ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть 12. Инфраструктура открытых ключей для МСПД

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть 12. Инфраструктура открытых ключей для МСПД

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

Опубликовано отдельными изданиями на русском, английском,
арабском, испанском, китайском и французском языках
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ ГРАЖДАНСКОЙ АВИАЦИИ.
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Загрузить и получить дополнительную информацию можно
на сайте www.icao.int/security/mrtd

Doc 9303. ***Машиносчитываемые проездные документы***
Часть 12. ***Инфраструктура открытых ключей для МСПД***
Заказ №: 9303P12
ISBN 978-92-9265-510-5 (бумажная копия)
ISBN 978-92-9275-569-0 (электронная копия)

ПОПРАВКИ

Об издании поправок сообщается в дополнениях к *Каталогу продуктов и услуг;* Каталог и дополнения к нему имеются на веб-сайте ИКАО www.icao.int. Ниже приводится форма для регистрации таких поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№	Дата	Кем внесено
1	14/6/24	ИКАО

ИСПРАВЛЕНИЯ		
№	Дата	Кем внесено

ОГЛАВЛЕНИЕ

Страница

1. СФЕРА ПРИМЕНЕНИЯ

В части 12 документа Doc 9303 определяется инфраструктура открытых ключей (PKI) для приложения электронного МСПД. Устанавливаются требования к государствам или организациям выдачи, включая деятельность сертифицирующего полномочного органа (CA), который выпускает сертификаты и составляет списки отзыва сертификатов (CRL). Кроме того, устанавливаются требования в отношении принимающих государств и их систем проверки, которые валидируют эти сертификаты и CRL.

В восьмом издании документа Doc 9303 содержатся спецификации, касающиеся видимых цифровых печатей (известных, как VDS), факультативных данных о регистрации поездок и виз и дополнительных биометрических приложений (известных, как LDS2), представляющих собой расширение обязательного приложения электронного МСПД (известного, как LDS1).

Часть 12 документа Doc 9303 рассматривается совместно с:

- частью 10 *"Логическая структура данных (LDS) для хранения биометрических и других данных на бесконтактной интегральной схеме (ИС)"* документа Doc 9303,
- частью 11 *"Механизмы защиты МСПД"* документа Doc 9303,
- частью 13 *"Видимые цифровые печати"* документа Doc 9303.

2. ОБЩИЙ ОБЗОР ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

Инфраструктура открытых ключей (PKI) электронных МСПД позволяет создавать и впоследствии верифицировать цифровые подписи на объектах электронных МСПД, включая объект защиты документа (SO_D), для подтверждения того, что подписанные данные являются аутентичными и не изменены. Отзыв сертификата, сбой в процедуре валидации пути сертификации или сбой в верификации цифровой подписи сами по себе еще не означают, что электронный МСПД должен считаться недействительным. Такой сбой означает, что результат электронной верификации целостности и аутентичности данных LDS оказался отрицательным, и тогда могут быть использованы другие неэлектронные механизмы, чтобы такое заключение было частью общей проверки электронного МСПД.

PKI электронного МСПД гораздо проще таких более общих инфраструктур PKI с множеством приложений, как PKI Интернета, определенная в документе [RFC 5280]. В PKI электронного МСПД каждое государство/каждый полномочный орган выдачи определяет единый сертифицирующий полномочный орган (CA), который выдает все сертификаты непосредственно конечным субъектам, в том числе лицам, подписывающим документы. Указанные CA называются национальными сертифицирующими полномочными органами с правом подписи (CSCA). Никаких других CA в этой инфраструктуре не существует. Принимающие государства непосредственно устанавливают доверие к ключам/сертификатам CSCA каждого государства или организации выдачи.

PKI электронного МСПД основана на общих стандартах PKI, включая [X.509] и [RFC 5280]. Указанные базовые стандарты PKI определяют большой набор факультативных характеристик и сложных взаимоотношений доверия между CA, которые не связаны с приложением электронного МСПД. В данной части документа Doc 9303 определяется профиль таких стандартов, специально адаптированных для приложения электронного МСПД. Некоторые из уникальных аспектов приложения электронного МСПД включают следующее:

- у каждого государства имеется только один CSCA;
- пути сертификации включают только один сертификат (например, лица, подписывающего документы);
- верификация подписи должна быть возможной в течение 5–10 лет после выдачи;
- изменение имени CSCA поддерживается;
- связующие сертификаты CSCA не обрабатываются как промежуточные сертификаты в пути сертификации.

В основном инфраструктура PKI электронных МСПД удовлетворяет требованиям документа [RFC 5280]. Однако тот факт, что CSCA могут изменять свое имя, накладывает на PKI электронного МСПД уникальные требования, которые несовместимы с некоторыми процедурами валидации CRL, определенными в документе [RFC 5280]. Эти различия были сведены к минимуму и четко определены.

Для VDS и LDS2 PKI цифровой подписи, обеспечивающей целостность и аутентичность объектов данных, представляет собой расширение PKI LDS1. Лица, подписывающие VDS и LDS2, назначаются тем же CSCA, который назначает лиц, подписывающих LDS1. В настоящем документе содержится информация об изменениях профилей сертификатов для этих новых приложений. В совокупности эта инфраструктура известна под названием **PKI электронных МСПД.**

PKI цифровой подписи включает в себя следующие элементы:

- национальный сертифицирующий полномочный орган с правом подписи (CSCA);
- сертификаты органов, подписывающих документы (DSC), используемые для подписи объектов защиты документов (SO_D);
- сертификаты органов, подписывающих LDS2, в число которых входят:
  - орган, подписывающий LDS2-TS – подписывает путевые отметки;
  - орган, подписывающий LDS2-V – подписывает электронные визы LDS2;
  - орган, подписывающий LDS2-B – подписывает дополнительные биометрические данные LDS2;
- сертификаты органов, подписывающих штрих-коды (BCSC), в отношении которых в настоящем документе определены два конкретных типа:
  - сертификаты органов, подписывающих визы (VSC);
  - сертификаты органов, подписывающих экстренно выдаваемые документы (ESC);
- сертификаты органов, подписывающих мастер-списки (MSC), используются для подписания мастер-списков;
- сертификаты органов, подписывающих списки отклонений (DLSC), используются для подписания списков отклонений;
- список отзыва сертификатов (CRL).

Все различные типы сертификатов подписываются одним и тем же CSCA. CSCA также подписывает CRL, в котором содержится информация о любом отозванном сертификате независимо от его типа. Все сертификаты, выданные в рамках процесса, предусмотренного CSCA, известны под названием **сертификатов органов, подписывающих документы**.

Для приложений LDS2 определена отдельная **PKI авторизации**. PKI авторизации позволяет государству или организации выдачи электронных МСПД контролировать деятельность и оказывать помощь зарубежным государствам, имеющим разрешение на внесение объектов данных LDS2 в свои электронные МСПД и считку этих объектов данных. Зарубежные государства, намеревающиеся считывать или вносить данные LDS2, должны получить сертификат авторизации непосредственно от государства или организации выдачи электронного МСПД.

PKI авторизации использует иную структуры сертификатов (ИСО 7816 сертификаты, верифицируемые карточкой) и поэтому для нее требуются дополнительные компоненты инфраструктуры.

Для LDS2 необходимо, чтобы терминал подтвердил бесконтактной ИС электронного МСПД свое право на внесение объектов данных LDS2 в бесконтактную ИС или на считывание объектов данных LDS2. Такой терминал имеет, как минимум, один закрытый ключ и соответствующий сертификат терминала, кодирующий открытый ключ терминала и права доступа. После подтверждения того, что терминалу известен этот закрытый ключ, чип МСПД предоставляет терминалу доступ к считыванию/записи данных LDS2, как указано в сертификате терминала.

PKI авторизации LDS2 включает в себя следующие элементы:

- национальные сертифицирующие полномочные органы с правом верификации (CVCA);
- органы, верифицирующие документы (DV);
- терминалы;
- единый центр обслуживания (SPOC).

Распределение и администрирование сертификатов авторизации между CVCA в одном государстве и DV в другом государстве осуществляются единым центром обслуживания (SPOC) каждого государства.

В части 12 документа Doc 9303 изложены спецификации профиля PKI электронных МСПД, профиля PKI авторизации и соответствующих объектов, включая:

- роли и обязанности субъектов в данной инфраструктуре;
- криптографические алгоритмы и управление ключами;
- содержание сертификатов и CRL;
- механизмы рассылки сертификатов и списков CRL;
- валидацию пути сертификации.

3. РОЛИ И ОБЯЗАННОСТИ

В данном разделе содержится подробная информация о субъектах и ролях и обязанностях PKI электронных МСПД и PKI авторизации.

3.1 PKI электронных МСПД

Аутентичность и целостность данных, хранящихся на электронных МСПД, защищаются посредством пассивной аутентификации. Этот механизм защиты основан на цифровых подписях и включает следующие субъекты PKI для PKI электронных МСПД:

- **Национальный сертифицирующий полномочный орган с правом подписи (CSCA).** Каждое государство/полномочный орган выдачи создает единый CSCA в качестве своего национального центра доверия в контексте электронных МСПД. CSCA выпускает сертификаты открытых ключей для одного или нескольких (в национальном масштабе) органов, подписывающих документы, и факультативно для других конечных субъектов, таких как органы, подписывающие мастер-списки, и органы, подписывающие списки отклонений. CSCA также периодически выпускает списки отзыва сертификатов (CRL), указывающие, отозван ли какой-либо из выпущенных сертификатов.

- **Органы, подписывающие документы (DS).** Орган, подписывающий документы, подписывает в цифровой форме данные, подлежащие хранению на электронных МСПД; эта подпись хранится в электронном МСПД в объекте защиты документа.

- **Органы, подписывающие LDS2.** Орган, подписывающий LDS2, подписывает в цифровой форме объекты данных LDS2 одного или нескольких типов.

- **Орган, подписывающий штрих-коды (BCS).** Орган, подписывающий штрих-коды, подписывает в цифровой форме данные (заголовок и сообщение), закодированные в штрих-коде. Эта подпись также хранится в штрих-коде. В настоящем коде конкретно определяются два варианта использования, касающихся лица, подписывающего штрих-коды, а именно визовые документы и проездные документы, выдаваемые в экстренных случаях.

- **Системы проверки (IS).** Система проверки верифицирует цифровую подпись, включая валидацию пути сертификации, для верификации аутентичности и целостности электронных данных, хранящихся на электронном МСПД, в рамках пассивной аутентификации.

- **Органы, подписывающие мастер-списки.** Орган, подписывающий мастер-списки, является факультативным субъектом, подписывающим в цифровой форме список сертификатов CSCA (внутренних и иностранных) в поддержку двустороннего механизма рассылки сертификатов CSCA.

- **Органы, подписывающие списки отклонений.** Органы, подписывающие списки отклонений, используются для подписания списков отклонений. Списки отклонений определены в части 3 документа Doc 9303.

Защищенные средства для генерирования пар ключей КОНТРОЛИРУЮТСЯ государством или организацией выдачи. Каждая пара ключей включает "закрытый" ключ и "открытый" ключ. Закрытые ключи и связанные с ними системы и средства надежно ЗАЩИЩАЮТСЯ от любого внешнего или несанкционированного доступа за счет собственной конструкции и средств защиты аппаратуры.

В то время как сертификат CSCA остается относительно статическим, со временем появляется большое количество сертификатов органов, подписывающих документы.

CSCA каждого государства или организации выдачи играет роль объекта доверия для принимающего государства. Государство или организация выдачи рассылают свой собственный открытый ключ CSCA принимающим государствам в виде сертификата. Принимающее государство устанавливает, что этот сертификат (и сертифицированный ключ) являются "доверительными", используя для этого внеполосные средства связи, и хранит "якорь доверия" для этого доверительного ключа/сертификата. Указанные сертификаты CSCA должны быть САМОПОДПИСАННЫМИ сертификатами, изданными непосредственно CSCA. Сертификаты CSCA НЕ ДОЛЖНЫ быть подчиненными или кросс-сертификатами в более крупной инфраструктуре PKI. Могут быть также выпущены связующие сертификаты CSCA для оказания помощи принимающему государству в установлении доверия к новому ключу/сертификату CSCA после смены ключей.

Примечание. В некоторых государствах существует требование, предусматривающее, чтобы централизованный регулятор сертифицирующего полномочного органа (CCA) был высшим полномочным органом для опубликования самоподписанных сертификатов для всех приложений. В этих случаях возможное решение состоит в том, чтобы CSCA создавал самоподписанный сертификат (удовлетворяющий требованиям документа ИКАО Doc 9303) и чтобы этот сертификат визировался CCA (для обеспечения удовлетворения требований собственного CCA государства). Однако эти завизированные сертификаты не являются частью PKI электронных паспортов и не будут рассылаться принимающим государствам.

3.1.1 Национальный сертифицирующий полномочный орган с правом подписи

РЕКОМЕНДУЕТСЯ, чтобы пара ключей CSCA (KPu_{CSCA}, KPr_{CSCA}) генерировалась и хранилась в надежно защищенной офлайновой инфраструктуре CA.

Закрытый ключ CSCA (KPr_{CSCA}) используется для подписания сертификатов органов, подписывающих документы (C_{DS}), других сертификатов и списков CRL.

Сертификаты национального сертифицирующего полномочного органа с правом подписи (C_{CSCA}) используются для валидации сертификатов органов, подписывающих документы, сертификатов органов, подписывающих мастер-списки, сертификатов органов, подписывающих списки отклонений, списков CRL и других сертификатов, выпускаемых CSCA.

Все сертификаты и CRL ДОЛЖНЫ соответствовать профилям, указанным в разделе 7, и ДОЛЖНЫ распространяться с помощью механизмов рассылки, изложенных в разделе 5.

В отношении участников ДОК каждый сертификат (C_{CSCA}) ДОЛЖЕН также направляться в ДОК (для целей валидации сертификатов лиц, подписывающих документы (C_{DS})).

Списки CRL ДОЛЖНЫ выпускаться на периодической основе, как указано в разделе 4.

3.1.2 Органы, подписывающие документы

РЕКОМЕНДУЕТСЯ, чтобы пары ключей (KPu_{DS}, KPr_{DS}) органов, подписывающих документы, генерировались и хранились в надежно защищенной инфраструктуре.

Закрытый ключ органа, подписывающего документы (KPr_{DS}), используется для подписания объектов защиты документов (SO_D).

Сертификаты органов, подписывающих документы (C_{DS}), используются для валидации объектов защиты документа (SO_D).

Каждый сертификат органа, подписывающего документы (C_{DS}), ДОЛЖЕН соответствовать профилю сертификата, определенному в разделе 7, и ДОЛЖЕН храниться на бесконтактной ИС каждого электронного МСПД, который был подписан с использованием соответствующего закрытого ключа DS (см. подробную информацию в части 10 документа Doc 9303). Это гарантирует, что принимающее государство имеет доступ к сертификату органа, подписывающего документы, применительно к каждому электронному МСПД.

Сертификаты органов, подписывающих документы, из числа участников ДОК ДОЛЖНЫ также направляться в ИКАО для опубликования в директории открытых ключей (ДОК) ИКАО.

3.1.3 Органы, подписывающие LDS2

Орган, подписывающий LDS2, подписывает в цифровой форме объекты данных LDS2 одного или нескольких типов.

При необходимости ссылки на орган, подписывающий LDS2, в качестве субъекта, который подписывает объект данных LDS2 конкретного типа, этим органом является:

- Орган, подписывающий LDS2-TS – подписывает путевые отметки LDS2;
- Орган, подписывающий LDS2-V – подписывает электронные визы LDS2;
- Орган, подписывающий LDS2-B – подписывает дополнительные биометрические данные LDS2.

Каждому государству РЕКОМЕНДУЕТСЯ иметь не более одного органа, подписывающего LDS2-TS, одного органа, подписывающего LDS2-V и одного органа, подписывающего LDS2-B. Кроме того, один орган, подписывающий LDS2, может совмещать выполнение некоторых или всех этих обязанностей.

Если требуется дополнительное дифференцирование, например, указание места, в котором проставлялась путевая отметка, представление информации о конкретном сотруднике, проверявшем пассажира, сотруднике, выдававшем визу, или пункте, в котором вносились дополнительные биометрические данные, то эту информацию можно включить в поле конфиденциальной информации соответствующего объекта данных LDS2.

3.1.4 Органы, подписывающие штрих-коды

РЕКОМЕНДУЕТСЯ, чтобы пара ключей (KPu_{BCS}, KPr_{BCS}) органа, подписывающего штрих-коды, генерировалась и хранилась в надежно защищенной инфраструктуре.

Закрытый ключ (KPr_{BCS}) органа, подписывающего штрих-код, используется для подписания данных (заголовок и сообщение), закодированных в штрих-коде. Эта подпись также хранится в штрих-коде.

Сертификаты органов, подписывающих штрих-коды (C_{BCS}), используются для валидации данных (заголовок и сообщение), закодированных в штрих-коде.

Все сертификаты органов, подписывающих штрих-коды (C_{BCS}), ДОЛЖНЫ соответствовать профилю сертификата, определенному в разделе 7. Сертификаты органов, подписывающих штрих-коды, в самой цифровой печати не содержатся. Таким образом, государство, выдающее документы, защищенные цифровыми печатями, ДОЛЖНО публиковать информацию обо всех своих сертификатах органов, подписывающих штрих-коды. Основными каналами рассылки сертификатов органов, подписывающих штрих-коды, являются ДОК /двусторонние каналы. Другие механизмы, например, размещение информации на веб-сайтах, являются дополнительными каналами.

Органу, выдающему сертификаты, СЛЕДУЕТ направлять сертификаты органов, подписывающих штрих-коды и являющихся участниками ДОК, в ИКАО для их публикации в директории открытых ключей (ДОК ИКАО).

Органы, подписывающие визы и экстренно выдаваемые проездные документы, относятся к особым категориям органов, подписывающих штрих-коды.

3.1.5 Система проверки

Система проверки выполняет пассивную аутентификацию, чтобы убедиться в целостности и аутентичности данных, хранящихся на бесконтактной ИС электронного МСПД. В рамках этого процесса системы проверки ДОЛЖНЫ проводить валидацию пути сертификации, как указано в разделе 6.

3.1.6 Орган, подписывающий мастер-списки

Для подписания мастер-списков CSCA используется закрытый ключ органа, подписывающего такие списки.

Для валидации мастер-списков CSCA используются сертификаты органа, подписывающего такие списки.

3.1.7 Орган, подписывающий списки отклонений

Для подписания списков отклонений используется закрытый ключ органа, подписывающего такие списки.

Для валидации списков отклонений используются сертификаты органа, подписывающего такие списки.

3.2 Авторизация PKI

В момент проведения персонализации государство или организация выдачи вносят приложение LDS2 в бесконтактную ИС электронного МСПД.

До того, как другое государство сможет записать объекты LDS2 на эту бесконтактную ИС, оно ДОЛЖНО получить разрешение на выполнение этой операции от государства или организации выдачи. Каждый объект данных LDS2 в цифровой форме подписывается органом, подписывающим LDS2 в государстве, осуществляющем запись, и впоследствии записывается на бесконтактную ИС авторизованным терминалом в этом государстве. Двухэтапный процесс подписи органом, подписывающим документы, и записи авторизованным терминалом аналогичен концепции LDS1, в рамках которой орган, подписывающий документы в цифровой форме, подписывает объекты защиты документов, однако впоследствии они записываются на бесконтактную ИС посредством реализации процедуры персонализации, иллюстрация которой приводится на рис. 1. Последующее считывание объектов LDS2 с бесконтактной ИС выполняется терминалами, которым разрешено считывание LDS2 рассматриваемого типа объекта LDS2.

Авторизация PKI позволяет государству или организации выдачи электронных МСПД контролировать доступ (считывание и запись) к данным LDS2 на бесконтактных ИС в выдаваемых ими электронных МСПД.

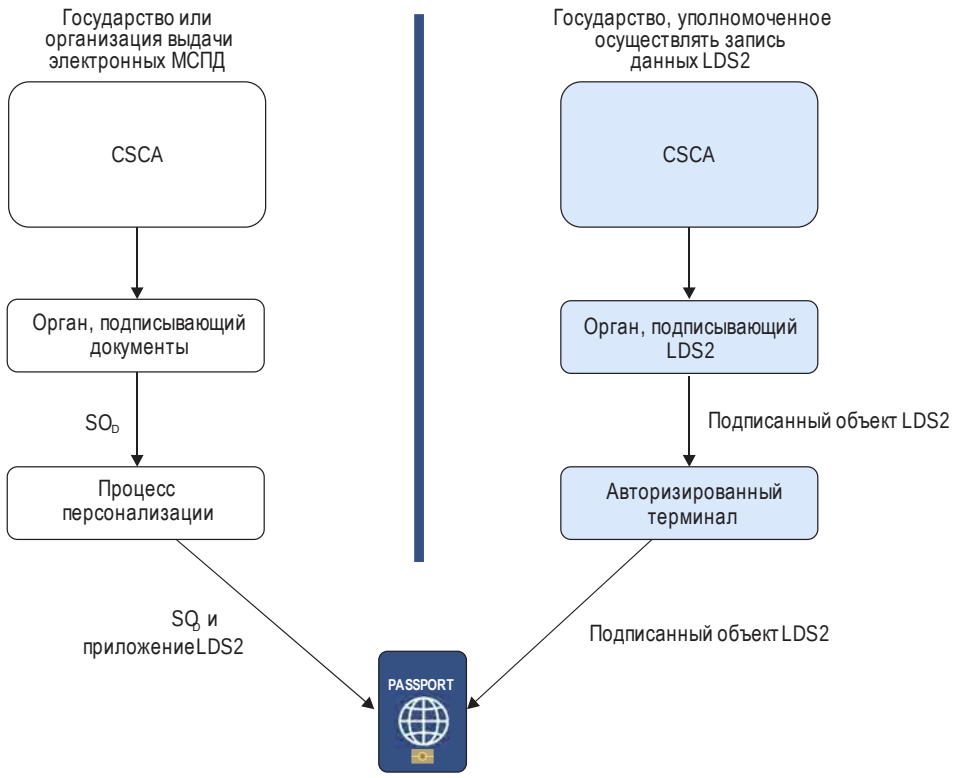

Рис. 1. Модель доверия LDS2 и архитектура записи

3.2.1 Национальный сертифицирующий полномочный орган с правом подписи

Каждое государство или организация выдачи, выдающее(щая) разрешения на внесение данных LDS2 в свои электронные МСПД, ДОЛЖНО определить единый национальный сертифицирующий полномочный орган с правом верификации (CVCA). Этот CVCA является сертифицирующим полномочным органом (CA), являющимся "якорем доверия" для авторизации PKI этого государства или организации и охватывающим все приложения LDS2. CVCA может представлять собой обособленную организацию или входить в состав CSCA этого государства или организации. Однако даже в случае совмещения CVCA ДОЛЖЕН использовать иную, чем CSCA пару ключей. CVCA определяет права доступа, которые будут предоставляться всем зарубежным и национальным органам по верификации документов (DV), и выдает сертификаты, содержащие индивидуальные разрешения, предоставленные каждому из этих DV.

3.2.2 Орган по верификации документов

Органом по верификации документов (DV) является CA, который, выполняя функции организационного подразделения, управляет группой терминалов (например, терминалов, эксплуатируемых пограничной полицией государства) и выдает этим терминалам сертификаты авторизации. Для осуществления деятельности по выдаче соответствующих сертификатов терминалов DV уже ДОЛЖЕН иметь сертификат авторизации, выданный ответственным CVCA. Сертификаты, выданные DV терминалам, МОГУТ содержать аналогичные или частичные сведения о разрешении, выданном органом по верификации документов (DV). В них НЕ ДОЛЖНЫ содержаться разрешения, выходящие за рамки разрешений, выданных DV.

3.2.3 Терминал/Система проверки

В контексте авторизации PKI терминал представляет собой устройство, которое имеет доступ к бесконтактной ИС электронного МСПД, осуществляет запись объектов данных LDS2 с цифровой подписью или считывает объекты данных. Терминал ДОЛЖЕН иметь сертификат авторизации, полученный от местного DV, который выдает необходимое разрешение. В отношении терминалов также используется термин "система проверки".

3.2.4 Единый центр обслуживания (SPOC)

Каждое государство, участвующее в деятельности по авторизации PKI LDS2, ДОЛЖНО создавать единый SPOC. SPOC представляет собой интерфейс, используемый доя осуществления всех видов связи между CVCA одного государства и DV другого государства. SPOC каждого государства обмениваются сообщениями, касающимися запросов и ответов в отношении сертификатов, используя для этого протокол SPOC, определенный в разделе 8.

