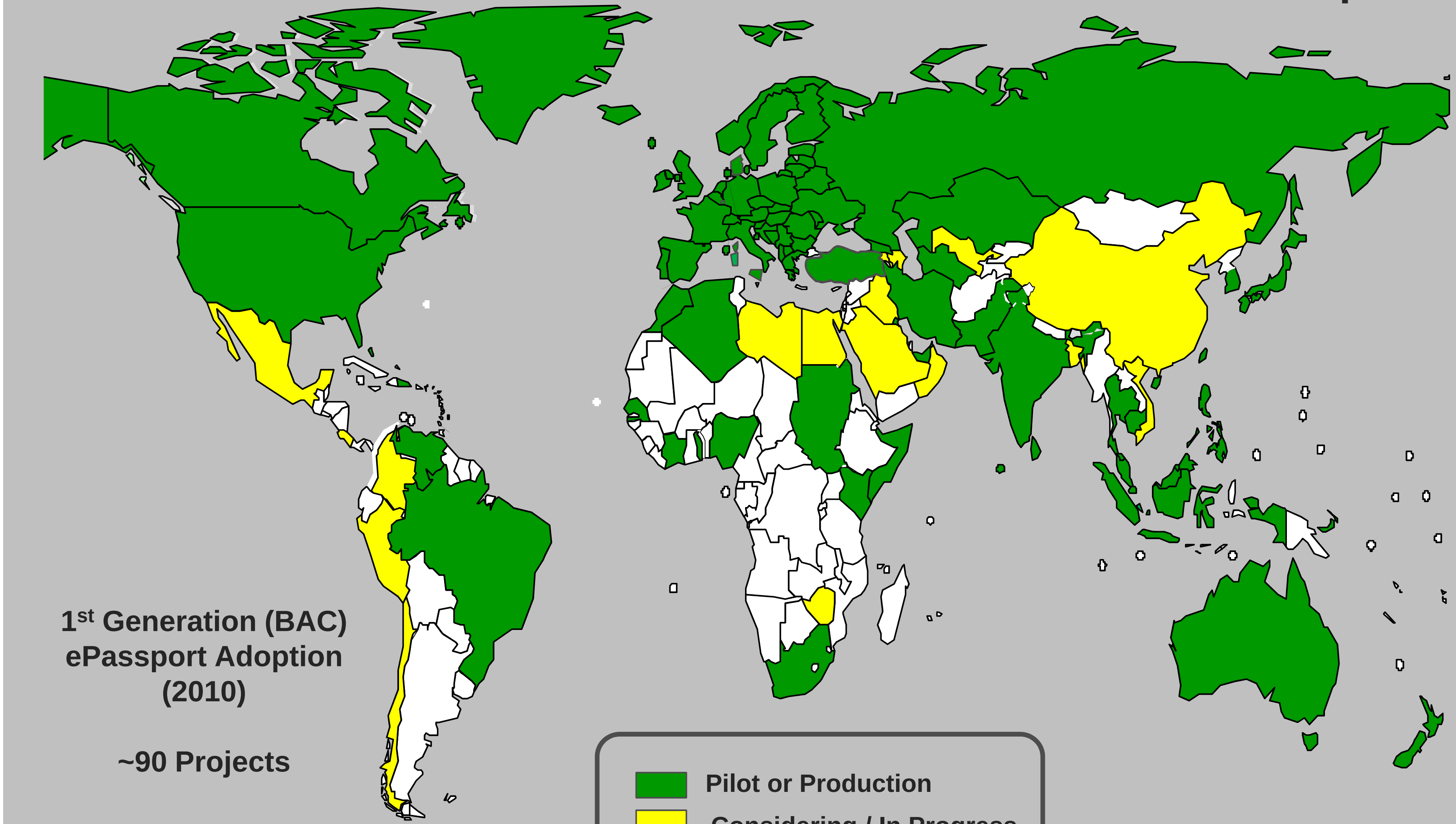
2004	2005	2006	2007	2008	2009	2010	2011	2012+
3	10	36	49	60	75	90	100	115?

