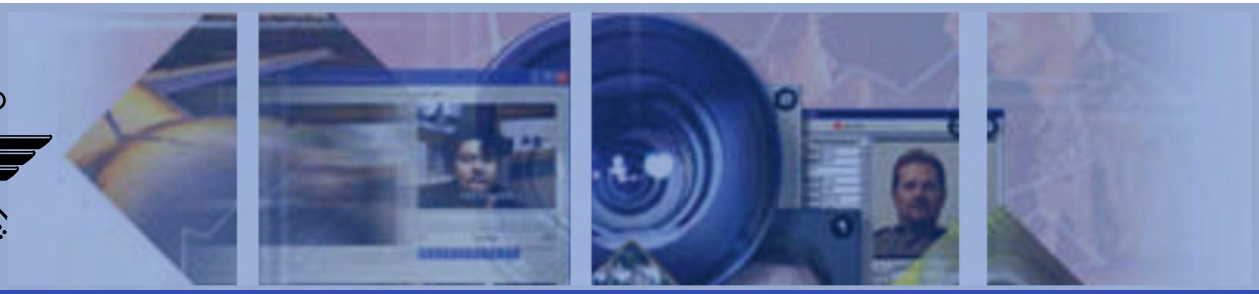


2nd Symposium on ICAO-Standard MRTDs, Biometrics and Security

The ICAO Public Key Directory

David Clark P.Eng
President
Caicos Technologies Inc.
tcidclark@earthlink.net

MRTD Symposium
ICAO Headquarters, Montréal
6 – 7 September 2006

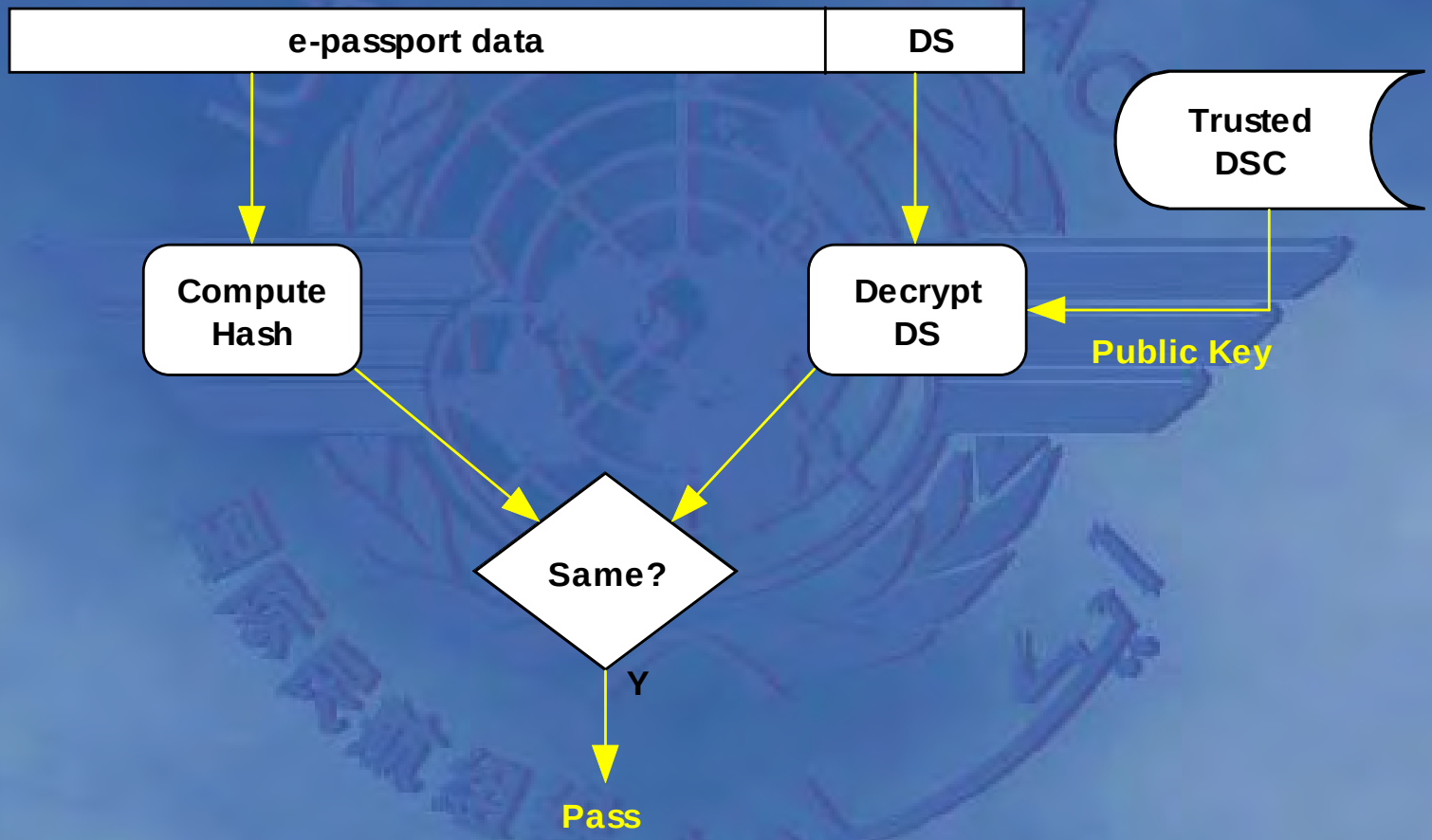
What Is The PKD?