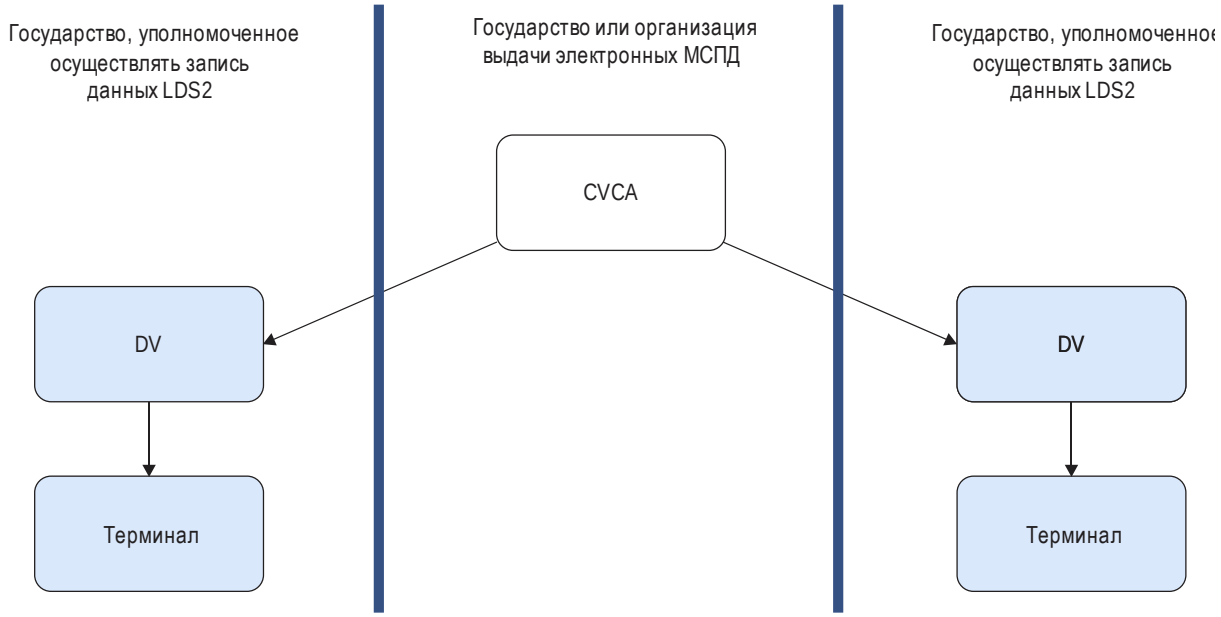

Рис. 2. Авторизация модели доверия PKI

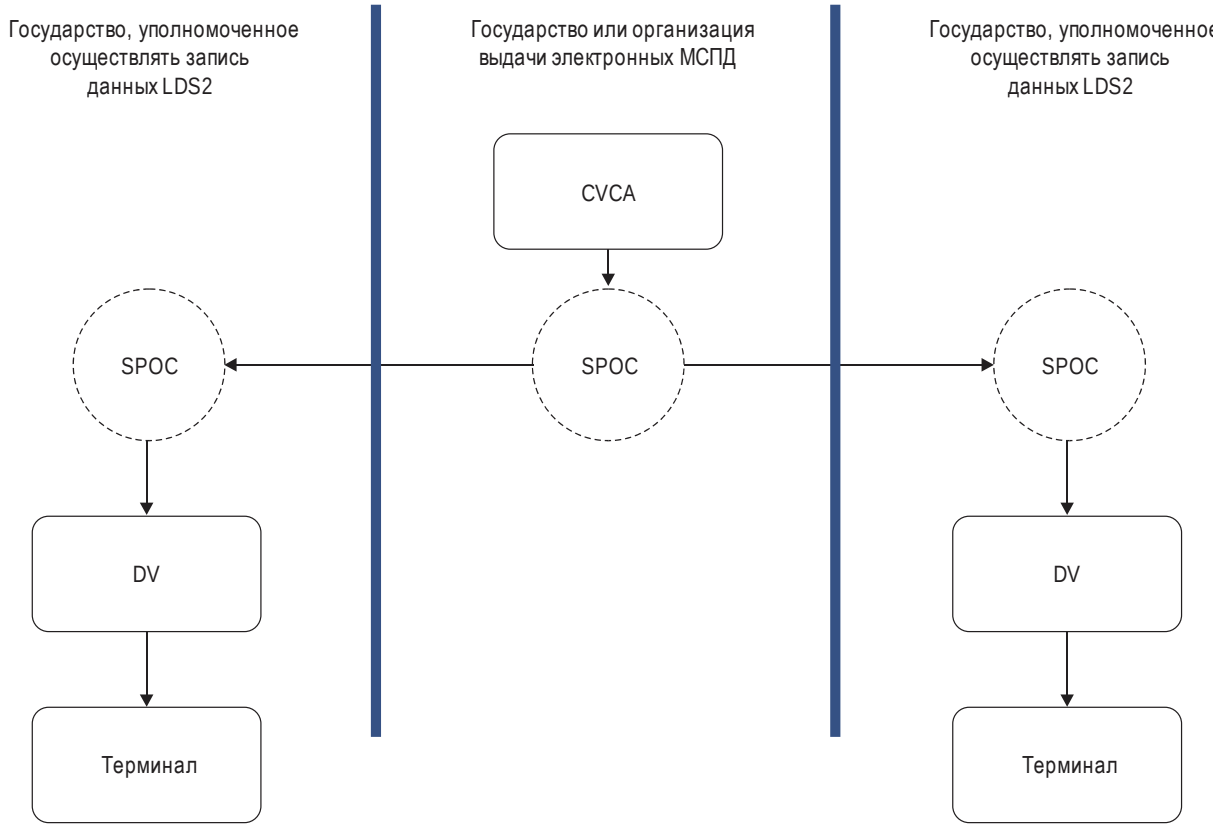

Рис. 3. Роль SPOC

4. УПРАВЛЕНИЕ КЛЮЧАМИ

Для двух инфраструктур открытых ключей управление ключами определяется отдельно.

4.1 PKI электронных МСПД

Государство или организация выдачи ИМЕЮТ по крайней мере два типа пар ключей:

- пара ключей национального CA с правом подписи;
- пара ключей органа, подписывающего документы.

Государство или организация выдачи МОГУТ иметь дополнительные типы ключей:

- пара ключей органа, подписывающего мастер-списки;
- пара ключей органа, подписывающего списки отклонений;
- пара ключей органа, подписывающего LDS2;

- пара ключей клиента SPOC;
- пара ключей сервера SPOC;
- пара ключей органа, подписывающего визы / пара ключей органа, подписывающего экстренно выдаваемые документы (оба относятся к типам органов, подписывающих штрих-коды).

Сертификаты открытых ключей национальных CA с правом подписи и сертификаты SPOC оформляются с использованием сертификатов формата [X.509]. Открытые ключи, содержащиеся в сертификатах CSCA, используются для верификации подписи CSCA на выданных сертификатах органов, подписывающих документы, сертификатах SPOC, CSCA и на оформленных CRL.

Для ключей и сертификатов органа, подписывающего мастер-списки, органа, подписывающего списки отклонений, и средств связи срок службы закрытого ключа и период действия сертификата устанавливаются по усмотрению государства или организации выдачи.

Как сертификаты CSCA, так и сертификаты органа, подписывающего документы, связаны с применимостью закрытого ключа и сроком действия открытого ключа, как указано в таблице 1.

Таблица 1. Применимость и сроки действия ключей

	Использование закрытого ключа	***Срок действия открытого ключа (предположительный срок действия паспорта 10 лет)***
Национальный CA с правом подписи	3–5 лет	13–15 лет
Орган, подписывающий документы	До 3 мес[1]	Приблизительно 10 лет
Орган, подписывающий LDS2-TS	1-2 года	10 лет + 3 месяца
Орган, подписывающий LDS2-V	1-2 года	10 лет + 3 месяца
Орган, подписывающий LDS2-B	1-2 года	10 лет + 3 месяца
Клиент SPOC	Не указано	6-18 месяцев
Сервер SPOC	Не указано	6-18 месяцев
Орган, подписывающий штрих-код визы	1-2 года	Срок применимости закрытого ключа + срок действия визы
Орган, подписывающий штрих-код экстренно выдаваемого проездного документа	1 год + 2 месяца (2 месяца предназначены для обеспечения плавного переоформления)	Срок применимости закрытого ключа + срок действия ETD
Орган, подписывающий мастер-списки	По усмотрению государства или организации выдачи	По усмотрению государства или организации выдачи
Орган, подписывающий список отклонений	По усмотрению государства или организации выдачи	По усмотрению государства или организации выдачи
Средства связи	По усмотрению государства или организации выдачи	По усмотрению государства или организации выдачи

1. Следует иметь в виду, что период, указанный в расширении `privateKeyUsage` (`ПрименимостьзакрытогоКлюча`) сертификата DS, может быть более продолжительным для обеспечения перекрытия или выполнения требований к производству.

4.1.1 Ключи и сертификаты органов, подписывающих документы

Период применимости закрытого ключа органа, подписывающего документы, гораздо короче, чем период действия сертификата DS для соответствующего открытого ключа.

4.1.1.1 Период действия открытого ключа органов, подписывающих документы

Срок службы (т. е. период действия сертификата) органа, подписывающего документы, определяется путем конкатенации следующих двух периодов:

- продолжительность времени использования соответствующего закрытого ключа для выдачи электронных МСПД и
- наиболее длительный период действия любого электронного МСПД, выданного под этим ключом[2].

Сертификат органа, подписывающего документы (C_{DS}), ДЕЙСТВИТЕЛЕН в течение всего этого периода, чтобы можно было осуществлять верификацию аутентичности электронных МСПД. Однако соответствующий закрытый ключ СЛЕДУЕТ использовать только для выдачи документов на ограниченный срок; по истечении срока действия последнего документа, для выдачи которого он использовался, указанный открытый ключ больше не требуется.

4.1.1.2 Период, на который выдается закрытый ключ органам, подписывающим документы

При внедрении своих систем государство или организация выдачи могут принять решение учитывать количество документов, которые будут подписываться одним индивидуальным закрытым ключом органа, подписывающего документы.

Государство или организация выдачи могут назначить один или несколько органов, подписывающих документы, каждый из которых имеет пару собственных уникальных ключей, которые будут обеспечивать выполнение соответствующих функций в любой момент времени.

В целях минимизации расходов, связанных с обеспечением бесперебойной деятельности в случае отзыва сертификата органа, подписывающего документы, государство или организация выдачи, которые выпускают большое количество электронных МСПД в день, могут принять решение о том, чтобы:

- устанавливать очень короткий период применимости закрытого ключа; и/или
- назначить одновременно несколько органов, подписывающих документы, которые будут функционировать в одно и то же время, причем у каждого будет свой собственный уникальный закрытый ключ и сертификат открытого ключа.

Государство или организация выдачи, которые выдают небольшое число электронных МСПД в день, могут принять решение о назначении одного органа, подписывающего документы, и они могут также принять решение о целесообразности установления несколько более продолжительного периода применимости закрытого ключа.

---

2. Некоторые государства или организации выдачи могут выдавать электронные МСПД до того, как они становятся действительными; например, при смене фамилии после вступления в брак. В этих случаях "наиболее длительный период действия любого электронного МСПД" включает фактический период действия электронного МСПД (например, 10 лет) плюс максимальный период времени с момента выдачи электронного МСПД до момента, когда он становится действительным.

Независимо от количества электронных МСПД, выпускаемых ежедневно, или количества одновременно функционирующих органов, которые подписывают документы, РЕКОМЕНДУЕТСЯ, чтобы максимальный период использования любого закрытого ключа органа, подписывающего документы, для подписания электронных МСПД составлял 3 мес.

После выдачи последнего документа, подписанного с использованием данного закрытого ключа, государствам или организациям выдачи РЕКОМЕНДУЕТСЯ стирать закрытый ключ поддающимся проверке и учету способом.

4.1.2 Ключи и сертификаты органов, подписывающих LDS2

Пары ключей органа, подписывающего LDS2, аналогичны парам ключей органа, подписывающего документы, в том плане, что период применимости закрытого ключа является намного меньшим, чем срок действия соответствующего сертификата. Сертификаты ДОЛЖНЫ оставаться действительными в течение срока действия электронного МСПД или подписанного объекта LDS2 (в зависимости от того, который из них является более длительным). Поскольку подписанные объекты данных будут вноситься в электронные МСПД из различных государств, эти сертификаты ДОЛЖНЫ быть действительными по крайней мере в течение самого длительного срока действия электронного МСПД (т. е. 10 лет).

4.1.2.1 Срок действия открытого ключа органа, подписывающего LDS2

Срок действия, т. е. период действия сертификата, открытого ключа органа, подписывающего LDS2, определяется посредством конкатенации следующих двух периодов:

- период времени, в течение которого закрытый ключ будет использоваться для подписания объектов LDS2;

- период действия, являющийся наиболее длительным из числа указанных ниже:

  - период действия любого электронного МСПД, который будет хранить объект данных LDS2, подписанный этим ключом; или

  - период действия объекта LDS2, подписанного этим ключом. Следует отметить, что в случае электронной визы LDS2 не исключена возможность того, что период действия подписанной электронной визы будет превышать срок действия электронного МСПД, содержащего эту визу.

4.1.3 Ключи и сертификаты органа, подписывающего штрих-коды

Орган, подписывающий штрих-коды, является особым видом сервера подписей, используемых для подписи особой категории документов, например виз, экстренно выдаваемых проездных документов и т. д. Согласно передовой практике, применяемой в этой области, РЕКОМЕНДУЕТСЯ использовать только ключи для подписания с ограниченным числом знаков (низкое однозначное число) параллельно с созданием подписей для цифровых печатей, за исключением тех случаев, когда эксплуатационные потребности обуславливают абсолютную необходимость использования большего количества ключей. Для обеспечения возможности использования органа, подписывающего штрих-коды, в случае инцидента в системе безопасности, связанного с ключами подписания, РЕКОМЕНДУЕТСЯ предусмотреть наличие мер по обеспечению устойчивости функционирования (например, подготовка резервных ключей, резервных позиций и т. д.).

Для упрощения обработки соответствующих сертификатов (см. раздел 5) количество опубликованных ключей валидации подписей ДОЛЖНО ограничиваться пятью ключами подписи в год.

4.1.3.1 Срок действия открытого ключа органа, подписывающего штрих-коды

Данный раздел относится ко всем органам, подписывающим штрих-коды, включая органы, подписывающие визы, и органы, подписывающие экстренно выдаваемые проездные документы.

Срок действия, т. е. период действия сертификата открытого ключа органа, подписывающего штрих-коды, определяется посредством конкатенации следующих двух периодов:

- период времени, в течение которого соответствующий закрытый ключ будет использоваться для выдачи визы или ETD;
- самого длительного периода действия любого документа, выданного с использованием этого ключа[3].

Сертификат органа, подписывающего штрих-коды, ДЕЙСТВУЕТ в течение этого полного периода, что обеспечивает возможность проверки аутентичности документа. Однако соответствующий закрытый ключ СЛЕДУЕТ использовать только для выдачи документов на ограниченный период времени; после истечения срока действия последнего документа, для выдачи которого он использовался, открытый ключ в дальнейшем не требуется.

Период использования закрытого ключа:	в соответствии с профилем документа
Срок действия сертификата:	время использования закрытого ключа + период действия документа

Пример

Примечание. Фактически периоды действия, используемые для расчета в этом примере, не подразумевают предоставления каких-либо рекомендаций.

Предположим, что период действия выданных документов составляет 5 лет, а период применения сертификата органа, подписывающего штрих-коды, составляет один год. В этом случае срок действия сертификата органа, подписывающего штрих-коды, составляет 1 + 5 = 6 лет. Если период применения закрытого ключа сертификата CSCA составляет 3 года, то срок действия сертификата CSCA составляет 3 + 6 = 9 лет.

4.1.4 Ключи и сертификаты CSCA

Период применения закрытого ключа CSCA является менее продолжительным, чем период действия сертификата CSCA для соответствующего открытого ключа.

4.1.4.1 Период действия открытого ключа национального CA с правом подписи

Срок службы, т. е. период действия сертификата открытого ключа CSCA, определяется путем конкатенации следующих периодов:

3. Некоторые государства или организации выдачи могут использовать электронные МСПД до того, как они станут действительными, например, в случае изменения фамилии после заключения брака. В этих случаях "самый длительный срок действия любого электронного МСПД" включает в себя фактический срок действия электронного МСПД (например, 10 лет), плюс максимальный период времени между датой выдачи электронного МСПД и датой вступления его в силу.

- период времени, в течение которого соответствующий закрытый ключ CSCA будет использоваться для подписания любых указанных ниже сертификатов CSCA;

- максимальный срок действия ключа любого указанного ниже выданного сертификата CSCA.

4.1.4.2 Период, на который выдается закрытый ключ национальному CA с правом подписи

Период применимости закрытого ключа CSCA для подписания сертификатов и списков CRL представляет собой тонкий баланс между следующими факторами:

- В маловероятном случае компрометации закрытого ключа национального CA с правом подписи государства или организации выдачи действительность всех электронных МСПД, выданных с использованием ключей органа, подписывающего документы, сертификаты которого были подписаны скомпрометированным закрытым ключом CSCA, подвергается сомнению. В этой связи государства или организации выдачи МОГУТ пожелать устанавливать довольно короткий срок применимости ключа.

- Однако поддержание очень короткого периода применимости в определенный момент приведет к одновременному наличию очень большого количества действующих открытых ключей CSCA. Это может усложнить управление сертификатами в пограничных системах обработки.

В этой связи пару ключей CSCA государства или организации выдачи РЕКОМЕНДУЕТСЯ менять каждые 3–5 лет.

4.1.4.3 Замена ключа национального CA с правом подписи

Ключи CSCA являются предметами доверия в рамках всей системы, без которых система разрушится. Поэтому государствам или организациям выдачи СЛЕДУЕТ тщательно планировать замену своих пар ключей CSCA. По истечении первоначального периода применимости закрытого ключа подписи CSCA государство или организация выдачи всегда должны будут иметь по крайней мере два одновременно действующих сертификата CSCA (C_{CSCA}).

Государства или организации выдачи ДОЛЖНЫ уведомить принимающие государства о запланированной замене ключа CSCA. Это уведомление ДОЛЖНО быть направлено за 90 дней до замены ключа. После замены ключа новый сертификат CSCA (удостоверяющий новый открытый ключ CSCA) рассылается принимающим государствам.

Если сертификат CSCA представляет собой новый самоподписанный сертификат, аутентификацию этого сертификата следует осуществлять с использованием внеполосного метода.

После замены ключа CSCA ДОЛЖЕН быть выпущен сертификат, связывающий новый ключ со старым, чтобы обеспечить защищенный переход для пользователей. Обычно это достигается путем выпуска самоизданного сертификата, где поля органа выдачи и субъекта идентичны, но ключ, использованный для верификации подписи, представляет собой старую пару ключей, а сертифицированный открытый ключ представляет новую пару ключей. Для этих связующих сертификатов CSCA не требуется верификация с использованием внеполосного метода, так как подпись на связующем сертификате CSCA верифицируется с использованием уже доверительного открытого ключа для данного CSCA. Для рассылки связующих и самоизданных исходных сертификатов CSCA могут также использоваться мастер-списки.

Государствам или организациям выдачи следует воздерживаться от использования своего нового закрытого ключа CSCA в течение первых двух дней после замены ключей CSCA для гарантии того, что соответствующий новый сертификат открытого ключа CSCA успешно разослан.

Для подписания всех сертификатов, а также для подписания списков CRL государства или организации выдачи ДОЛЖНЫ использовать самый новый закрытый ключ CSCA.

4.1.5 Отзыв сертификатов

В случае инцидента (например, компрометация ключа) у государств или организаций выдачи может возникнуть необходимость в отзыве сертификатов.

Все CSCA ДОЛЖНЫ периодически готовить информацию об отзывах в виде списка отзыва сертификатов (CRL).

CSCA ДОЛЖНЫ выпускать по крайней мере один CRL каждые 90 дней, даже если никаких сертификатов со времени выпуска предыдущего CRL не было отозвано. CRL МОГУТ выпускаться чаще, чем каждые 90 дней, но не чаще, чем каждые 48 ч.

Когда отзывается тот или иной сертификат, в течение 48 ч ДОЛЖЕН быть разослан CRL с указанием такого отзыва.

Отзываться могут только сертификаты, а не объекты защиты документа. Использование CRL сводится к уведомлениям об отозванных сертификатах, которые были ранее выданы CSCA, выпустившим CRL (включая уведомление об отзывах для сертификатов CSCA; сертификатов DS; сертификатов органа, подписывающего мастер-списки; сертификатов органа, подписывающего списки отклонений, и другие типы сертификатов, выпущенные этим CA).

В приложении электронного МСПД секционированные CRL не используются. Все сертификаты, отозванные CSCA, включая сертификаты DS, сертификаты CSCA; сертификаты органа, подписывающего мастер-списки, и сертификаты органа, подписывающего списки отклонений, перечисляются в одном и том же CRL. Хотя CRL всегда подписывается самым последним (текущим) закрытым ключом подписи CSCA, CRL включает уведомление по сертификатам, подписанным тем же закрытым ключом, а также по сертификатам, подписанным предыдущими закрытыми ключами подписи CSCA.

4.1.5.1 Отзыв сертификатов CSCA

Отзыв сертификата CSCA является одновременно крайней и сложной мерой. После информирования принимающего государства об отзыве сертификата CSCA все другие сертификаты, подписанные с использованием соответствующего закрытого ключа CSCA, фактически отзываются.

Если связующий сертификат CSCA был подписан с использованием старого закрытого ключа CSCA для подтверждения нового открытого ключа CSCA (см. "Замена ключа национального CA с правом подписи" в разделе 4.1.4.3), то отзыв старого сертификата CSCA также влечет за собой ОТЗЫВ нового сертификата CSCA.

Если необходимо отозвать сертификат CSCA, то CSCA может выпустить CRL, подписанный закрытым ключом, который соответствует отзываемому открытому ключу, поскольку это единственные пользователи ключа в рамках CRL, которых можно верифицировать в этом время. Открытый ключ CSCA следует рассматривать действительным только для целей верификации этой подписи CRL. После верификации подписи CRL пользователем CRL закрытый подписывающий ключ CSCA считается скомпрометированным, а сертификат отозванным для всех будущих верификаций.

Для выдачи новых документов государство или организация выдачи ДОЛЖНЫ вернуться к начальной загрузке своего процесса аутентификации путем выпуска нового исходного сертификата CSCA, рассылки этого сертификата принимающим государствам и обеспечения внеполосного подтверждения того, что полученный каждым принимающим государством сертификат фактически является текущим аутентичным сертификатом CSCA.

4.1.5.2 Отзыв других сертификатов

Когда государство или организация выдачи решают отозвать сертификат, выданный CSC, им не надо ждать до тех пор, пока истечет очередной период обновления текущего CRL для составления нового CRL. Новый CRL РЕКОМЕНДУЕТСЯ выпускать в течение 48 ч с момента уведомления об отзыве.

4.1.6 Криптографические алгоритмы

Государство или организация выдачи МОГУТ поддерживать различные алгоритмы для использования в своих CSCA и ключах подписи сертификатов. Например, CSCA мог осуществить выдачу с использованием алгоритм RSA, однако сертификаты подписывающих органов могут определяться эллиптической кривой DSA (ECDSA) и на оборот.

Государства или организации выдачи ВЫБИРАЮТ надлежащую длину ключей, обеспечивающую защиту от атак. СЛЕДУЕТ учитывать соответствующие криптографические каталоги.

Принимающие государства ДОЛЖНЫ поддерживать все алгоритмы в пунктах, где они намерены проверять подлинность подписи на электронных МСПД.

Для использования в своих CSCA, ключах подписи документов и, где применимо, объектах защиты документов, государства или организации выдачи ПОДДЕРЖИВАЮТ один из нижеуказанных алгоритмов.

4.1.6.1 RSA

Государства или организации выдачи, применяющие алгоритм RSA для генерирования подписи и верификации сертификатов и объекта защиты документа (SO_D), ИСПОЛЬЗУЮТ документ [RFC 4055]. В документе [RFC 4055] определены два механизма подписи: RSASSA-PSS и RSASSA-PKCS1_v15. Государствам или организациям выдачи РЕКОМЕНДУЕТСЯ генерировать подписи в соответствии с RSASSA-PSS, но принимающие государства ДОЛЖНЫ также быть готовы верифицировать подписи, соответствующие RSASSA-PKCS1_v15.

4.1.6.2 Алгоритм цифровой подписи (DSA)

Государства или организации выдачи, применяющие алгоритм DSA для генерирования или верификации подписей, ИСПОЛЬЗУЮТ стандарт [FIPS 186-4].

4.1.6.3 DSA на основе эллиптической кривой (ECDSA)

Государства или организации выдачи, применяющие алгоритм ECDSA для генерирования или верификации подписи, ИСПОЛЬЗУЮТ стандарты [X9.62] или [ИСО/МЭК 15946]. Параметры области эллиптической кривой, используемые для генерирования пары ключей ECDSA, ДОЛЖНЫ быть ясно описаны в параметрах открытого ключа, т. е. параметры ДОЛЖНЫ быть типа EC-параметров (без наименованных кривых, без подразумеваемых параметров) и ДОЛЖНЫ включать факультативный сомножитель. Точки EC ДОЛЖНЫ быть в несжатом формате.

РЕКОМЕНДУЕТСЯ следовать рекомендациям, изложенным в документе [TR 03111].

4.1.6.4 Алгоритмы хэширования

SHA-224, SHA-256, SHA-384 и SHA-512 являются единственными разрешенными алгоритмами хэширования. См. документ [FIPS 180-2].

4.1.7 Криптографические алгоритмы для органов, подписывающих сертификаты LDS2

Поскольку сертификаты LDS2 и подписанные объекты хранятся на бесконтактной ИС, они должны быть в максимально возможной степени компактными. В этой связи, органы, подписывающие LDS2, ДОЛЖНЫ использовать ECDSA независимо от алгоритма, использовавшегося в ключах CSCA и органах, подписывающих документы.

4.1.8 Криптографические алгоритмы для органов, подписывающих визы или сертификаты ETD

Органы, подписывающие визы или ETD, ДОЛЖНЫ использовать ECDSA независимо от алгоритма, использовавшегося в ключах CSCA и органах, подписывающих документы.

4.2 Авторизация PKI

Государства и организации выдачи, реализующие LDS2, ИМЕЮТ следующие типы пар ключей:

- пара ключей национального CA с правом верификации (CVCA);
- пара ключей органа по верификации (DV);
- пара ключей терминала.

Открытые ключи CVCA и DV сертифицируются CVCA. Открытые ключи терминалов сертифицируются DV. Сертификаты открытых ключей CVCA, DV и терминалов представляют собой сертификаты, верифицируемой карточкой, которые ДОЛЖНЫ отвечать требованиям своих соответствующих профилей сертификатов, определенных в разделе 7. В отношении сертификатов CVCA, DV или терминалов механизм отзыва отсутствует. В этой связи сроки их действия являются намного меньшими, чем сроки действия типов сертификатов X.509.

