

RELEASED IN PART

B2, B7(E)

United States Department of State



Washington, D.C. 20520

UNCLASSIFIEDMEMORANDUM

TO: CA - Ms. Maura Harty

FROM: CA/PPT - Frank Moss

SUBJECT: Special Meeting of PKI Sub-Group of ICAO New Technologies Working Group

The International Civil Aviation Organization (ICAO) New Technologies Working Group (NTWG) is one of three working groups formed by the ICAO Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD). The NTWG is currently involved in preparing final technical specifications for biometrics and the use of integrated circuit IC chip technology in travel documents. The NTWG is scheduled to meet next in Glasgow on September 22 - 25 to refine specifications for the use of chips in passports.

To prepare for the technical deliberations at the Glasgow meeting, the NTWG has created three sub-groups that will meet prior to the Glasgow meeting to discuss Public Key Infrastructure (PKI), chip communication issues, and chip command sets, respectively. The sub-group that will specifically address issues related to the use of Public Key Infrastructure (PKI) technology to secure data that will be written to the chip in a passport will meet on September 4 and 5 in London. Representatives of NTWG countries, including Canada, Australia, UK, New Zealand, Germany, The Netherlands, Japan and others will attend the meeting.

The PKI sub-group meeting is necessary to allow sufficient time to discuss the complex issues regarding securing data on chips in preparation for the full meeting of the NTWG in Glasgow. The goal of the PKI subgroup will be to prepare issues for decision regarding the use of private and public keys that must be made in order to finalize the specifications for use of chips in passports. These include include:

UNCLASSIFIED

UNCLASSIFIED

2

- Requirements for writing data to chips.
 - U.S. position: Data will be written to the chip once only. No amendments will be allowed.
- The need for encrypting data.
 - U.S. position: Data written to chip and data exchanged between a reader and a passport will be free and clear without the need for encryption. DHS concurs with this position.
- Data Skimming (the ability to maliciously copy information from a person's passport).
 - U.S. position: There is little risk here since we plan to store only currently collected data and a facial image which are already stored visibly on the passport. In order to facilitate travel through automated border crossing gates, the U.S. will recommend against the use of pins or other methods that might be required to unlock a chip for reading. DHS concurs with this position.
- Key length requirements.
 - U.S. position: Countries should use largest key lengths available to prevent compromise of our private keys. We will suggest
- Process for distribution of public keys by ICAO.
 - U.S. position: U.S. supports ICAO key distribution scenario approved by ICAO TAG in May.
- Standardized best practices for protecting private keys.
 - U.S. position: As there are ICAO minimum security requirements that were approved for passports and passport issuance processes, there should also be ICAO best practices for protecting private keys and using public keys.

B2, B7(E)

It is planned that Richard McClevey of PPT and a contract representative from General Data Systems will attend the meeting of the PKI subgroup.

Drafted:CA/PPT/IML:Richard McClevey
08/28/03 ext. 32409

Clearance:CA/PPT:Frank Moss

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

3

CA/PPT:Ann Barrett

CA/PPT:Judy Penn

UNCLASSIFIED

UNCLASSIFIED