- A directory of all country Document Signing Certificates (DSCs) and certificate revocations (CRLs) needed to validate e-passport data.
- A highly secure facility and service
- Openly available to border control, airlines, and other entities using e-passports
- An integral component of e-passport PKI security

How Does It Work?

- e-passport data is “signed” by the issuing country and the “digital signature” (DS) is stored with the data.
- The DS is really an *encrypted hash* of the data
- The separate decryption (public) key is distributed via the PKD.

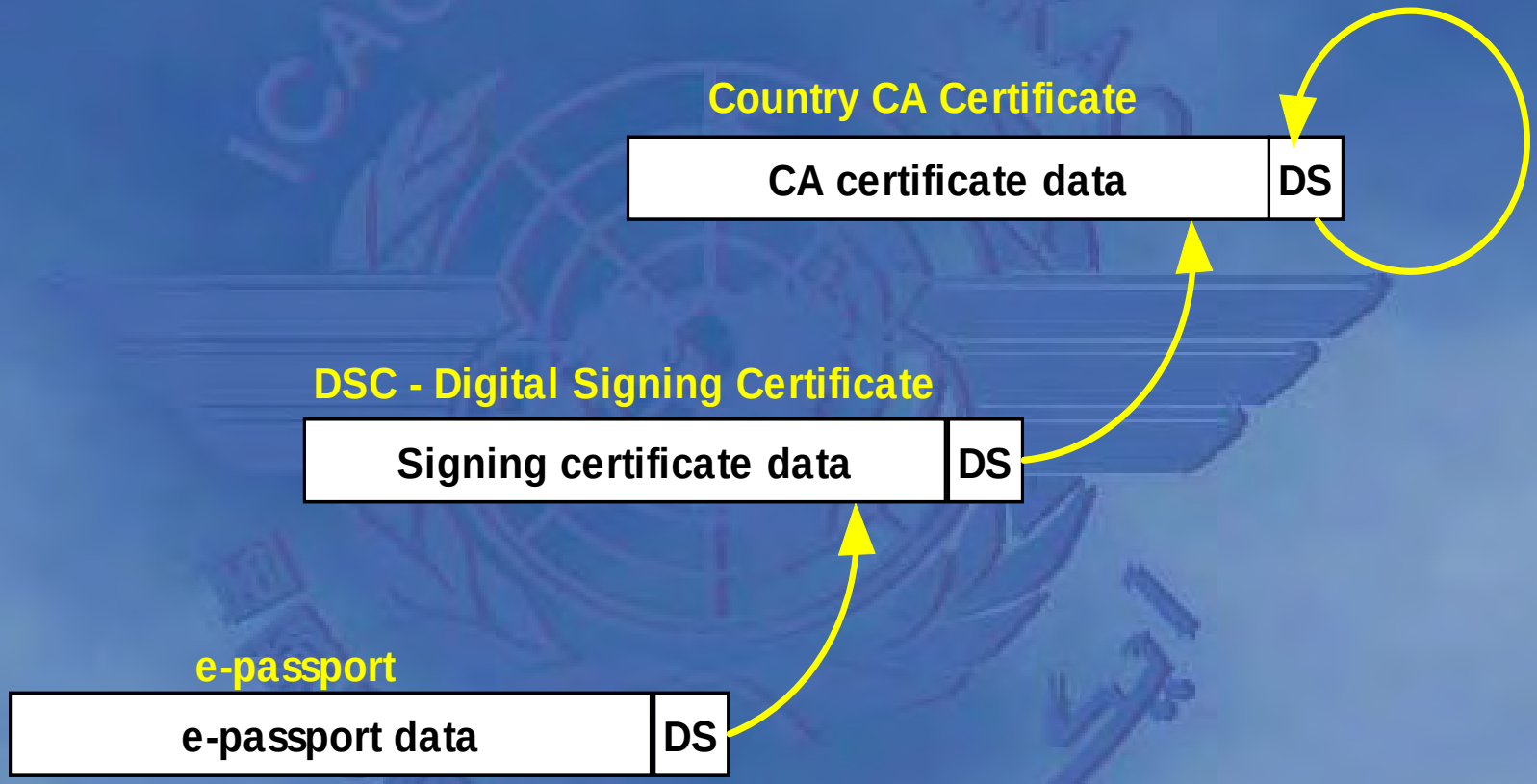
The Basic Process



The ICAO PKI Trust Hierarchy

- e-passports data is validated by the DS through use of the proper DSC (containing the public decryption key for the DS)
- The DSC used must also be trusted and so must also be validated.
- The Country Certificate Authority (CA) key certificates are the highest trust level in the ICAO PKI hierarchy.
- CA certificates are ONLY distributed to other participating (e-passport issuing) countries, and to ICAO.