Период использования закрытого ключа конкретно не указывается, поэтому он определяется по усмотрению государства. Однако период использования открытого ключа ДОЛЖЕН, как максимум, быть равным периоду действия открытого ключа. Информация о периоде действия открытого ключа пар ключей CVCA, DV и терминала приводится в таблице 2.

Таблица 2. Период действия верифицируемого карточкой сертификата на использование ключа

	Срок действия открытого ключа
CVCA	6 месяцев – 3 года
DV	2 недели – 3 месяца
Терминал	1 день – 1 месяц

4.2.1 Криптографические алгоритмы для аутентификации терминалов

Алгоритм, используемый для аутентификации терминалов при авторизации PKI, определяется CVCA государства, выдающего электронные МСПД. В рамках цепочки сертификатов (т. е. сертификатов CVCA, DV и терминалов для заданной авторизации) ДОЛЖНЫ использоваться аналогичные алгоритмы подписей, параметры доменов и размеры ключей. В этой связи органам по верификации документов и терминалам потребуется предоставить несколько пар ключей. Связующие сертификаты CVCA МОГУТ включать открытый ключ, получаемый на основе действующих параметров, т. е. CVCA МОЖЕТ переключиться на новый алгоритм подписи, новые параметры домена или размеры ключей.

Для аутентификации терминалов МОГУТ использоваться RSA или ECDSA. Подробная информация приводится в части 11 документа Doc 9303.

4.2.2 Криптографические алгоритмы для SPOC

Перечень наборов для кодирования TLS, подлежащих использованию в рамках протокола SPOC, приводится в таблице 3.

Таблица 3. Наборы для кодирования TLS

Набор шифрования	Сертификат и алгоритм обмена ключами
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA

В ходе согласования TLS клиент ПОДДЕРЖИВАЕТ все наборы шифрования TLS, определенные в таблице 3. Сервер и клиент ПОДДЕРЖИВАЮТ RSA и аутентификацию, основанную на ECDSA. Серверу разрешается направлять запрос, а клиенту – посылать сертификат клиента, тип которого отличается от сертификата сервера.

Использование соглашения относительно ключей ECDHE_ECDSA при согласовании TLS производится в соответствии с дополнениями, определенными в документах [TLSECC], [TLS1.2] и [TLSEXT]. Клиент и сервер ПОДДЕРЖИВАЮТ соответствующие расширения эллиптических кривых, как указано в спецификации [TLSECC], используемой в рамках согласования TLS. Поддерживаемые эллиптические кривые и форматы точек EC определяются в разделе 5 документа [TLSECC]. Использование дополнительных наборов шифрования TLS, определенных в таблице 3, в которой для шифрования предусматривается применение усовершенствованного стандарта шифрования (AES), ПРОИЗВОДИТСЯ в соответствии со спецификацией [TLSAES].

5. МЕХАНИЗМЫ РАССЫЛКИ

Для PKI электронных МСПД принимающим государствам необходимо рассылать объекты PKI. Используется целый ряд различных механизмов рассылки в зависимости от типа объекта и эксплуатационных требований. Важно отметить, что рассылка этих объектов НЕ устанавливает доверие к этим объектам или к связанным с ними закрытым/ открытым ключам. Механизмы создания доверия изложены в разделе 6.1.

Механизм рассылки для авторизации PKI рассматривается в разделе 8.

Объекты, которые государствам или организациям выдачи необходимо рассылать принимающим государствам, включают следующее:

- сертификаты CSCA;
- связующие сертификаты CSCA;
- сертификаты органов, подписывающих документы;
- сертификаты органов, подписывающих LDS2;
- первоначальные сертификаты CVCA;
- связующие сертификаты CVCA;
- сертификаты DV;
- сертификаты органов, подписывающих штрих-коды;
- списки CRL (null (пустые) и non-null (не пустые));
- сертификаты органа, подписывающего мастер-списки; мастер-списки;
- сертификаты органа, подписывающего списки отклонений; списки отклонений.

Механизмы рассылки, используемые в PKI электронных МСПД и авторизации, включают следующее:

- ДОК;
- двусторонний обмен;
- SPOC;
- мастер-списки;
- списки отклонений;
- бесконтактные ИС электронных МСПД.

Для каждого объекта устанавливается первичный и вторичный (в соответствующих случаях) механизм рассылки, как это определено в таблице 4.

Таблица 4. Рассылка объектов PKI

	Бесконтактная ИС	SPOC	Двусторонний обмен	PKD	Список отклонений	Мастер-список	Примечания
Сертификаты CSCA			Y (основной)			Y (дополн.)	
Сертификаты органов, подписывающих документы	Y (основной)			Y (дополн.)			Сертификаты, внесенные одновременно с внесением SOD
Сертификаты органов, подписывающих LDS2	Y						Сертификаты, внесенные одновременно с внесением подписанных объектов
Первоначальный сертификат CVCA	Y						Сертификат, внесенный в процессе персонализации электронного МСПД
Связующие сертификаты CVCA	Y	Y					Сертификаты, рассылаемые DV через центры SPOC и якорь доверия CVCA и обновляемые на бесконтактной ИС при следующей верификации
Сертификаты DV		Y					Рассылаются только адресным DV
Списки CRL (нулевые и не нулевые)			Y (дополн.)	Y (основной)			CRL, выданные CSCA, содержат информацию об отзывах, касающуюся объектов PKI LDS2
Сертификаты органов, подписывающих мастер-списки						Y	
Сертификаты органов, подписывающих штрих-коды			Y (дополн.)	Y (основной)			Информация об органах, подписывающих штрих-коды, в штрих-кодах не кодируется, поэтому для валидации штрих-кода рассылка должна гарантироваться
Мастер-списки			Y	Y			
Сертификаты органов, подписывающих списки отклонений					Y		

Технически принимающие государства не обязаны использовать оба источника, т. е. и первичный и вторичный. В процессе повседневной эксплуатации системы проверки решение о том, использовать ли первичный или вторичный источник, принимает проверяющий полномочный орган. Если в своей повседневной деятельности проверяющий полномочный орган принимающего государства использует вторичный источник для сертификата или CRL, тем не менее, ему следует быть готовым использовать также первичный источник.

Государствам или организациям выдачи необходимо планировать свои стратегии смены пары ключей как для ключей CSCA, так и для ключей органов, подписывающих документы, с целью обеспечения своевременной передачи сертификатов и CRL в системы пограничного контроля принимающих государств. В идеальном случае передача будет происходить в течение 48 ч, однако некоторые принимающие государства могут иметь удаленные и плохо подключенные пограничные посты, и для передачи в них сертификатов и CRL может требоваться больше времени. Принимающим государствам СЛЕДУЕТ делать все возможное для рассылки сертификатов и CRL всем пограничным пунктам в течение 48 ч.

Государствам или организациям выдачи следует ожидать, что сертификаты CSCA (C_{CSCA}) будут распространяться принимающими государствами в течение 48 ч.

Государства или организации выдачи обеспечивают своевременное распространение сертификатов органов, подписывающих документы (C_{DS}), путем включения таких сертификатов в объекты защиты документов (SO_D). Им следует ожидать, что сертификаты органов, подписывающих документы (C_{DS}), опубликованные в ДОК, также будут рассылаться пограничным пунктам в течение 48 ч.

В цифровые печати информация о сертификатах органов, подписывающих штрих-коды, не вносится. Поэтому страна, выдающая документы, защищенные цифровыми печатями, ДОЛЖНА публиковать информацию обо всех своих органах, подписывающих штрих-коды. Основным каналом рассылки сертификатов организаций, подписывающих штрих-коды, являются ДОК/двусторонние каналы. Другие механизмы, например размещение информации на веб-сайтах, являются дополнительными каналами.

Публикация информации об органах, подписывающих штрих-коды, ДОЛЖНА осуществляться на основе следующих принципов:

- после оформления сертификата информация о нем ДОЛЖНА публиковаться с задержкой, не превышающей 48 ч;
- опубликованная информация о сертификатах ДОЛЖНА сохраняться до истечения срока их действия или отзыва.

Принимающим государствам СЛЕДУЕТ делать все возможное, используя либо электронные, либо другие средства, для реагирования на CRL, включая CRL, выпущенные в исключительных обстоятельствах.

Своевременное распространение сертификатов органа, подписывающего мастер-списки, обеспечивается путем включения их в каждый мастер-список.

5.1 Механизм рассылки через ДОК

ИКАО предоставляет услуги директории открытых ключей (ДОК). Этот вид услуг ПРИНИМАЕТ объекты PKI, включая сертификаты, CRL и мастер-списки, от участников ДОК, хранит их в директории и обеспечивает доступ к ним для всех принимающих государств.

Сертификаты CSCA (C_{CSCA}) не хранятся отдельно в рамках предоставляемого ИКАО обслуживания ДОК. Однако они могут присутствовать в ДОК, если они не содержатся в мастер-списках.

Каждый сертификат остается в ДОК до тех пор, пока не истечет срок его действия, независимо от того, используется ли по-прежнему соответствующий закрытый ключ.

Сертификаты, CRL и мастер-списки, хранимые в ДОК всеми участниками ДОК, ПРЕДОСТАВЛЯЮТСЯ всем сторонам (в том числе сторонам, не участвующим в ДОК), которым эта информация необходима для подтверждения аутентичности и целостности хранящихся в цифровой форме данных электронных МСПД, объектов LDS2 и объектов VDS.

5.1.1 Загрузка ДОК

Загружать в ДОК сертификаты, списки CRL и мастер-списки МОГУТ только участники ДОК. Все сертификаты и CRL ДОЛЖНЫ соответствовать профилям, описанным в разделе 7. Все мастер-списки ДОЛЖНЫ удовлетворять спецификациям, изложенным в разделе 9.

ДОК состоит из "Директории для записи" и "Директории для чтения". Для загрузки своих объектов в "Директорию для записи" участники ДОК ИСПОЛЬЗУЮТ упрощенный протокол доступа к каталогу (LDAP). После верификации цифровой подписи на объекте и выполнения других надлежащих проверок в рамках мер предосторожности указанный объект публикуется в "Директории для чтения".

5.1.2 Скачивание ДОК

Доступ с правом чтения ко всем сертификатам, CRL и мастер-спискам, опубликованным в ДОК, ПРЕДОСТАВЛЯЕТСЯ как участникам ДОК, так и не участвующим сторонам. Контроль доступа в случае доступа к ДОК с правом чтения НЕ ОСУЩЕСТВЛЯЕТСЯ.

В сферу ответственности принимающего государства входят рассылка скачанных из ДОК объектов своим системам проверки и поддержание текущей буферной памяти CRL вместе с сертификатами, необходимыми для верификации подписи на данных электронного МСПД.

5.2 Механизм рассылки через канал двустороннего обмена

Основным каналом рассылки CRL и сертификатов CSCA (C_{CSCA}) является двусторонний обмен между государствами или организациями выдачи и принимающими государствами. Двусторонний обмен может также использоваться для рассылки мастер-списков.

Конкретный метод, используемый при таком двустороннем обмене, может быть различным в зависимости от политики каждого государства или организации выдачи, у которых имеется потребность в рассылке своих сертификатов, CRL и мастер-списков, а также от политики каждого принимающего государства, которому необходим доступ к таким объектам. К примерам методов, которые могут использоваться при двустороннем обмене, относятся:

- дипломатический курьер/дипломатическая почта;
- обмен электронными сообщениями;
- скачивание данных с веб-сайта, связанного с выдающим CSCA;
- скачивание данных с сервера LDAP, связанного с выдающим CSCA.

Данный перечень не является исчерпывающим, и могут также использоваться другие методы.

5.3 Механизм рассылки мастер-списков

Мастер-списки являются поддерживающей технологией для схем двусторонней рассылки. В этом качестве рассылка сертификатов CSCA посредством мастер-списков является разновидностью схемы двусторонней рассылки.

Мастер-список представляет собой оформленный с помощью цифровой подписи список сертификатов CSCA, которым "доверяет" принимающее государство или организация, выпустившее мастер-список. В мастер-список могут быть включены самоподписанные исходные сертификаты CSCA и связующие сертификаты CSCA. Структура и формат мастер-списка определены в разделе 8. Выпуск мастер-списка позволяет другим принимающим государствам или организациям получать набор сертификатов CSCA из единого источника (орган, выпускающий мастер-списки), а не заключать соглашение о прямом двустороннем обмене с каждым полномочным органом или организацией выдачи, представленными в этом списке.

Орган, подписывающий мастер-списки, уполномочен CSCA составлять, подписывать в цифровой форме и выпускать мастер-списки. Мастер-списки НЕ ДОЛЖНЫ подписываться и выпускаться непосредственно CSCA. Сертификаты органа, подписывающего мастер-списки, ДОЛЖНЫ удовлетворять профилю сертификата, определенному в разделе 7.

Прежде чем выпустить мастер-список, органу, выпускающему мастер-списки, СЛЕДУЕТ провести всестороннюю проверку сертификатов CSCA, подлежащих визированию, в том числе убедиться в их действительной принадлежности к соответствующим CSCA. Процедуру, используемую для внеполосной валидации, СЛЕДУЕТ отразить в политике применения сертификатов, опубликованной CSCA, который выпустил сертификат органа, подписывающего мастер-списки.

Каждый мастер-список ДОЛЖЕН включать сертификат органа, подписывающего мастер-списки, который будет использоваться для верификации подписи на этом мастер-списке, а также сертификатов того самого CSCA, который выпустил сертификат данного органа, подписывающего мастер-списки.

Если принимающее государство получило новые сертификаты CSCA и завершило свои процедуры валидации, РЕКОМЕНДУЕТСЯ составить и выпустить новый мастер-список.

Для некоторых принимающих государств использование мастер-списка не обеспечивает более эффективной рассылки сертификатов CSCA. Однако принимающее государство, использующее мастер-списки, тем не менее ДОЛЖНО определить свою политику установления доверия к сертификатам, содержащимся в этом списке (подробная информация приводится в разделе 6).

6. ДОВЕРИЕ И ВАЛИДАЦИЯ В РАМКАХ PKI

Доверие и валидация PKI электронных МСПД и PKI авторизации отличаются.

6.1 PKI электронных МСПД

В контексте электронных МСПД системы проверки в принимающих государствах играют роль пользователей PKI. Успешная верификация цифровой подписи на объекте защиты документа электронного МСПД обеспечивает аутентичность и целостность данных, хранящихся на бесконтактной ИС этого электронного МСПД. Указанный процесс верификации подписи требует от пользователя установить, что использованный для верификации подписи открытый ключ лица, подписавшего документ, сам является "доверительным".

Различные механизмы рассылки, изложенные в разделе 5, позволяют принимающим государствам получить доступ к сертификатам и CRL, в которых им необходимо верифицировать соответствующие цифровые подписи. Однако эти схемы рассылки не создают доверия к этим сертификатам, CRL или открытым ключам, которые будут использоваться для верификации подписи на указанных сертификатах и CRL.

Открытые ключи, содержащиеся в сертификатах CSCA (CCSCA), используются для верификации цифровых подписей на сертификатах и списках CRL. Поэтому для принятия электронного МСПД другого государства выдачи принимающее государство ДОЛЖНО предварительно поместить в какое-либо доверительное хранилище, доступное его системе пограничного контроля, достоверную копию сертификата CSCA (CCSCA) государства или организации выдачи или извлеченную из этого сертификата информацию "якоря доверия" другой формы для данного открытого ключа CSCA.

Установление доверия к сертификатам CSCA (C_{CSCA}) и хранение сертификатов (или информации, извлеченной из сертификатов) в качестве "якоря доверия" защищенным способом для использования системами проверки своих пограничных органов являются обязанностью принимающего государства.

6.1.1 Управление механизмом "якоря доверия"

Как указано в документе [RFC 5280], должен быть установлен "якорь доверия", который можно использовать в качестве точки опоры в процедуре валидации конкретного сертификата лица, подписывающего документы, органа, подписывающего мастер-списки, органа, подписывающего списки отклонений, или сертификата иного типа.

Каждый "якорь доверия" состоит из доверительного открытого ключа и соответствующих метаданных. "Якорь доверия" ДОЛЖЕН, как минимум, включать следующее:

- доверительный открытый ключ и любые соответствующие параметры ключа;
- алгоритм открытых ключей;
- имя владельца ключа;
- значение расширения "альтернативное имя субъекта" сертификата CSCA, содержащее трехбуквенный код ИКАО, присвоенный полномочному органу или организации выдачи. Хотя оно не используется в пути сертификации или процедурах валидации CRL, его применяют в процессе пассивной аутентификации, определенной в части 11 документа Doc 9303.

В приложении электронного МСПД для каждого открытого ключа данного CSCA устанавливается отдельный "якорь доверия". Для начального открытого ключа, полученного от CSCA, доверие ДОЛЖНО устанавливаться через внеполосный механизм. Например, если сертификат CSCA был скачан с сервера, связанного с CSCA, для проверки того, что скачанный сертификат действительно является аутентичным сертификатом этого CSCA, может быть использована внеполосная связь (например, телефон или электронная почта). Кроме того, пользователь может проанализировать политику, процедуры и практику выдающего CSCA для выяснения, достаточно ли они надежны, чтобы удовлетворять местным требованиям к использованию сертификатов. После установления начального "якоря доверия" применительно к данному CSCA этот процесс для последующих ключей того же CSCA может быть упрощен. Если CSCA выпускает связующий сертификат CSCA, то внеполосная связь с CSCA для верификации аутентичности нового сертификата может быть опущена, поскольку для верификации подписи на этом связующем сертификате CSCA используется уже доверительный открытый ключ.

Информация "якоря доверия" может храниться в доверительной копии самого сертификата CSCA или в каком-нибудь другом доверительном формате.

Поскольку подписи на сертификатах, выпущенных CSCA, необходимо верифицировать еще в течение длительного времени после того, как этот CSCA обновит свою пару ключей, принимающее государство в любой данный момент будет, как правило, иметь несколько "якорей доверия" для того же CSCA. Если какой-либо CSCA сменил имя, то в некоторых из этих "якорей доверия" будет содержаться старое имя CSCA, а в других – новое имя.

6.1.2 Валидация сертификатов/CRL и проверка их отзыва

В рамках процесса верификации аутентичности и целостности объектов данных в приложении электронного МСПД (например, объекты защиты документа, мастер-списки, списки отклонений и т. д.) принимающее государство:

- валидирует сертификат, используемый для верификации подписи на объекте данных (например, сертификат лица, подписывающего документы, сертификат органа, подписывающего мастер-списки, сертификат органа, подписывающего списки отклонений);
- валидирует CRL, используемый для проверки статуса отзыва соответствующего сертификата;
- обрабатывает CRL для верификации статуса отзыва соответствующего сертификата.

Для таких процессов существуют образцы алгоритмов, например, указанные в документе [RFC 5280]. Принимающим государствам нет необходимости применять конкретный алгоритм, указанный в документе RFC 5280, но они ДОЛЖНЫ обеспечить эквивалентную функциональность внешнего поведения, получаемую в результате этой процедуры. В том или ином конкретном варианте реализации можно использовать любой алгоритм, если он дает правильный результат.

В добавлении D содержатся рекомендации для принимающих государств, которые предпочитают основывать свой алгоритм на варианте, описанном в документе [RFC 5280].

6.1.3 Полномочный орган по валидации штрих-кодов

Полномочный орган по валидации штрих-кодов осуществляет проверку цифровой печати на основе применения политики валидации. Подробная информация о критериях валидации и алгоритмах формирования статуса валидации содержится в части 13 документа Doc 9303.

Рис. 4 иллюстрирует функциональную архитектуру полномочного органа по валидации штрих-кодов. Полномочный орган по валидации штрих-кодов использует программные средства валидации, которые могут быть реализованы на любом компьютере органов пограничного контроля.

Программные средства валидации работают в комплекте со считывающим устройством, использующим изображение штрих-кода для извлечения штрих-кода и МСЗ документа, а также изображение документа для извлечения информации его МСЗ. Для проверки достоверности подписи цифровой печати СЛЕДУЕТ обеспечить синхронизацию программных средств валидации с пунктом публикации PKI по крайней мере каждые 24 часа с целью получения самых последних сертификатов органов, подписывающих штрих-коды, и CRL.

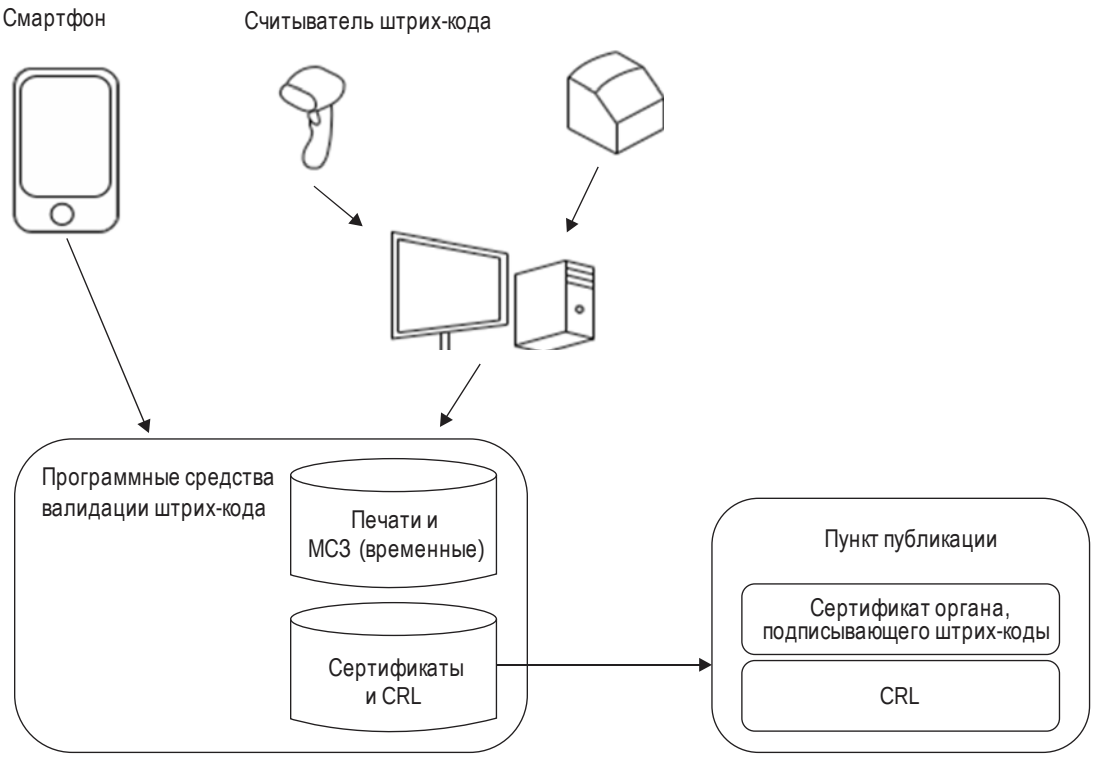

Рис. 4. Валидация штрих-кода

Программные средства валидации штрих-кода расшифровывают цифровую печать и МСЗ любых соответствующих документов (например, виз или паспорта), валидируют подпись цифровой печати и применяют политику валидации (см. часть 13 документа 9303) для формирования статуса валидации документа.

В рамках мобильных сценариев программные средства валидации могут также непосредственно использоваться на смартфонах. В тех случаях, когда достоверность печати можно проверить с помощью программного обеспечения смартфона, НЕОБХОДИМО провести сравнение (подписанных) данных, содержащихся в печати, с данными, внесенными в МСЗ (например, данных визы или паспорта), вручную или посредством OCR МСЗ, из захваченного изображения, что зачастую на практике является сложной проблемой.

Указанные ниже данные обрабатываются программными средствами валидации штрих-кода:

- входные данные, предоставляемые считывающими устройствами, например, изображения виз и паспортов;
- сертификаты и списки CRL.

6.2 Авторизация PKI

При авторизации PKI процессы обработки информации о "якорях доверия" и валидации отличаются.

6.2.1 Валидация сертификатов, верифицируемых карточкой

В отношении сертификатов DV и терминалов, используемых в процессе авторизации PKI, "якорем доверия" является самый последний открытый ключ CVCA государства, выдавшего электронный МСПД. На этапе изготовления или (предварительной) персонализации информация о первоначальном "якоре доверия" надежно ХРАНИТСЯ в бесконтактной ИС электронного МСПД. В связи с тем, что с течением времени пара ключей, используемых CVCA, изменяется, выпускаются связующие сертификаты CVCA. Бесконтактная ИС электронного МСПД ДОЛЖНА обеспечивать внутреннее обновление информации о своем "якоре(ях) доверия" в соответствии с полученным и действующим связующим сертификатом. В связи с установлением очередности выдачи связующих сертификатов CVCA в любой момент времени на бесконтактной ИС будет храниться информация максимум о двух "якорях доверия" CVCA.

Для валидации сертификата терминала бесконтактной ИС электронного МСПД ДОЛЖНА быть представлена цепочка сертификатов с началом в "якоре доверия", хранимом на бесконтактной ИС электронного МСПД.

Процедура валидации, используемая в отношении DV и сертификатов терминалов, для протокола аутентификации терминалов LDS2 является специфичной и подробно рассматривается в части 11 документа Doc 9303.

7. ПРОФИЛИ СЕРТИФИКАТОВ И CRL

Профили сертификатов определяются как для PKI электронных МСПД, так и для PKI авторизации.

7.1 PKI электронных МСПД

Государства или организации выдачи ДОЛЖНЫ выпускать сертификаты и CRL, соответствующие указанным ниже профилям. Все сертификаты и CRL ДОЛЖНЫ создаваться в формате особого правила кодирования (DER) для сохранения целостности содержащихся в них подписей. Профили сертификатов CSCA и DS, которые были включены в шестое издание этих спецификаций, отличаются по некоторым областям от текущих профилей. Системы проверки ДОЛЖНЫ быть способны обрабатывать сертификаты, которые были выпущены в соответствии с теми более ранними профилями (см. добавление C), а также текущими профилями.