# Countries Deploying ePassports

BAC PKI Progression

- 2006: ICAO 9303 Standards
- 2007: PKD deployment
- 2008: PKD Master List Signing (MLS)
- 2010: Validation channels
- Future: Supplemental Access Control (SAC)

1st Generation ePassport



1st Generation (BAC) ePassport Adoption (2010)

~90 Projects

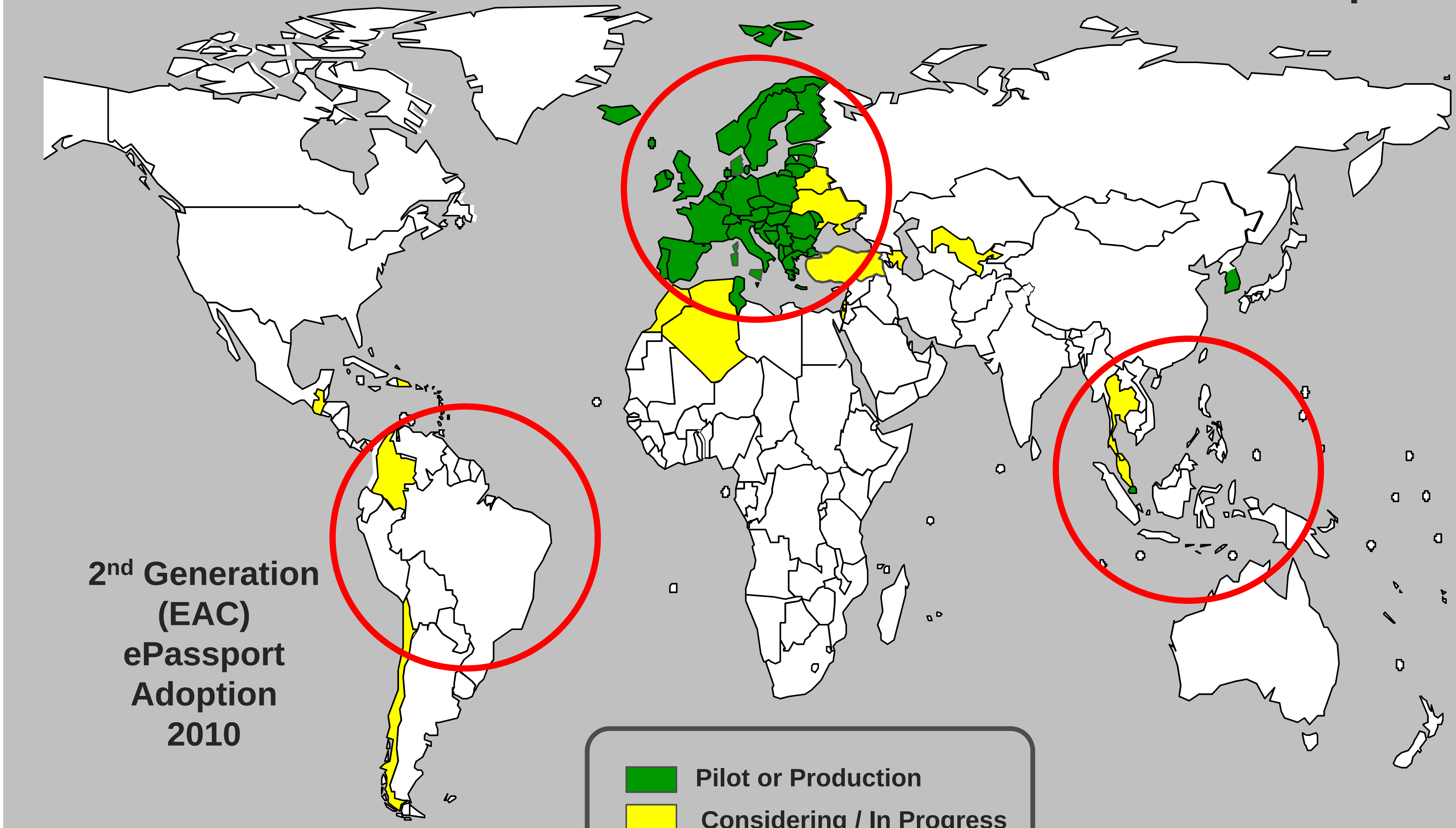
🟩 Pilot or Production

🟨 Considering / In Progress

EAC PKI Progression

- 2006: EU EAC specification
- 2009: EU SPOC specification
- 2010: Validation channels
- 2010: Emergence of other ‘communities of interest’
- 2011: Other applications (National ID smart cards)
- Future: LDS 2.0, Border Control Optimization

