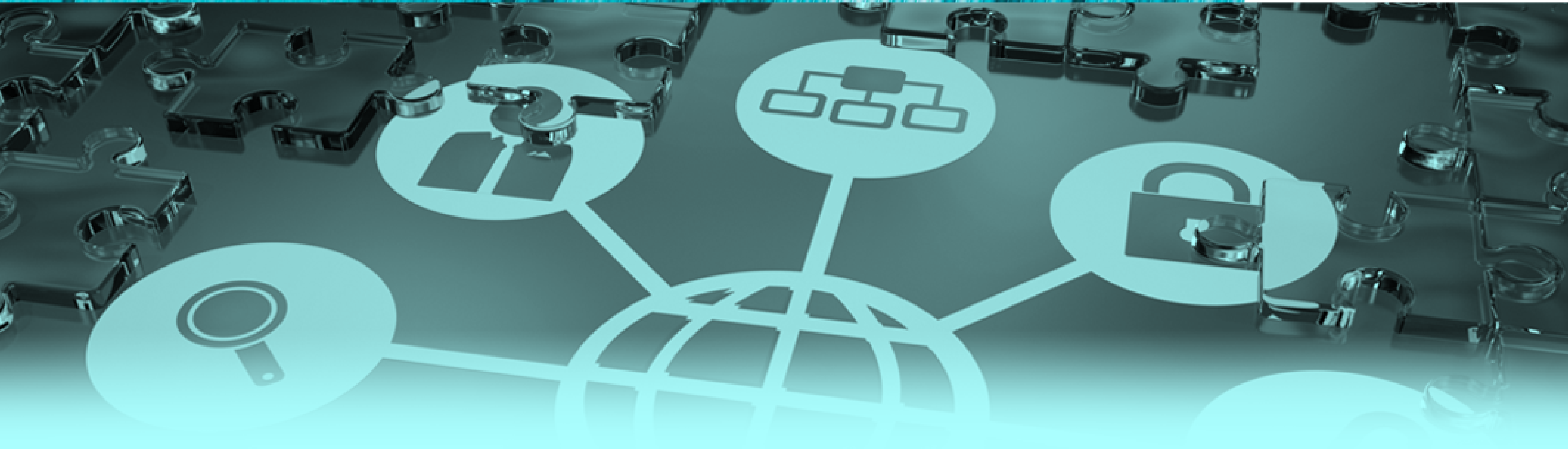


Future Expansion for eMRTD PKI

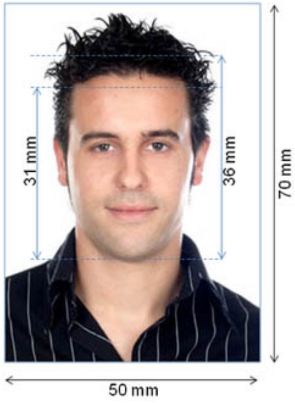
Mark Joynes, Entrust

What are we trying to achieve

- Prevent:
  - Production of credible false documents
  - Tampering with legitimate documents
  - Breach of sovereignty
- Provide:
  - Strong binding to true identity
  - Integrity
  - Authenticity
  - Privacy protection
- Facilitate Travel & Expedite Border Crossing

1st Generation eMRTD (ICAO BAC)

- Primary Biometric – face
- Electronic version of Data Page
- Open read of chip data (when document in hand)
- Integrity of chip and contents
  - Digital Signature
  - Integrity of Book/Chip - Active Authentication
- Assurance of Authenticity
  - Passive Authentication
- BAC/SAC – Secure Messaging
  - Mitigate threat of skimming and eavesdropping
- Controls implemented by Issuing Authority



2nd Generation eMRTD (EU-EAC)

- Secondary Biometrics
  - Impact of breach
  - Increased sensitivity
- Stronger authenticity
  - Chip Authentication
- Access Control – Terminal Authentication
  - Authenticated Access
  - Specific Authorization
- Controls:
  - Chip auth implemented by Issuing Country
  - Terminal Auth chained trust to Issuing Country

3rd Generation eMRTD (LDS2) - Coming

- Additional content on Chip being considered
  - Electronic version of other facets of paper book
- Travel Stamps
  - For rapid assessment of travel history
  - Legibility & structure
- eVisa
  - On-chip vs. Centralized database
    - Australia and others - independent of book
  - eVisa – not dependent on connectivity
- Additional biometrics
  - Add biometrics where none present in LDS 1
  - Add supplemental biometrics
  - Update where biometrics have changed

Implications for 3rd Generation LDS2 Document

- LDS1 – written at time of issuance and then locked
- LDS2 – written at time of issuance; separate application; not locked but controlled write thereafter
- Security Services – under control of issuing authority
  - Strong binding to vetted identity
  - Authenticity and Integrity
  - Strong Session security
  - Open/anonymous read for some data groups
  - Granular access control for read of other data groups
  - Granular access control for write of each application