Указанные профили основаны на требовании о том, что каждое государство, или организация, или орган выдачи СОЗДАЮТ единый CSCA для целей подписания всех электронных МСПД, отвечающих спецификациям документа Doc 9303.

Профили сертификата определяются в настоящем разделе для следующих типов сертификата:

- национальный CA с правом подписи;
- орган, подписывающий документы;
- орган, подписывающий мастер-списки CSCA;
- орган, подписывающий списки отклонений;
- средства связи – даже если это не является абсолютно необходимым элементом в настоящее время. Это – будущий этап подтверждения. Указанные сертификаты могут использоваться для доступа к ДОК или для связи между государствами с применением LDAP/электронной почты/ HTTP. Рекомендуется, чтобы эти сертификаты издавались CSCA.

Объекты национального CA с правом подписи, органа, подписывающего документы, органа, подписывающего списки отклонений, и органа, подписывающего мастер-списки CSCA, определяются в разделе 3.

Профиль CRL определяется в разделе 7.1.4.

Для указания требований в отношении присутствия, предусмотренных каждым из компонентов/ расширений, профили используют следующую терминологию:

m обязательное – поле ДОЛЖНО присутствовать;
x не использовать – поле НЕ ДОЛЖНО присутствовать;
o факультативное – поле МОЖЕТ присутствовать.
C условно обязательное – поле ПРИСУТСТВУЕТ при определенных условиях.

Для требований в отношении критичности расширений, которые могут/должны быть включены, профили используют следующую терминологию:

c критичное – принимающие приложения ДОЛЖНЫ быть способны обрабатывать это расширение;
nc не критичное – принимающие приложения, которые не распознают это расширение, МОГУТ его игнорировать.

Некоторые из требований, указанных в этих профилях, унаследованы от упоминаемых здесь базовых профилей (например, RFC 5280). Для удобства соответствующие выдержки из базового профиля, которые охватывают данное конкретное требование, воспроизводятся в таблице в добавлении B.

7.1.1 Профили сертификатов

В таблице 5 определены предусмотренные профилем сертификатов и общие для всех сертификатов требования к полям основной части сертификата. В таблице 6 указаны требования к расширениям сертификатов.

Таблица 5. Профиль полей сертификата

Компонент сертификата	***Присутствие***	***Замечания***
Сертификат	m	
СертификатTBS	m	См. таблицу 6
Алгоритмподписи	m	Вводимые здесь значения зависят от выбранного алгоритма
Значениеподписи	m	Вводимые здесь значения зависят от выбранного алгоритма
СертификатTBS		
версия	m	ДОЛЖНА быть v3
серийныйНомер	m	ДОЛЖНО быть положительное целое число и максимум 20 октетов. ДОЛЖНО использоваться дополнительное кодирование 2's и представление с наименьшим количеством октетов

Компонент сертификата	*Присутствие*	*Замечания*
подпись	m	Вводимое здесь значение ДОЛЖНО быть таким же, как в компоненте Алгоритмподписи последовательности Сертификат
выдающийорган	m	названиестраны и серийныйНомер, если таковые присутствуют, ДОЛЖНЫ быть ПечатаемойСтрокой. Другие атрибуты, имеющие синтаксис СтрокиКаталога, ДОЛЖНЫ быть либо ПечатаемойСтрокой, либо СтрокойформатаUTF8. названиетраны ДОЛЖНО состоять из прописных букв. Информация по соглашениям об именовании приводится в п. 7.1.1.1
срок действия	m	Данные ДОЛЖНЫ заканчиваться буквой Z. Элемент "секунды" ДОЛЖЕН присутствовать. Сроки вплоть до 2049 года ДОЛЖНЫ указываться в форматеВремениUTC. ВремяUTC ДОЛЖНО быть представлено в виде YYMMDDHHMMSSZ. Сроки после 2050 года ДОЛЖНЫ указываться в обобщенномформатеВремени. ОбобщенныйформатВремени НЕ ДОЛЖЕН содержать долей секунд. ОбобщенныйформатВремени ДОЛЖЕН быть представлен в виде YYYYMMDDHHMMSSZ
субъект	m	Названиестраны и серийныйНомер, если таковые присутствуют, ДОЛЖНЫ быть ПечатаемойСтрокой. Другие атрибуты, имеющие синтаксис СтрокиКаталога, ДОЛЖНЫ быть лицо ПечатаемойСтрокой, либо СтрокойформатаUTF8. Названиестраны ДОЛЖНО состоять из прописных букв. Названиестраны в поле выдающийорган и в поле субъект ДОЛЖНО совпадать. Информация по соглашениям об именовании приводится в п. 7.1.1
ИнформацияобОткрытом Ключесубъекта	m	
УникальныйИдентифи-каторвыдающегооргана	x	
УникальныйИдентифи-каторсубъекта	x	

Компонент сертификата	***Присутствие***	***Замечания***
расширения	m	См. таблицу 6, где указано, какие расширения следует включать. Значения по умолчанию для расширений НЕ ДОЛЖНЫ шифроваться

Таблица 6. Профиль расширений сертификата

Название расширения	***Самоподписанные исходные сертификаты CSCA***		***Связующие сертификаты CSCA***		***Орган, подписывающий документы***		***Орган, подписывающий мастер-списки, и орган, подписывающий списки отклонений***		***Средства связи***		***Замечания***
	Присутствие	***Критичность***	***Присутствие***	***Критичность***	***Присутствие***	***Критичность***	***Присутствие***	***Критичность***	***Присутствие***	***Критичность***	
ИдентификаторКлюча Полномочногооргана	**o**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	
Идентификатор ключа	m		m		m		m		m		
полномочныйОрган выдающийсертификат			o		o		o		o		
СерийныйНомерСертификата полномочногооргана	o		o		o		o		o		
ИдентификаторКлюча Субъекта	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
ИдентификаторКлюча субъекта	m		m		m		m		m		
ПрименимостьКлюча	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	
цифроваяПодпись	x		x		m		m		o		Некоторые сертификаты средств связи (например, сертификаты TLS) предусматривают, чтобы биты поля "Применимость ключа" устанавливались в соответствии с конкретным используемым набором шифров. Некоторые наборы шифров требуют установки битов цифровой подписи, а некоторые не требуют

Название расширения	*Самоподписанные исходные сертификаты CSCA*		*Связующие сертификаты CSCA*		*Орган, подписывающий документы*		*Орган, подписывающий мастер-списки, и орган, подписывающий списки отклонений*		*Средства связи*		*Замечания*
неотказуемость	x		x		x		x		x		
Шифрованиеключа	x		x		x		x		o		
Шифрованиеданных	x		x		x		x		x		
Согласованиеключей	x		x		x		x		o		
ПодписьСертификата ключа	m		m		x		x		x		
подписьCRL	m		m		x		x		x		
Толькошифратор	x		x		x		x		x		
Толькодешифратор	x		x		x		x		x		
ПериодПрименимости ЗакрытогоКлюча	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	
неРанее	o		o		o		o		o		ДОЛЖНО присутствовать по крайней мере одно из полей "не ранее" или "не позднее" . ДОЛЖНО шифроваться с использованием обобщенного формата времени
неПозднее	o		o		o		o		o		
Политикаприменения Сертификата	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
ИнформацияоПолитике	m		m		m		m		m		
Идентификаторполитики	m		m		m		m		m		
Квалификаторыполитики	o		o		o		o		o		
СоответствиеПолитик	**x**		**x**		**x**		**x**		**x**		См. примечание 1
АльтернативноеИмя Субъекта	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	См. п. 7.1.1.2
АльтернативноеИмя выдающегооргана	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	См. п. 7.1.1.2
АтрибутыКаталога Субъекта	**x**		**x**		**x**		**x**		**x**		
ОсновныеОграничения	**m**	**c**	**m**	**c**	**x**		**x**		**x**		
cA	m		m		x		x		x		
ОграничениеДлины Пути	m		m		x		x		x		Всегда ДОЛЖНО быть ‘0’
Ограниченияотношении Имени	**x**		**x**		**x**		**x**		**x**		См. примечание 1
Ограниченияотношении Политики	**x**		**x**		**x**		**x**		**x**		См. примечание 1
Расширенная ПрименимостьКлючей	**x**		**x**		**x**		**m**	**c**	**m**	**c**	См. п. 7.1.1.3
ПунктыРаспределения CRL	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	

Название расширения	***Самоподписанные исходные сертификаты CSCA***		***Связующие сертификаты CSCA***		***Орган, подписывающий документы***		***Орган, подписывающий мастер-списки, и орган, подписывающий списки отклонений***		***Средства связи***		***Замечания***
пунктРаспределения	m		m		m		m		m		ДОЛЖНЫ использоваться ldap, http или https См. п. 7.1.1.4
причины	x		x		x		x		x		
орган, выпускающий cRL	x		x		x		x		x		
ЛюбаяПолитикаЗапрета	**x**		**x**		**x**		**x**		**x**		См. примечание 1
СамыйсвежийCRL	**x**		**x**		**x**		**x**		**x**		См. примечание 2
частноеРасширение вИнтернете	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	См. примечание 3
ИзменениеИмени	**o**	**nc**	**o**	**nc**	**x**		**x**		**x**		См. п. 7.1.1.5
ТипДокумента	**x**		**x**		**m**	**nc**	**x**		**x**		См. п. 7.1.1.6
Тип Сертификата браузера Netscape	**x**		**x**		**x**		**x**		**x**		См. примечание 4
Другие частные расширения	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	

Примечание 1. Данное расширение, по определению, может появиться только в посреднических сертификатах CA (сертификатах, выданных одним CA другому CA). В PKI электронных МСПД посреднические сертификаты CA не используются. Таким образом, использование этого расширения в сертификатах электронных МСПД запрещено.

Примечание 2. Расширение самого свежего CRL используется для указания дельта-списка. Дельта-список не поддерживается в PKI электронных МСПД. Поэтому данное расширение запрещено.

Примечание 3. Существуют два частных расширения Интернета (доступ к информации полномочного органа и доступ к информации субъекта), определенные в документе RFC 5280, которые используются для указания информации о выдающем органе или субъекте сертификата. Эти расширения не требуются для PKI электронного МСПД. Однако поскольку они не влияют на интероперабельность и не являются критичными, то они могут быть включены на факультативной основе в сертификаты электронных МСПД.

Примечание 4. Расширение типа сертификата браузера Netscape может использоваться для ограничения целей, для которых может использоваться сертификат. Расширения "расширенная применимость ключей" и "основные ограничения" являются в настоящее время стандартными расширениями для таких целей и используются в приложениях электронных МСПД. В связи с потенциальным противоречием между значениями стандартных расширений и собственным расширением браузера Netscape расширение Netscape запрещено.

7.1.1.1 Требования в отношении полей выдающего органа и субъекта

Поля выдающего органа и субъекта являются характерными для всех сертификатов, однако в отношении сертификатов органов, подписывающих LDS2, применяются конкретные ограничения.

7.1.1.1.1 Общие требования

ТРЕБУЮТСЯ следующие соглашения об именовании и адресации для полей выдающего органа и субъекта:

- поле "название страны" ДОЛЖНО присутствовать. Значение содержит код страны, который ДОЛЖЕН соответствовать формату двухбуквенных кодов страны, указанных в части 3 документа 9303;
- поле "обычное название" ДОЛЖНО присутствовать.

По усмотрению государства или организации выдачи МОГУТ быть также включены другие атрибуты.

7.1.1.1.2 Требования в отношении сертификатов органов, подписывающих LDS2

Сертификаты органов, подписывающих LDS2, ДОЛЖНЫ соответствовать определенному выше профилю сертификатов органов, подписывающих документы, за исключением определенных в пункте 7.1.2.

7.1.1.2 Требования в отношении альтернативного имени выдающего органа и субъекта

Поскольку функции, выполняемые альтернативными именами в приложении электронных МСПД, являются специфическими для данного приложения и отличаются от тех, которые определены для PKI Интернета в документе [RFC 5280], содержащиеся в расширении "альтернативное имя субъекта" сертификатов электронных МСПД значения, как правило, не идентифицируют однозначно субъект сертификата.

В приложении электронного МСПД альтернативные имена выполняют следующие две функции.

Первая функция заключается в предоставлении контактной информации для субъекта и/или органа выдачи сертификата. Для этой цели в эту функцию СЛЕДУЕТ включать по крайней мере один из следующих элементов:

- `rfc822Name`;
- `dNSName`; или
- `uniformResourceIdentifier`.

Вторая функция заключается в предоставлении строки каталога, состоящей из присвоенных странам кодов ИКАО. Для этой цели сертификаты, выпущенные с использованием этого профиля, ДОЛЖНЫ дополнительно включать имя каталога, которое строится следующим образом:

- поле `localityName` (`название местности`), содержащее код страны ИКАО, как он представлен в МСЗ;
- если этот код страны не идентифицирует однозначно государство или организацию выдачи, то ИСПОЛЬЗУЕТСЯ атрибут `stateOrProvinceName` (`название государства или провинции`) для указания трехбуквенного кода ИКАО, присвоенного государству или организации выдачи;
- другие атрибуты не разрешены.

В самоподписанных исходных сертификатах CSCA расширения "имя выдающего" и "альтернативное имя субъекта" ДОЛЖНЫ быть идентичны. В связующих сертификатах CSCA значения могут различаться. Например, если произошло изменение в `rfc822Name` (имя rfc822) CSCA непосредственно перед выдачей связующего сертификата CSCA, расширение "альтернативное имя выдающего" будет содержать старое имя `rfc822Name`, а расширение "альтернативное имя субъекта" будет содержать новое имя `rfc822Name`. Любые последующие связующие сертификаты CSCA будут затем содержать новое имя `rfc822Name` в обоих расширениях.

7.1.1.3 Требования расширения "расширенная применимость ключей"

Идентификатором объекта (OID), который должен быть включен в расширение "расширенная применимость ключей" для сертификатов органа, подписывающего мастер-списки, является `2.23.136.1.1.3`.

Идентификатором объекта (OID), который должен быть включен в расширение "расширенная применимость ключей" для сертификатов органа, подписывающего списки отклонений, является `2.23.136.1.1.8`.

Для сертификатов средств связи значение этого расширения зависит от используемого протокола связи (см. раздел 4.2.1.12 документа RFC 5280).

7.1.1.4 Требования расширения "пункты рассылки CRL"

CSCA могут публиковать свои CRL в нескольких местах, включая ДОК, свой собственный веб-сайт и т. д.

Для CRL, которые публикуются в местах, отличных от ДОК (например, веб-сайт или локальный сервер LDAP), значение, подлежащее включению в это расширение, контролируется CSCA, выдающим соответствующие сертификаты и CRL.

В отношении CRL, представленных в ДОК, участники ДОК МОГУТ включить два значения URL для своих CRL, используя нижеследующий шаблон (заменить "код страны" трехбуквенным кодом, присвоенным ИКАО государству или организации выдачи). Если этот код страны не идентифицирует однозначно государство или организацию выдачи, запись будет создана путем добавления символа "_" к трехбуквенному коду страны в МСЗ и затем трехбуквенного кода, присвоенного ИКАО государству или организации выдачи, который однозначно идентифицирует данное государство или данную организацию выдачи:

https://pkddownload1.icao.int/CRLs/CountryCode.crl
https://pkddownload2.icao.int/CRLs/CountryCode.crl

Это расширение является обязательным, и проверки статуса отзыва являются обязательной частью процедуры валидации. Поэтому по крайней мере одно значение ДОЛЖНО быть включено:

- значения ДОК могут быть единственными значениями в этом расширении;
- могут быть дополнительные значения (например, CSCA может также пожелать опубликовать свой CRL на веб-сайте и включить адресную ссылку на этот источник); или
- CSCA может также пожелать включить только одно значение (например, адресную ссылку на свой веб-сайт как источник), даже если он также представляет свой CRL в ДОК.

Нижеследующие примеры иллюстрируют значения ДОК, которые вносились бы в сертификаты, выпускаемые полномочным органом выдачи Сингапура и Гонконга:

пример с ДОК по Сингапуру:
https://pkddownload1.icao.int/CRLs/SGP.crl
https://pkddownload2.icao.int/CRLs/SGP.crl

пример по Гонконгу:
https://pkddownload1.icao.int/CRLs/CHN_HKG.crl
https://pkddownload2.icao.int/CRLs/CHN_HKG.crl

7.1.1.5 Расширение "изменение имени"

После смены ключа CSCA ДОЛЖЕН быть выпущен сертификат, связывающий старый открытый ключ с новым открытым ключом, чтобы обеспечить защищенный переход для пользователей. Обычно это достигается путем выпуска самоизданного сертификата, где поля "выдающий" и "субъект" идентичны, но ключ, использованный для верификации подписи, представляет старую пару ключей, а сертифицированный открытый ключ представляет новую пару ключей.

РЕКОМЕНДУЕТСЯ, чтобы CSCA без необходимости не меняли свои отличительные имена (DN), так как это неблагоприятно сказывается на участниках (они должны сохранять как старые, так и новые имена в качестве действительных имен CSCA для того же государства или той же организации выдачи до тех пор, пока не истечет срок действия всех электронных МСП, подписанных старым именем). Однако если изменение имени необходимо, это ДОЛЖНО быть сообщено участвующим сторонам посредством выпуска связующего сертификата CSCA, в котором поле "выдающий" содержит старое имя, а поле "субъект" содержит новое имя. Этот связующий сертификат CSCA также передает данные о смене ключей, где ключ, используемый для верификации подписи, представляет старую пару ключей, а сертифицированный открытый ключ представляет новую пару ключей. Сертификаты, которые передают данные как об изменении имени CSCA, так и о смене ключей для этого CSCA, ДОЛЖНЫ включать расширение "изменение имени" для идентифицирования сертификата как такового. Это никоим образом не влияет на поле "ограничение длины пути": оно остается "0".

Кроме того, расширение "изменение имени" МОЖЕТ быть также включено в новый самоподписанный сертификат CSCA, созданный после изменения отличительного имени (DN) CSCA. В таком самоподписанном исходном сертификате CSCA как поле "выдающий", так и поле "субъект" содержит новое DN. В отличие от самоподписанного связующего сертификата CSCA, содержащего как старые, так и новые DN CSCA, включение расширения "изменение имени" в самоподписанный исходный сертификат CSCA просто указывает, что имело место изменение имени, и не связывает старое DN с новым.

CSCA НЕ ДОЛЖЕН повторно использовать серийные номера сертификатов. Каждый сертификат, выпущенный CSCA, независимо от того, сменил ли CSCA имя или нет, ДОЛЖЕН быть уникальным.

Формат ASN.1 для расширения "изменение имени":

```
nameChange EXTENSION ::= {
   SYNTAX                NULL
   IDENTIFIED BY     id-icao-mrtd-security-extensions-nameChange}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::=
{id-icao-
mrtd-security-extensions 1}
```

7.1.1.6 Расширение "тип документа"

Расширение "тип документа" ДОЛЖНО использоваться для указания типов документа, аналогичных отраженным в МСЗ, которые разрешено выпускать лицу, подписывающему документы. Данное расширение всегда ДОЛЖНО задаваться как некритичное.

Формат ASN.1 для расширения "перечень типов документа":

```
documentTypeList EXTENSION ::= {
   SYNTAX                DocumentTypeListSyntax
   IDENTIFIED BY     id-icao-mrtd-security-extensions-
documentTypeList}

DocumentTypeListSyntax ::= SEQUENCE {
   version           DocumentTypeListVersion,
   docTypeList       SET OF DocumentType }

DocumentTypeListVersion ::= INTEGER {v0(0)}

-- тип документа, аналогичный отраженному в МСЗ, например, "P" или "ID", где
  одна буква означает все типы документа, начинающегося с этой буквы
DocumentType ::= PrintableString(SIZE(1..2))

id-icao-mrtd-security-extensions-documentTypeList OBJECT
IDENTIFIER ::= {id-icao-mrtd-security-extensions 2}
```

7.1.2 Профиль сертификата органа, подписывающего LDS2

Сертификаты органов, подписывающих LDS2, ДОЛЖНЫ соответствовать профилю сертификата органов, подписывающих документы, определенному в разделе 7.1.1, с учетом следующих исключений:

Поле субъекта:
Поле "субъекта" сертификатов органов, подписывающих LDS2, ДОЛЖНО заполняться следующим образом:

- `Названиестраны`: ДОЛЖНО присутствовать. Это значение содержит код страны, который ДОЛЖЕН соответствовать формату двухбуквенных кодов стран, как указано в части 3 документа Doc 9303.
- `общееНазвание`: ДОЛЖНО присутствовать. Длина этого значения в атрибуте НЕ ДОЛЖНА превышать девять знаков.
- Другие атрибуты включаться НЕ ДОЛЖНЫ.

Расширения сертификатов:
Сертификаты органов, подписывающих LDS2, ДОЛЖНЫ содержать расширения сертификатов, указанные в таблице 7 ниже. Все другие расширения сертификатов включаться НЕ ДОЛЖНЫ.

Таблица 7. Обязательные расширения сертификатов для LDS2

Название расширения	Орган, подписывающий LDS2		Замечания
	Присутствие	Критичность	
ИдентификаторКлючаПолномочногоОргана (AuthorityKeyIdentifier)	**m**	**nc**	
идентификаторКлюча (keyIdentifier)	m		
Орган, выдающий сертификат полномочного органа (authorityCertIssuer)	o		
СерийныйНомерСертификата-полномочногооргана (authorityCertSerialNumber)	o		
ПрименимостьРасширенияКлюча (ExtKeyUsage)	**m**	**c**	См. примечание 1

Примечание 1. Расширение EKU для каждого типа сертификата органа, подписывающего LDS2, ДОЛЖНО заполняться, как указано ниже. Следует отметить, что один орган, подписывающий LDS2, может быть уполномочен подписывать несколько типов объектов данных LDS2. В этом случае в расширении EKU будут содержаться все соответствующие OID этого подписывающего органа:

```
id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}
id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-
security-lds2 8}
```

- LDS2 Travel Stamp Signer (LDS2-TS) certificates
  `id-icao-tsSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 1}`

- LDS2 Visa Signer (LDS2-V) certificates:
  `id-icao-vSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 2}`

- LDS2 Biometrics Signer (LDS2-B) certificates:
  `id-icao-bSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 3}`

Примечание 2. Сертификаты органов, подписывающих LDS2, должны соблюдать ограничения на размер, предусмотренный в части 10 документа Doc 9303 для файла EF.Certificates.

Несмотря на то, что эти сертификаты расширения, касающиеся пунктов рассылки CRL, не включены, обязательной является проверка статуса отзыва каждого сертификата, выполняемая в рамках обычного процесса верификации. CRL, выпущенный CSCA, выдавшим рассматриваемый сертификат, представляет собой CRL, используемый для верификации его статуса отзыва.

7.1.3 Профиль сертификата органа, подписывающего штрих-коды

Сертификаты органов, подписывающих штрих-коды, ДОЛЖНЫ соответствовать профилю сертификатов органов, подписывающих LDS2. Поскольку функция, выполняемая сертификатами органов, подписывающих штрих-коды, отличается от функции сертификатов LDS2, в некоторых отношениях их профили отличаются. В частности, имеются особые требования в отношении отличительного имени (subjectDN) сертификата органа, подписывающего штрих-коды, и серийного номера (см. часть 13 документа Doc 9303).

Поле субъекта:
Поле "субъекта" сертификатов органов, подписывающих штрих-коды, должно заполняться следующим образом:

- `общееНазвание`: ДОЛЖНО присутствовать. ДОЛЖНО включать два прописных знака, иметь формат печатаемой строки, однозначно определяющий орган одной страны, подписывающий штрих-коды, и ДОЛЖНО соответствовать буквам 3 и 4 идентификатора подписывающего органа, как указано в части 13 документа Doc 9303.

- `Названиестраны`: ДОЛЖНО состоять из двухбуквенного кода страны (см. часть 3 документа Doc 9303) органа, подписывающего штрих-коды, включать прописные знаки, иметь формат печатаемой строки и ДОЛЖНО соответствовать буквам 1 и 2 идентификатора подписывающего органа в штрих-коде, как указано в части 13 документа Doc 9303.

- Другие атрибуты включаться НЕ ДОЛЖНЫ.

Расширения сертификатов:
Сертификаты органов, подписывающих штрих-коды, ДОЛЖНЫ содержать расширения сертификатов, указанные в таблице 8 ниже. Все другие расширения сертификатов включаться НЕ ДОЛЖНЫ.

Таблица 8. Расширения, предусмотренные для сертификатов органов, подписывающих штрих-коды

Название расширения	**Орган, подписывающий LDS2**		**Замечания**
	Присутствие	**Критичность**	
ИдентификаторКлючаПолномочногоОргана (AuthorityKeyIdentifier)	**m**	**nc**	
идентификаторКлюча (keyIdentifier)	m		
Орган, выдающий сертификат полномочного органа (authorityCertIssuer)	o		
СерийныйНомерСертификатаполномочногооргана (authorityCertSerialNumber)	o		
ТипДокумента	**o**		Это расширение определяет тип документа, который разрешено выпускать органу, подписывающему штрих-коды
ПрименимостьРасширенияКлюча (ExtKeyUsage)	**m**	**c**	См. примечание ниже

Примечание. Расширение EKU для каждого типа сертификата органа, подписывающего штрих-коды, ДОЛЖНО заполняться, как указано ниже.

```
id-icao-mrtd-security-vds OBJECT IDENTIFIER ::= {id-icao-mrtd-security 11}
id-icao-vdsSigner OBJECT IDENTIFIER ::= {id-icao-mrtd-security-vds 1}
```

7.1.4 Профиль CRL

В таблице 9 определяются требования к профилю CRL для полей тела CRL. В таблица 10 определяются требования к профилю CRL для CRL и расширений записей CRL.