2nd Generation ePassport



2nd Generation (EAC) ePassport Adoption 2010

🟩 Pilot or Production

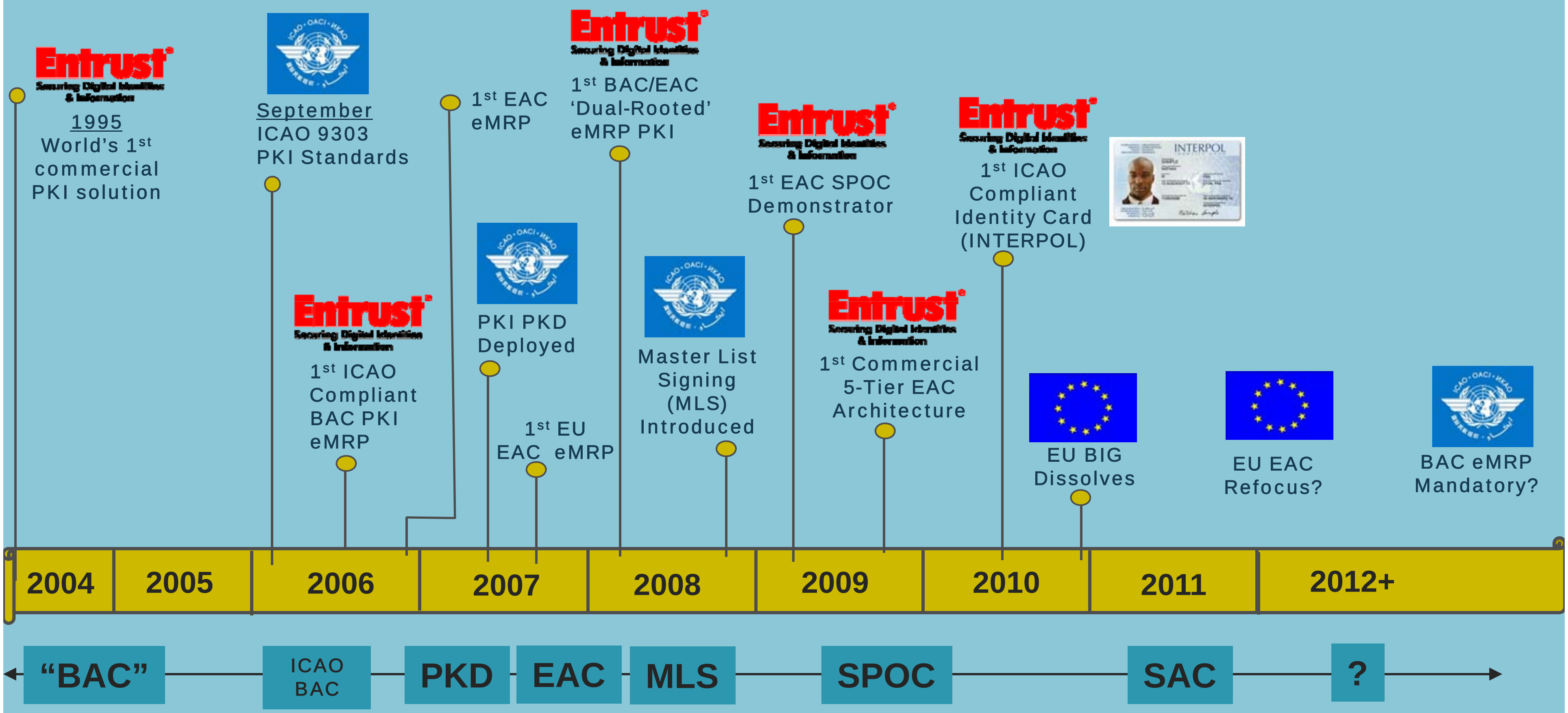
🟨 Considering / In Progress

BAC and EAC Validation Channel

- From CA down to Inspection Station Client
  - CA > DS/DV > MLS/SPOC > Concentrator > Client
- For ongoing, automated distribution of PKI material
  - Certificates (DS, Link), Master Lists, CRLs, etc.
- Secure: Authenticated, encrypted channel
- Certificate path validation

The March of eMRP PKI

1995 – 2012+



1995
World's 1st commercial PKI solution

September
ICAO 9303 PKI Standards

1st ICAO Compliant BAC PKI eMRP

1st EAC eMRP

PKI PKD Deployed

1st EU EAC eMRP

1st BAC/EAC 'Dual-Rooted' eMRP PKI

Master List Signing (MLS) Introduced

1st EAC SPOC Demonstrator

1st Commercial 5-Tier EAC Architecture

1st ICAO Compliant Identity Card (INTERPOL)

