Часто задаваемые вопросы

(23 августа 2013 года)

i. Что представляет собой Директория открытых ключей (ДОК)?

ДОК ИКАО – это централизованная база данных, предназначенная для обмена сертификатами и листами аннулирования сертификатов по всему миру. Такие сертификаты и листы аннулирования сертификатов применяются для удостоверения подлинности электронной подписи в данных, размещенных на чипе RFID электронных паспортов и других электронных МСПД. Содержащаяся в ДОК информация проходит предварительную проверку и может быть скачана бесплатно.

ii. В чем заключается практическая ценность ДОК?

Несмотря на то, что все больше государств вводят в обращение электронные паспорта, ДОК гарантирует, что процесс обмена данными между государствами останется простым и быстрым. ДОК играет важную роль в минимизации объемов обмена сертификатами и листами аннулирования сертификатов, в своевременном обновлении вносимых и скачиваемых данных и в соответствии системы техническим стандартам для обеспечения и поддержания эксплуатационной совместимости.

iii. Почему так важна поддержка ДОК со стороны ИКАО?

В качестве основного справочного материала по электронным паспортам и другим электронным МСПД, базирующимся на стандартах ИСО, ИКАО выпускает документ 9303. Экспертные возможности и репутация ИКАО делают ее поддержку ДОК естественным и само собой разумеющимся процессом, не имеющим какого-либо сравнимого альтернативного решения.

iv. Кто входит в число участников ДОК?

Участники ДОК перечислены на веб-сайте ДОК.

<http://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx>

(see "ICAO PKD – Current Operational Status") (см. "ДОК ИКАО – текущее оперативное состояние")

v. Где можно найти уведомление об участии?

Уведомление об участии можно скачать на веб-сайте ДОК.

<http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofParticipation-Model.pdf>

(see "Procedures for the ICAO Public Key Directory") (см."Процедуры ДОК ИКАО")

13-3925



vi. Где можно найти уведомление о регистрации?

Уведомление о регистрации можно скачать на веб-сайте ДОК.

<http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofRegistration-Model.pdf>

(see "Procedures for the ICAO Public Key Directory") (см. "Процедуры ДОК ИКАО ")

vii. Каковы размеры взносов за участие?

Шкалу взносов ДОК можно скачать на веб-сайте ДОК.

<http://www.icao.int/Security/FAL/PKD/Documents/PKDFinanceDocuments/B-Fin-123-PKD%20Fee%20Schedule%202016.pdf>

(see "PKD Fee Schedule") (см. Шкала взносов ДОК")

viii. Сколько должен платить пользователь системы?

Все содержание ДОК может быть скачано бесплатно с использо- ванием простого и быстрого доступа на веб-сайт (<https://pkddownloadsg.icao.int/>). Тем не менее для реализации функций пограничного контроля или подобных операций государствам или негосударственным организациям, не являющимся участниками ДОК, может потребоваться универсальный доступ к ДОК. Поскольку процесс установки и поддержки такого рода доступа требует постоянного участия оператора ДОК, Меморандум о взаимопонимании предусматривает покрытие соответствующих расходов за счет взносов пользователей. Детальное разъяснение содержится в Шкале взносов ДОК.

ix. Что означает "активное участие"?

После регистрации уведомления об участии и оплаты регистрационного взноса, т. е. когда начинается действительное участие, участник ДОК готовится к подключению своей национальной ДОК к центральной ДОК. Процесс подключения происходит при поддержке со стороны оператора ДОК. По окончании этого подготовительного этапа участник ДОК начинает загружать в базу данных ДОК и скачивать из нее необходимую информацию, что и делает его "активным участником".

x. Что предлагает ДОК для скачивания?

ДОК предлагает для скачивания сертификаты подписи документа (DSC) и листы аннулирования сертификатов (CRL), а также основные списки CSCA (ML).

xi. Каким образом осуществляется проверка электронных паспортов при помощи

ДОК?

Для проверки электронного паспорта необходимо следовать всей цепочке доверия. Эта цепочка доверия включает в себя проверку подлинности электронной подписи в данных чипа RFID при помощи сертификата подписи документа (DSC). Далее следует проверка достоверности DSC с использованием сертификата национального центра удостоверения подписей (CSCA) страны выдачи паспорта. Все использованные в процессе сертификаты должны быть

электронных паспортах?

Нет. Поскольку проверка подписей в электронных паспортах и доступ к заложенным в электронных паспортах отпечаткам пальцев осуществляется при помощи технологии инфраструктуры открытых ключей (PKI), получить доступ к отпечаткам пальцев с использованием данных ДОК невозможно.

xiii. Что подразумевается под 15-месячным сроком активации?

После того, как участие становится действительным, у участника ДОК есть

15 месяцев на то, чтобы начать активную работу. При активном участии годовой взнос увеличивается, чтобы покрыть расходы на поддержку активного участия (см. Шкалу взносов ДОК).

xiv. В чем заключаются преимущества размещения ДОК в сети интернет?