Таблица 9. Профили полей CRL

Компоненты списка сертификатов	*CSCA CRL*	*Замечания*
Списоксертификатов	m	
списоксертификатов tBS	m	См. таблицу 10
Алгоритмподписи	m	Вводимое здесь значение зависит от выбранного алгоритма
Значениеподписи	m	Вводимое здесь значение зависит от выбранного алгоритма
Списоксертификатов tBS		
Версия	m	ДОЛЖНА быть v2
Подпись	m	Вводимое здесь значение ДОЛЖНО быть таким же, как в компоненте Алгоритмподписи последовательности СписокСертификатов
Выдающийорган	m	Названиестраны и серийныйНомер, если таковые присутствуют, ДОЛЖНЫ быть печатаемой строкой. Другие атрибуты, имеющие синтаксис СтрокиКаталога, ДОЛЖНЫ быть либо ПечатаемойСтрокой, либо СтрокойформатаUTF8. Названиестраны ДОЛЖНО состоять из прописных букв
Текущееобновление	m	Данные ДОЛЖНЫ заканчиваться буквой "Z". Элемент "секунды" ДОЛЖЕН присутствовать. Даты вплоть до 2049 года ДОЛЖНЫ указываться в форматевремениUTC. ВремяUTC ДОЛЖНО быть представлено в виде YYMMDDHHMMSSZ. Даты в 2050 году и в последующие годы ДОЛЖНЫ указываться в ОбобщенномФорматеВремени. ОбобщенныйФорматВремени

Компоненты списка сертификатов	***CSCA CRL***	***Замечания***
		НЕ ДОЛЖЕН содержать долей секунд. ОбобщенныйФорматВремени ДОЛЖЕН быть представлен в виде YYYYMMDDHHMMSSZ
следующееОбновление	m	Данные ДОЛЖНЫ заканчиваться буквой "Z". Элемент "секунды" ДОЛЖЕН присутствовать. Сроки вплоть до 2049 года ДОЛЖНЫ указываться в форматеВремениUTC. ВремяUTC ДОЛЖНО быть представлено в виде YYMMDDHHMMSSZ. Сроки после 2050 года ДОЛЖНЫ указываться в ОбобщенномформатеВремени. ОбобщенныйформатВремени НЕ ДОЛЖЕН содержать долей секунд. ОбобщенныйформатВремени ДОЛЖЕН быть представлен в виде YYYYMMDDHHMMSSZ
отозванныеСертификаты	m	ПРИСУТСТВУЕТ, если имеются отозванные сертификаты. Если отозванных сертификатов нет, то этот компонент НЕ ПРИСУТСТВУЕТ. Если таковые имеются, этот компонент НЕ ДОЛЖЕН быть пустым
РасширенияcRL	m	См. таблицу 10, где указано, какие расширения следует включать. Значения по умолчанию для расширений НЕ ДОЛЖНЫ шифроваться

Таблица 10. Профиль расширений CRL и записей CRL

Название расширения	***CSCA CRL***	***Критич-ность***	***Замечания***
Расширения CRL			
Идентификаторключа полномочногооргана	**m**	**nc**	ДОЛЖЕН быть таким же, как значение в поле ИдентификаторКлючасубъекта в сертификате органа выдачи CRL
Идентификаторключа	m		
орган, выдающий Сертификатполномочного органа	o		
СерийныйНомерСертификата полномочного органа	o		

Название расширения	*CSCA CRL*	*Критич-ность*	*Замечания*
Альтернативноеимяоргана выдачи	**o**	**nc**	См. примечание 1
НомерCRL	**m**	**nc**	ДОЛЖЕН быть неотрицательным целым числом длиной максимум 20 октетов. ДОЛЖНО применяться шифрование 2's с использованием дополнительного кода и номер ДОЛЖЕН представляться в формате наименьшего количества октетов
Индикатордельта-спискаCRL	**x**		
выдающийПунктРассылки	**x**		
СамыйсвежийCRL	**x**		
РасширениязаписейCRL			
Кодпричин	**x**		
Кодвременного приостановлениядействия сертификата	**x**		
Датаутратывалидности	**x**		
Органвыдачисертификата	**x**		
Другие частные расширения	**o**	**nc**	

Примечание 1. Если CSCA изменил имя, данное расширение МОЖЕТ быть включено в списки CRL, выпущенные после смены имени CSCA. В случае наличия такового, значение(я) в данном расширении ДОЛЖНЫ быть идентичны значению в поле выдающий орган *сертификата, выпущенного CSCA под предыдущим именем. После истечения срока действия всех сертификатов, выпущенных под предыдущим именем CSCA, упомянутое имя CSCA может быть исключено из последующих CRL. Системы проверки не обязаны обрабатывать это расширение. С учетом того, что документ Doc 9303 ИКАО предписывает наличие единственного CSCA на страну, компонент* названиеСтраны *поля органа выдачи достаточен для однозначной идентификации CSCA. Для верификации подписи CRL используется самый последний открытый ключ CSCA. Поскольку CSCA выпускает единственный CRL, этот CRL охватывает все сертификаты, выпущенные с этим* названиемСтраны*. В дополнение к этой обязательной проверке МОЖЕТ также производиться факультативная проверка того, что значение поля* выдающий орган *данного сертификата идентично значению поля "выдающий орган" списка CRL или одному из значений расширения* АльтернативноеИмявыдающегооргана *в CRL.*

Примечание 2. CRL может содержать другую, связанную с отзывом информацию, касающуюся, например, сертификатов оператора системы или полномочного органа регистрации.

7.2 Авторизация PKI

Авторизация PKI охватывает сертификаты X.509 для SPOC, сертификаты, верифицируемые карточкой для CVCA, DV и терминалов. В настоящем разделе определяются профили для сертификатов SPOC, сертификатов CVCA, DV и IS. Приводится общее описание объектов данных, содержащихся в сертификатах, верифицируемых карточкой, а также рассматривается вопрос о кодировании этих объектов.

7.2.1 Профиль сертификатов SPOC

Для непосредственной выдачи сертификатов SPOC с учетом приводимых ниже ограничений в отношении профилей самоподписываемых сертификатов CA может использоваться отдельная процедура CA:

- сертификат CA ДОЛЖЕН соответствовать положениям документа [RFC 5280];
- SHA-224, SHA-256, SHA-384 и SHA-512 являются единственными разрешенными алгоритмами хэширования;
- `Названиестраны` ДОЛЖНО присутствовать в поле субъекта.

Сертификаты SPOC LDS2 (клиент и сервер) ДОЛЖНЫ соответствовать профилю сертификатов, определенному в разделе 7.1, с учетом следующих ограничений.

Поле выдающего органа:
Сертификаты SPOC выдаются CSCA или отдельным CA, созданным специально для выдачи сертификатов SPOC.

Поле субъекта:
Для сертификатов SPOC LDS2 поле субъекта ДОЛЖНО заполняться следующим образом:

- `Названиестраны`: ДОЛЖНО присутствовать. Это значение содержит код страны, который должен соответствовать формату двухбуквенных кодов стран, как указано в части 3 документа Doc 9303.
- `общееНазвание`: ДОЛЖНО присутствовать. Для сертификатов клиентов TLS SPOC этот СЛЕДУЕТ указывать как "клиент TLS SPOC". Для сертификатов сервера TLS SPOC этот параметр СЛЕДУЕТ указывать как "сервер TLS SPOC ".
- Другие атрибуты МОГУТ включаться по усмотрению государства или организации выдачи.

Расширения применимости ключа
Для сертификатов SPOC параметр(ы) зависит(ят) от используемого набора шифрования.

Расширения альтернативных имен субъектов
В дополнение к параметрам, указанным в профиле сертификата связи, сертификаты сервера TLS SPOC ДОЛЖНЫ также содержать параметр dNSName, являющийся серверной частью SPOC URL.

Расширения более широкой сферы применимости ключа
Для сертификатов клиентов SPOC и сервера НЕОБХОДИМО включить соответствующие параметры, указанные ниже.

- Сертификаты клиентов SPOC: OID = 2.23.136.1.1.10.1;
- Сертификаты сервера SPOC: OID = 2.23.136.1.1.10.2.

Расширения пунктов рассылки CRL
В сертификатах клиентов SPOC и сервера это расширение является обязательным.

7.2.2 Профили сертификатов CVCA, DV и терминалов

Связующие сертификаты CVCA, сертификаты DV и сертификаты терминалов подлежат валидации интегральной схемой (ИС). В связи с вычислительными ограничениями этих чипов сертификаты ДОЛЖНЫ представляться в формате, верифицируемом карточкой (сертификаты CV).

ИСПОЛЬЗУЮТСЯ формат и профиль сертификатов, указанные в таблице 11. Подробная информация о параметрах кодирования содержится в части 11 документа Doc 9303.

Таблица 11. Профиль сертификатов CV

Объект данных	Наличие сертификата
Сертификат CV	m
Тело сертификата	m
Идентификатор профиля сертификата	m
Указатель сертифицирующего полномочного органа	m
Открытый ключ	m
Указатель владельца сертификата	m
Шаблон авторизации владельца сертификата	m
Дата вступления сертификата в силу	m
Дата истечения срока действия сертификата	m
Расширения сертификата	o
Подпись	m

7.2.2.1 Идентификатор профиля сертификата

Версия профиля указывается идентификатором профиля сертификата. ИСПОЛЬЗУЕТСЯ версия 1, идентифицируемая значением 0.

7.2.2.2 Указатель сертифицирующего полномочного органа и указатель владельца сертификата

Каждый сертификат ДОЛЖЕН содержать два указателя открытых ключей (указатель владельца сертификата и указатель сертифицирующего полномочного органа).

Указатель сертифицирующего полномочного органа представляет собой ссылку на (внешний) открытый ключ сертифицирующего полномочного органа (CVCA или DV), которая ИСПОЛЬЗУЕТСЯ для верификации подписи сертификата.

Указатель владельца сертификата является идентификатором для открытого ключа, предоставляемого в сертификате, который подлежит использованию в качестве ссылки на открытый ключ.

Примечание. В этой связи указатель сертифицирующего полномочного органа, содержащийся в сертификате, ДОЛЖЕН быть аналогичным указателю владельца сертификата в соответствующем сертификате сертифицирующего полномочного органа выдачи.

Указатель владельца сертификата СОСТОИТ из следующих конкатенированных элементов: код страны, мнемоническое имя владельца и номер последовательности. Эти элементы ДОЛЖНЫ выбираться в соответствии с таблицей 12 и следующими правилами:

a) код страны:

- код страны СООТВЕТСТВУЕТ двухбуквенному коду страны владельца сертификата, предусмотренному частью 3 документа Doc 9303.

b) мнемоническое имя владельца:

- мнемоническое имя владельца ПРИСВАИВАЕТСЯ в качестве уникального идентификатора следующим образом:
  - мнемоническое имя владельца CVCA ПРИСВАИВАЕТСЯ самим CVCA;
  - мнемоническое имя владельца DV ПРИСВАИВАЕТСЯ национальным CVCA;
  - мнемоническое имя владельца IS ПРИСВАИВАЕТСЯ контролирующим DV.

c) номер последовательности:

- номер последовательности ПРИСВАИВАЕТСЯ владельцем сертификата;
- номер последовательности ДОЛЖЕН быть цифровым или алфавитно-цифровым;
  - цифровой номер последовательности состоит из цифр "0…9".
  - алфавитно-цифровой номер последовательности состоит из цифр "0…9" и букв "A…Z".
- номер последовательности ДОЛЖЕН начинаться с предусмотренного частью 3 документа Doc 9303 двухбуквенного кода страны сертифицирующего полномочного органа, а остающиеся три знака ПРИСВАИВАЮТСЯ в качестве алфавитно-цифрового номера последовательности;
- номер последовательности МОЖЕТ быть восстановлен, если все имеющиеся номера последовательности исчерпаны.

Таблица 12. Указатель владельца сертификата

	Кодирование	**Длина**
Код страны	Doc 9303, часть 3	2F
Мнемоническое имя владельца	ИСО/МЭК 8859-1	9V
Номер последовательности	ИСО/МЭК 8859-1	5F

7.2.2.3 Открытый ключ

В этом поле содержится открытый ключ, подлежащий сертификации.

В самоподписанных сертификатах CVCA ДОЛЖНЫ содержаться параметры доменов. Параметры доменов МОГУТ содержаться в связующих сертификатах CVCA за исключением случаев изменения параметров домена. В этих случаях связующий сертификат ДОЛЖЕН содержать новые параметры домена.

Сертификаты DV и терминалов НЕ ДОЛЖНЫ содержать параметры домена. Параметры домена открытых ключей DV и терминалов наследуются от соответствующего открытого ключа CVCA.

7.2.2.4 Шаблон авторизации владельца сертификата

Функция и авторизация владельца сертификата КОДИРУЮТСЯ в шаблоне авторизации владельца сертификата. Этот шаблон представляет собой последовательность, состоящую из следующих объектов данных:

a) идентификатор объекта, определяющий тип терминала и формат шаблона;

b) объект дискретных данных, кодирующий относительную авторизацию, т. е. функцию и авторизацию владельца сертификата по отношению к сертифицирующему полномочному органу.

Конкретные значения определены в части 10 документа Doc 9303.

7.2.2.5 Дата вступления сертификата в силу и дата истечения срока действия сертификата

Сочетание этих двух дат определяет период действия сертификата. Датой вступления сертификата в силу ДОЛЖНА быть дата формирования сертификата. Датой истечения срока действия сертификата является дата, после которой сертификат аннулируется.

7.2.2.6 Расширения сертификатов (расширения авторизации)

Информация о расширениях может включаться в сертификаты CVCA, DV и терминала. Эти расширения предоставляют права в дополнение к правам, предусмотренным содержащимся в сертификате шаблоном авторизации владельца сертификата.

Расширение авторизации представляет собой последовательность шаблонов дискретных данных, в рамках которой шаблон дискретных данных СОДЕРЖИТ последовательность следующих объектов данных, которые также показаны в таблице 13:

a) идентификатор объекта, определяющий контент и формат расширения;

b) контекстный объект данных, содержащий закодированную информацию об авторизации.

Таблица 13. Расширения сертификата

Объект данных
Расширения сертификата
Шаблон дискретных данных
Идентификатор объекта
Контекстный объект данных
Шаблон дискретных данных
Идентификатор объекта
Контекстный объект данных
…

Примечание. Процедура валидации сертификатов, описание которой приводится в части 11 документа Doc 9303, не учитывает расширения сертификатов. Таким образом, расширения представляют собой некритические атрибуты, и ИС НЕ ДОЛЖНА отклонять сертификаты по причине неизвестных расширений.

7.2.2.7 Подпись

Подпись на сертификате формируется посредством закодированного тела сертификата (т. е., включая тег и длину). Для проверки подписи указатель сертифицирующего полномочного органа идентифицирует открытый ключ.

7.2.3 Объекты данных

В таблице 14 приводится общая информация о тегах, длинах и значениях объектов данных, используемых в сертификатах CVCA, DV и терминалов.

Таблица 14. Общая информация об объектах данных (с разбивкой по тегам)

Название	**Тег**	**Длина**	**Значение**	**Замечания**
Идентификатор объекта	0x06	V	Идентификатор объекта	-
Указатель сертифицирующего полномочного органа	0x42	16V	Строка символов	В сертификате идентифицирует открытый ключ сертифицирующего полномочного органа выдачи
Дискретные данные	0x53	V	Октетная строка	Содержит произвольные данные
Указатель владельца сертификата	0x5F20	16V	Строка символов	Связывает содержащийся в сертификате открытый ключ с идентификатором
Дата истечения срока действия сертификата	0x5F24	6F	Дата	Дата, после которой сертификат аннулируется
Дата вступления сертификата в силу	0x5F25	6F	Дата	Дата формирования сертификата

Название	Тег	Длина	Значение	Замечания
Идентификатор профиля сертификата	0x5F29	1F	Целое число без знака	Версия сертификата и формат запроса на сертификат
Подпись	0x5F37	V	Октетная строка	Цифровая подпись, созданная ассиметричным криптографическим алгоритмом
Расширения сертификата	0x65	V	Последова-тельность	Встраивает расширения сертификатов
Аутентификация	0x67	V	Последова-тельность	Содержит объекты данных, связанные с аутентификацией
Шаблон дискретных данных	0x73	V	Последова-тельность	Встраивает объекты произвольных данных
Сертификат CV	0x7F21	V	Последова-тельность	Встраивает тело сертификата и подпись
Открытый ключ	0x7F49	V	Последова-тельность	Встраивает значение открытого ключа и параметры домена
Шаблон авторизации владельца сертификата	0x7F4C	V	Последова-тельность	Кодирует функцию владельца сертификата (т. е. CVCA, DV, терминала) и выдает права доступа к считыванию/записи
Тело сертификата	0x7F4E	V	Последова-тельность	Встраивает объекты данных тела сертификата

F: фиксированная длина (точное количество октетов), V: переменная длина (вплоть до количества октетов).

7.2.3.1 Кодирование значений

Базовыми типами значений, используемых в этой спецификации, являются следующие: целые числа (без знаков), точки эллиптической кривой, даты, строки символов, октетные строки, идентификаторы объектов и последовательности.

7.2.3.1.1 Целые числа без знака

Все целые числа, используемые в данной спецификации, являются целыми числами без знака. Целое число без знака ПРЕОБРАЗУЕТСЯ в октетную строку с использованием двоичного представления целого числа в формате для хранения и передачи двоичных данных. ИСПОЛЬЗУЕТСЯ минимальное количество октетов, т. е. начальные октеты со значением 0x00 использоваться НЕ ДОЛЖНЫ.

Примечание. В отличие от этого ЦЕЛОЕ ЧИСЛО типа ASN.1 всегда является целым числом со знаком.

7.2.3.1.2 Точки эллиптической кривой

Порядок преобразования точек эллиптической кривой в октетные строки определяется в документе [TR-03111]. ИСПОЛЬЗУЕТСЯ несжатый формат.

7.2.3.1.3 Даты

Дата кодируется шестизначной цифрой "d1…d6" в формате YYMMDD с использованием часового пояса GMT. Она преобразуется в октетную строку "o1…o6" посредством кодирования каждой цифры dj в октет oj, в качестве неупакованных BCD ($1 \le j \le 6$).

Год YY кодируется двумя цифрами и интерпретируется как 20YY, т. е. этот год находится в диапазоне от 2000 до 2099 года.

7.2.3.1.4 Строки символов

Строка символов "c1…cn" является результатом конкатенации n символов cj с $1 \le j \le n$. Она ПРЕОБРАЗУЕТСЯ в октетную строку "o1…on" посредством преобразования каждого символа cj в октет oj с использованием набора символов, предусмотренного стандартом ИСО/МЭК 8859-1.

Коды символов 0x00-0x1F и 0x7F-0x9F являются неназначенными и использоваться НЕ ДОЛЖНЫ. Результатом преобразования октета в неназначенный символ ЯВЛЯЕТСЯ ошибка.

7.2.3.1.5 Октетные строки

Октетная строка "o1…on" является результатом конкатенации n октетов oj $1 \le j \le n$. Каждый октет oj состоит из 8 битов.

7.2.3.1.6 Идентификаторы объектов

Идентификатор объекта "i1.i2…in" кодируется в качестве упорядоченного списка n целых чисел без знака ij с $1 \le j \le n$. Он ПРЕОБРАЗУЕТСЯ в октетную строку "o1…on−1" с использованием следующей процедуры:

1) первые два числа i1 и i2 объединяются в одно целое число i, которое затем преобразуется в октетную строку o1. Это значение рассчитывается следующим образом:

$$i=i1\cdot 40+i2$$

2) остальные целые числа ij непосредственно преобразуются в октетные строки oj−1 с $3 \le j \le n$. Более подробная информация о кодировании содержится в документе [X.690].

Примечание. Целые числа без знака кодируются в качестве октетных строк с использованием формата для хранения и передачи двоичных данных, предусмотренного частью 11 документа Doc 9303, однако при этом используются только биты 1-7 каждого октета. Бит 8 (самый левый бит), устанавливаемый на единицу, используется для индикации того, что этот октет не является последним октетом в строке.

7.2.3.1.7 Последовательности

Последовательность "D1…Dn" представляет собой упорядоченный список n объектов данных Dj, с $1 \le j \le n$. Эта последовательность ПРЕОБРАЗУЕТСЯ в конкатенированный список октетных строк "O1…On" посредством DER кодирования каждого объекта данных Dj в октетную строку Oj.

7.2.3.2 Кодирование объектов данных открытых ключей

Объект данных открытого ключа содержит последовательность идентификатора объекта и нескольких контекстных объектов данных:

- Идентификатор объекта связан с конкретным приложением и относится не только к формату открытого ключа (т. е. к контекстам объектных данных), но также и к его использованию.
- Контекстные объекты данных определяются идентификатором объекта и содержат значение открытого ключа и параметра домена.

Описание формата объектов данных открытых ключей, используемого в настоящей спецификации, приводится ниже.

7.2.3.2.1 Открытые ключи RSA

Объекты данных, содержащиеся в открытом ключе RSA, представлены в таблице 15. Порядок объектов данных является фиксированным.

Таблица 15. Открытый ключ RSA

Объект данных	Сокращ.	Тег	Тип	Сертификат CV
Идентификатор объекта		0x06	Идентификатор объекта	m
Составной модуль	n	0x81	Целое число без знака	m
Открытая экспонента	e	0x82	Целое число без знака	m

7.2.3.2.2 Открытые ключи эллиптической кривой

Объекты данных, содержащиеся в открытом ключе EC, показаны в таблице 16. Порядок объектов данных является фиксированным. УСЛОВНО ОБЯЗАТЕЛЬНЫЕ параметры доменов ДОЛЖНЫ либо все присутствовать, за исключением ко-фактора, либо все отсутствовать, как указано ниже:

- самоподписанные сертификаты CVCA СОДЕРЖАТ параметры доменов;
- связующие сертификаты CVCA МОГУТ содержат параметры доменов;
- сертификаты DV и терминалов НЕ ДОЛЖНЫ содержать параметры доменов. Параметры доменов открытых ключей DV и терминалов НАСЛЕДУЮТСЯ от соответствующего открытого ключа;
- в запросах на сертификаты ДОЛЖНЫ всегда содержаться параметры доменов.

Таблица 16. Открытый ключ EC

Объект данных	Сокращ.	Тег	Тип	Сертификат CV
Идентификатор объекта		0x06	Идентификатор объекта	m
Первичный модуль	p	0x81	Целое число без знака	c
Первый коэффициент	a	0x82	Целое число без знака	c
Второй коэффициент	b	0x83	Целое число без знака	c
Базовая точка	G	0x84	Точка эллиптической кривой	c
Порядок точки	r	0x85	Целое число без знака	c
Открытая точка	Y	0x86	Точка эллиптической кривой	m
Ко-фактор	f	0x87	Целое число без знака	c

8. ПРОТОКОЛ SPOC

Единый центр обслуживания (SPOC) является единственным интерфейсом, предоставляемым государством для выполнения операций по управлению ключами с зарубежными государствами в целях авторизации PKI LDS2. Протокол SPOC является протоколом управления ключами для осуществления операций между CVCA и DV в различных государствах. Несмотря на то, что протокол SPOC МОЖЕТ также использоваться для связи на национальном уровне между CVCA и его национальными DV, а также между DV и комплексом управляемых ими местных терминалов, этого делать не требуется. Для местного управления ключами могут использоваться другие протоколы управления ключами.

Протокол SPOC используется для обмена ключами и сертификатами, с тем чтобы:

- DV мог направлять запрос на сертификат зарубежному CVCA;
- CVCA мог направлять оформленный сертификат запрашивающему DV;
- CVCA и DV могли запрашивать набор действующих сертификатов у зарубежных CVCA;
- DV и CVCA могли осуществлять обмен сообщениями.

В рамках государства:

- CVCA ИСПОЛЬЗУЕТ свой местный SPOC для приема поступающих из-за рубежа запросов на сертификаты и отправки готовых сертификатов или уведомлений об отказе;

- DV ИСПОЛЬЗУЮТ свои национальные SPOC для отправки зарубежным CVCA запросов на сертификаты и получения готовых сертификатов или уведомлений об отказе;

- SPOC ДОЛЖЕН обрабатывать запросы и ответы, поступающие от национальных CVCA и DV и направлять их SPOC государства получателя;

- SPOC ДОЛЖЕН обрабатывать запросы и ответы, поступающие от SPOC других государств, и направлять их соответствующему национальному CVCA/DV.

Веб-служба связи SPOC ИСПОЛЬЗУЕТ протоколы HTTPS с авторизацией TLS клиента и сервера.

Примечание. SPOC представляют собой узлы связи между объектами авторизации PKI, которые, в этой связи, должны находиться в эксплуатационной готовности круглосуточно в течение всей недели (24/7) и быть доступны для зарубежных SPOC.

Каждый SPOC отдельно регистрируется во всех других SPOC, представляющих для него интерес, предоставляя, как минимум, следующую информацию:

- государство SPOC – государство, для которого SPOC предоставляет коммуникационный интерфейс;

- URL SPOC – URL WSDL, описывающий интерфейс SPOC и местоположение службы;

- сертификат CA SPOC – сертификат(ы), используемый(е) для проверки сертификатов связи SPOC.

8.1 Структуры, связанные с SPOC

Для использования в сообщениях SPOC определены приводимые ниже структуры.

8.1.1 Структура запроса на сертификат

Запросы на сертификат представляют собой сокращенные, верифицируемые карточками сертификаты, которые могут содержать дополнительную подпись. ИСПОЛЬЗУЕТСЯ профиль запроса на сертификат, указанный в таблице 17.

