

Trip Report**ICAO NTWG PKI Subcommittee Meeting****London, England – September 4 & 5, 2003**

Prepared by: Simon Godwin and Richard McClevey

Meeting Purpose:

To discuss PKI topics as they relate to the Electronic Passport and where possible develop an international consensus with regard to implementation and use of PKI.

Attendees:

The following persons attended:

- Chairperson, John Davies – Director of Systems, UK Passport
- Ulrich Schneider – BKA, German Police
- Uwe Seidel – BKA, German Police
- Dennis Kugler – German cryptography expert
- Jacques Perron – Canada Passport Office
- Stefano Petecchia – Italy
- Dave Clark – ICAO Consultant
- Simon Johnson – UK PKI expert
- Bill Perry – UK Passport Systems (Contractor)
- Rich McClevey – US Department of State
- Simon Godwin – US Department of State (Contractor)
- Tom Kinneging – ISO, (Netherlands Contractor)
- Chuck Baggeroer – ISO, Datacard
- Charlie Stevens – UK Immigration
- Andrew Kay – Sharp
- Shunji Ueda, Sharp
- Yung Weng, Sharp
- Hiroshi Ban, Minoru Umehara, Ayako Komatse, (Japan NTT Contractors)

Overview:

The meeting took place over two days. All items on the original agenda supplied by John Davies were discussed. Where possible consensus was reached and documented. Some items we left as optional (e.g. the use of fingerprints or iris scans). At the end of the meeting one item was left open: whether there should be a mechanism to protect from skimming. John Davies will distribute official notes from the meetings.

Notes:

The meeting began with introductions and a quick overview of PKI technology. This quickly turned into a discussion of what data should be in the LDS and what data should be signed.

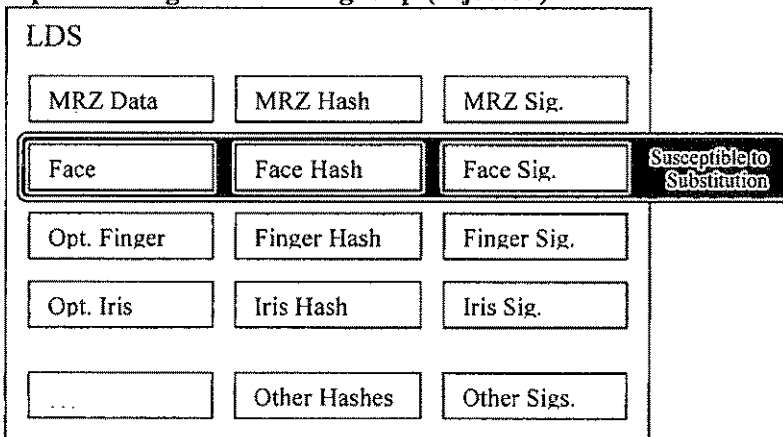
Data Set in the LDS:

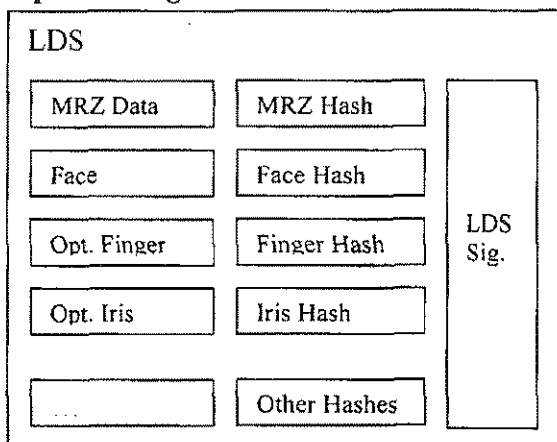
It was decided to continue with the current ICAO LDS spec largely unchanged. That is, the LDS should consist of several blocks of data:

- Mandatory
 - OCRB Information (MRZ)
 - Face
 - Digital Signature
- Optional
 - Fingerprint
 - Iris
 - Document security features
 - Image of data page
 - Document key (unique to the document)

The initial direction was to have a digital signature for each data group. There was a broad discussion on what to sign and how many certificates to use that was parked for day two. Day two saw the discussion on what to sign revisited with the decision being to generate one digital signature for the entire LDS.

Option 1: Sign each data group (rejected)



Option 2: Sign the LDS as a whole collection (accepted)**Who will access data?**

For version 1 of the LDS, it was agreed that:

- Only the issuing country can add data to a passport.
- Additionally, only the issuing country can sign the document.
- The physical data page data should not differ from the chip.

It was initially agreed that data should be able to be read by anyone who chooses to invest in the infrastructure to do so (this point proved to be controversial when skimming is considered and it came back up on day two). All data from the data page, including the digital facial image should remain free and clear and not encrypted. Fingerprint and Iris are considered sensitive and should be encrypted by those choosing to use them. If countries chose to encrypt other biometric features (fingerprint and iris) they would share encryption algorithms on a bilateral basis with those countries that they would permit to view that data.

