



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 12 повестки дня. Программы упрощения формальностей

ВОЗМОЖНОСТИ ДЛЯ БОЛЕЕ УСПЕШНОГО ВНЕДРЕНИЯ ДИРЕКТОРИИ ОТКРЫТЫХ КЛЮЧЕЙ (ДОК) И ЭЛЕКТРОННЫХ ПАСПОРТОВ НА ПОГРАНИЧНОМ КОНТРОЛЕ

(Представлено Аргентиной при поддержке Белиза, Боливии (Многонационального Государства), Гватемалы, Гондураса, Доминиканской Республики, Колумбии, Кубы, Мексики, Никарагуа, Панамы, Перу, Сальвадора, Уругвая, Чили, Эквадора и Ямайки)

КРАТКАЯ СПРАВКА

Внедрение ДОК Международной организации гражданской авиации (ИКАО) и использование электронных паспортов повысили безопасность и эффективность пограничного контроля. Вместе с тем были выявлены возможности для совершенствования, которые при более широкой поддержке со стороны ИКАО могли бы облегчить переход на эти системы и их интеграцию в странах, которые в настоящее время занимаются их разработкой или внедрением.

Вызовы во внедрении ДОК:

а) Трудности с доступом к ДОК и его использованием. Из-за отсутствия инфраструктуры или экспертных знаний некоторые страны сталкиваются с техническими и административными вызовами при включении ДОК в свои национальные системы.

б) Ограниченная интероперабельность. Отсутствие более гибких стандартов для интеграции с другими национальными инфраструктурами создает технические барьеры для валидации паспортов.

в) Обновление и обслуживание. В некоторых странах сертификаты и списки отзыва сертификатов загружаются нерегулярно, что может поставить под угрозу безопасность и надежность системы.

Действия: Ассамблее предлагается обратиться к ИКАО с просьбой усилить свою роль следующими мерами:

а) Специализированная техническая помощь. Разработка специальных программ подготовки персонала и технической помощи для стран, находящихся на стадии внедрения, с акцентом на передовом опыте и оптимальном использовании ДОК.

б) Централизованная платформа валидации. Изучение возможности разработки защищенной предварительной информации о пассажирах (API), которую страны могли бы использовать для ознакомления с сертификатами и списками отзыва сертификатов в режиме реального времени в качестве дополнительной альтернативы регулярным загрузкам.

в) Региональное сотрудничество. Поощрение региональной интеграции на основе соглашений по вопросам инфраструктуры и обмена ноу-хау для снижения затрат и повышения эффективности внедрения ДОК.

¹ Испанская версия предоставлена Аргентиной.

<i>Стратегические цели</i>	Данный рабочий документ связан со стратегическими целями <i>"Каждый полет безопасен и защищен"</i> и <i>"Авиация обеспечивает беспрепятственную, доступную и надежную мобильность для всех"</i>
<i>Финансовые последствия</i>	Меры, упомянутые в настоящем документе, будут зависеть от наличия средств из регулярного бюджета на 2025–2026 гг. или внебюджетных взносов.
<i>Справочный материал</i>	

1. ВВЕДЕНИЕ

1.1 Когда страна регистрирует свой национальный сертифицирующий полномочный орган с правом подписи (CSCA) в Директории открытых ключей (ДОК) Международной организации гражданской авиации (ИКАО), пограничные контрольно-пропускные пункты в этой стране и в других странах должны предпринять ряд мер и применять соответствующие технологии, чтобы воспользоваться теми преимуществами в области безопасности, которые обеспечиваются подписанными сертификатами для электронных машиночитываемых проездных документов (электронных МСПД). Им необходимы:

1.1.1 Загрузка сертификатов CSCA и сертификатов подписи документов (DSC) и управление ими

1.1.1.1 Страны, осуществляющие проверку проездных документов, должны регулярно загружать сертификаты CSCA и сертификаты подписи документов (DSC) из ДОК ИКАО.

1.1.1.2 CSCA является сертифицированным источником DSC, а DSC — это сертификаты, используемые для подписи данных на чипах электронных паспортов.

1.1.1.3 Примечание в отношении DSC. Это цифровой сертификат, выдаваемый CSCA лицу, подписавшему документ. DSC содержит открытый ключ лица, подписывающего документ. При проверке электронного паспорта система использует открытый ключ DSC, чтобы проверить цифровую подпись на паспортных данных и гарантировать, что данные не подвергались манипуляциям и исходят от законного полномочного органа, официально выдающего проездные документы.

1.1.2 Обновление баз данных пограничных контрольно-пропускных пунктов

1.1.2.1 Загруженные сертификаты должны быть направлены во все системы досмотра документов в аэропортах, портах и других пунктах въезда.

1.1.3 Использование пассивной аутентификации (РА)

1.1.3.1 Пассивная аутентификация проверяет целостность данных на чипе проездного документа. На контрольно-пропускных пунктах сканеры паспортов проверяют, не подвергались ли данные, хранящиеся на чипе, манипуляциям, сравнивая цифровую подпись с соответствующим DSC.

1.1.4 Внедрение активной аутентификации (АА) (факультативно)

1.1.4.1 Некоторые электронные паспорта используют активную аутентификацию для предотвращения клонирования чипа. Этот процесс включает в себя криптографический тест между сканером и чипом, чтобы подтвердить, что чип является подлинным, а не копией.

