POLICY BRIEF

OSCE Action against terrorism Unit (ATU)

Enhancing Travel Document Security - Promoting the ICAO PKD

September 2010

Action against Terrorism Unit (ATU) Policy Brief No. 1/2010

"PARTICIPATING STATES WILL PREVENT THE MOVEMENT OF TERRORIST INDIVIDUALS OR GROUPS THROUGH EFFECTIVE BORDER CONTROLS AND CONTROLS RELATING TO THE ISSUANCE OF IDENTITY PAPERS AND TRAVEL DOCUMENTS", OSCE CHARTER ON PREVENTING AND COMBATING TERRORISM (7 DECEMBER 2002)

Executive Summary

This brief presents the policy recommendations and findings from an *OSCE Workshop on Promoting the ICAO Public Key Directory,* held in Vienna in May 2010.

An electronic Passport (ePassport) is only as good as the biometric and biographic information contained in its chip. Information on the chip in turn is only useful if it can be validated quickly and securely. The large amount of ePassports being issued by a growing number of States has challenged the practice of bilaterally exchanging electronic certificates that prove and vouch for the validity of ePassport data.

In response, under the aegis of the International Civil Aviation Organization (ICAO) the Public Key Directory (PKD) has been installed which simplifies and modernizes the exchange of certificates and revocation lists. Using the certificates in the PKD provides border control authorities with an assurance that documents are genuine and unaltered. In turn, the biometric data can be trusted allowing for a more secure and faster identity verification process at border control matching the document and the bearer.

Context

Currently 54 OSCE participating States and Partner States issue technologically more advanced and biometrically-enabled ePassports. Electronic passports represent a vital tool for border control authorities to enhance border security and at the same time facilitate cross border movement.

Validation of ePassports through the exchange of Public Key Infrastructure (PKI) certificates, used during the production and personalization process of ePassports, is essential to realize the benefits of ePassports. Specifically the validation of the chip signature through the complete check of all relevant certificates enables border control authorities to determine whether a document held by a traveller has been issued by the responsible authority; whether biographic and biometric information on the chip has been altered after issuance; and whether a certificate necessary to validate the document has been revoked.

With more and more States issuing ePassports, the bilateral exchange of certificates has increasingly become error-prone, cumbersome and ineffective. Yet without full and timely access to these certificates ePassports should be treated as non-electronic passports at the border. This diminishes the considerable public investments in ePassport systems and erodes trust in ePassports among border officials and citizens.

In response, the ICAO PKD has been developed and put into operation. The PKD constitutes a scalable database of Country Signing Certificate Authority (CSCA) certificates, Document Signer Certificates (DSC) and Certificate Revocation Lists (CRL) as well as CSCA Master Lists (ML). The PKD offers border control authorities a system that allows them to access a central database of the latest certificates and revocation lists of passport issuing authorities that vouch for the authenticity and integrity of ePassport data.

POLICY BRIEF

OSCE Action against terrorism Unit (ATU)

Policy Options

Two policy options exist:

- Maintain the current practice which involves State officials travelling around the world to deliver CDs containing certificates to their counterparts; or sending such CDs via diplomatic mailing services. Both options are cumbersome and time consuming, carry considerable administration costs and represent a security risk.
- Participate in the ICAO PKD which enables national authorities to automatically upload certificates to a single and secure multilateral technical platform after a secure initial CSCA certificate exchange with ICAO. The result is a more cost efficient, secure and seamless way of exchanging certificates, promoting trust in ePassports among border officials and the public.

Benefits of the ICAO PKD

- **The ICAO PKD completes the authentication process of ePassports at border control.** The PKD offers timely information needed to validate the authenticity of ePassports. This enables border control to provide real time assurance that documents are genuine and unaltered.
- **The ICAO PKD facilitates fast and secure cross border movement.** The PKD simplifies and enhances the security of the ePassport validation process at border control providing citizens with the tangible benefit of being able to cross borders even quicker and easier. In turn, the validation of ePassports through the ICAO PKD offers border control authorities the highest possible chance of preventing terrorists and other criminals to cross borders undetected under false identities.
- **The ICAO PKD is a resource for enhancing trust in ePassports.** By sharing certificates and revocation lists via the PKD with foreign border control agencies, States promote trust in their travel documents. Specifically the timely information on compromised or false certificates - the certificate revocation lists - via the PKD enables border controls to detect potential fraud. Using the PKD also serves as a measure to address citizens' privacy and data protection concerns often associated with ePassports.
- **The ICAO PKD is cost effective and efficient**. The bilateral exchange of certificates and certificate revocation lists is complex, cumbersome and time consuming. Sharing such data via the PKD streamlines this process and consequently reduces administration costs. Costs are further reduced by more States participating in the PKD which lowers the Annual Fee for each PKD Participant. Considering the high expenses of introducing ePassports and creating the related electronic infrastructure to process such data, the expenditure of participating in the PKD is comparatively low. For details on current fees visit http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx

Policy Recommendations

1. The introduction of ePassports should go parallel with preparations to participate in the PKD. The PKD is central to enhancing the security and trustworthiness of any State's ePassport. The PKD has benefitted from years of development and operation, and is set to become the norm for validating ePassport data.

