ICAO PUBLIC KEY DIRECTORY
(ICAO PKD)

2007 ANNUAL REPORT TO PARTICIPANTS

Purpose

1. This annual report provides information on the operation of, and issues facing, the ICAO PKD.

Background

2. An essential element in the introduction of ePassports is the implementation of a global system for ePassport validation achieved via the exchange of Public Key Infrastructure (PKI) certificates. The system is privacy enhancing. It does not require or involve any exchange of the personal data of passport holders and the validation transactions help combat identity theft.

3. The business case for validating ePassports is compelling:
    - Border control authorities can confirm that the document held by the traveller:
    - was issued by a bonafide authority.
    - has not subsequently been altered.
    - is not a copy (cloned document).
    - if the document has been reported lost or has been cancelled, the validation check can confirm whether the document remains in the hands of the person to whom it was issued.
    - Passport Issuing Authorities can better engage border control authorities in all participating countries in identifying and removing from circulation bogus documents.

4. It is these validation features that enable automation of identity and warning list checking of ePassport holders (eg Australia's Smartgate and similar solutions in Singapore, Hong Kong and Portugal) to be undertaken with confidence. Without PKI or alternative database validation checks and effective checks for lost and stolen passports, automation would be higher risk.

5. ePassport validation is therefore an essential element to capitalise on the investment made by States in developing ePassports to contribute to improved border security and safer air travel globally. Because the benefits of ePassport validation are collective, cumulative and universal, the broadest possible implementation of a scheme or schemes of ePassport validation is desirable.

6. The exchange of PKI certificates (and the exchange of the certificate revocation lists that are the essential recovery layer in the system) must be reliable and timely. The emerging consensus is that this exchange cannot be achieved by other than electronic means.

7. The system of ePassport validation must operate on an open ended, indefinite basis.

8. The PKD's founding participants, and the new members that have joined during 2007, believe that a central broker minimises the volume of exchange of certificates and that ICAO, as the global agency responsible for travel document standards represents the best vehicle for achieving a sustainable global scheme.

Issues Identified by the PKD Board During 2007

Engagement with Border Control Authorities

9. The primary beneficiaries of a global scheme of ePassport validation are border control authorities.

10. However, while there is a broad acceptance of the importance of ePassport PKI validation in the passport issuing community, awareness of the issues is less amongst the border control community.

11. More than 40 States are now issuing ePassports. The number of ePassports in circulation globally is estimated at more than 60 million. More than 2 million Australian ePassports have been issued since October 2005 and already more than 30% of Australian passport holders crossing the Australian border are holders of ePassports.

12. Traffic across borders is approaching volumes where the large systems integration investments required to support ePassport validation are viable. Once the tipping point is reached, demand for a central brokerage to support the exchange of ePassport PKI certificates will increase.

13. In the meantime there is a communication challenge, and the PKD Board is putting greater effort in engaging with border control authorities. This is however a short term issue as it is considered that the growth in ePassports in circulation will inevitably bring the question of how best to achieve ePassport PKI validation to the fore.

14. During 2007 members of the PKD Board, and others engaged on their behalf were active in promoting the ICAO PKD in IOM's IGC, in the IATA-CAWG, in the OSCE, in the APEC Business Mobility Group and in a number of other fora where border control authorities meet.

Participation

15. The ICAO PKD currently has 8 members, of which only 3 are active in uploading their ePassport certificates and revocation lists (Singapore, New Zealand and Australia). Japan will commence certificate uploads shortly as will the United States who completed the membership formalities this month. Germany are expected to commence uploads soon. The United Kingdom are members but do not have any immediate plans to commence uploads of their certificates. Canada is also a member of the ICAO PKD but as they are not yet issuing ePassports and will not do so in 2008 they are not candidates to upload certificates in the near term.

16. The major challenge facing the ICAO PKD is to grow the membership so that States considering membership can be confident they are joining a viable, global solution. Promotion of the PKD is ongoing, but needs to also address the other, related issues facing the ICAO PKD.

Technical Design

17. After the technical design of the ICAO PKD was finalised, the United States made it a requirement for participation in the US-VISIT program that the Document Signing Certificate public key (C_{DS}) be included in ePassports. Subsequently, most ePassport issuing countries decided to include the C_{DS} on the chip in their ePassports.

18. Germany had been vocal in advocating changes to the design of the ICAO PKD to change the technical design to improve security and simplify validation. The PKD Board finalised a compromise agreement with Germany on a European proposal for a modified approach to ePassport validation in October 2007. The changes, once implemented, will both improve and simplify the ICAO PKD, and their adoption has been the single most important achievement of the ICAO PKD during 2007.

19. Germany has subsequently lodged their notices of participation in the ICAO PKD and will become an active member during December 2007. Germany's decision to join the ICAO PKD is expected to be influential in the consideration of other European States considering their approach to achieving ePassport PKI validation.

Cost of Participation - Registration Fees and Annual Fees

20. A number of countries have indicated that the level of the ICAO PKD Registration and Annual fees is an impediment to membership. The fees that were initially set were poorly designed in terms of incentives, favouring smaller countries and countries that delayed decisions to join and were set high to recover the costs of establishing the validation service.

21. Subject to ICAO Council agreement, Registration Fees will reduce from USD85,000 to USD25,000 or less. Annual fees are set by the PKD Board and in future will be set to recover the forward budgeted operating costs. A system of credits against future annual fees will be introduced to deal equitably with excess fee collections that will result from additional participants joining the PKD during the period after the level of annual fee has been set. Annual fees will therefore vary according to the number of participants. It is estimated annual fees could reduce to USD20~30,000 per annum with 20 participating States, but uncertainty over fee levels will continue while the number of participants remains small and until the terms of the operational contract are confirmed with Netrust, the external service partner.

Supporting ICAO in the Performance of Their Broker Role

22. ICAO is a United Nations agency. Service delivery and coordination of service delivery are not core organisational competencies. Doubt exists in the community of potential member States over the ability of ICAO to manage an efficient and effective ePassport PKI validation system. At the same time a number of States are concerned about liability issues associated with errors, omissions or oversight in the upload of certificates.

23. However, it is also the case that a central broker is essential, and the broker role must be able to be sustained, and to be trusted by the broadest range of States in order for the collective, cumulative benefits of the system to be realised. ICAO is the logical broker.

24. The ICAO PKD Board is responsible for operational and financial oversight and success will rely on the Board being seen to be effective in this role. The recent appointment in ICAO Montreal of a staff member dedicated to PKD issues is a positive and the Board is active in its oversight role. PKD participating States need to support the ICAO Secretariat in performing their role.

Concerns over the Third Party Service Provider

25. Netrust, a Singapore based company, was engaged by ICAO to build and run the validation service.

26. All indications are that Netrust are thoroughly professional and competent to perform their role, but some potential members have expressed concern regarding the involvement of a third party provider in a process that is integral to border control.

27. Close operational oversight by the PKD Board and the growing involvement of major States in the ICAO PKD should, over time, allay these unfounded concerns.

Recommendation

28. This annual report describes the range of issues facing the ICAO PKD and the progress being made to address them to ensure the viability of a global scheme for ePassport PKI validation. No further action is required.

ROSS GREENWOOD
2007 Chairperson
ICAO PKD
(on behalf of the ICAO PKD Board)

17 December 2007