



ОБЗОР



Использование в полном объеме преимуществ новых технологий

Каждый электронный паспорт имеет встроенный электронный чип, на котором хранятся фотография владельца и его персональные данные, размещенные на странице с паспортными данными. В электронных паспортах используется технология инфраструктуры открытых ключей (PKI), которая не позволяет изменять информацию, хранящуюся на чипе.

Кроме информации о владельце на чипе электронного паспорта хранится конкретный для страны цифровой элемент защиты, известный как электронная цифровая подпись, которая взята из защищенных сертификатов государства, например, сертификатов органа, подписывающего документ (DSC), и национального центра удостоверения подписей (CSCA). Индивидуальные для каждого паспорта и страны цифровые подписи могут быть проверены путем использования сертификатов открытых ключей выдающей документы страны. Когда электронный паспорт сканируется и считываются данные с чипа, то аутентифицированная электронная цифровая подпись служит для пограничных органов подтверждением того, что данные на чипе подлинные, и что он был выдан и подписан конкретной страной и не был подделан.

Совместная работа

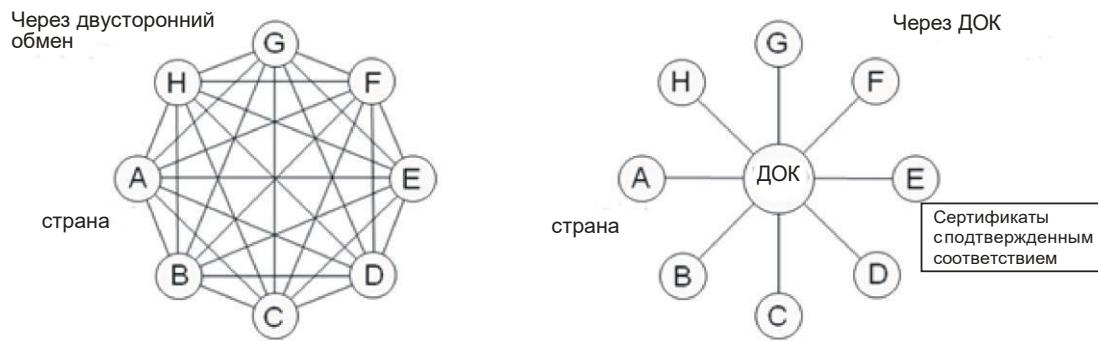
Чтобы работать эффективно, пограничные органы и другие соответствующие полномочные органы должны иметь доступ к сертификатам безопасности всех стран, которые выдают электронные паспорта. С этой целью Международная организация гражданской авиации (ИКАО) создала систему, которая облегчает обмен открытой ключевой информацией между странами, а именно: Директорию открытых ключей ИКАО (ДОК). В ДОК хранятся данные, которые позволяют ее участникам в установленном порядке вносить в директорию свои сертификаты CSCA, DSC, списки отзывов сертификатов (CRL) и основные списки, а также иметь доступ к прошедшим проверку сертификатам безопасности всех участников ДОК, которые завершили загрузку своих документов в директорию.



ОБЗОР



ДОК является хорошо организованной, простой, безопасной и рентабельной системой обмена информацией, прошедшей к данному моменту апробацию. Без такой системы ДОК каждой стране пришлось бы обеспечивать на индивидуальной основе безопасный обмен своими DSC и CRL. Благодаря системе ДОК обмен сертификатами, который потребовал бы сотен транзакций и часов работы, может быть выполнен, как простые два обмена – загрузка и разгрузка информации, прошедшей проверку. Более того, имеющиеся основные списки, содержащие прошедшие проверку CSCA других стран, являющихся также участниками этой системы, позволяют вам иметь доступ к CSCA, даже если не было первоначального обмена CSCA со всеми странами.



Еще одно дополнительное ценное преимущество, которое дает система ДОК своим участникам, заключается в том, что она предоставляет такую услугу, как подтверждение соответствия сертификата. Обеспечивая подтверждение соответствия и происхождения сертификата в мировом масштабе, она облегчает верификацию подтверждения документа и его беспрепятственную доставку.

Система ДОК ИКАО не содержит каких-либо персональных данных о каком-либо владельце паспорта и не обеспечивает доступ ко вторичным биометрическим данным паспортного чипа, таким как отпечатки пальцев.



ОБЗОР



Двери открыты для путешественников

Каждая страна, а не только участники ДОК, могут иметь бесплатный доступ к ДОК¹. Эта дирекция для обмена информацией позволяет пограничным органам всех стран, которые связали свою инфраструктуру пограничного контроля с ДОК, проводить быструю проверку электронных паспортов, что в значительной мере облегчает въезд путешественникам, имеющим на это законное право. Такая система также помогает всем странам объединить свои усилия в борьбе с подделкой паспортов и таким образом внести свой вклад в обеспечение внутренней и международной безопасности.

Для получения дополнительной информации просьба обращаться
к веб-сайту ДОК:

<http://www.icao.int/Security/FAL/PKD/Pages/default.aspx>

или связаться с:

ICAO-PKD@ICAO.INT

¹ Свободный доступ предназначен для отдельных случаев скачивания информации, и это не предназначено для использования в целях пограничного контроля, которое требует регулярных действий оператора ДОК и не обеспечивает технической поддержки.