2. Comprehensive ePassport and PKD upgrades should be part of strengthening overall national identity management. Preventing criminals or terrorists from obtaining a genuine ePassport under a false identity is an important policy goal. Hence the development of robust issuing systems that are interlinked with civil registry information is vital. Moreover, any State investing in a national PKI should also consider its versatile applicability beyond travel document security. The PKI could serve as the foundation of an even more advanced and interlinked border, travel, and identity management environment serving broader national security and mobility objectives in areas such as aviation, trade and social services.

3. The introduction of the PKD should be properly prepared. States should ensure compliance with ICAO guidelines from the beginning. Specifically States need to address national administrative steps; international administrative steps; technical issues related to the implementation of the PKD at the national level; and technical issues related to the integration of the national PKD into the ICAO PKD.

POLICY BRIEF

OSCE Action against terrorism Unit (ATU)

Practical steps to implement the ICAO PKD

- **Review national legislation.** A thorough review of the national legislative framework is essential before introducing ePassports and participating in the ICAO PKD. Particular note should be taken of privacy and data protection regulations.
- **Define roles and responsibilities and implement a national PKD**. States have the responsibility to ensure the quality of the material they share via the ICAO PKD. This requires that roles and responsibilities of national stakeholders are clearly defined, and technical standards are adhered to and maintained. This applies especially to National PKDs which will upload and download certificates to and from the ICAO PKD, and the Country Signing Certificate Authority (CSCA).
- **Register for the ICAO PKD**. The first step a State must take to participate in the ICAO PKD is to sign the PKD Memorandum of Understanding (MoU) with ICAO. This is followed by a window of 15 months to connect the National PKD to the ICAO PKD and to start active up- and download. States seeking to participate in the ICAO PKD should consult with ICAO in addressing the registration process details.
- **Address Technical Specifications**. States need to ensure that the National PKD is technically compatible with the ICAO PKD. To ensure such compatibility, ICAO and the ICAO PKD Operator Netrust offer comprehensive technical support at all stages from connecting to the ICAO PKD as well as daily operations.
- **Integrate the National PKD with the ICAO PKD.** The final step involves the full integration of the National PKD with the ICAO PKD. This includes National PKDs uploading and downloading certificates and revocation lists to and from the ICAO PKD. All entries are automatically checked for compliance, origin and duplication.
- Concrete steps of participating in the ICAO PKD and the MoU can be downloaded at http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx

Potential OSCE Role

The OSCE has been **active in the area of travel document security since 2003**, including enhancing handling and issuance procedures, connecting to INTERPOL databases for real-time border control, and forged documents detection trainings.

In 2009 the OSCE was mandated to raise awareness and facilitate participation in and use of the ICAO PKD through the organization of an expert workshop in 2010. Possible follow-up OSCE role could include:

- **Organizing national and regional awareness raising workshops** to increase participation in and use of the ICAO PKD. This could include:
  - Facilitating the exchange of experiences and best practices between PKD Participants and States interested in participating in the PKD;
  - Demonstrating the technical, operational and administrative elements related to the PKD.
- **Facilitating national ICAO PKD training programmes** targeted at decision makers and senior officers as part of preparing States to participate in the ICAO PKD. This could include:
  - Drafting and providing model legislation to overcome initial legislative obstacles in the accession process;
- **Conducting expert technical assessment visits** to assist OSCE participating States with reviewing national identity management systems as part of enhancing the security and trustworthiness of ePassports.

Contact Information

For more information please contact the OSCE ATU Travel Document Security Programme Officers:

Ben.Hiller@osce.org or Christopher.Hornek@osce.org
Action against Terrorism Unit / OSCE Secretariat
Wallnerstrasse 6
A-1010 Vienna, Austria

Tel: +43 1 514 36 6702
atu@osce.org
osce.org/atu

The Organization for Security and Co-operation in Europe (OSCE) works for stability, prosperity and democracy in 56 States through political dialogue about shared values and through practical work that makes a lasting difference.