



РАБОЧИЙ ДОКУМЕНТ

ГРУППА ЭКСПЕРТОВ ПО УПРОЩЕНИЮ ФОРМАЛЬНОСТЕЙ (FALP)

ПЯТОЕ СОВЕЩАНИЕ

Монреаль, 31 марта – 4 апреля 2008 года

Пункт 3 повестки дня. Другие поправки к Приложению 9

УПРОЩЕНИЕ ФОРМАЛЬНОСТЕЙ В ОТНОШЕНИИ ПАССАЖИРОВ И ДОК ИКАО

(Представлено Правлением ДОК ИКАО*)

Оговорка

В связи с ограниченными ресурсами переведены только аннотация, действия Группы экспертов и поправки к нормативным документам.

АННОТАЦИЯ

Включение биометрической информации в электронные паспорта создает возможность для автоматизации некоторых аспектов процесса оформления пассажиров, включая подтверждение личности и первичную проверку в случае сигнала тревоги. Эти возможности уже используются в ряде стран (например, в Сингапуре, Португалии и Австралии). Однако выгоды упрощения формальностей в результате автоматизации процесса оформления пассажиров могут быть получены только при наличии высокой степени уверенности в целостности электронного паспорта, предъявляемого в качестве удостоверения личности, и определенного уровня понимания того, как это может быть достигнуто посредством процесса подтверждения подлинности с помощью ИОК. Этот процесс имеет важное значение, поскольку подтверждает, что документ является подлинным экземпляром, выданным истинным полномочным органом, и что впоследствии он не был изменен. Открывание микросхемы электронного паспорта и сравнение данных на микросхеме без этапа подтверждения подлинности не дает той степени уверенности, какую обеспечивает такое подтверждение. ДОК ИКАО являет логичным и желательным средством управления обменом цифровыми сертификатами, позволяющими производить эффективное подтверждение подлинности электронных паспортов с помощью ИОК на пунктах пограничного контроля. ДОК ИКАО вступила в эксплуатацию в марте 2007 года.

Действия Группы экспертов FAL

Группе экспертов FAL предлагается рассмотреть и одобрить поправки к Приложению 9, приведенные в п. 3.1.

* Австралия, Канада, Новая Зеландия, Сингапур, Соединенное Королевство, Соединенные Штаты Америки и Япония.

1. INTRODUCTION

1.1 The introduction of ePassports is intended to improve both aviation security, by combating identity fraud, and passenger safety/facilitation by offering an opportunity to improve the efficiency of aviation operations by enabling identification checks in passenger clearance processes at the primary control to be automated. Moreover, the security and process efficiency benefits of ePassports are equally applicable for international travel by sea and land.

1.2 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.

2. DISCUSSION

2.1 The business case for validating ePassports is compelling. Border control authorities can confirm that the document held by the traveller:

- was issued by a *bona fide* 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.

2.2 As a result, Passport issuing authorities can better engage border control authorities in all participating countries in identifying and removing from circulation bogus documents. It is important to stress that only by validating ePassports will the assurances set out at 2.1 above be met. Opening the ePassport chip without validating it does not provide that same level of assurance.

2.3 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 of ePassport validation is desirable.

2.4 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. Since the system of ePassport validation must also operate on an open ended, indefinite basis it is apparent that a central broker is required. ICAO is the logical candidate to perform this role because it is accepted globally as the agency responsible for setting and managing travel document standards.

2.5 The number of ePassports in circulation is approaching a tipping point where border control authorities will reap returns from the investments required in systems hardware and integration to support ePassport PKI validation. Validation of ePassports enables automation of identity and warning list checking of ePassport holders to be undertaken with confidence. Without PKI or alternative database validation checks and effective checks for lost and stolen passports, any such automation would be higher risk.

2.6 It is for all these reasons that the 2007 ICAO Assembly resolved to urge all ICAO ePassport issuing States to join the ICAO PKD.

3. ДЕЙСТВИЯ ГРУППЫ ЭКСПЕРТОВ FAL

3.1 Группе экспертов FAL предлагается рассмотреть и одобрить следующие предлагаемые поправки к Приложению 9:

- а) включить в главу 1 Приложения 9 определения терминов "электронный паспорт" и "Директория открытых ключей ИКАО (ДОК)" следующего содержания:

"Электронный паспорт (или МСП с электронным носителем): машиносчитываемый паспорт (МСП), соответствующий спецификациям тома I части 1 документа Doc 9303, который дополнительно включает в себя бесконтактную интегральную схему, позволяющую осуществлять биометрическую идентификацию владельца МСП в соответствии со спецификациями тома II части 1 документа Doc 9303.

Директория открытых ключей ИКАО (ДОК ИКАО): центральная база данных, служащая хранилищем сертификатов подписей документов (C_{DS}) (содержащих открытые ключи подписи документов), основного списка CSCA (ML_{CSCA}), сертификатов соединения национальных центров удостоверения подписей (IC_{CSCA}) и листов аннулирования сертификатов, выпускаемых участниками, вместе с системой их распределения во всем мире, поддерживаемой ИКАО от имени участников в целях обеспечения подтверждения достоверности данных, содержащихся в электронных паспортах".

- б) В главу 3 Приложения 9 включить текст новой Рекомендуемой практики следующего содержания:

"3.9.1 Рекомендуемая практика. *Договаривающимся государствам, а) выдающим или намеревающимся выдавать электронные паспорта, и/или б) осуществляющим автоматизированные проверки электронных паспортов на пунктах пограничного контроля, следует присоединяться к Директории открытых ключей ИКАО (ДОК)".*