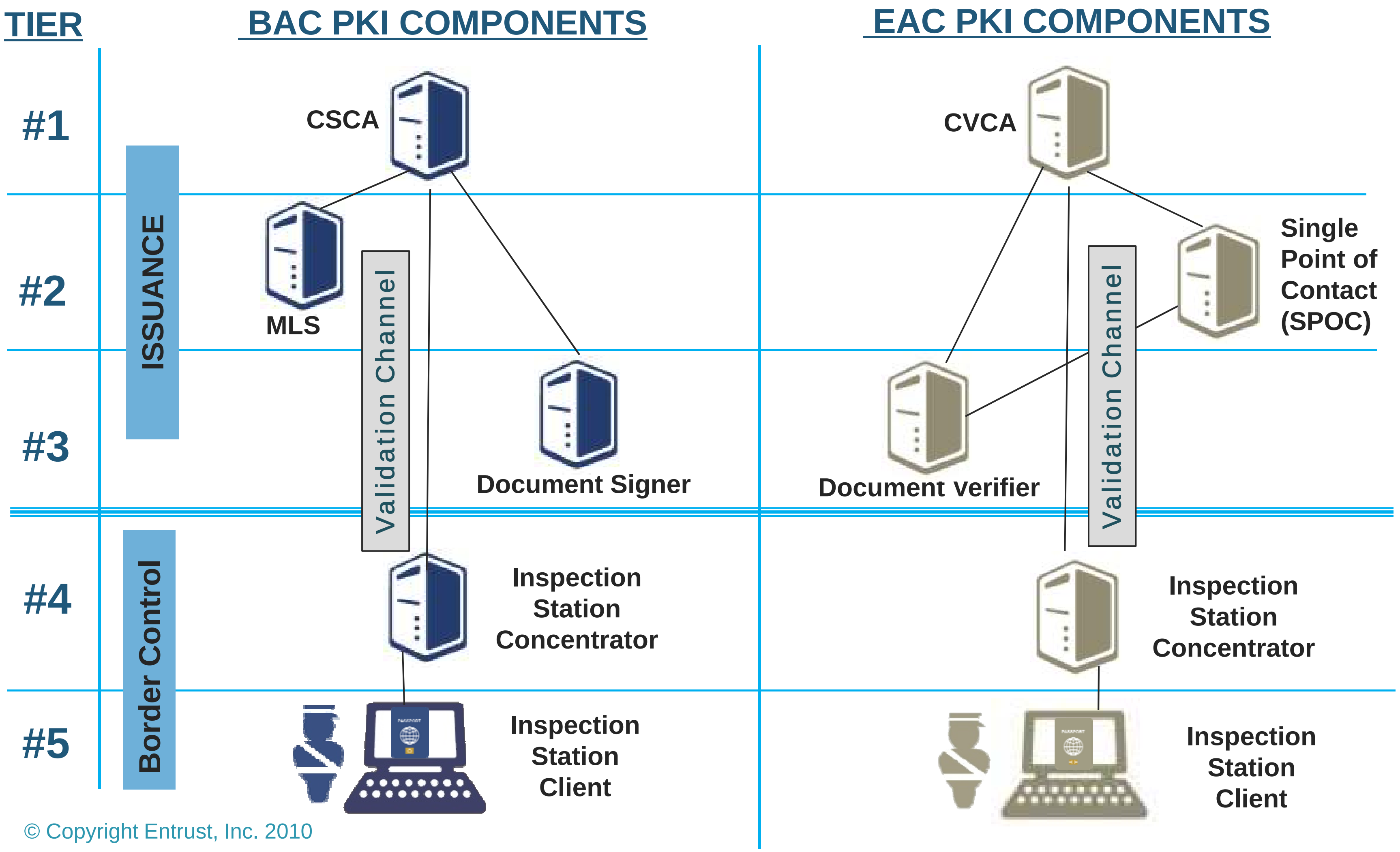
EU BIG Dissolves

EU EAC Refocus?