Обмен сертификатами и листами аннулирования сертификатов должен осуществляться надежно и своевременно. Обеспечить такой обмен другими средствами, помимо электронных, не представляется возможным. Для защиты ДОК от атак через Интернет предпринимаются все обычные и соответствующие меры.

xv. Существует ли риск загрузки вирусов или других вредоносных программ при использовании ДОК?

Нет. Данные в ДОК размещены в виде текстовых файлов, не содержащих каких-

либо скриптов или исполняемых кодов.

xvi. Где можно найти дополнительную информацию?

Веб-сайт ДОК находится по адресу <http://www.icao.int/Security/FAL/PKD/Pages/default.aspx> и содержит как информацию для предварительного ознакомления, так и большое количество скачиваемых документов для детального изучения. Можно установить контакт с Секретариатом ИКАО по адресу [ICAO-PKD@ICAO.INT](mailto:ICAO-PKD@ICAO.INT) или с председателем Правления ДОК. Кроме того, имеется адрес для размещения жалоб и осуществления обратной связи.

xvii. ДОК используется для подтверждения цифровых подписей в чипах электронных паспортов. Каким образом это может помочь в распознавании лже- двойников?

Современные биометрические системы способны за несколько секунд сравнить изображение лица, хранящееся в электронном паспорте, с реальным изображением предъявителя паспорта. Надежно определяются даже небольшие различия, типичные для мошеннической подделки внешнего вида, , и человека направляют для прохождения дальнейшей проверки.

данных электронного чипа, включая биометрию. Проверка чипа чрезвычайно важна, если основным критерием подлинности является хранящееся в нем изображение лица, в особенности, когда службам пограничного контроля приходится действовать в режиме плотных пассажиропотоков.

xviii. Предусмотрена ли в ДОК возможность обмениваться сертификатами для доступа к отпечаткам пальцев?

В Меморандуме о взаимопонимании (МОВ) ДОК не указана возможность обмена сертификатами верификации документов и соответствующей информацией о вторичных биометрических признаках в электронных паспортах.

xix. В чем заключается практическая ценность ДОК для выпускающих электронные паспорта государств, не имеющих автоматизированной системы пограничного контроля?

Активное участие в ДОК означает, что достоверность проездных документов государств-участников может быть проверена другими государствами, использующими ДОК. Это, в свою очередь, значит, что граждане государств- участников могут в ходе своих поездок пользоваться облегченной процедурой пограничного контроля, что представляет для них ощутимое преимущество.

xx. Почему ДОК содержит совместимые данные, не отвечающие стандартам?

В обращении находится некоторое количество действительных электронных паспортов, выпущенных еще до того, как многочисленные усилия Правления ДОК по повышению качества данных возымели эффект. Поскольку замена таких электронных паспортов – процесс непростой, необходимо четко определить, какие данные, использовавшиеся при выпуске этих паспортов, подлежат особо тщательной проверке при удостоверении подлинности подписи в чипе.

xxi. Какие меры предпринимаются Правлением ДОК для повышения качества данных ДОК?

При намерении участников ДОК загрузить совместимые данные, не отвечающие стандартам, такие действия разрешаются только после соответствующего рассмотрения Правлением ДОК. Процесс рассмотрения включает обязательство внести соответствующие исправления в течение переходного периода, не превышающего 6 месяцев. По истечении переходного периода данным, по-прежнему не соответствующим принятым стандартам, будет отказано в размещении. Участники ДОК могут направить сертификаты CSCA или сертификаты соединения CSCA оператору ДОК заранее до импорта или загрузки в целях проверки на соответствие стандартам.

дипломатических контактов, дипломатической вализы или других подобных процедур или средств. Также для этой цели могут быть использованы электронная почта или веб-сайт, но в этом случае получатель обязан подтвердить целостность полученного сертификата способом передачи по неэлектронным каналам, т. е. в виде напечатанного криптографического сообщения, пересылаемого по каналам дипломатической почты.

xxiii. Могут ли сертификаты CSCA быть размещены на государственном веб-сайте, или это будет расценено как нарушение стандартов ИКАО?

Сертификаты являются открытой информацией и в этом качестве могут быть размещены на веб-сайте. Это не является нарушением стандартов ИКАО.

xxiv. Где можно получить информацию технического характера для загрузки данных в ДОК?

Ответы на все технические вопросы содержатся в той документации, которая будет направлена бюро ДОК ИКАО и оператором ДОК в ваш адрес, как только вы станете участником ДОК. Можно также ознакомиться со скачиваемой документацией ДОК на веб-сайте ДОК. В частности, следует ознакомиться с документами "Правила ДОК" и "Процедуры ДОК". Кроме того, рекомендуется загрузить Дополнение к Doc 9303, имеющееся на веб-сайте МСПД. Там содержится самая свежая информация по спецификациям МСПД.

xxv. Как различить сертификаты CSCA, сертификаты подписи документа (DSC) и листы аннулирования сертификатов (CRL) Китайской Народной Республики, Гонконга (КНР) и Макао (КНР)?

