International Civil Aviation Organization

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

ICAO Headquarters, Montréal, Canada
12 - 15 September 2011

ePassport Compliance Challenges: The Border Perspective

David Clark
Caicos Management Associates
Ottawa, Canada

- Invincible
- Absolutely secure with passport data on the chip
- Utterly reliable; can always be counted on. The authentication certificate on the chip further proves it.
- May render “old” passports obsolete?

Early ePassport Beliefs?

“I always thought he was dead, but he has an e-Passport.”

Really?

- e-Passports are a significant advance in passport security, but:
  - They must be understood, and authenticated properly, in order to achieve this enhanced security. Otherwise they may deceive and create false trust.
  - They do not replace other passport security features or render them obsolete, but rather augment them.
  - Proper e-Passport issuance must be complemented by proper e-Passport border authentication.

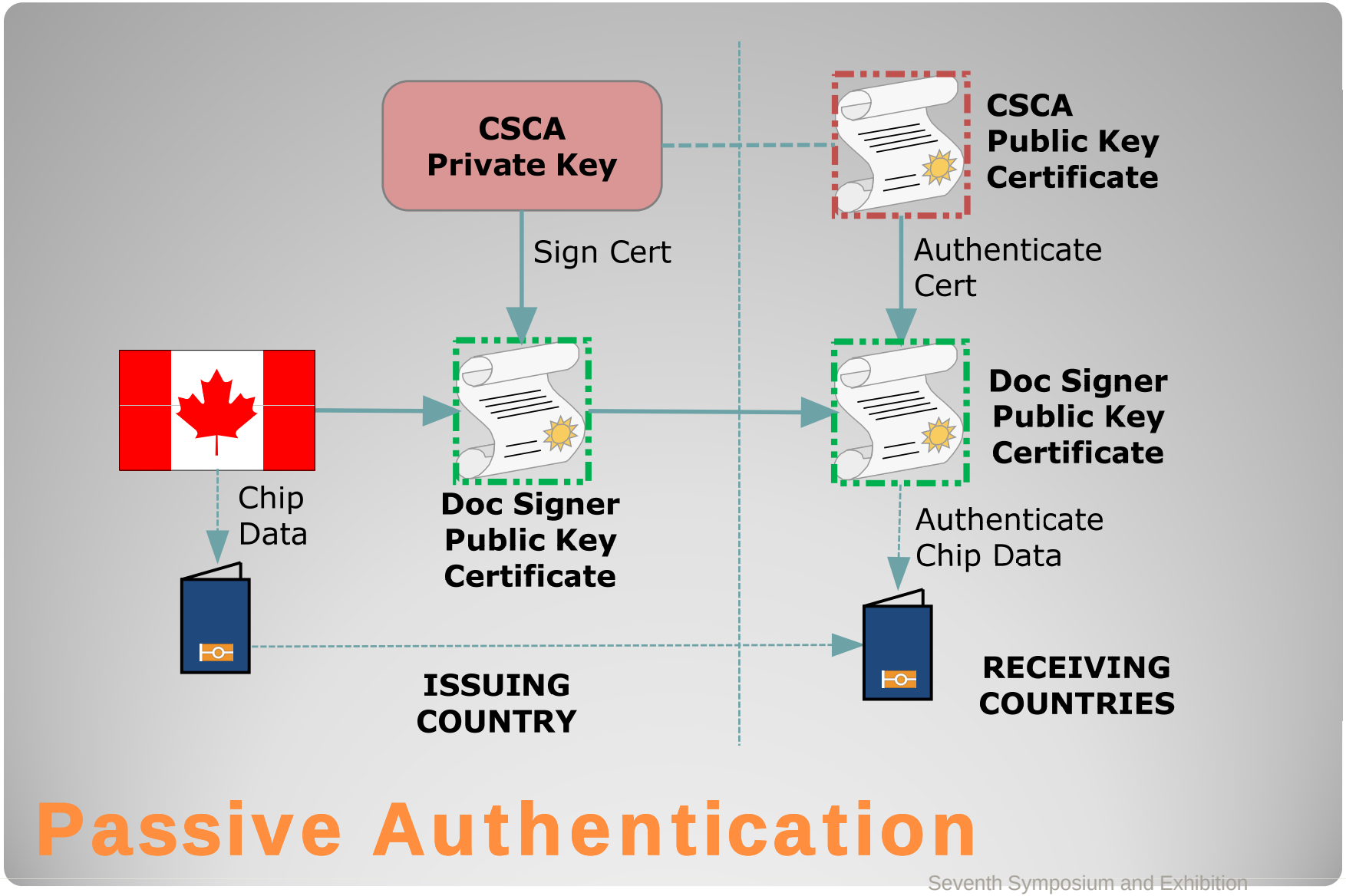
How can this be? - The Facts

- 250,000,000 e-passports now in circulation
- e-Passports represent half of all passports issued globally, with most countries issuing now or soon.
- BUT:
  - Border reader deployment is still very limited
  - Border processing of ePassports often does not represent best practices for ePassport security

