

INTELLIGENT PASSPORT PROJECT INITIATIVES

- Purchase several chip readers/writers.
 - Begin now to establish PKI knowledge and capability.
- Line up PKI consultant.
 - Get DS PKI personnel on board.
 - Need to develop plan for entire key scenario.
 - Transport Keys.
 - Load Keys to overwrite Transport Keys.
 - Creating certificates by hashing/digitally signing data.
 - Locking down written data.
 - Creating necessary key scenario to amend data.
(amendments/endorsements).
 - Need to establish plan for security of data transfers between the central CA and the remote issuance agency.
 - Need to establish plan for security keys/certificates passed/stored on the local issuance system servers.
 - Need to establish plan for storage and protection of keys at all sites.
 - Develop Certificate Authority Site Plan and equipment (Chrysallis) scenario.
 - Develop plan to secure storage of keys locally and in PIERS to be able to re-call a key and amend data on a chip.
 - Develop plan for destruction of private keys. (index to public keys)
 - Develop plan to link to ICAO for distribution of public keys.
 - Develop plan and infrastructure for link to ICAO.
 - Develop plan for revocation of keys and expiration of keys as well as use of new keys.
 - Involve DS in plan to develop key management/protection/distribution. (must advise them).
- Need to procure books for testing.
 - Must test all methods of integrating chip in book.
 - Kangaroo Passport. (Card in Pouch).
 - Chip in back cover.
 - Chip in middle pages.
 - Chip added after personalization.
- Develop proposal on how to link the chip to the book. (Whether separated or not).
- Issue of Skimming must be addressed.
- Determine if we want to adopt a scenario whereby the passport number must be read out from the MRZ in order to open the chip for reading.
- For John H. and Sharon: Re-think the issue of permitting citizen to see data that is stored on the chip.
- Coordinate funding of ICAO with Department Bureau of IO.
- Procure Chip Test Software Kit. (\$30K).
- Need to conclude the procurement scenario soonest.
 - DOS Office of Acquisitions must meet with GSA Smart Card Procurement officials soonest.

- Don't forget that part of this project must be to establish a support infrastructure to conduct operational support of the PKI/key management scenario following implementation.

Issues for the Document Development Team

- Must look at all options of book configuration.
- Why not the Kangaroo passport of a laminate inlay?
 - Cuts into spoilage.
 - Must link to the passport book by reading the MRZ to unlock the chip.
 - A chip unlocked by reading the MRZ cures the issue of skimming.
 - We cannot underestimate the issue that ICAO must protect the full images of the fingerprint and the iris. (Access to systems.)
 - Curing the skimming issue will allow us to go to the oversight committee with full confidence that we have protected the privacy of our citizens.