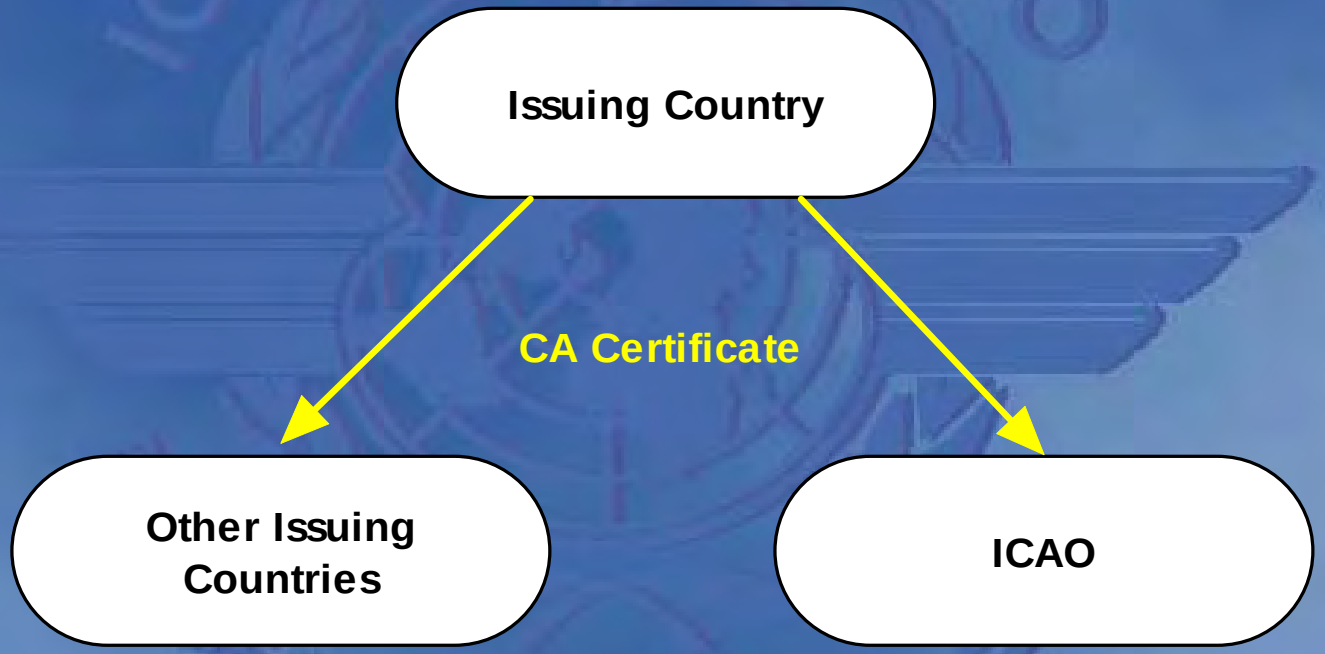
ICAO PKI Chain of Trust



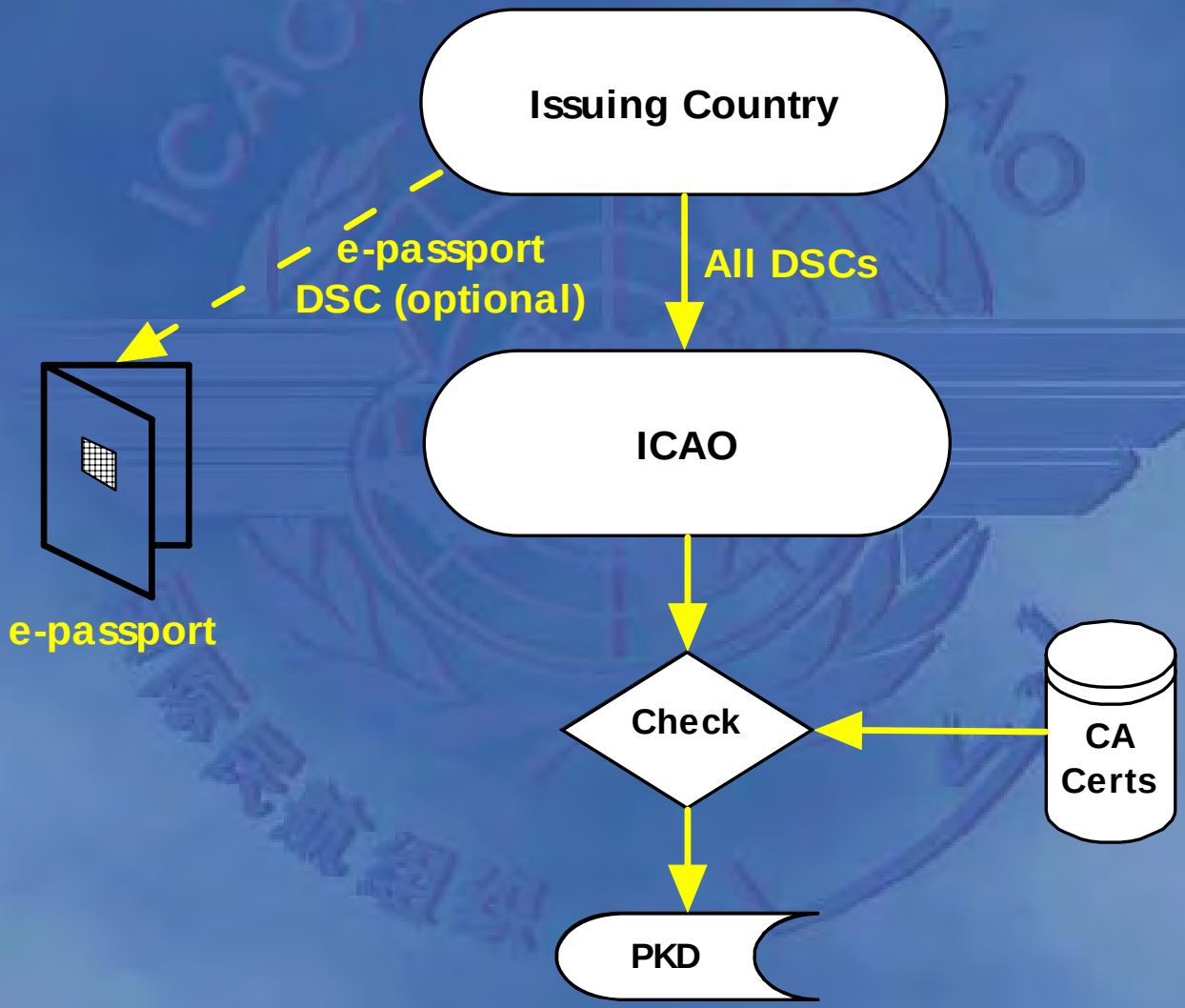
Requirements for Reading

- Availability of trusted DSCs, or the means to validate the DSCs (with country CA certificates).
- Availability of relevant certificate revocations (CRLs) if any.
- Validation of the e-passport DS