1.1.5 Использование расширенного контроля доступа (ЕАС) (для защищенных биометрических данных)

1.1.5.1 Для доступа к конфиденциальным биометрическим данным, например, к отпечаткам пальцев, системы пограничного контроля должны использовать ЕАС. ЕАС требует, чтобы сканеры имели авторизованные сертификаты и обменивались ключами для верификации разрешений на доступ к биометрическим данным.

1.1.6 **Инфраструктура открытых ключей (PKI)**

1.1.6.1 Для валидации сертификатов необходима инфраструктура открытых ключей (PKI), которая может проверить цепочку доверия от CSCA до DSC и подпись чипа. Она может включать:

- a) Списки отзыва сертификатов (CRL) для обнаружения отозванных сертификатов;
- b) Протокол статуса онлайн-сертификата (OCSP) для проверки в режиме реального времени.

1.1.7 **Проверка списков похищенных и утерянных проездных документов (SLTD)** Международной организации уголовной полиции (Интерпол)

1.1.7.1 Пограничные системы также должны сверяться с международными базами данных, например, с SLTD Интерпола, чтобы выявлять проездные документы, заявленные как утерянные или украденные.

2. **РЕЗЮМЕ**

2.1 Для того чтобы органы пограничного контроля могли воспользоваться преимуществами в сфере безопасности, предусмотренными сертификатами для проездных документов после присоединения страны к ДОК ИКАО, они должны:

- a) регулярно загружать и обновлять сертификаты CSCA и DSC из ДОК;
- b) распространять эти сертификаты среди систем пограничного контроля;
- c) внедрять РА для проверки целостности данных чипа;
- d) при необходимости использовать АА или ЕАС;
- e) поддерживать в рабочем состоянии PKI, чтобы валидировать цепочки доверия сертификатов;
- f) внедрять инструменты обнаружения утерянных/украденных документов.

2.2 Эти меры гарантируют подлинность электронных паспортов и предотвращают подделку документов на иммиграционном контроле.

2.3 Без надлежащего использования инфраструктуры ДОК ИКАО для проверки подлинности электронных паспортов открывается ряд возможностей для мошенников. Ниже приводятся некоторые из наиболее распространенных видов мошенничества:

2.3.1 **Кража личных данных с использованием поддельных паспортов**

2.3.1.1 Полностью поддельные паспорта. Лица могут создавать электронные паспорта, которые выглядят подлинными, но содержат ложную биографическую и биометрическую информацию. Без проверки на соответствие ДОК, которая позволяет подтвердить, что сертификат DSC является законным и был выдан признанным полномочным органом, эти поддельные документы будет сложнее обнаружить.

2.3.1.2 Измененные паспорта. В подлинные электронные паспорта могут вноситься изменения, например, в фотографию или биографическую информацию в зоне визуального считывания или даже на чипе. Без проверки цифровой подписи в ДОК эти изменения могут остаться незамеченными.

2.3.1.3 Мошенническое использование подлинных паспортов. Украденные или утерянные паспорта могут быть использованы лицами, не являющимися их законными владельцами. Если бы системы контроля не проверяли действительность паспортного сертификата через ДОК (и, возможно, сверялись со списком украденных или утерянных документов), мошенничество было бы проще.

2.3.2 Манипулирование данными чипа

2.3.2.1 Несмотря на то, что в электронные паспорта встроены меры безопасности, если проверка в ДОК отсутствует, тогда хакер, обладающий необходимыми инструментами, может манипулировать данными, хранящимися на чипе, в том числе биографической и биометрической информацией. Верификация в ДОК обеспечивает целостность этих данных, поскольку подтверждается действительность цифровой подписи.

2.3.3 Повторное использование личности

2.3.3.1 Человек может попытаться использовать несколько поддельных электронных паспортов с разными личностями для многократного пересечения границ или совершения других преступлений. Отсутствие проверки в ДОК затрудняет выявление этих несоответствий на международном уровне.

2.3.4 Атаки на цепочку доверия

2.3.4.1 Без ДОК, представляющей собой центральный пункт доверия, проверка подлинности паспорта становится более зависимой от двусторонних соглашений или надежности информации, предоставляемой отдельными странами. Это делает систему более уязвимой для проникновения поддельных сертификатов, если строгие стандарты безопасности не поддерживаются во всем мире. ДОК создает надежную инфраструктуру для снижения этого риска.

2.3.5 Подводя итог, можно сказать, что инфраструктура ДОК имеет решающее значение в выстраивании глобальной цепочки доверия к аутентификации электронных паспортов. Без этого системы пограничного контроля гораздо более уязвимы для различных изощренных методов мошенничества, эксплуатирующих трудности, которые возникают при проверке подлинности документов и личности международных пассажиров. Внедрение ДОК позволяет органам пограничного контроля подтверждать, что электронный паспорт был выдан законным полномочным органом и его данные не подвергались манипуляциям.

3. ВЫВОДЫ

3.1 Неэффективное внедрение ДОК ИКАО подвергает пограничный контроль высокому риску мошеннических схем с документами, например, краже личных данных и манипуляции с данными электронных паспортов. Неспособность обновлять и проверять сертификаты ставит под угрозу цепочку доверия, подрывая глобальную безопасность. Для снижения этих рисков крайне важно усилить техническую помощь, улучшить интероперабельность и разработать централизованные инструменты для обеспечения эффективной валидации в режиме реального времени.