It should be considered that both border control and airlines will need access to data on the chip.

Risk assessment

It was agreed that:

- Security policy needs to be developed by ICAO and by each country as it relates to the EP.
- The group recommends Common Criteria certification of the chip (EAL4+ mentioned).
- A risk assessment should be developed (list of threats) in time for Glasgow. Security police may fall out of this effort. UK prepared a draft of lists of threats that was modified by the U.S., The Netherlands, Germany and Canada. The latest revision is attached.

Concerns over chip copying were raised and the probability of such an event (low in the US position) discussed. Concern over using a protective pouch to smuggle weapons onto a plane was discussed.

Different threat types were mentioned:

- Document threats:
 - Counterfeit
 - Alteration
 - Imposters
- Data Misuse
 - Privacy
- Internal threats
 - Data compromise
 - Key compromise

Germany discussed an internal need to certify against skimming for privacy and legislative reasons. European nations seemed intent upon being able to show their privacy commissioners that they had taken reasonable steps to thwart skimming. Canada stated that it 'could not support doing nothing to address the issue of skimming'.

It is up to individual states to determine how they want to use and protect fingerprints and iris images.

Skimming

There was a broad discussion on skimming. The US position presented is that the risk is low enough that advanced anti-skimming techniques are not warranted at this time for the following reasons:

- Face and MRZ data are readily available on the data page of the passport and via other methods.
- The impact of skimming MRZ and facial data from a passport is minimal. What can one do with the information that is attained.
- It is somewhat difficult to skim data without one knowing it given fact that for coupling to occur antenna and transceiver must be so close and for a fixed period of time in order to attain capture.
- The use of pins or the requirement to scan the passport to unlock a chip are not good alternatives since they would drive the cost of readers higher and could negatively impact processing time.
- The use of MRZ scans or pins could also negatively impact the most efficient use of automated border gate scenarios.
- If skimming were an issue, metalized pouches or other mechanical methods could serve as an anti-skimming measure.

Other countries (most notably Germany) maintain that they need to address skimming before moving forward. UK, Canada and The Netherlands also presented concerns about skimming.

Several options with regard to skimming were discussed:

- Do nothing
- Encrypt the data (document private key)
- Use some form of PIN (e.g. passport #)
- Create some form of physical protection.

This discussion was not resolved but it was recommended that Terry Hartman's help be requested with regard to skimming.

What information should be shared between issuing states?

It was agreed that:

- Issuing states should bilaterally share country keys (public). The initial exchange should be through trusted diplomatic pouch as a certificate. Future exchanges could be electronic if the keys have not been compromised.
- Document signing keys (public) should be available prior to their use.
- Document signing keys should be shared as certificates.
- Document signing keys should be available through some directory service.

Directory and key sharing

There was broad discussion on the utility of a central directory. In the end it was agreed that such a directory could serve as a convenience to states but that it does not necessarily impart any greater degree of trust. It was also noted that the use of a central ICAO key distribution point added a formality and administrative structure that would be particularly beneficial to Member States with lesser technical ability. It was agreed that:

- A directory could be used to share signing keys
- A directory could be used to share revocation lists.
- There should be multiple mechanisms for revocation lists.
 - In the directory
 - Bilaterally
 - By appending to your countries travel documents (optional, initiated by Germany).
- Revocation lists:
 - There should be a notification mechanism for CRL's
 - CRL's should be polled randomly and frequently
 - A document with an invalid certificate would not have trustable digital information and it should be subject to more scrutiny
- A directory should not be the central source for country keys – these would be shared bilaterally.
- The basis of trust will be the country key
- X500/509 should be the standard directory and message formats (509 specifics to be determined).
- There should be multiple ways to transmit revocation

- Only governments would be able to add, modify or delete data in the directory.
- It is not clear if non-government organizations will be granted access to the directory, however, airlines should be able to confirm authenticity of public keys and revocation lists in their use of documents.

Algorithm and Key Length

There was general agreement on PKI technology

- Germany uses elliptic curve technology
- The US uses RSA but supports both in the FIPS 186-2 federal PKI standard.
- General agreement that countries should be able to process both at their borders
- Group recommendation was to support algorithms from the initial ICAO PKI report.
- Agreement to support SHA2, 512. This will cause an editorial change to p.19 of the original ICAO PKI report.
- Agreement that the ICAO spec needs to contain more detail on hash algorithm's
- Countries need to develop an opinion on how often to rotate keys.
- Passive authentication is proposed as a default standard, but active authentication is an option that can provide an additional level of confidence, and should be offered as an alternative as an anti-fraud measure.
- Active authentication could prevent copying of data to put in another chip.
- Decision to support both active and passive authentication will require readers to support both.