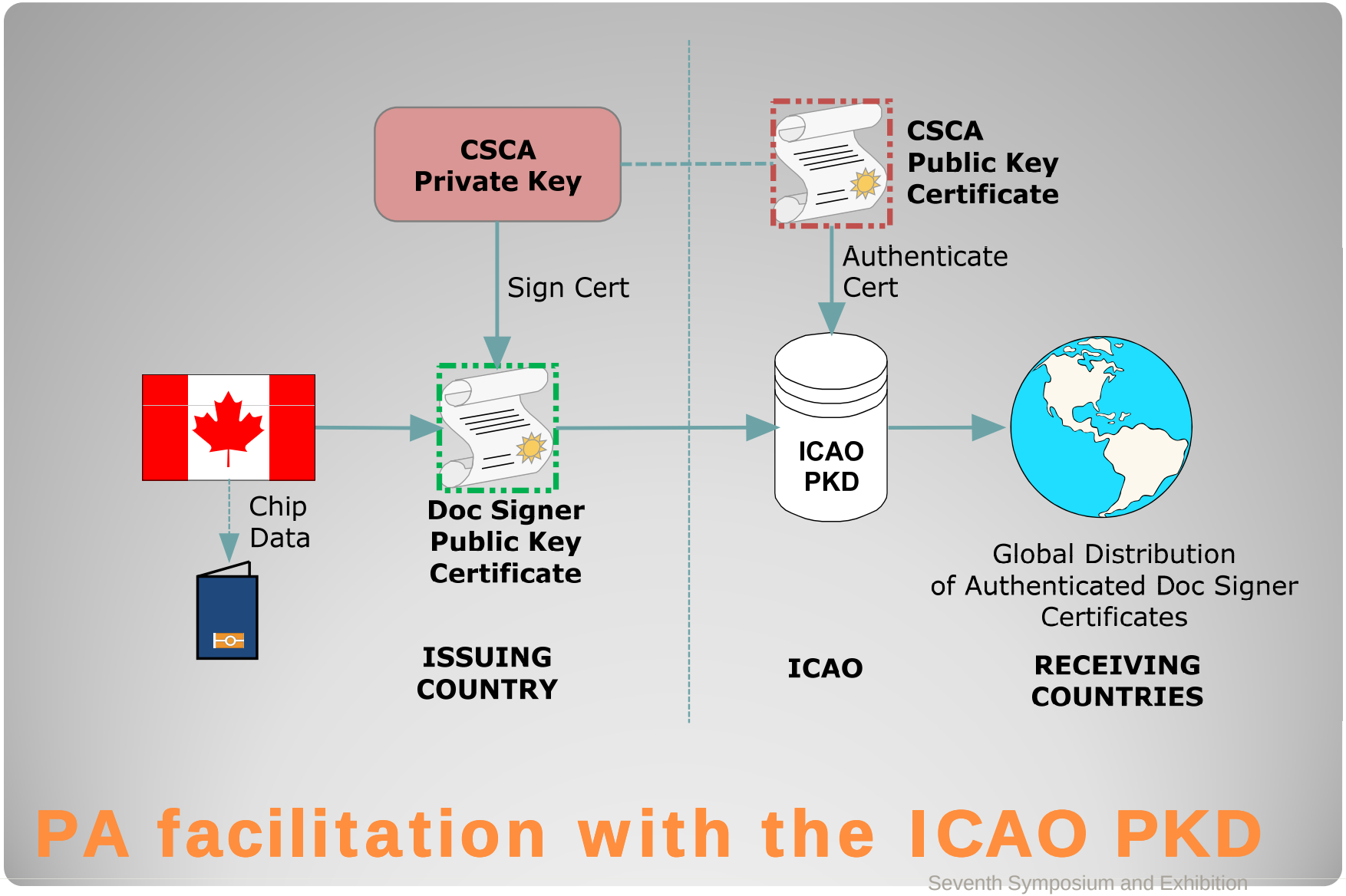
ePassport Reality Today

- Chip data can only be considered reliable if:
  - The decrypted digital signature matches the corresponding hash of the chip data, **AND:**
    - **either**: the Doc Signer Public Key Certificate used to decrypt the digital signature is also authenticated with the trusted Country Signer Certificate Authority (CSCA) certificate;
    - **or** the Doc Signer Public Key Certificate used is listed as valid in the ICAO Public Key Directory (PKD)
  - This is “Passive Authentication”, an essential part of ICAO e-Passport standards.

A Reminder: how ePassports work



Passive Authentication



PA facilitation with the ICAO PKD

- To understand possible illicit border entry attempts with e-Passports.
- To understand the limitations of some e-Passport border processing practices without PA.