Таблица 17. Профиль запроса на сертификат CV

Объект данных	**Наличие сертификата**
Аутентификация	c
Сертификат CV	m
Тело сертификата	m
Идентификатор профиля сертификата	m
Указатель сертифицирующего полномочного органа	r
Открытый ключ	m
Указатель владельца сертификата	m
Подпись	m
Указатель сертифицирующего полномочного органа	c
Подпись	c

8.1.1.1 Идентификатор профиля сертификата

Версия 1 идентифицируется значением 0.

8.1.1.2 Указатель сертифицирующего полномочного органа

Указатель сертифицирующего полномочного органа СЛЕДУЕТ использовать для информирования сертифицирующего полномочного органа относительно открытого ключа, который заявитель планирует использовать для подписания сертификата. Если содержащийся в запросе указатель сертифицирующего полномочного органа отличается от указателя сертифицирующего полномочного органа, содержащегося в выданном сертификате (т. е. выданный сертификат подписан закрытым ключом, на который заявитель не рассчитывал), то в ответ заявителю СЛЕДУЕТ также представить соответствующий сертификат сертифицирующего полномочного органа.

8.1.1.3 Открытый ключ

В запросах на сертификаты ДОЛЖНЫ всегда содержаться параметры доменов.

8.1.1.4 Указатель владельца сертификата

Указатель владельца сертификата используется для идентификации открытого ключа, содержащегося в запросе и готовом сертификате.

8.1.1.5 Подпись(и)

В запросе на сертификат могут содержаться до двух подписей: внутренняя подпись и внешняя подпись.

Внутренняя подпись (ОБЯЗАТЕЛЬНАЯ)

Тело сертификата является самоподписанным, т. е. внутренняя подпись верифицируется открытым ключом, содержащимся в запросе на сертификат. Эта подпись СОЗДАЕТСЯ с помощью закодированного тела сертификата (т. е. включает тег и длину).

Внешняя подпись (УСЛОВНО ОБЯЗАТЕЛЬНАЯ)

- Эта подпись является ФАКУЛЬТАТИВНОЙ, если субъект обращается за получением первоначального сертификата. В этом случае запрос МОЖЕТ быть дополнительно подписан другим субъектом, которому доверяет принимающий сертифицирующий полномочный орган (например, национальный CVCA может аутентифицировать запрос DV, направленный зарубежному CVCA).

- Эта подпись является ОБЯЗАТЕЛЬНОЙ, если субъект обращается за получением последующего сертификата. В этом случае запрос ДОЛЖЕН быть дополнительно подписан заявителем с использованием последней пары ключей, зарегистрированной принимающим сертифицирующим полномочным органом.

В случае использования внешней подписи объект данных аутентификации ПРИМЕНЯЕТСЯ для размещения информации сертификата CV (запрос), указателя сертифицирующего полномочного органа и дополнительной подписи. Указатель сертифицирующего полномочного органа ИДЕНТИФИЦИРУЕТ открытый ключ, подлежащий использованию для верификации дополнительной подписи. Эта подпись создается посредством конкатенации закодированного сертификата CV и закодированного указателя сертифицирующего полномочного органа (т. е. оба включают тег и длину).

8.2 Протокольные сообщения SPOC

В настоящем разделе приводится подробная информация о сообщениях, используемых в протоколе SPOC.

8.2.1 Сообщение, касающееся запроса на сертификат

Предполагаемое использование:

Сообщение, касающееся запроса на сертификат, используется SPOC для передачи запроса на получение нового сертификата для одного из своих DV от зарубежного CVCA.

Входные параметры:

callerID: (обязательный)
Этот параметр содержит идентификатор запроса, направляемого государством. Данное значение СООТВЕТСТВУЕТ двухбуквенному коду страны, предусмотренному частью 3 документа Doc 9303. Значение callerID ВЕРИФИЦИРУЕТСЯ принимающим SPOC с использованием зафиксированного значения, представлнного исходящим SPOC в процессе регистрации.

messageID: (обязательный)
Этот параметр содержит информацию, идентифицирующую сообщение. Он ДОЛЖЕН однозначно идентифицировать сообщение из числа всех сообщений, переданных этим отправителем. Если ответное сообщение будет направлено отправителю в результате получения упомянутого сообщения, то в ответном сообщении будет содержаться аналогичный messageID. Таким образом, входящее ответное сообщение может быть отнесено к соответствующему первоначальному сообщению. Решение о составлении и передаче messageID может быть принято составителем и принимающей стороной не верифицироваться.

certReq: (обязательный)
Этот параметр содержит фактический запрос сертификата. Он ДОЛЖЕН составляться в соответствии с положениями раздела 8.1.1. Кодирование ДОЛЖНО выполняться в соответствии со спецификациями, изложенными в разделе 7.2.3.1.

Выходные параметры:

CertificateSeq: (условно обязательный)
Этот параметр будет содержать результат (один или несколько сертификатов) после обработки этого сообщения, если сообщение было успешно и синхронизировано обработано получателем. Это НЕОБХОДИМО, если сертификаты должны направляться с ответом. Данный параметр НЕ ДОЛЖЕН присутствовать, если с этим сообщением сертификаты направляться не будут.

Коды возврата:

- ok_cert_available: это сообщение обработано успешно и синхронизировано. Выходной параметр certificateSeq содержит один или несколько сертификатов.

- ok_reception_ack: принятие сообщения подтверждено. Дополнительная верификация сообщения пока не выполнена. Обработка сообщения будет выполняться асинхронно. Результат обработки будет направлен зарегистрированному URL с использованием сообщения SendCertificates.

- failure_inner_signature: верификация внутренней подписи фактического запроса на сертификат не выполнена.

- failure_outer_signature: верификация внешней подписи фактического запроса на сертификат не выполнена.

- failure_syntax: синтаксически сообщение является неправильным.

- failure_request_not_accepted: сообщение обработано правильно, но запрос не принят.

- failure_request_syntax: запрос на сертификат является неправильным (например, синтаксис или формат файла).

- failure_expired: срок действия сертификата, подлежащего использованию для верификации внешней подписи запроса, истек.

- failure_domain_parameters: параметры домена, содержащиеся в запросе, не соответствуют параметрам домена сертификата CVCA, предназначенного для подписи запрашиваемого сертификата DV.

- failure_internal_error: ошибка, не относящаяся к вышеуказанным категориям.

Замечания:

СЛЕДУЕТ обеспечить, чтобы в теле запроса на сертификат содержался указатель сертифицирующего полномочного органа (CAR) для информирования CVCA о том, какой закрытый ключ, по мнению запрашивающей стороны, будет использоваться для подписания сертификата. Если CAR, содержащийся в запросе, отличается от CAR, содержащегося в выданном сертификате, в ответе также УКАЗЫВАЕТСЯ соответствующий сертификат CVCA. В этом случае, а также, если сообщение обрабатывалось одновременно, сертификат CVCA ЯВЛЯЕТСЯ составной частью выходного параметра certificateSeq. Сертификат DV ЯВЛЯЕТСЯ первым сертификатом в последовательности. Порядок сертификатов CVCA (корневых или связующих) определяется датой вступления в силу (в порядке возрастания).

8.2.2 Сообщение Send Certificates

Предполагаемое использование:

Сообщение SendCertificates используется SPOC для отправки нового сертификата или цепочки сертификатов запрашивающему SPOC. Это сообщение ГЕНЕРИРУЕТСЯ в ответ на команду:

- RequestCertificate: при успешной асинхронной обработке запроса после выдачи сертификата;

- GetCACertificates

Кроме того, это сообщение ДОЛЖНО использоваться при создании нового сертификата (корневого и связующего сертификата CVCA) с целью внесения этих сертификатов в зарегистрированный зарубежный SPOC.

Входные параметры:

callerID: (обязательный)
Этот параметр содержит идентификатор государства-отправителя. Данное значение ПРЕДСТАВЛЯЕТ собой двухбуквенный код страны, указанный в части 3 документа Doc 9303. Значение callerID ВЕРИФИЦИРУЕТСЯ принимающим SPOC с использованием зафиксированного значения, представленного исходящим SPOC в процессе регистрации.

messageID: (условно обязательный)
При формировании сообщения в ответ на сообщение, содержащее запрос, этот параметр ДОЛЖЕН содержать значение, аналогичное параметру messageID сообщения, содержащего запрос. Когда формирование сообщения инициируется без внешнего вмешательства (замена ключа сертификата CVCA), значение параметра statusInfo ПРЕДСТАВЛЯЕТ собой уведомление_о_наличии_нового_сертификата, и параметр messageID МОЖЕТ не включаться, а в случае представления он ИГНОРИРУЕТСЯ.

statusInfo: (обязательный)
Этот параметр содержит код состояния, отражающий результат обработки соответствующего сообщения. Могут быть следующие типы состояния:

- new_cert_available_notification: передающий SPOC хочет уведомить о том, что новый(е) сертификат(ы) CVCA имеется(ются) без запроса.
- ok_cert_available: запрос обработан успешно. Входной параметр certificateSeq содержит один или несколько сертификатов.
- failure_inner_signature: проверка внутренней подписи фактического запроса на сертификат не удалась.
- failure_outer_signature: проверка внешней подписи фактического запроса на сертификат не удалась.
- failure_syntax: синтаксически соответствующее сообщение является неправильным.
- failure_request_not_accepted: соответствующее сообщение обработано правильно, но запрос не принят.
- failure_certificate: один или несколько отправленных сертификатов является(ются) неправильным(и) (синтаксис или подпись).
- failure_internal_error: ошибка, не является ошибкой, характеризуемой параметром certificateSeq выше (условно обязательный).

Этот параметр является ОБЯЗАТЕЛЬНЫМ, если сертификат должен быть направлен с сообщением. Он ДОЛЖЕН отсутствовать, если с сообщениями сертификаты направляться не будут. Эти сертификаты КОДИРУЮТСЯ двоичным кодом с использованием TLV DER, как определено в разделе 7.2.3.

В тех случаях, когда сообщение генерируется в ответ на сообщение GetCACertificates или в связи с наличием нового сертификата, последовательность содержит список сертификатов CA. Этот список является упорядоченным. В рамках последовательности порядок этих сертификатов CVCA (связующих и/или корневых) определяется датой вступления их в силу. Если в последовательности имеются сертификаты с различными параметрами доменов, то для каждой разновидности доменов включается по крайней мере один сертификат с параметрами доменов. ВКЛЮЧАЮТСЯ все действующие сертификаты CA.

В тех случаях, когда сообщение генерируется в ответ на сообщение RequestCertificate, содержание последовательности является аналогичным содержанию, предусмотренному для синхронного ответа на запрос сертификата (RequestCertificate).

Выходные параметры:

Отсутствуют.

Коды возврата:

- ok_received_correctly: сообщение получено правильно.
- failure_syntax: синтаксически сообщение является неправильным.
- failure_messageID_unknown: содержащийся параметр messageID не поддается согласованию с ранее переданным сообщением.
- failure_internal_error: ошибка не относится к категориям, указанным выше.

8.2.3 Сообщение Get CA Certificates

Предполагаемое использование:

Это сообщение направляется национальным SPOC зарубежному SPOC для получения всех действующих сертификатов CVCA (связующих сертификатов и самоподписанных сертификатов) этого государства.

Входные параметры:

callerID: (обязательный)
Этот параметр содержит идентификатор государства-отправителя. Данное значение ПРЕДСТАВЛЯЕТ собой двухбуквенный код страны, указанный в части 3 документа Doc 9303. Значение callerID ВЕРИФИЦИРУЕТСЯ принимающим SPOC с использованием зафиксированного значения, представленного исходящим SPOC в процессе регистрации.

messageID: (обязательный)
Этот параметр содержит информацию, идентифицирующую сообщение. Он ДОЛЖЕН однозначно идентифицировать сообщение из числа всех сообщений отправителя. Если ответное сообщение будет направляться отправителю в результате получения этого сообщения, то в ответном сообщении будет содержаться тот же параметр messageID. Таким образом, входящее ответное сообщение может быть закреплено за соответствующим исходящим сообщением. Решение о составлении и назначении параметра messageID может приниматься отправителем.

Выходные параметры:

certificateSeq: (условно обязательный)
После обработки сообщения этот параметр будет содержать результат (один или несколько сертификатов), если получатель успешно и синхронизировано обработал это сообщение. Он является ОБЯЗАТЕЛЬНЫМ, если сертификаты подлежат отправке с ответом. Он НЕ ДОЛЖЕН присутствовать, если с сообщением сертификаты отправляться не будут.

Коды возврата:

- ok_cert_available: сообщение обработано успешно и синхронизировано. Выходной параметр certificateSeq содержит один или несколько сертификатов CA.
- ok_reception_ack: прием сообщения подтвержден. Дополнительная верификация пока не выполнена. Обработка сообщения будет осуществляться асинхронно. Результат обработки будет направлен зарегистрированному URL посредством сообщения SendCertificates.
- failure_syntax: синтаксически сообщение является неправильным.
- failure_internal_error: ошибка не относится к категориям, указанным выше.

Замечания:

Если сообщение обработано успешно и принято, то в ответе CVCA ДОЛЖЕН отправить все действующие сертификаты CVCA либо в качестве выходного параметра certificateSeq (синхронная обработка), либо в соответствующем ответном сообщении SendCertificates (асинхронная обработка).

8.2.4 Общие сообщения

Предполагаемое использование:

Это сообщение направляется национальным SPOC зарубежному SPOC в целях передачи уведомления или другого удобочитаемого для человека сообщения, содержащего тест общего характера.

Входные параметры:

callerID: (обязательный)
Этот параметр содержит идентификатор государства-отправителя. Данное значение ПРЕДСТАВЛЯЕТ собой двухбуквенный код страны, указанный в части 3 документа Doc 9303. Значение callerID ВЕРИФИЦИРУЕТСЯ принимающим SPOC с использованием значения, представленного исходящим SPOC в процессе регистрации, включая элементы защиты сообщения (сертификат цифровой подписи/сертификат клиента TLS зарегистрированый для соответствующего государства).

messageID: (обязательный)
Этот параметр содержит информацию, идентифицирующую сообщение. Он ДОЛЖЕН однозначно идентифицировать сообщение из числа всех сообщений отправителя. Если ответное сообщение будет направлено отправителю в результате получения этого сообщения, то в ответном сообщении будет содержаться аналогичный параметр messageID. Таким образом, входящее ответное сообщение может быть закреплено за соответствующим исходящим сообщением. Решение о составлении и назначении параметра messageID может приниматься отправителем.

субъект: (обязательный)
Этот параметр содержит субъект сообщения. В данном субъекте СЛЕДУЕТ представить краткое описание содержания тела сообщения. В отношении субъекта ДОЛЖЕН использоваться английский язык.

тело: (обязательный)
Этот параметр содержит тело сообщения. Данное тело ПРЕДСТАВЛЯЕТ собой удобочитаемый человеком открытый текст, который для непосредственной автоматизированной обработки не предназначен. В отношении тела сообщения ДОЛЖЕН использоваться английский язык.

Коды возврата:

- ok: сообщение принято к доставке.
- failure_syntax: синтаксически сообщение является неправильным.
- failure_internal_error: ошибка не относится к категориям, указанным выше.

8.3 Веб-служба

Интерфейс веб-службы представляет собой интерфейс для обычного обмена данными между SPOC. Этот интерфейс ИСПОЛЬЗУЕТ простой протокол доступа к объектам [SOAP] через протокол [HTTPS]. Интерфейс веб-службы соответствует формату WSDL, конкретно рассматриваемому в разделе 8.3.3.

8.3.1 Использование SOAP

Для реализации интерфейсов веб-службы используется простой протокол доступа к объектам [SOAP] через протоколы [HTTPS]. Любые другие расширения SOAP (например, WS-адресация, WS-защита, WS-защищенная переписка, WS-авторизация, WS-федерирование, WS-авторизация, WS-политика, WS-доверие, WS-конфиденциальность, WS-тесты и другие расширения WS) НЕ ИСПОЛЬЗУЮТСЯ.

Посреднический узел SOAP НЕ ИСПОЛЬЗУЕТСЯ. ИСПОЛЬЗУЕТСЯ только прямое взаимодействие SPOC с конфигурацией сервера SPOC.

Элемент ошибки SOAP ИСПОЛЬЗУЕТСЯ только тогда, когда возникает ошибка обработки на транспортном уровне, которая настоящей спецификацией не охватывается. Ошибки прикладного уровня ПЕРЕДАЮТСЯ как обычные ответы SOAP с использованием механизма погрешности, предусмотренного для каждого сообщения.

Внедрять интерфейс веб-службы РЕКОМЕНДУЕТСЯ в соответствии с требованиями [WS-IBP] и [WSI-SSBP].

Интерфейс SPOC SOAP ДОЛЖЕН соответствовать определениям WSDL, описание которых приводится в разделе 8.3.3.

8.3.2 Соображения, касающиеся защиты

При ведении связи SPOC, обеспечиваемый веб-службой, используется защищенный и аутентифицированный канал. ИСПОЛЬЗУЕТСЯ SOAP через HTTPS. ИСПОЛЬЗУЕТСЯ версия TLS v1.2.

Клиент TLS ВЫПОЛНЯЕТ следующие верификации:

- сертификат сервера полностью ВАЛИДИРУЕТСЯ в соответствии с документом [RFC5280], включая статус отзыва;
- ДОЛЖНО быть представлено расширение ExtKeyUsage сертификата сервера, СОДЕРЖАЩЕЕ OID, в соответствии с разделом 7.2.1 сертификата сервера SPOC TLS;

- субъект сертификата сервера страны равен значению параметра callerID. В случае любого сбоя клиент TLS ДОЛЖЕН закрыть соединение.

Сервер TLS ВЫПОЛНЯЕТ следующие верификации:

- для использования сертификата клиент ЯВЛЯЕТСЯ полностью аутентифицированным;
- сертификат клиента полностью ВАЛИДИРУЕТСЯ в соответствии с документом [RFC5280], включая статус отзыва;
- ДОЛЖНО быть представлено расширение ExtKeyUsage сертификата клиента, СОДЕРЖАЩЕЕ OID, в соответствии с разделом 7.2.1 сертификата клиента SPOC TLS;
- субъект сертификата сервера страны СООТВЕТСТВУЕТ субъекту, предполагаемому для использования.

В случае неудовлетворительных результатов какой-либо верификации запрос ОТКЛОНЯЕТСЯ с использованием кода несанкционированного ответа HTTP 401.

В рамках обсуждения условий TLS клиент ПОДДЕРЖИВАЕТ все наборы шифрования TLS, определенные в разделе 4.2.2. Сервер и клиент ПОДДЕРЖИВАЮТ аутентификацию, основанную на RSA и ECDSA. Сервер может делать запрос, а клиент – направлять сертификат клиента, тип которого отличается от сертификата сервера.

Использование соглашения о ключах ECDHE_ECDSA при установлении соединения TLS производится в соответствии с дополнениями, определенными в документах [TLSECC], [TLS1.2] и [TLSEXT]. В рамках установления соединения TLS клиент и сервер ПОДДЕРЖИВАЮТ соответствующие расширения эллиптических кривых, как указано в спецификации [TLSECC]. Поддерживаемые эллиптические кривые и форматы EC с точкой определяются в разделе 5 документа [TLSECC]. Использование поддерживаемых наборов шифрования TLS, определенных в разделе 4.2.2, которые для шифрования используют улучшенный стандарт шифрования (AES), производится в соответствии со спецификацией [TLSAES].

8.3.3 Язык WSDL для интерфейса веб-службы SPOC

Интерфейс SPOC SOAP ДОЛЖЕН соответствовать следующим определениям WSDL:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/
  " xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:SPOC="http://namespaces.icao.int/lds2"
  targetNamespace="http://namespaces.
  icao.int/lds2">

  <wsdl:types>
    <xs:schema xmlns="http://namespaces.icao.int/lds2"
      targetNamespace="http://namespaces."
      elementFormDefault="qualified" attributeFormDefault="unqualified">
      <xs:element name="certificateSequence">
        <xs:complexType>
          <xs:sequence>
```

```
            <xs:element name="certificate" type="xs:base64Binary" minOccurs="1"
maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:complexType>
       </xs:element>
       <xs:element name="RequestCertificateRequest">
      <xs:complexType>
       <xs:sequence>
            <xs:element name="callerID" type="xs:string"/>
            <xs:element name="messageID" type="xs:string"/>
            <xs:element name="certificateRequest" type="xs:base64Binary"/>
       </xs:sequence>
      </xs:complexType>
       </xs:element>
       <xs:element name="RequestCertificateResponse">
      <xs:complexType>
       <xs:sequence>
            <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
            <xs:element name="result">
          <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:enumeration value="ok_cert_available"/>
                <xs:enumeration value="ok_reception_ack"/>
                <xs:enumeration value="failure_inner_signature"/>
                <xs:enumeration value="failure_outer_signature"/>
                <xs:enumeration value="failure_syntax"/>
                <xs:enumeration value="failure_request_not_accepted"/>
                <xs:enumeration value="failure_request_syntax"/>
                <xs:enumeration value="failure_expired"/>
                <xs:enumeration value="failure_domain_parameters"/>
                <xs:enumeration value="failure_internal_error"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
       </xs:sequence>
      </xs:complexType>
       </xs:element>
       <xs:element name="SendCertificatesRequest">
      <xs:complexType>
       <xs:sequence>
            <xs:element name="callerID" type="xs:string"/>
            <xs:element name="messageID" type="xs:string" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
            <xs:element name="statusInfo">
          <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:enumeration value="new_cert_available_notification"/>
                <xs:enumeration value="ok_cert_available"/>
                <xs:enumeration value="failure_inner_signature"/>
                <xs:enumeration value="failure_outer_signature"/>
                <xs:enumeration value="failure_syntax"/>
                <xs:enumeration value="failure_request_not_accepted"/>
```

```
            <xs:enumeration value="failure_certificate"/>
            <xs:enumeration value="failure_internal_error"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="SendCertificatesResponse">
<xs:complexType>
      <xs:sequence>
      <xs:element name="result">
     <xs:simpleType>
         <xs:restriction base="xs:string">
           <xs:enumeration value="ok_received_correctly"/>
           <xs:enumeration value="failure_syntax"/>
           <xs:enumeration value="failure_messageID_unknown"/>
           <xs:enumeration value="failure_internal_error"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="GetCACertificatesRequest">
<xs:complexType>
  <xs:sequence>
      <xs:element name="callerID" type="xs:string"/>
      <xs:element name="messageID" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="GetCACertificatesResponse">
<xs:complexType>
  <xs:sequence>
      <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
      <xs:element name="result">
     <xs:simpleType>
         <xs:restriction base="xs:string">
           <xs:enumeration value="ok_cert_available"/>
           <xs:enumeration value="ok_reception_ack"/>
           <xs:enumeration value="failure_syntax"/>
           <xs:enumeration value="failure_internal_error"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="GeneralMessageRequest">
<xs:complexType>
  <xs:sequence>
```

```
        <xs:element name="callerID" type="xs:string"/>
        <xs:element name="messageID" type="xs:string"/>
        <xs:element name="subject" type="xs:string"/>
        <xs:element name="body" type="xs:string"/>
    </xs:sequence>
   </xs:complexType>
    </xs:element>
    <xs:element name="GeneralMessageResponse">
   <xs:complexType>
    <xs:sequence>
        <xs:element name="result">
       <xs:simpleType>
           <xs:restriction base="xs:string">
             <xs:enumeration value="ok"/>
             <xs:enumeration value="failure_syntax"/>
             <xs:enumeration value="failure_internal_error"/>
         </xs:restriction>
       </xs:simpleType>
     </xs:element>
    </xs:sequence>
   </xs:complexType>
</xs:element>
  </xs:schema>
</wsdl:types>

<wsdl:message name="RequestCertificateRequest">
  <wsdl:part name="RequestCertificateRequest" element="SPOC:RequestCertificateRequest"/>
</wsdl:message>
<wsdl:message name="RequestCertificateResponse">
  <wsdl:part name="RequestCertificateResponse" element="SPOC:RequestCertificateResponse"/>
</wsdl:message>

<wsdl:message name="SendCertificatesRequest">
  <wsdl:part name="SendCertificatesRequest" element="SPOC:SendCertificatesRequest"/>
</wsdl:message>
<wsdl:message name="SendCertificatesResponse">
  <wsdl:part name="SendCertificatesResponse" element="SPOC:SendCertificatesResponse"/>
</wsdl:message>

<wsdl:message name="GetCACertificatesRequest">
  <wsdl:part name="GetCACertificatesRequest" element="SPOC:GetCACertificatesRequest"/>
</wsdl:message>
<wsdl:message name="GetCACertificatesResponse">
  <wsdl:part name="GetCACertificatesResponse" element="SPOC:GetCACertificatesResponse"/>
</wsdl:message>

<wsdl:message name="GeneralMessageRequest">
  <wsdl:part name="GeneralMessageRequest" element="SPOC:GeneralMessageRequest"/>
</wsdl:message>
<wsdl:message name="GeneralMessageResponse">
  <wsdl:part name="GeneralMessageResponse" element="SPOC:GeneralMessageResponse"/>
</wsdl:message>
```

```
 <wsdl:portType name="SPOCPortType">
  <wsdl:operation name="RequestCertificate">
   <wsdl:input message="SPOC:RequestCertificateRequest"/>
   <wsdl:output message="SPOC:RequestCertificateResponse"/>
  </wsdl:operation>
  <wsdl:operation name="SendCertificates">
   <wsdl:input message="SPOC:SendCertificatesRequest"/>
   <wsdl:output message="SPOC:SendCertificatesResponse"/>
  </wsdl:operation>
  <wsdl:operation name="GetCACertificates">
   <wsdl:input message="SPOC:GetCACertificatesRequest"/>
   <wsdl:output message="SPOC:GetCACertificatesResponse"/>
  </wsdl:operation>
  <wsdl:operation name="GeneralMessage">
   <wsdl:input message="SPOC:GeneralMessageRequest"/>
   <wsdl:output message="SPOC:GeneralMessageResponse"/>
  </wsdl:operation>
 </wsdl:portType>