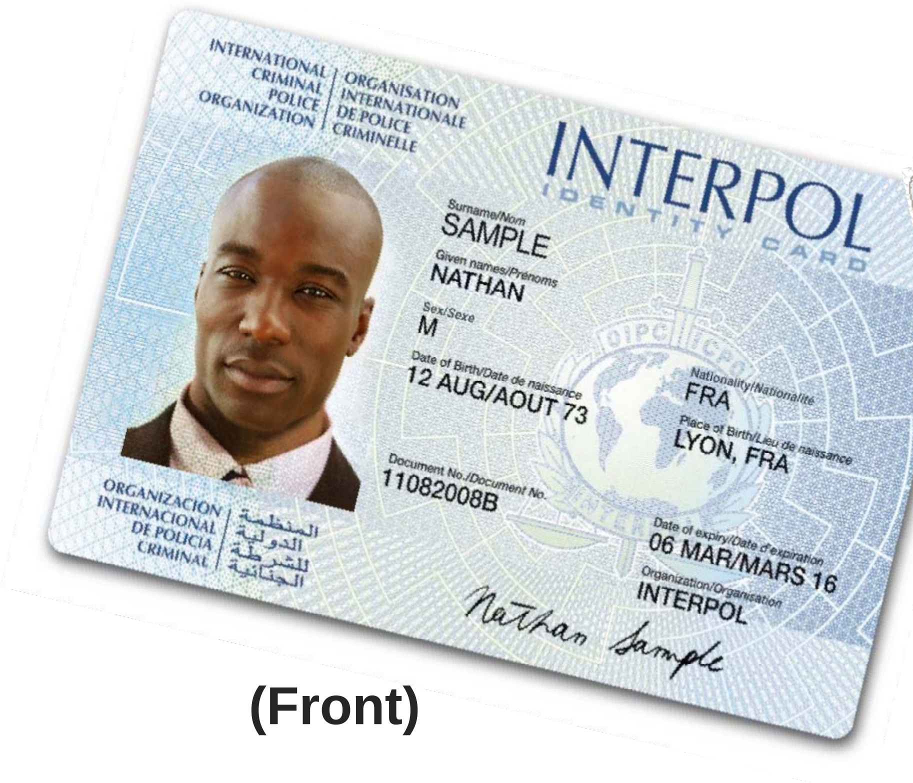
BAC eMRP Mandatory?

PKI Evolution

PKI: 5 Tier Architecture



2010: World's First ICAO 9303 Compliant Identity Card (with BAC/EAC)



INTERNATIONAL CRIMINAL POLICE ORGANIZATION | ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE

INTERPOL
IDENTITY CARD

Surname/Nom
SAMPLE

Given names/Prénoms
NATHAN

Sex/Sexe
M

Date of Birth/Date de naissance
12 AUG/AOUT 73

Nationality/Nationalité
FRA

Place of Birth/Lieu de naissance
LYON, FRA

Document No./Document No.
11082008B

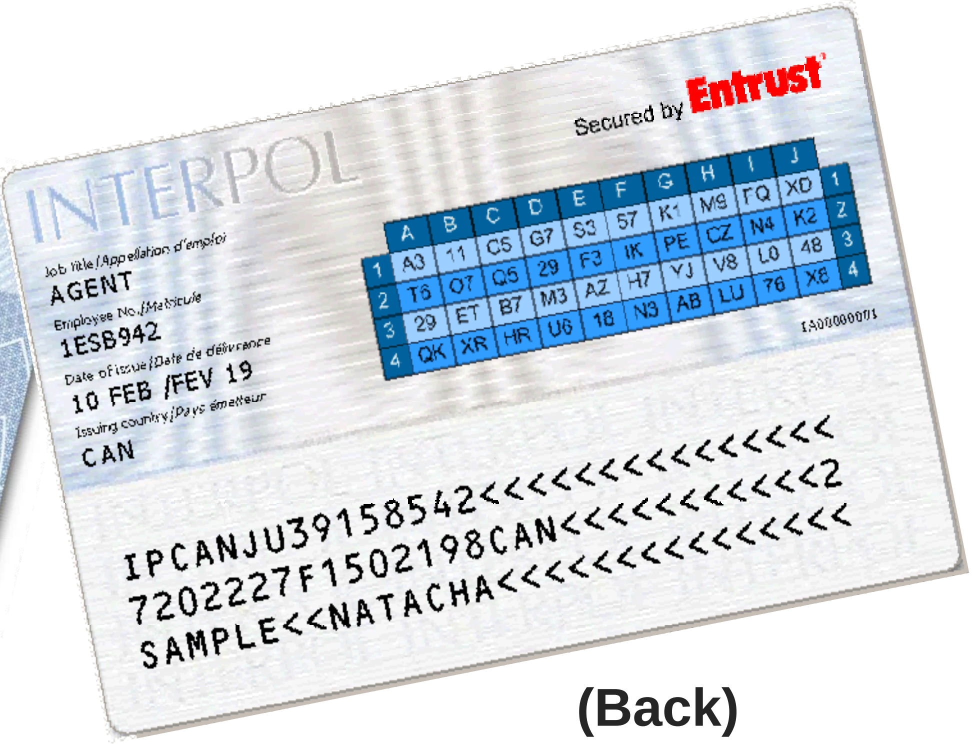
Date of expiry/Date d'expiration
06 MAR/MARS 16