Sovereignty of Document

- Property of the issuing country
  - Sovereignty – Root of trust for all chip access
  - Trust chained to Issuing Root
- Who is allowed to write to the chip
  - What states
  - What authorities
  - What object

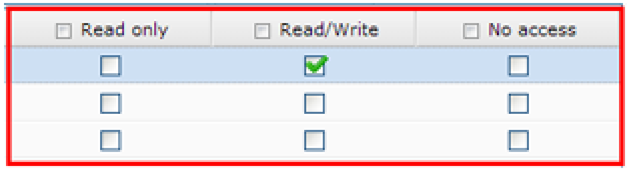
- Organization
  - Domestic & Foreign Signing functions
  - Distinct functions /containers – eVisa / Travel Stamp / Biometrics
  - Perhaps distinct organizations with authorization to write e.g. Embassies vs. Border control

Signing PKI Alternatives

- ✈ X509 (1st Gen PKI)
  - Object signing rooted to existing Country Signing CA
  - Object signing rooted to CSCA owning the signed object (control of write with document owner)
  - In addition to DS: eVS, TSS, ABS
- ✈ ISO7816 (2nd Gen PKI)
  - New Infrastructure for most (CVCA/DV)
  - Issuance of signing certs by DV in object owner State

Authorization PKI – Chip Access

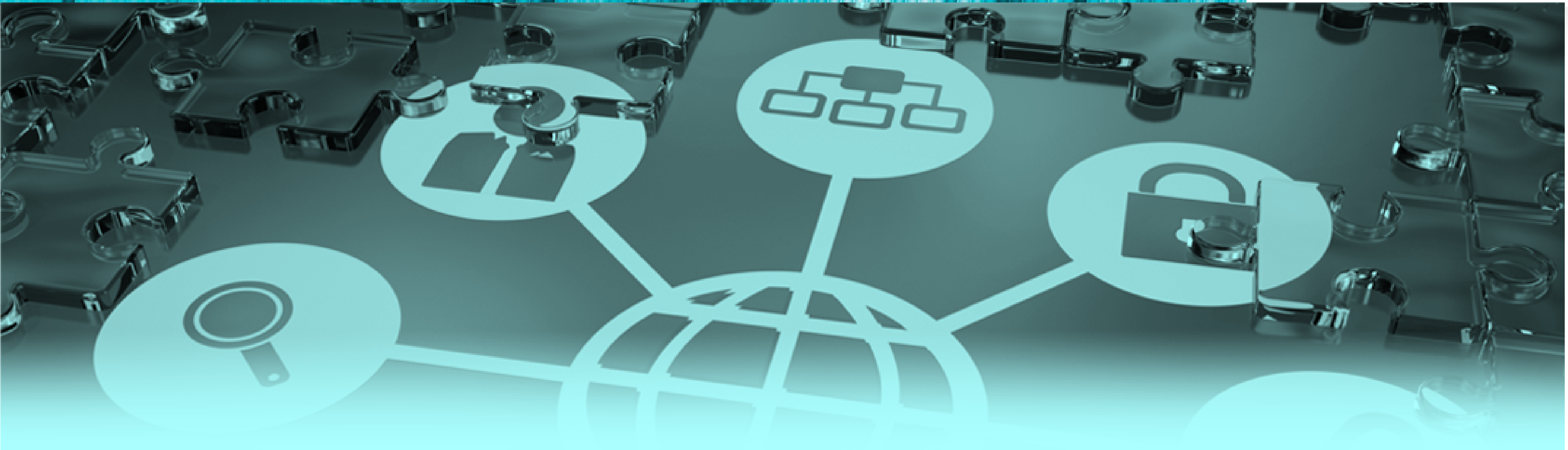
- ISO7816 - 2nd Gen PKI only one being currently considered
    - All authorization for write rooted to document issuing country
    - Selected write privileges provisioned to subordinate DVs for eVS, TSS and/or ABS
- Writing Stations (New, in a distributed sense)
    - eVisa, eTS, AB
- Terminal certificates with;
    - Authentication and read access to base and extended data sets (2nd Gen PKI)
    - DV issues certificates with “Write” privileges specific to object - (3rd Gen PKI)



☐ Read only	☐ Read/Write	☐ No access
☐	☑	☐
☐	☐	☐
☐	☐	☐

Next Gen PKI - Take Aways

- State Level
  - What would LDS2 do for you? Domestic? International?
- Issuing Authorities
  - Document/Chip refresh cycle and where LDS-2 activity may intersect;
  - Start thinking about distributed signing and implications
- Validating Authorities
  - Verifying 1st Gen documents – If not, why not?
  - Deployed 2nd Generation (EAC) books ?
    - Leveraging value? Domestically? Internationally?
  - Can the 3rd Gen LDS-2 changes streamline border control processing



Questions?