- To understand the important role of the ICAO Public Key Directory (PKD) in implementing PA.
- To set out rational steps for border implementation for proper e-Passport treatment.

Border Deployment Planning Needs

Some Attacks

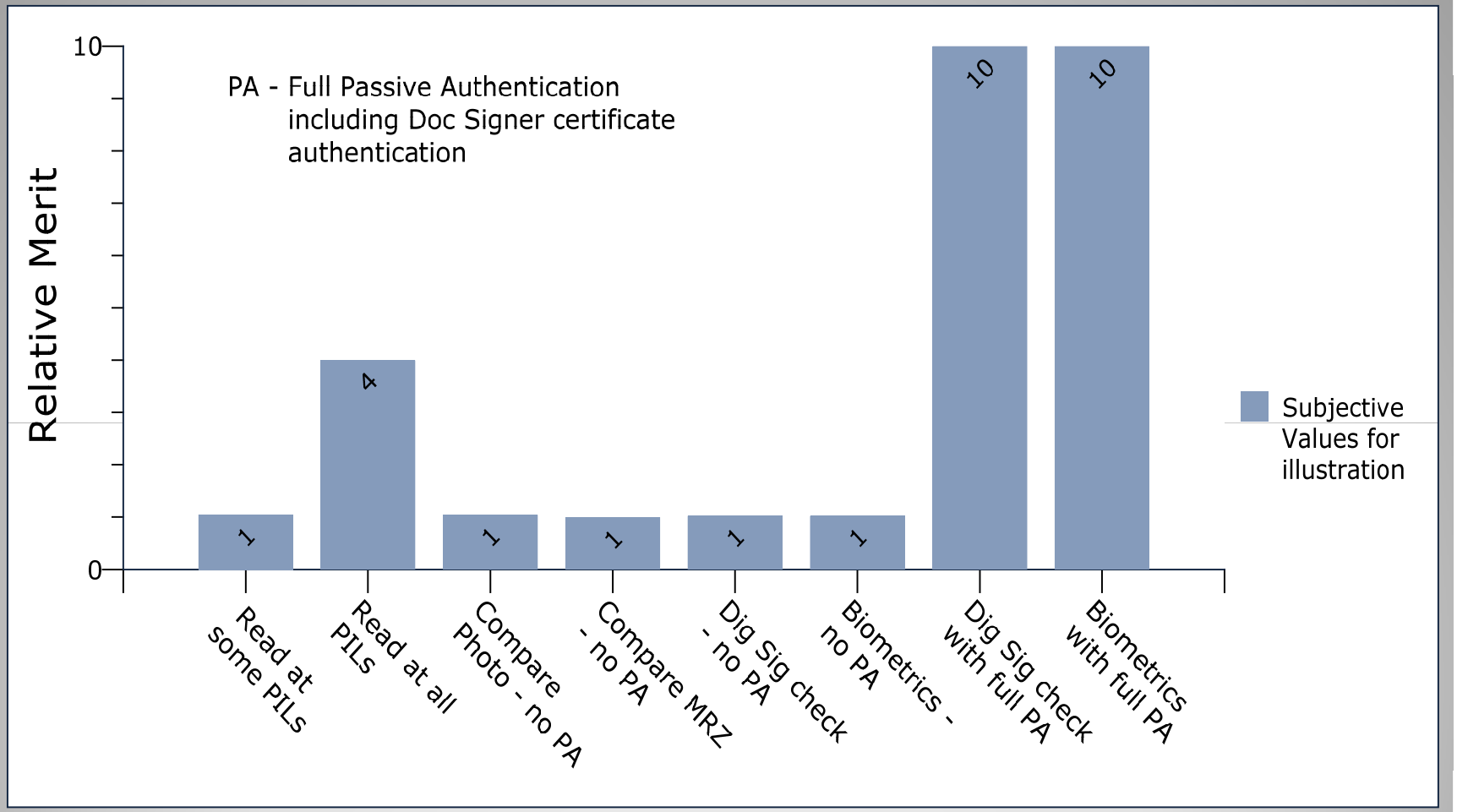
- Stolen ePassport – simple impersonation
  - E-Passports not read?
  - No electronic biometric checks at borders?
- Stolen ePassport – destroy the chip
  - Still a valid passport according to ICAO standards.
  - E-Passports not read?
  - No policies for special treatment?
- Stolen ePassport – substitute chip
  - Fake photo, validity dates, digital signature, and Doc Signer certificate on chip?
  - E-Passports not read?
  - No PA checks with certificate authentication?
- Counterfeit ePassport – both data page and chip
  - Digital signature checks out with certificate on chip but no PA with certificate authentication?