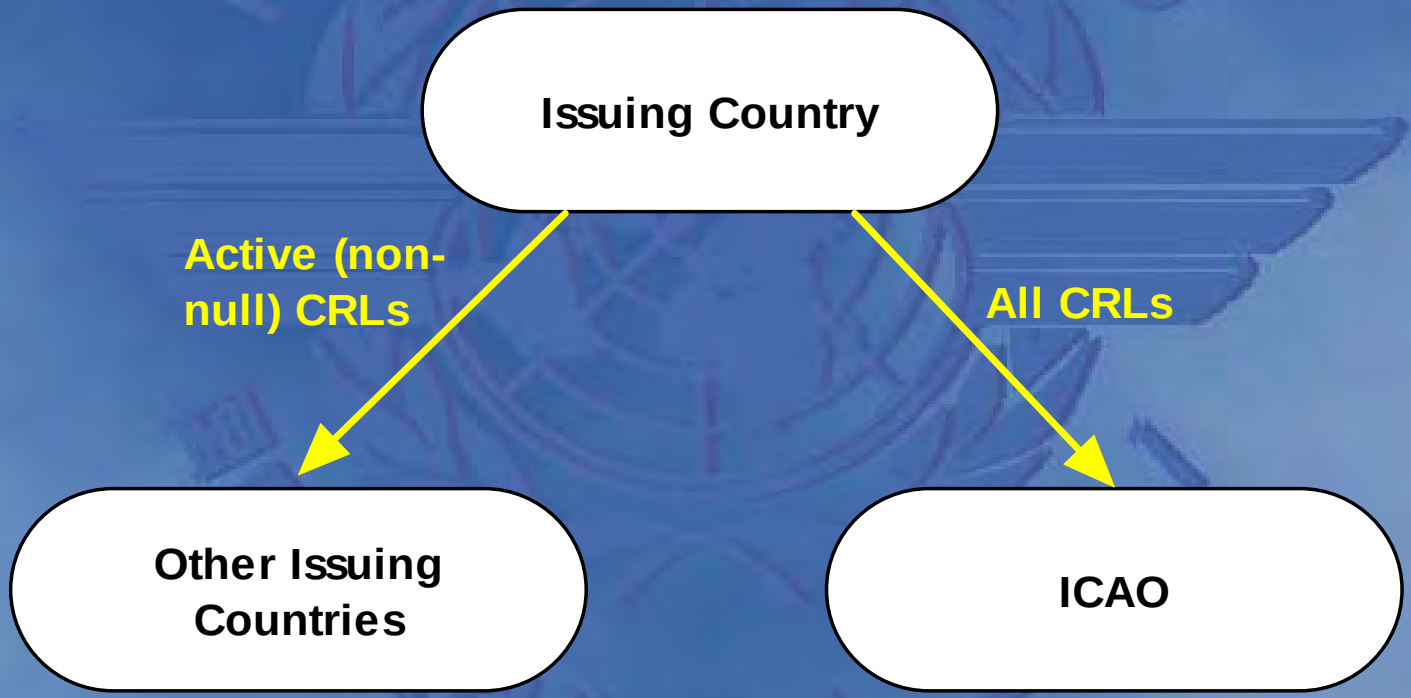
Country CA Certificate Distribution



DSC Distribution



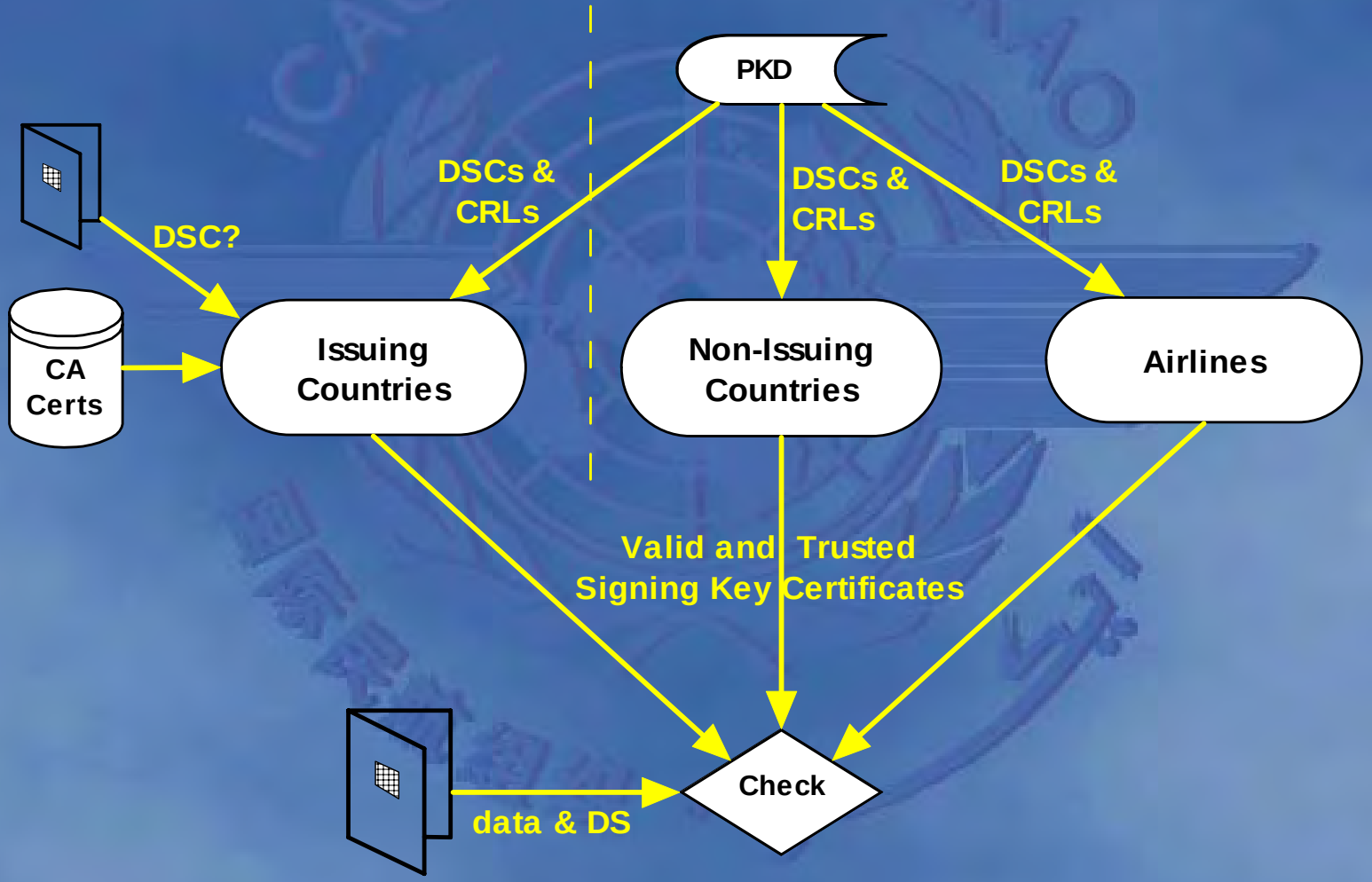
CRL Distribution



Resulting Distribution Scenario

- Issuing countries have all CA certificates from other countries.
- Issuing countries have all active CRLs – real revocations
- ICAO has the above, plus all DSCs
- The e-passport may also have its DSC

How Does This Work For All Entities?



Results

- Issuing countries CAN deal independently with a DSC appearing on an e-passport:
  - Validate the DS on the DSC with the proper CA certificate
  - Ensure no CRLs for that DSC from the active revocations list
- Issuing countries may also use the PKD and submit DSCs there to a double-check process (as above)
- All other entities MUST rely on the PKD to receive trusted DSCs and CRLs.
  - “Trusted” because ICAO has already verified each DSC against the country CA certificates and CRLs

Conclusions

- The role of the PKD in the ICAO e-passport PKI is integral and essential, particularly for non-issuing countries and airlines.
- Understanding its use and planning for its integration into e-passport processes is essential
- Workshop – Friday Sept 8 at 2:00pm