В КНР имеется три пункта выдачи паспортов:

i) один для материковой части Китая;

ii) один для Гонконга (КНР);

iii) один для Макао (КНР).

В своих сертификатах CSCA, DSC и CRL они используют один и тот же код страны (т. е. С=CN) по ИСО 3166. Поэтому все эти сертификаты и CRL хранятся в одном и том же разделе ДОК под кодом страны CN. Службы пограничного контроля могут различить эти сертификаты и CRL трех пунктов выдачи паспортов путем одновременного использования кода страны (С) и выдающей организации (О). Тогда атрибуты сертификатов КНР, Гонконга (КНР) и Макао (КНР) в сравнении будут выглядеть следующим образом:

|  |  |  |
| --- | --- | --- |
| КНР | Макао (КНР) | Гонконг (КНР) |
| C = CN | C = CN | C = CN |
| O = правительство КНР | O = САР Макао | O = Гонконг (КНР) |

пользоваться бесплатно?

Основные списки, включенные в ДОК, охватывают значительную часть сертификатов CSCA сообщества, выпускающего электронные паспорта. Эти сертификаты CSCA позволяют проверить цепочку сертификатов соответ- ствующего государства, выдавшего данный электронный паспорт. Однако пользователь основного списка, не являющийся участником ДОК, должен иметь в виду следующее:

- Передача принадлежащих государству сертификатов подписи документа (DSC) и листов аннулирования сертификатов (CRL) для пользователей основных списков остается проблемой.

- Если скачанный из ДОК основной список является единственной "точкой доверия", пользователю этого основного списка предстоит еще установить отношения доверия с тем, кто такой основной список выпустил, а это в любом случае будет участник ДОК.

- Участники ДОК не несут каких-либо обязательств по выпуску основных списков или по включению в них определенных сертификатов CSCA. Нет у них и обязательств по обновлению основных списков в течение какого-то определенного периода времени после выпуска новых сертификатов CSCA. Поэтому, рассчитывая исключительно на основные списки, пользователь сознательно обрекает себя на более или менее длительный срок отсутствия доступа к сертификатам CSCA.

- То, что пользователи, не являющиеся участниками ДОК, не платят взносы, это правда. Однако, не будучи участниками ДОК, такие пользователи вынуждены, как правило, скачивать данные вручную, а не автоматически (см. Шкалу взносов ДОК). Такой режим требует постоянного участия оператора и последующей обработки скачанных данных, а это означает, что разница между участием и неучастием в ДОК в денежном отношении значительно меньше чем кажется.

- В качестве Рекомендуемой практики в Приложение 9 Чикагской конвенции включено положение о том, что Договаривающимся государствам ИКАО, выдающим или намеревающимся выдавать электронные паспорта и/или осуществляющим автоматизированную проверку электронных паспортов на пунктах пограничного контроля, следует участвовать в ДОК. К тому же, ДОК пользуется политической поддержкой со стороны ОБСЕ, ЕС и стран "Большой восьмерки".

xxvii. В чем заключается условие снижения взносов?

Размер взносов снижается по мере увеличения количества участников ДОК. Как было предусмотрено в контракте на эксплуатацию, плата за услуги оператора ДОК должна быть снижена по достижении ДОК количества участников, равного 31. В результате с 1 января 2014 года плата за услуги оператора ДОК будет снижена с 43 тыс. долл. США до 34 тыс. долл. США. Контракт на эксплуатацию также предусматривает дальнейшее снижение платы по достижении ДОК числа участников, равного 65.

xxviii. Может ли участвовать в ДОК орган по осуществлению пограничного контроля?

Да, орган, осуществляющий функции пограничного контроля, может быть участником ДОК. В соответствии со статьей 2.1 МОВ ДОК, любое "Договаривающееся государство ИКАО" (т. е. государство, ратифицировавшее Чикагскую конвенцию), выдающее или намеревающееся выдавать электронные МСПД, может участвовать в ДОК ИКАО. В МОВ не уточняется, какая именно государственная структура должна инициировать процедуру вступления. В то же время следует отметить, что государство может быть представлено только одной структурой, выполняющей положения МОВ и принимающей предусмотренные в нем обязательства от имени данного государства. Таким образом, решение о том, какую именно структуру назначить ответственной за выполнение МОВ, остается в суверенной компетенции государства. В Стандартах и Рекомендуемой практике 3.9.1 Приложения 9 "Упрощение формальностей" к Чикагской конвенции особенно рекомендуется участие в ДОК ИКАО для государств, осуществляющих автоматизированные проверки электронных паспортов на пунктах пограничного контроля.

**-----**