- Don’t read the ePassport, or don’t always read the ePassport, even if readers are deployed.
- Read the chip and visually compare the chip photo against the data page photo.
- Read the chip and compare the MRZs on the chip and the data page.
- Read the chip and check the digital signature using the certificate on the chip, but without full PA authentication of the certificate on the chip.
- Don’t check biometrics electronically, or don’t ever check biometrics electronically.

Some Common Border Practices?

- Are such methods effective at all without PA?
  - “Mistakes” made by counterfeiters:
    - MRZ on chip not compliant with check digits?
    - Data on chip not the same as on data page?
    - Certificate on chip has a Doc Signer key that does not work with the fake data?
- Answer: perhaps in a very limited way, but…

Assessment of these practices


PA - Full Passive Authentication including Doc Signer certificate authentication
Relative Merit
10
0
1
4
1
1
1
1
10
10
Read at some PILs
Read at all PILs
Compare Photo - no PA
Compare MRZ - no PA
Dig Sig check - no PA
Biometrics - no PA
Dig Sig check with full PA
Biometrics with full PA
Subjective Values for illustration

The Reality

- Deploy e-Passports readers and always use them, even without PA initially:
  - Criminal doesn't know what will be checked when you read e-Passports:
    - He knows altered or counterfeit chip data will be detected with full Passive Authentication
    - He knows a stolen book will risk detection with electronic biometric checks
- Strong incentive for the criminal to go elsewhere, or not try.

Interim Tools and Protection - 1

- Implement electronic biometric checks by clear policy and practices:
  - Any operator uncertainty with a visual check?
  - Sampling at primary – equip some primary stations with biometric capture devices (cameras?) as well as readers?
  - Any inoperative chip – send to secondary?
    - Very low international experience with such failures.
- Strong incentive for the criminal to go elsewhere, or not try.

Interim Tools and Protection - 2

- Initiate full Passive Authentication in all border readers/systems as soon as possible:
  - Initiate PA implementation simultaneously with border reader deployment plans.
  - This must be treated as a high priority border security requirement.
    - ABC facilities must use full PA of course.
  - Join and use the PKD as part of this exercise. Low cost; very high benefit.

Ultimate Protection - 3

Conclusions

- If you don't deploy readers and always read e-Passports, you are the target for access attempts by criminals that are deterred or denied to them elsewhere.
- If you don't deploy and use Passive Authentication with your other practices, you are at serious risk of false document trust and undetected entry by sophisticated criminals.
- If you don't use the PKD, you probably can't implement the above realistically.
- Mantra: "*Proper e-Passport issuance must be complemented by proper e-Passport border authentication.*"

David Clark P.Eng.
Caicos Management Associates
(dclark@caicosmanagement.com)

T: 613-824-2208 M: 954-821-5825

Thank you.

Questions?