 <wsdl:binding name="SPOCSOAPBinding" type="SPOC:SPOCPortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="RequestCertificate">
   <soap:operation soapAction="RequestCertificate"/>
 <wsdl:input>
     <soap:body parts="RequestCertificateRequest" use="literal"/>
    </wsdl:input>
    <wsdl:output>
     <soap:body parts="RequestCertificateResponse" use="literal"/>
    </wsdl:output>
</wsdl:operation>
  <wsdl:operation name="SendCertificates">
   <soap:operation soapAction="SendCertificates"/>
   <wsdl:input>
    <soap:body parts="SendCertificatesRequest" use="literal"/>
 </wsdl:input>
    <wsdl:output>
     <soap:body parts="SendCertificatesResponse" use="literal"/>
    </wsdl:output>
</wsdl:operation>
  <wsdl:operation name="GetCACertificates">
   <soap:operation soapAction="GetCACertificates"/>
   <wsdl:input>
    <soap:body parts="GetCACertificatesRequest" use="literal"/>
 </wsdl:input>
    <wsdl:output>
     <soap:body parts="GetCACertificatesResponse" use="literal"/>
    </wsdl:output>
</wsdl:operation>
  <wsdl:operation name="GeneralMessage">
   <soap:operation soapAction="GeneralMessage"/>
   <wsdl:input>
```

```
        <soap:body parts="GeneralMessageRequest" use="literal"/>
      </wsdl:input>
        <wsdl:output>
          <soap:body parts="GeneralMessageResponse" use="literal"/>
        </wsdl:output>
      </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="SPOC">
      <wsdl:port name="SPOCPort" binding="SPOC:SPOCSOAPBinding">
        <soap:address location="http://spoc-server/SPOC"/>
      </wsdl:port>
    </wsdl:service>
  </wsdl:definitions>
```

9. СТРУКТУРА МАСТЕР-СПИСКА CSCA

Мастер-списки реализуются как конкретные образцы типа `ИнформациионоСодержании`, определенные в документе [RFC 5652]. `ИнформациясоСодержании` ДОЛЖНА содержать единственный конкретный образец типа `ПодписанныеДанные` нижеуказанного профиля. Никакие другие типы данных в поле `ИнформациясоСодержании` не включаются. Все мастер-списки ДОЛЖНЫ составляться в формате DER для сохранения целостности содержащихся в них подписей.

9.1 Тип подписываемых данных

Применяются правила обработки, содержащиеся в документе [RFC 5652].

Для требований в отношении присутствия каждого поля в спецификациях структуры мастер-списков используется следующая терминология.

m обязательное – поле ДОЛЖНО присутствовать;
r рекомендуемое – поле СЛЕДУЕТ включить;
x не использовать – поле НЕ ДОЛЖНО присутствовать;
o факультативное – поле МОЖЕТ присутствовать.

Таблица 18. Мастер-список

Значение		***Замечания***
`ПодписываемыеДанные`		
`Версия`	m	Значение = v3
`Алгоритмыпредставления вКраткойформе`	m	
`Информацияобинкапсули-рованномСодержании`	m	

Значение		*Замечания*
ТипЭлектронного Содержания	m	id-icao-cscaMasterList
электронноеСодержание	m	Зашифрованное содержание поля мастер-спискаcsca
Сертификаты	m	ДОЛЖЕН быть включен сертификат органа, подписывающего мастер-списки, и СЛЕДУЕТ включить сертификат CSCA, который может быть использован для верификации подписи в поле Информацияоподписавшемся
Crls	x	
Информация оподписавшихся	m	Государствам РЕКОМЕНДУЕТСЯ включать в это поле только одну единицу информации о подписавшемся
Информация оПодписавшемся	m	
Версия	m	Значение этого поля диктуется полем sid. См. правила, касающиеся этого поля, в документе [RFC 5652]
Sid	m	
ИдентификаторКлюча субъекта	r	РЕКОМЕНДУЕТСЯ, чтобы поддерживалось это поле, а не поле орган выдачи и порядковый номер
Алгоритмпредставления вКраткойформе	m	Алгоритмный идентификатор алгоритма, используемого для выдачи хэш-значения над инкапсулированным Содержанием и ПодписаннымиАтрибутами. См. примечание ниже.
ПодписанныеАтрибуты	m	Могут быть включены дополнительные атрибуты. Однако они должны обрабатываться принимающими государствами только для верификации значения подписи. Поле ПодписанныеАтрибуты ДОЛЖНО включать время подписания (см. [PKCS #9])
Алгоритмподписи	m	Алгоритмный идентификатор алгоритма, используемого для выдачи значения подписи и любых связанных с ней параметров. См. примечание ниже.
подпись	m	Результат процесса генерации подписи
неподписанныеАтрибуты	o	Хотя это поле МОЖЕТ быть включено, принимающие государства могут принять решение об его игнорировании

Примечание. *Идентификаторыалгоритмапредставлениявкраткой форме* ***(Digest) ДОЛЖНЫ опускать параметры NULL (пустые), в то время как*** *идентификатор алгоритма подписи* ***(как это определено в документе RFC 3447) ДОЛЖЕН включать NULL в качестве параметра, если никакие***

параметры не присутствуют, даже в случае использования алгоритмов SHA2 в соответствии с документом RFC 5754. Варианты реализации ДОЛЖНЫ принимать *ИдентификаторыАлгоритма-представленияв Краткой форме* ***при обоих условиях: при отсутствии параметров или с параметрами NULL.***

9.2 Спецификации мастер-списка формата ASN.1

```
CscaMasterList
{ joint-iso-itu-t(2) international-organization(23) icao(136) mrtd(1)
security(1) masterlist(2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

 -- Imports from RFC 5280 [PROFILE], Appendix A.1
     Certificate
       FROM PKIX1Explicit88
         { iso(1) identified-organization(3) dod(6)
           internet(1) security(5) mechanisms(5) pkix(7)
             mod(0) pkix1-explicit(18) };
-- CSCA Master List

CscaMasterListVersion ::= INTEGER {v0(0)}

CscaMasterList ::= SEQUENCE {
  version            CscaMasterListVersion,
  certList           SET OF Certificate }

-- Object Identifiers

id-icao-cscaMasterList OBJECT IDENTIFIER ::=
                                 {id-icao-mrtd-security 2}
id-icao-cscaMasterListSigningKey OBJECT IDENTIFIER ::=
                                 {id-icao-mrtd-security 3}
END
```

10. СТРУКТУРА СПИСКА ОТКЛОНЕНИЙ

Список отклонений реализуется как тип подписанных данных, как определено в документе [RFC 3852]. Все списки отклонений ДОЛЖНЫ составляться в формате DER для сохранения целостности содержащихся в них подписей.

Диапазон отклонений будет ограничиваться:

- диапазоном дат (включая даты выдачи и истечения срока действия);
- названием органа выдачи и серийным номером;

- идентификатором ключа субъекта DSC;
- списком номеров электронных МСПД.

Соответствующие комбинации этих значений будут использоваться для точной увязки диапазона соответствующих МСПД. При комбинировании значений они должны обрабатываться в качестве значений, объединенных логической "И" (AND). Отсутствует вариант обработки значений в качестве значений, объединенных с использованием логического "ИЛИ" (OR).

10.1 Тип подписываемых данных

Применяются правила обработки, указанные в документе [RFC 3852]:

m обязательное – поле ДОЛЖНО присутствовать;
r рекомендуемое – поле СЛЕДУЕТ включить;
x не использовать – поле НЕ ДОЛЖНО присутствовать;
o факультативное – поле МОЖЕТ присутствовать.

Таблица 19. Список отклонений

Значение		Замечания
ПодписываемыеДанные		
Версия	m	Значение = v3
Алгоритмыпредставления вКраткой форме	m	
Информацияобинкапсули-рованномСодержании	m	
Типэлектронного Содержания	m	id-icao-DeviationList
электронноеСодержание	m	Зашифрованное содержание поля списка отклонений
Сертификаты	m	ДОЛЖЕН быть включен сертификат органа, подписывающего списки отклонений, и СЛЕДУЕТ включить сертификат CSCA, который может быть использован для верификации подписи в поле ИнформацияоПодписавшемся.
Crls	x	
Информация оподписавшемся	m	Государствам РЕКОМЕНДУЕТСЯ включать в это поле только одну единицу Информацииоподписавшемся
Информация оПодписавшемся	m	
Версия	m	Значение этого поля диктуется полем sid. См. правила, касающиеся этого поля, в разделе 5.3 документа [RFC 3852].

Значение		Замечания
sid	m	
ИдентификаторКлюча субъекта	r	РЕКОМЕНДУЕТСЯ, чтобы поддерживалось это поле, а не поле органвыдачииСерийныйномер.
Алгоритмпредставления вКраткойформе	m	Алгоритмный идентификатор алгоритма, используемого для выдачи хэш-значения над инкапсулированным Содержанием и ПодписаннымиАтрибутами. См. примечание ниже.
подписанныеАтрибуты	m	Могут быть включены дополнительные атрибуты. Однако они должны обрабатываться принимающими государствами только для верификации значения подписи. Поле подписанныеАтрибуты ДОЛЖНО включать время подписания (см. [PKCS #9])
Алгоритмподписи	m	Алгоритмный идентификатор алгоритма, используемого для выдачи значения подписи и любых связанных с ней параметров. См. примечание ниже.
подпись	m	Результат процесса генерации подписи
неподписанныеАтрибуты	x	

10.2 Спецификация ASN.1

```
DeviationList
{ joint-iso-itu-t (2) international-organization(23) icao(136) mrtd(1) security(1)
deviationlist(7)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

  -- Imports from RFC 3280 [PROFILE], Appendix A.1
       AlgorithmIdentifier
          FROM PKIX1Explicit88
                 { iso(1) identified-organization(3) dod(6)
                   internet(1) security(5) mechanisms(5) pkix(7)
                   mod(0) pkix1-explicit(18) }

  -- Imports from RFC 3852
       SubjectKeyIdentifier, Digest, IssuerAndSerialNumber
          FROM CryptographicMessageSyntax2004
                 { iso(1) member-body(2) us(840) rsadsi(113549)
```

```
                    pkcs(1) pkcs-9(9) smime(16) modules(0)
                    cms-2004(24) };

DeviationListVersion ::= INTEGER {v0(0)}

DeviationList ::= SEQUENCE {
 version     DeviationListVersion,
 digestAlgorithm AlgorithmIdentifier OPTIONAL,
 deviations  SET OF Deviation
}

Deviation ::= SEQUENCE{
 documents       DeviationDocuments,
 descriptions SET OF DeviationDescription
}

DeviationDescription ::= SEQUENCE{
 description     PrintableString OPTIONAL,
 deviationType   OBJECT IDENTIFIER,
 parameters  [0] ANY DEFINED BY deviationType OPTIONAL,
 nationalUse     [1] ANY OPTIONAL

 -- The nationalUse field is for internal State use, and is not governed
 -- by an ICAO specification.
}

DeviationDocuments ::= SEQUENCE {
 documentType    [0] PrintableString (SIZE(2)) OPTIONAL,
          -- per MRZ, e.g. 'P'
 dscIdentifier   DocumentSignerIdentifier OPTIONAL,
 issuingDate     [4] IssuancePeriod OPTIONAL,
 documentNumbers    [5] SET OF PrintableString OPTIONAL
}

DocumentSignerIdentifier ::= CHOICE{
 issuerAndSerialNumber [1] IssuerAndSerialNumber,
 subjectKeyIdentifier [2] SubjectKeyIdentifier,
 certificateDigest  [3] Digest   --  if  used,  digestAlgorithm  must  be  present  in
DeviationList
}

IssuancePeriod ::= SEQUENCE {
 firstIssued   GeneralizedTime,
 lastIssued   GeneralizedTime
}

-- CertField is used to define which part of a certificate is
  affected by a coding error. Parts of the Body are identified by
  the corresponding value of CertificateBodyField, extensions
  by the corresponding OID identifying the extension.

CertField ::= CHOICE {
```

```
 body  CertificateBodyField,
 extension OBJECT IDENTIFIER
}
CertificateBodyField ::= INTEGER {
 generic(0), version(1), serialNumber(2), signature(3), issuer(4),
 validity(5), subject(6), subjectPublicKeyInfo(7),
 issuerUniqueID(8), subjectUniqueID(9)
}

Datagroup ::= INTEGER
              {dg1(1), dg2(2), dg3(3), dg4(4), dg5(5), dg6(6),
               dg7(7), dg8(8), dg9(9), dg10(10), dg11(11),
               dg12(12), dg13(13), dg14(14), dg15(15), dg16(16),
               sod(20), com(21)}

MRZField ::= INTEGER
              {generic(0), documentCode(1), issuingState(2), personName(3),
               documentNumber(4), nationality(5), dateOfBirth(6),
               sex(7), dateOfExpiry(8), optionalData(9)}

-- Base Object Identifiers

id-icao OBJECT IDENTIFIER ::= {2 23 136 }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security 8}

-- Deviation Object Identifiers and Parameter Definitions

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}
id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 1}
id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 2}
id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 3}
id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 4}
id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}
id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}
id-Deviation-LDS-DGHashWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 2}
id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 3}
id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}
id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}
id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}