Organization/Organisation
INTERPOL

Nathan Sample

ORGANIZACION INTERNACIONAL DE POLICIA CRIMINAL | المنظمة الدولية للشرطة الجنائية

(Front)



INTERPOL

Secured by Entrust

Job title/Appellation d'emploi
AGENT

Employee No./Matricule
1ESB942

Date of issue/Date de délivrance
10 FEB /FEV 19

Issuing country/Pays émetteur
CAN

	A	B	C	D	E	F	G	H	I	J	
1	A3	11	C5	G7	S3	57	K1	M9	FQ	XD	1
2	T6	O7	Q5	29	F3	IK	PE	CZ	N4	K2	Z
3	29	ET	B7	M3	AZ	H7	YJ	V8	L0	48	3
4	QK	XR	HR	U6	18	N3	AB	LU	76	X8	4

IA00000071

```
IPCANJU39158542<<<<<<<<<<<<<<<
7202227F1502198CAN<<<<<<<<<<<2
SAMPLE<<NATACHA<<<<<<<<<<<<<<<
```

(Back)

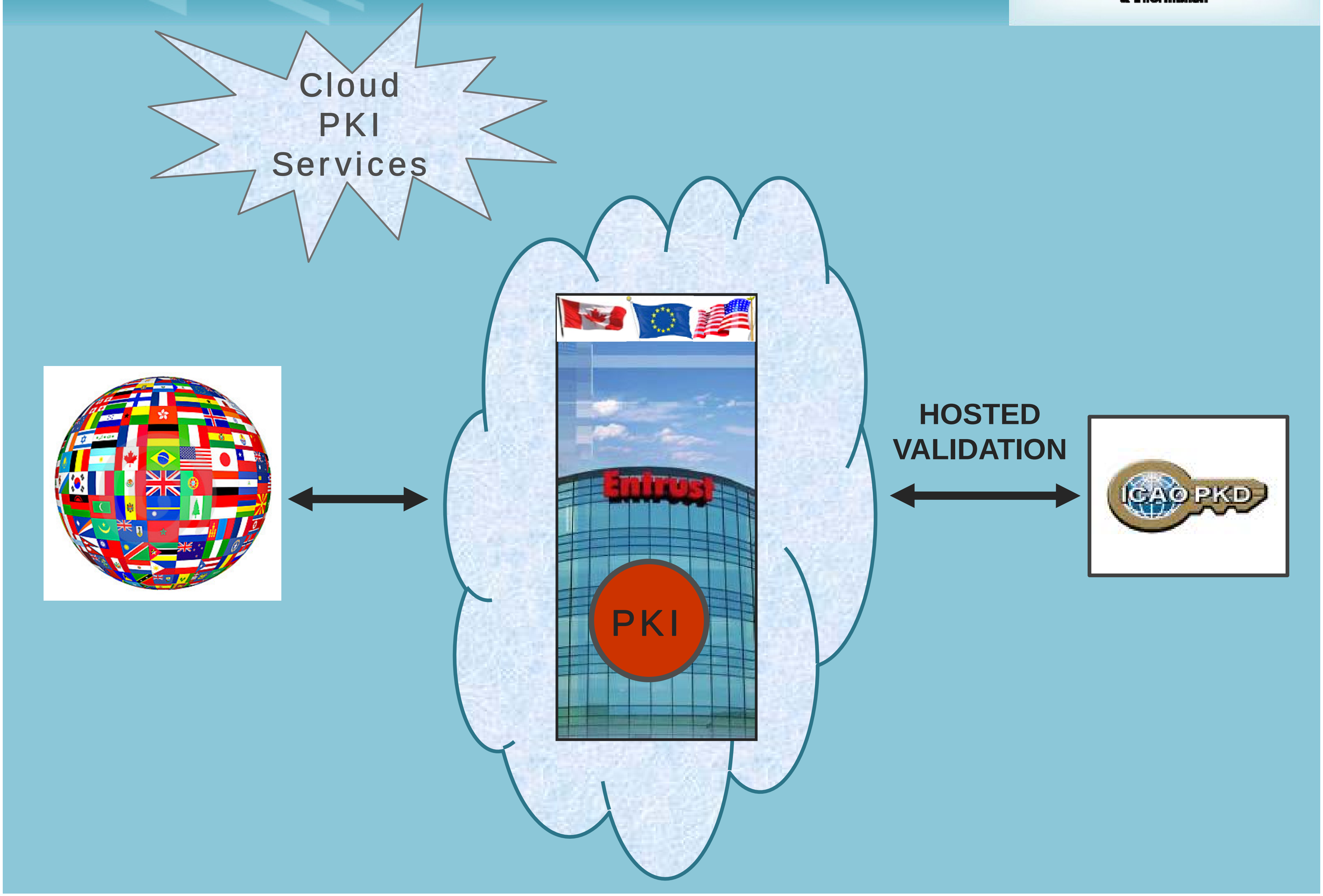
Employee ID – Physical Access – Logical Access

