

ICAO/NTWG e-Passports Task ForceTask Force Scope and Issues

- Formats in which suppliers need to provide chips for compatibility with passport manufacturing lines
 - Chip + antennae + substrate must be provided to passport manufacturer as a complete unit
 - Substrate - Dimensions ?
 - Substrate - Material ?
 - Confidence in the robustness and durability of the chip/antennae/substrate combination
 - Delivery to the line eg cards, 2-up's, labels, rolls etc
 - Chip and Antennae placement considerations with respect to visa stamping, booklet perforation, image-perforation, other ?
- Current and planned state of the market in terms of chip size and availability
- Current and planned state of the market in terms of
 - Chip readers
 - Combi chip and mrz readers
- Where to place the chip in the booklet
 - Back cover
 - Centre
 - How is it physically secured/tamperproof ?
 - Is insertion of a smart-card in a sleeve in back of the passport acceptable ? Why not?
 - Is insertion post-personalisation acceptable ?
 - Is any migration path possible/permitted ?
- Chip issues
 - Read speed
 - Write speed
 - Common technical specifications including minimums eg temperature ranges etc
 - Storage available for data after overheads including operating system are deducted
 - Power to activate the chip to enable a read
 - Durability
 - Technical performance eg Lamination and pressure tolerances
 - Use of unique chip serial number, distribution with respect to inventory from manufacture to agency, transportation keys, opening chip up for QA then initial use etc
 - Radiation eg US postal service beams to kill anthrax spores, microwave etc
 - Are there any ISO14443 specifications that need qualification or augmentation ?

- Reader issues
 - Speed – time to transfer a 15 Kilobyte data block ?; effects of operating systems overheads – needs to run at speed in a Windows environment
 - Should read distance be within the 0-10cm range or be tighter ?
 - External influences on readers eg electronic noise, background noise. Airports are noisy environments
 - Communication between the passport, the chip and the reader
 - Power to activate the chip to enable a read
 - Anti-tear - What happens if card taken off chip before writing is finished
 - Impact of having 4-5 passports next to the reader ?
 - If first read is not successful what is time for the chip to reset ?
 - Are there any ISO14443 specifications that need qualification or augmentation ?

- Anti-skimming (consider initiatives that come out of the PKI Task Force meetings on September 3-4)
 - Is foil around your passport is a solution ?
 - Unlock the chip at the time of reading to avoid anti-skimming ?
 - Use of the MRZ to encrypt data - The MRZ could be used to protect the chip from skimming by making the data meaningless without the OCR (but what then about failure in reading the OCR?). Use of passport number ?

- Certification
 - Testing and endorsement regime for chips and chip readers/writers as ICAO-compliant ?

- Use of chips in Visas

- Border practicalities
 - Reading data page and chip simultaneously ?
 - How to know there is a chip in the passport – icon on data page ?

- Best practices statements – is there a need ?
 - for States for how to protect chips and safeguard processes eg is there a need to map out best practice processes from the chip inlay leaving the manufacturer, through booklet insertion with (pre and post qa), through personalization (with qa), through delivery to the applicant ?
 - at the Border eg chip failure on its own must not be a reason to refuse entry – the individual may however be referred to secondary.