Other Related Advancements

- Automated Border Control (ABC) integration
- Elliptic curve cryptography (ECC)
- Hosted BAC/EAC PKI (cloud services)
- Hosted validation services
- LDS 2.0
- Emergence of ‘Virtual Borders’

Hosted PKI

Entrust
Securing Digital Identities
& Information



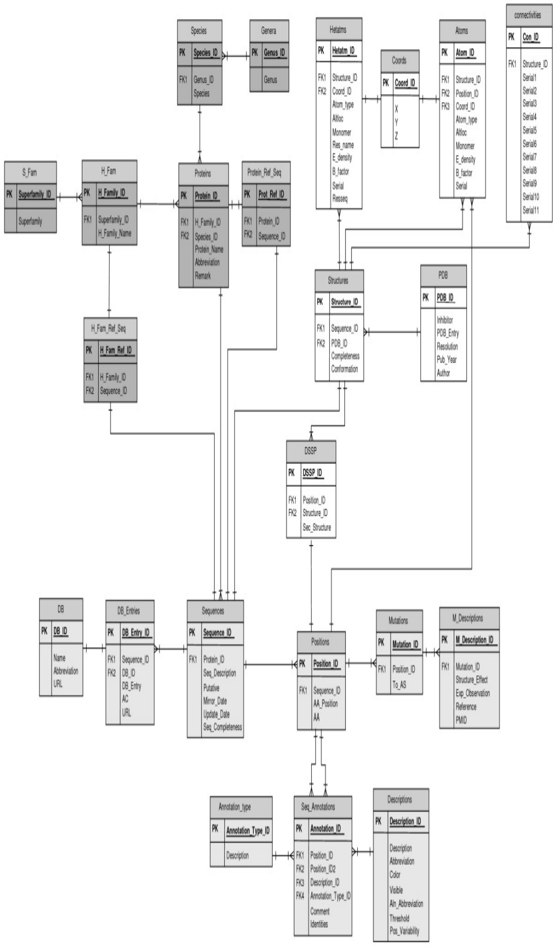
Cloud
PKI
Services

PKI

HOSTED
VALIDATION

LDS 2.0

- Potential for additional applications
- Potential for Additional biometrics
- Storage and retrieval of visa info
- Recording and retrieval of entry/exit
- Implications for PKI
  - Additional support for CV PKI
  - Which objects to digitally sign?



Portable, Virtual Border Solutions

Summary

- BAC and EAC evolution continues
  - More advancements coming – e.g. SAC, LDS 2.0
  - Starting to be used for other applications
- EU EAC deadline missed
  - SPOC will ease deployment
- eMRP architecture will continue evolve
  - Additional applications
  - Migration toward smart card formats
- PKI has kept up!

PKI is ready for future challenge!

Entrust® Securing Digital Identities & Information

<Let's Talk

Want to learn more?

Craig Delmage, CISSP

Director, Entrust Ltd.

craig.delmage@entrust.com

+1 (613) 270-3489