END
```

11. СПРАВОЧНЫЕ МАТЕРИАЛЫ (НОРМАТИВНЫЕ)

FIPS 180-2	FIPS 180-2. Публикация федеральных стандартов по обработке информации (FIPS PUB) 180-2. *Стандарт хэш-функции защиты*. Август 2002 г.
FIPS 186-4	FIPS 186-4. Публикация федеральных стандартов по обработке информации (FIPS PUB) 186-4. *Стандарт на цифровую подпись (DSS)*. Июль 2013 г. (Заменяет FIPS PUB 186-3 от июня 2009 г.).
ИСО 3166-1	ИСО/МЭК 3166-1: 2006. Коды для представления названий страны и единиц их административно-территориального деления. Часть 1. Коды стран.
ИСО/МЭК 15946	ИСО/МЭК 15946: 2002. Информационные технологии. Методы защиты. Криптографические методы на основе эллиптических кривых.
RFC 3280	RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.
RFC 4055	RFC 4055, J. Schaad, B. Kaliski, R. Housley, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, June 2005.
RFC 5652	RFC 5652, R. Housley, Cryptographic Message Syntax, September 2009.
RFC 5280	RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May, 2008.
TR 03111	BSI TR-03111. Криптография на основе эллиптических кривых, v 2.0, 2012 г.
X9.62	X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 7 January 1999.
X.509	ITU-T X.509 | ISO/IEC 9594-8, 2008: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
X.690	ITU-T X.690 2008: Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
RFC-RSA	Jonsson, Jakob and Kaliski, Burt RFC 3447, Public-key cryptography standards (PKCS)#1: RSA cryptography specifications version 2.1, 2003
PKCS#1	RSA Laboratories RSA Laboratories Technical Note, PKCS#1 v2.2: RSA cryptography standard, 2012
TLSAES	Chown, P., “Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)”, RFC 3268, June 2002
TLSECC	Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)”, RFC 4492, May 2006
TLS1.2	Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, August 2008

TLSEXT	Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, “Transport Layer Security (TLS) Extensions”, RFC 4366, April 2006
SOAP	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007
HTTPS	E. Rescorla., “HTTP Over TLS”, RFC 2818, May 2000
WSI-BP	WS-I Basic Profile available at http://www.ws-i.org/Profiles/BasicProfile-1.1.html
WSI-SSBP	WS-I Basic Binding available at http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html

— — — — — — — —

Добавление A к части 12

СРОКИ СЛУЖБЫ (ИНФОРМАЦИОННОЕ)

Нижеследующие примеры иллюстрируют расчет периода применимости закрытых ключей и срока действия сертификата открытого ключа для различных сценариев, описанных в разделе 4.

A.1 ПРИМЕР 1

Первый пример иллюстрирует сценарий, когда срок действия электронных МСПД составляет 5 лет. В связи с выдачей относительно большого количества электронных МСПД в день политика состоит в том, чтобы период применимости закрытых ключей и срок действия сертификата открытых ключей были минимальными. В этом примере минимальный период применимости закрытого ключа для сертификатов лиц, подписывающих документы, составляет 1 мес.

Наименование	***Период применимости/ срок действия***
Срок действия электронного МСПД	5 лет
Период применимости закрытого ключа лица, подписывающего документы	1 мес
Срок действия сертификата лица, подписывающего документы	5 лет + 1 мес
Период применимости закрытого ключа CSCA	3 года
Срок действия сертификата CSCA	8 лет + 1 мес

Из данного примера следует вывод о том, что к моменту, когда первый сертификат CSCA станет недействительным, будет выпущено по крайней мере 36 сертификатов лица, подписывающего документы (один на каждый закрытый ключ, период применимости которого равен 1 мес). В последние несколько месяцев, перед тем как первый сертификат CSCA станет недействительным, будут выпущены по крайней мере 2 дополнительных сертификата CSCA (один на каждый закрытый ключ, период применимости которого составляет 3 года).

A.2 ПРИМЕР 2

Второй пример иллюстрирует сценарий, когда срок действия электронных МСПД составляет 10 лет. Политика состоит в том, чтобы период применимости закрытых ключей и срок действия сертификата открытых ключей были средними.

Наименование	***Период применимости/ срок действия***
Срок действия электронного МСПД	10 лет
Период применимости закрытого ключа лица, подписывающего документы	2 мес
Срок действия сертификата лица, подписывающего документы	10 лет + 2 мес
Период применимости закрытого ключа CSCA	4 года
Срок действия сертификата CSCA	14 лет + 2 мес

Из данного примера следует вывод о том, что к моменту, когда первый сертификат CSCA станет недействительным, будет выпущено по крайней мере 24 сертификата лица, подписывающего документы (один на каждый закрытый ключ, период применимости которого равен 2 мес). В последние несколько месяцев, перед тем как первый сертификат CSCA станет недействительным, будут выпущены по крайней мере 3 дополнительных сертификата CSCA (один на каждый закрытый ключ, период применимости которого составляет 4 года).

A.3 ПРИМЕР 3

Последний пример иллюстрирует сценарий, когда срок действия электронных МСПД составляет 10 лет, а политика состоит в установлении максимальных периодов применимости закрытых ключей и сроков действия сертификатов открытых ключей.

Наименование	***Период применимости/ срок действия***
Срок действия электронного МСПД	10 лет
Период применимости закрытого ключа лица, подписывающего документы	3 мес
Срок действия сертификата лица, подписывающего документы	10 лет + 3 мес
Период применимости закрытого ключа CSCA	5 лет
Срок действия сертификата CSCA	15 лет + 3 мес

Из данного примера следует вывод о том, что к моменту, когда первый сертификат CSCA станет недействительным, будет выпущено по крайней мере 20 сертификатов лица, подписывающего документы (один на каждый закрытый ключ, период применимости которого равен 3 мес). В последние несколько месяцев, перед тем как первый сертификат CSCA станет недействительным, будут выпущены по крайней мере три дополнительных сертификата CSCA (один на каждый закрытый ключ, период применимости которого составляет 5 лет).

— — — — — — — —

Добавление B к части 12

ВЫДЕРЖКИ ИЗ СПРАВОЧНЫХ МАТЕРИАЛОВ, КАСАЮЩИЕСЯ ПРОФИЛЯ СЕРТИФИКАТОВ И CRL (ИНФОРМАЦИОННОЕ)

Профили сертификатов и CRL, указанные в разделе 7, основаны на определениях и базовых требованиях к профилю, содержащихся в справочных документах. В нижеследующих таблицах воспроизводятся краткие выдержки из некоторых соответствующих разделов вышеупомянутых источников (на момент подготовки настоящего документа). Эти выдержки приводятся для оказания помощи читателю в понимании истоков некоторых требований, установленных для сертификатов и CRL электронных МСПД. Они не предназначаются для использования вместо справочных документов. Во всех случаях для получения спецификаций указанных в таблицах компонентов/расширений и получения самых последних спецификаций ДОЛЖНЫ использоваться указанные здесь фактические документы.

Таблица B-1. Поля и расширения сертификатов

Компонент/расширение	*Ссылка*	*Соответствующие выдержки*
Сертификат	RFC 5280, раздел 4.1.1	
сертификатTBS	RFC 5280, раздел 4.1.1.1	
Алгоритмподписи	RFC 5280, раздел 4.1.1.2	
Значениеподписи	RFC 5280, раздел 4.1.1.3	
СертификатTBS	RFC 5280, раздел 4.1.2	
версия	RFC 5280, раздел 4.1.2.1	При использовании расширений, как это ожидается в данном профиле, ДОЛЖНА быть версия 3 (значение 2)
серийныйНомер	RFC 5280, раздел 4.1.2.2	Серийный номер ДОЛЖЕН быть положительным целым числом, присваиваемым CA каждому сертификату. Он ДОЛЖЕН быть уникальным для каждого сертификата, выпускаемого CA (т. е. имя выдающего и серийный номер идентифицируют уникальный сертификат). CA ДОЛЖНЫ обеспечивать, чтобы серийный Номер был неотрицательным целым числом. С учетом вышеупомянутых требований к уникальности ожидается, что серийные номера будут содержать длинный ряд целых чисел.

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
		Пользователи сертификата ДОЛЖНЫ быть способны обрабатывать значение `серийногоНомера` длиной до 20 октетов. CA, соблюдающие требования, НЕ ДОЛЖНЫ использовать значение `серийногоНомера` длиной более 20 октетов
	X.690, п. 8.3.2	Если октеты содержания кодировки значения целого числа включают более одного октета, то биты первого октета и бит 8 второго октета: a) не являются все единицами; b) не являются все нулями. *Примечание.* Эти правила гарантируют, чтобы значение целого числа всегда шифровалось с использованием возможно наименьшего количества октетов
	X.690, п. 8.3.3	Октеты содержания являются двоичным числом дополнительного кода, равным значению целого числа и состоящим из битов 8–1 первого октета, за которыми следуют биты 8–1 второго октета, затем биты 8–1 каждого очередного октета вплоть до и включая последний октет в октетах содержания
`подпись`	RFC 5280, раздел 4.1.1.2	Это поле ДОЛЖНО содержать тот же самый идентификатор алгоритма, что и поле `Алгоритмаподписи` в последовательности `Сертификат`
`выдающийорган`	RFC 5280, добавление A.1	`X520countryName ::= PrintableString (SIZE (2))` `X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))`
	RFC 5280, раздел 4.1.2.4	CA, удовлетворяющие этому профилю, ДОЛЖНЫ использовать кодировку поля `DirectoryString` в виде `PrintableString` или `UTF8String`
	ИСО 3166-1	
`срок действия`	RFC 5280, раздел 4.1.2.5	Поля `неРанее` и `неПозднее` могут шифроваться в `формателремениUTC` или с использованием `ОбобщенногоформатаВремени`. CA, удовлетворяющие этому профилю, ДОЛЖНЫ всегда шифровать даты срока действия сертификата с использованием `формателремениUTC` вплоть до 2049 года. Сроки действия сертификатов после 2050 года ДОЛЖНЫ шифроваться с использованием `ОбобщенногоформатаВремени`

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
(если кодируется в форматевремениUTC)	X.690, п. 11.8.1	Кодировка заканчивается буквой "Z", как указано в пункте документа ITU-T X.680 | ИСО/МЭК 8824-1, касающемся форматавремениUTC
	X.690, п. 11.8.2	Элемент "секунды" всегда присутствует
(если кодируется с использованием Обобщенногоформата Времени)	X.690, п. 11.7.1	Кодировка заканчивается буквой "Z", как указано в пункте документа ITU-T Rec. X.680 | ИСО/МЭК 8824-1, касающемся Обобщенногоформата Времени
	X.690, п. 11.7.2	Элемент "секунды" всегда присутствует
	RFC 5280, раздел 4.1.2.5.2	Значения в ОбобщенномформатеВремени НЕ ДОЛЖНЫ содержать долей секунды. Для целей этого профиля значения в ОбобщенномформатеВремени ДОЛЖНЫ выражаться с использованием среднего гринвичского времени и ДОЛЖНЫ включать секунды (т. е. сроки указываются как YYYYMMDDHHMMSSZ), даже если количество секунд равно нулю
субъект	RFC 5280, добавление A.1	X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
	RFC 5280, раздел 4.1.2.6	CA, удовлетворяющие этому профилю, ДОЛЖНЫ использовать кодировку поля DirectoryString в виде PrintableString или UTF8String
ИнформацияобОткрытом Ключесубъекта	RFC 5280, раздел 4.1.2.7	
УникальныйИдентификатор выдающего	RFC 5280, раздел 4.1.2.8	CA, удовлетворяющие этому профилю, НЕ ДОЛЖНЫ генерировать сертификаты с уникальными идентификаторами
УникальныйИдентификатор субъекта	RFC 5280, раздел 4.1.2.8	CA, удовлетворяющие этому профилю, НЕ ДОЛЖНЫ генерировать сертификаты с уникальными идентификаторами
расширения	X.690, п. 11.5	Шифрование значения набор или значения последовательность не включает кодировку какого-либо значения компонента, равного своему значению по умолчанию
ИдентификаторКлюча Полномочногооргана	RFC 5280, раздел 4.2.1.1	Для упрощения построения пути сертификации поле Идентификаторакключа расширения ИдентификаторКлючаполномочногооргана ДОЛЖНО включаться во все сертификаты,

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
		генерируемые CA, удовлетворяющими соответствующим требованиям. Существует одно исключение. В том случае, когда CA рассылает свой закрытый ключ в виде "самоподписанного" сертификата, идентификатор ключа полномочного органа МОЖЕТ быть опущен
ИдентификаторКлюча		
Орган,выдающий Сертификатполномочного органа		
Серийный номер Сертификатаполномочного органа		
ИдентификаторКлючаСубъекта	RFC 5280, раздел 4.2.1.2	Для упрощения построения пути сертификации данное расширение ДОЛЖНО присутствовать во всех сертификатах всех CA, удовлетворяющих требованиям, т. е. во всех сертификатах, включающих расширение основные ограничения (раздел 4.2.1.9), где значение "cA" соответствует "ВЕРНО"
ИдентификаторКлючаСубъекта		
ПрименимостьКлюча	RFC 5280, раздел 4.2.1.3	Ограничения по применимости ключа могут применяться в тех случаях, когда ключ, который мог бы использоваться более чем для одной операции, должен быть ограничен
цифроваяПодпись		Бит поля цифровойПодписи задается, когда открытый ключ субъекта используется вместе с механизмом цифровой подписи для поддержки средств защиты, отличных от подписания сертификата (бит 5) или подписания CRL (бит 6)
неотказуемость		
шифрованиеКлюча		
шифрованиеДанных		
Согласованиеключей		
ПодписьСертификатаключа		Бит поля ПодписинаСертификате ключа задается, когда открытый ключ субъекта используется для верификации подписи на сертификатах открытых ключей
подписьcRL		Бит поля подписиcRL задается, когда открытый ключ субъекта используется для верификации подписи на списке отзыва сертификатов

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
		(например, CRL, дельта-списки или ARL). Этот бит ДОЛЖЕН задаваться в сертификатах, которые используются для верификации подписи на списках CRL
Толькошифратор		
Толькодешифратор		
ПериодПрименимостиЗакрытого Ключа	RFC 3280, раздел 4.2.1.4	CA, удовлетворяющие этому профилю, НЕ ДОЛЖНЫ генерировать сертификаты с расширениями, касающимися периода применимости закрытого ключа, если только не присутствует по крайней мере один из этих двух компонентов и расширение не является критичным
неРанее		В случае их использования поля неРанее и неПозднее представляются в ОбобщенномформатеВремени и ДОЛЖНЫ указываться и интерпретироваться, как изложено в разделе 4.1.2.5.2
неПозднее		
Политикаприменения Сертификата	RFC 5280, раздел 4.2.1.4	Если это расширение является критичным, то программное обеспечение пути валидации ДОЛЖНО быть способно интерпретировать данное расширение (включая факультативный квалификатор) или ДОЛЖНО отвергнуть этот сертификат
ИнформацияоПолитике		
Идентификаторполитики		
Квалификаторыполитики		
СоответствиеПолитик	RFC 5280, раздел 4.2.1.5	
АльтернативноеИмяСубъекта	RFC 5280, раздел 4.2.1.6	
АльтернативноеИмяВыдающего	RFC 5280, раздел 4.2.1.7	
АтрибутыКаталогаСубъекта	RFC 5280, раздел 4.2.1.8	
Основные ограничения	RFC 5280, раздел 4.2.1.9	Расширение "основные ограничения" идентифицирует, является ли CA субъектом сертификата, а также максимальную глубину валидных путей сертификации, которые включает данный сертификат. CA, удовлетворяющие требованиям, ДОЛЖНЫ включать это расширение во все сертификаты CA, которые содержат открытые

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
		ключи, используемые для валидации цифровых подписей на сертификатах, и ДОЛЖНЫ помечать данное расширение в таких сертификатах как критичное
cA		Булеан cA указывает, принадлежит ли сертифицированный открытый ключ органу CA. Если булеан cA не задается, то бит поля ПодписьСертификатаключа в расширении применимости ключа НЕ ДОЛЖЕН задаваться
ОграничениеДлиныПути		
ОграниченияИмени	RFC 5280, раздел 4.2.1.10	
ОграниченияПолитики	RFC 5280, раздел 4.2.1.11	
РасширеннаяПрименимость Ключей	RFC 5280, раздел 4.2.1.12	Данное расширение указывает одну или несколько целей, для которых может использоваться сертифицированный открытый ключ, в дополнение или вместо основных целей, указанных в расширении "применимость ключа"
ПунктыРассылкиCRL	RFC 5280, раздел 4.2.1.13	
Пунктрассылки		
причины		
Орган,выпускающийCRL		
ЛюбаяПолитикаЗапрета	RFC 5280, раздел 4.2.1.14	
СамыйсвежийCRL	RFC 5280, раздел 4.2.1.15	
частныеРасширенияИнтернета	RFC 5280, раздел 4.2.2	
ИзменениеИмени		
ТипДокумента		
ТипСертификата браузера Netscape		
другие частные расширения		

Таблица B-2. Поля и расширения CRL

Компонент / расширение	*Ссылка*	*Соответствующие выдержки*
СписокСертификатов	RFC 5280, раздел 5.1.1	
СписокСертификатов tBS	RFC 5280, раздел 5.1.1.1	
Алгоритмподписи	RFC 5280, раздел 5.1.1.2	
Значениеподписи	RFC 5280, раздел 5.1.1.3	
	RFC 5280, раздел 5.1.2	
версия	RFC 5280, раздел 5.1.2.1	В этом факультативном поле указывается версия зашифрованного CRL. При использовании расширений, как это ожидается в данном профиле, это поле ДОЛЖНО присутствовать и ДОЛЖНО указывать версию 2 (значение целого числа 1)
подпись	RFC 5280, раздел 5.1.2.2	Это поле ДОЛЖНО содержать тот же идентификатор алгоритма, что и поле подписи в последовательности СписокСертификатов
выдающий	RFC 5280, добавление A.1	X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE 1..ub-serial-number))
	RFC 5280, разделы 5.1.2.3 и 4.1.2.4	CA, удовлетворяющие этому профилю, ДОЛЖНЫ использовать кодировку поля DirectoryString в виде PrintableString или UTF8String
текущееОбновление	RFC 5280, раздел 5.1.2.4	Удовлетворяющие требованиям этого профиля органы, выпускающие CRL, ДОЛЖНЫ шифровать поле текущее Обновление в формате времениUTC для дат до конца 2049 года. Удовлетворяющие требованиям этого профиля органы, выпускающие CRL, ДОЛЖНЫ шифровать поле текущееОбновление в оОбобщенном форматеВремени для дат после 2050 года
(если кодируется в формате времени UTC)	X.690, п. 11.8.1	Кодировка заканчивается буквой "Z", как указано в пункте документа ITU-T X.680 | ИСО/МЭК 8824-1, касающемся форматавремениUTC
	X.690, п. 11.8.2	Элемент "секунды" всегда присутствует

Компонент / расширение	***Ссылка***	***Соответствующие выдержки***
(если кодируется в ОбобщенномформатеВремени)	X.690, п. 11.7.1	Кодировка заканчивается буквой "Z", как указано в пунке документа ITU-T Rec. X.680 | ИСО/МЭК 8824-1, касающемся ОбобщенногоформатаВремени
	X.690, п. 11.7.2	Элемент "секунды" всегда присутствует
	RFC 5280, раздел 4.1.2.5.2	Значения в ОбобщенномформатеВремени НЕ ДОЛЖНЫ содержать долей секунды. Для целей этого профиля значения в ОбобщенномформатеВремени ДОЛЖНЫ выражаться с использованием среднего гринвичского времени и ДОЛЖНЫ включать секунды (т. е. сроки указываются как YYYYMMDDHHMMSSZ), даже если количество секунд равно нулю
Отозванные сертификаты	RFC 5280, раздел 5.1.2.6	При отсутствии отозванных сертификатов список отзыва сертификатов ДОЛЖЕН отсутствовать. В противном случае отозванные сертификаты указываются в списке по их серийным номерам
РасширенияCRL	RFC 5280, раздел 5.2	Отвечающие требованиям органы, выпускающие CRL, ДОЛЖНЫ включать во все выпущенные CRL расширения "идентификатор ключа полномочного органа" (раздел 5.2.1) и "номер CRL" (раздел 5.2.3)
	X.690, п. 11.5	Кодировка значения поля набор или значения поля последовательность не включает кодировку любого значения компонента, которое равно его значению по умолчанию
ИдентификаторКлюча полномочногооргана	RFC 5280, раздел 5.2.1	Отвечающие требованиям органы, выпускающие CRL, ДОЛЖНЫ использовать метод идентификатора ключа и ДОЛЖНЫ включать это расширение во все выпускаемые CRL
АльтернативноеИмя выдающего	RFC 5280, раздел 5.2.2	
Номер CRL	RFC 5280, раздел 5.2.3	Отвечающие требованиям этого профиля органы, выпускающие CRL, ДОЛЖНЫ отметить это расширение как некритичное. `CRLNumber ::= INTEGER (0..MAX)` С учетом вышеупомянутых требований ожидается, что номера CRL могут содержать длинный ряд целых чисел. Средства верификации CRL ДОЛЖНЫ быть способны обрабатывать значения номераCRL длиной до 20 октетов. Отвечающие требованиям органы,

Компонент / расширение	***Ссылка***	***Соответствующие выдержки***
		выпускающие CRL, НЕ ДОЛЖНЫ использовать значения номераCRL длиной более 20 октетов
	X.690, п. 8.3.2	Если октеты содержания кодировки значения целого числа включают более одного октета, то биты первого октета и бит 8 второго октета: a) не являются все единицами и b) не являются все нулями. *Примечание.* Эти правила гарантируют, чтобы значение целого числа всегда шифровалось с использованием возможно наименьшего количества октетов
	X.690, п. 8.3.3	Октеты содержания являются двоичным числом дополнительного кода, равным значению целого числа и состоящим из битов 8–1 первого октета, за которыми следуют биты 8–1 второго октета, затем биты 8–1 каждого очередного октета вплоть до и включая последний октет в октетах содержания
Индикатордельта-спискаCRL	RFC 5280, раздел 5.2.4	
ВыдающийПункт Распределения	RFC 5280, раздел 5.2.5	
самыйсвежийCRL	RFC 5280, раздел 5.2.6	
Кодпричин	RFC 5280, раздел 5.3.1	
Кодвременного приостановления сертификата	RFC 5280, раздел 5.3.2	
Дата утраты валидности сертификата	RFC 5280, раздел 5.3.3	
Органвыдачи сертификата	RFC 5280, раздел 5.3.4	

— — — — — — — —

Добавление C к части 12

БОЛЕЕ РАННИЕ ПРОФИЛИ СЕРТИФИКАТОВ (ИНФОРМАЦИОННОЕ)

Профили сертификатов в настоящем добавлении были определены в шестом издании документа ИКАО Doc 9303. Хотя CSCA ДОЛЖНЫ выпускать сертификаты, удовлетворяющие требованиям текущих профилей, определенных в разделе 7, более ранние профили приводятся здесь только для сведения, поскольку сертификаты, которые были выпущены в соответствии с более ранними профилями, будут находиться в обращении и обрабатываться системами проверки в течение нескольких лет.

Таблица C-1. Тело сертификата

Компонент сертификата	***Раздел в документе RFC 3280***	***Сертификат подписывающегося CA страны***	***Сертификат лица, подписывающего документы***	***Замечания***
Сертификат	4.1.1	m	m	
СертификатTBS	4.1.1.1	m	m	См. таблицу C-2
Алгоритм Подписи	4.1.1.2	m	m	Вводимое здесь значение зависит от выбранного алгоритма
Значение Подписи	4.1.1.3	m	m	Вводимое здесь значение зависит от выбранного алгоритма
СертификатTBS	4.1.2			
версия	4.1.2.1	m	m	ЯВЛЯЕТСЯ версией v3
серийныйНомер	4.1.2.2	m	m	
подпись	4.1.2.3	m	m	Вводимое здесь значение СОВПАДАЕТ с OID в поле Алгоритмаподписи
выдающийорган	4.1.2.4	m	m	
срокдействия	4.1.2.5	m	m	В вариантах реализации УКАЗЫВАЕТСЯ использование времени UTC до 2049 года, после чего используется ОбобщенныйформатВремени
субъект	4.1.2.6	m	m	

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося СА страны*	*Сертификат лица, подписывающего документы*	*Замечания*
ИнформацияобОткрытомКлючесубъекта	4.1.2.7	m	m	
УникальныйIDВыдающего	4.1.2.8	x	x	
УникальныйIDсубъекта	4.1.2.8	x	x	
расширения	4.1.2.9	m	m	См. таблицу С-2 для получения информации о том, какие расширения СЛЕДУЕТ использовать

Таблица С-2. Расширения

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося СА страны*	*Сертификат лица, подписывающего документы*	*Замечания*
ИдентификаторКлючаПолномочногооргана	4.2.1.1	o	m	Обязательное во всех сертификатах, за исключением самоподписанных сертификатов CSCA
ИдентификаторКлючаСубъекта	4.2.1.2	m	o	
ПрименимостьКлюча	4.2.1.3	mc	mc	Это расширение УКАЗЫВАЕТСЯ как КРИТИЧНОЕ
ПериодПрименимостиЗакрытогоКлюча	4.2.1.4	o	o	Таковым будет период, на который выдается закрытый ключ
ПолитикаПрименения Сертификата	4.2.1.5	o	o	
СоответствиеПолитик	4.2.1.6	x	x	
АльтернативноеИмя Субъекта	4.2.1.7	x	x	

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося CA страны*	*Сертификат лица, подписывающего документы*	*Замечания*
АльтернативноеИмя Выдающего	4.2.1.8	x	x	
АтрибутыКаталога субъектов	4.2.1.9	x	x	
ОсновныеОграничения	4.2.1.10	mc	x	Это расширение УКАЗЫВАЕТСЯ как КРИТИЧНОЕ
Ограничения вотношенииИмени	4.2.1.11	x	x	
Ограничения вотношенииПолитики	4.2.1.12	x	x	
Расширенная ПрименимостьКлючей	4.2.1.13	x	x	
ПунктыРассылкиCRL	4.2.1.14	o	o	Если государства или организации выдачи предпочитают использовать это расширение, то в качестве пункта распределения они ВКЛЮЧАЮТ ДОК ИКАО. Варианты реализации могут также включать связанные с этой функцией пункты распределения CRL для местных целей; другие принимающие государства могут их игнорировать
ЛюбаяПолитика Запрета	4.2.1.15	x	x	
СамыйсвежийCRL	4.2.1.16	x	x	
частноеРасширение Интернета	4.2.2	x	x	
Другие частные расширения	N/A	o	o	Если какое-либо частное расширение включается для национальных целей, тогда оно НЕ МАРКИРУЕТСЯ. Государствам или организациям выдачи не рекомендуется включать какие-либо частные расширения

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося CA страны*	*Сертификат лица, подписывающего документы*	*Замечания*
ИдентификаторКлюча Полномочногооргана	4.2.1.1			
ИдентификаторКлюча		m	m	Если данное расширение используется, то это поле как минимум ПОДДЕРЖИВАЕТСЯ
Орган,выдающий Сертификат Полномочногооргана		o	o	
Серийныйномер Сертификата Полномочногооргана		o	o	
ИдентификаторКлюча Субъекта	4.2.1.2			
идентификаторКлюча субъекта		m	m	
ПрименимостьКлюча	4.2.1.3			
цифроваяПодпись		x	m	
неотказуемость		x	x	
Шифрованиеключа		x	x	
Шифрованиеданных		x	x	
Согласованиеключей		x	x	
ПодписьСертификата Ключа		m	x	
ПодписьcRL		m	x	
Толькошифратор		x	x	
Толькодешифратор		x	x	
ОсновныеОграничения	4.2.1.10			
cA		m	x	Поле ДОСТОВЕРНЫЙ для сертификатов CA

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося CA страны*	*Сертификат лица, подписывающего документы*	*Замечания*
ОграничениеДлины Пути		m	x	0 – для нового сертификата CSCA, 1 – для связующего сертификата CSCA
ПунктыРассылкиCRL	4.2.1.14			
Пунктрассылки		m	x	
причины		m	x	
Орган,выпускающий cRL		m	x	
ПолитикаПрименения Сертификатов	4.2.1.5			
Информация оПолитике				
Идентификатор Политики		m	m	
Квалификаторы Политики		o	o	

— — — — — — — —

Добавление D к части 12

СОВМЕСТИМОСТЬ ПРОЦЕДУР ВАЛИДАЦИИ СТАНДАРТА RFC 5280 (ИНФОРМАЦИОННОЕ)

Настоящее добавление содержит рекомендации для принимающих государств, которые намерены использовать системы, применяющие указанные в документе [RFC 5280] алгоритмы валидации пути сертификации и CRL.

Модель доверия PKI электронного МСПД представляет собой сокращенный вариант модели, используемой процедурами валидации, определенными в документе [RFC 5280]. В разделе D.1 указана подгруппа этапов, взятых из содержащегося в документе [RFC 5280] определения, которые требуются для приложения электронного МСПД, и приводятся необходимые вводные данные и значения инициализации, а также процессы, используемые для валидации пути сертификации, валидации CRL и проверки статуса отзыва.

Раздел D.2 охватывает оставшиеся этапы из определения в документе [RFC 5280], которые не относятся к приложению электронного МСПД. В нем приводятся вводные данные и значения инициализации для валидации пути сертификации и валидации CRL. Инструктивный материал в этом разделе предназначен для использования в ситуациях, когда указанный инструментарий обеспечивает реализацию полных алгоритмов [RFC 5280], а не просто подгруппу этапов, описанную в разделе D.1.

В разделе D.3 приводится инструктивный материал для поддержки расширения обработки CRL, основанной на документе [RFC 5280], с включением проверки статуса отзыва после того, как CSCA изменил имя.

D.1 ЭТАПЫ, ОТНОСЯЩИЕСЯ К ЭЛЕКТРОННОМУ МСПД

Изложенные здесь процедуры валидации пути сертификации для электронного МСПД основаны на процедуре, описанной в документе [RFC 5280]. Используются та же терминология и то же описание процесса. Профили сертификата электронного МСПД ограничивают пути сертификации только одним сертификатом и запрещают использование многих факультативных характеристик, которые применяются в других приложениях, таких как PKI Интернета, описанные в документе [RFC 5280]. Этапы валидации пути, связанные с этими характеристиками, исключаются из процедуры валидации сертификации пути для электронного МСПД.

D.1.1 Процедура валидации пути сертификации

D.1.1.1 Вводные данные

Документ [RFC 5280] определяет набор из девяти вводных данных для алгоритма валидации пути. С приложением электронного МСПД связаны только следующие три элемента:

- Путь сертификации. Единственный сертификат (например, сертификат лица, подписывающего документы).
- Текущие дата/время.

- Информация "якоря доверия", включая:

  - доверительное имя органа выдачи. Если "якорь доверия" представляет собой сертификат CSCA, то имя доверительного органа выдачи соответствует значению поля `субъекта` этого сертификата;

  - алгоритм доверительных открытых ключей. Если "якорь доверия" представляет собой сертификат CSCA, то алгоритм доверительных открытых ключей берется из поля `Информацияоботкрытомключесубъекта` данного сертификата;

  - доверительный открытый ключ. Если "якорь доверия" представляет собой сертификат CSCA, то доверительный открытый ключ берется из поля `ИнформацияобОткрытомКлючеСубъекта` данного сертификата;

  - параметры доверительного открытого ключа. Это факультативные вводные данные, которые включаются только в том случае, когда для алгоритма доверительного открытого ключа требуются параметры. Если "якорь доверия" представляет собой сертификат CSCA, то эти параметры берутся из поля `ИнформацияобОткрытомКлючеСубъекта` данного сертификата.

В том случае, если вариант реализации требует предоставления дополнительных шести вводных элементов, соответствующие рекомендации для них приводятся в разделе D.2.

Для CSCA, выдавшего сертификат, который подлежит валидации, могут существовать несколько "якорей доверия". Из числа этих "якорей доверия" использоваться ДОЛЖЕН тот, который содержит открытый ключ, соответствующий значению в расширении идентификатора ключа полномочного органа в сертификате, который валидируют.

D.1.1.2 Инициализация

В документе [RFC 5280] определены 11 переменных параметров для государства. К приложению электронного МСПД имеют отношение только 5 следующих элементов:

- приложение: "максимальная_длина_пути": инициализация с установкой на "0";

- "рабочее_имя_органа_выдачи": инициализация с установкой значения доверительного имени органа выдачи;

- "рабочий_алгоритм_открытого_ключа": инициализация с установкой значения доверительного алгоритма открытого ключа;

- "рабочий_открытый_ключ": инициализация с установкой значения доверительного открытого ключа;

- "рабочие_параметры_открытого_ключа": инициализация с установкой значений доверительных параметров открытого ключа.

Если вариант реализации предусматривает инициализацию дополнительных шести переменных параметров, рекомендации по ним приводятся в разделе D.2.

D.1.1.3 Обработка сертификатов

Этапы обработки сертификата электронного МСПД представляют собой подмножество этапов, описанных в документе [RFC 5280]. Результат обработки сертификата электронного МСПД, используя этот упрощенный процесс, будет соответствовать результату, полученному с использованием полного алгоритма RFC 5280. Если дополнительные вводные данные и переменные параметры государства сконфигурированы, как это описано в разделе D.2, следует выполнить следующее:

a) Проверить основную информацию о сертификате. Сертификат ДОЛЖЕН удовлетворять каждому из нижеследующих условий:

- подпись на сертификате может быть верифицирована с использованием рабочего алгоритма открытого ключа, рабочего открытого ключа и рабочих параметров открытого ключа;
- период действия сертификата включает текущее время;
- в текущий период сертификат не отзывается (подробная информация приведена в п. 6.3);
- имя органа, выпустившего сертификат, является рабочим_именем_выдающего органа.

b) Задать рабочему_открытому_ключу_поле `ОткрытыйКлючсубъекта` сертификата.

c) Если поле `ИнформацияобОткрытомКлючесубъекта` сертификата содержит поле алгоритма с параметрами "non-null" (не пустые), задать указанные параметры переменному элементу "рабочие_параметры_открытого_ключа". Если поле `ИнформациобОткрытом Ключесубъекта` сертификата содержит поле алгоритма с параметрами "null" (пустые) или параметры опущены, сравнить алгоритм в поле `ОткрытыйКлючсубъекта` сертификата с "рабочим_алгоритмом_открытого_ключа". Если алгоритм в поле `ОткрытыйКлючсубъекта` и рабочий алгоритм открытого ключа отличаются друг от друга, установить параметры_рабочего_открытого_ключа на "null" (пустые).

d) Задать переменной рабочего_алгоритма_открытого_ключа поле `ОткрытыйКлючсубъекта` алгоритма сертификата.

e) Распознать и обработать другие критичные расширения, присутствующие в сертификате.

f) Обработать любые другие идентифицированные некритичные расширения, присутствующие в сертификате.

Если какая-либо проверка на этапе a) дает сбой или если в сертификате имеются какие-либо неидентифицированные критичные расширения, которые нельзя обработать, процедура валидации пути является неуспешной. В противном случае процедура является успешной.

D.1.1.4 Выходные данные

Если валидация пути проходит успешно, указанная процедура завершается выдачей индикации успешной операции вместе с выдачей рабочего_открытого_ключа, рабочего_алгоритма_открытого_ключа и параметров_рабочего_открытого_ключа.

Если валидация пути оказывается неуспешной, эта процедура завершается выдачей индикации сбоя и соответствующей причины.

D.1.2 Валидация CRL и проверка статуса отзыва

Алгоритм валидации CRL, содержащийся в документе [REC 5280], охватывает различные типы CRL, включая дельта-списки CRL, секционированные CRL, косвенные CRL и т. д. Профиль CRL для приложения электронного МСПД является очень ограничительным и запрещает использование каких-либо из этих характеристик. Использование расширения `выдающийПунктРаспределения`, а также всех стандартизированных расширений для записей CRL также запрещено. Как результат, валидация CRL и проверка статуса отзыва для приложения электронного МСПД являются относительно простыми.

D.1.2.1 Вводные данные

В документе [RFC 5280] определены два вида вводных данных для алгоритма валидации CRL. Приложение электронного МСПД связано только с одним из этих видов данных. Если вариант реализации предусматривает предоставление дополнительных вводных данных, рекомендации по ним приводятся в разделе D.2.

- Сертификат: серийный номер сертификата и имя органа выдачи.

D.1.2.2 Инициализация

В документе [RFC 5280] определены три переменных параметра для государства. Приложение электронного МСПД связано только со следующим из этих параметров. Если вариант реализации предусматривает инициализацию дополнительных двух переменных, рекомендация по ним приводится в разделе D.2.

- Статус_ сертификата: инициализировать с установкой значения НЕ ОТОЗВАН.

D.1.2.3 Обработка CRL

Все CRL в электронном МСПД являются полными списками CRL, охватывающими все текущие сертификаты, выданные CSCA, которые выпустили CRL. Никаких секционированных CRL, дельта-списков CRL или косвенных CRL не существует. Этапы алгоритма обработки CRL для приложения электронного МСПД включают следующее:

a) Получение текущего CRL для CSCA, выпустившего данный сертификат. Если этот CRL невозможно получить, переменная статуса_сертификата устанавливается на "НЕ ОПРЕДЕЛЕН" и обработка прекращается.

b) Верификация того, что орган, выпустивший CRL, является тем же CSCA, который выпустил рассматриваемый сертификат. Поскольку в каждой стране имеется единственный CSCA, а приложение электронного МСПД является закрытым приложением с системами проверки, сохраняющими буферную память списков CRL, являющуюся уникальной для данного приложения, проверка того, что название страны совпадает с тем, что содержится в поле выдающего органа CRL и в поле выдающего органа сертификата, является достаточной.

    - Если CSCA не сменил имя после выпуска данного сертификата, поле органа выдачи в CRL и поле органа выдачи в сертификате будут идентичными.

    - Если CSCA сменил имя после выпуска сертификата, атрибут страны его имени в поле выдающего органа сертификата и в поле выдающего органа CRL будет одинаковым, однако некоторые другие атрибуты могут быть изменены.

- Если пользователь пожелает убедиться в том, что некоторый не связанный с электронным МСПД список CRL не заменен, он может в факультативном порядке проверить, что у него имеются "якоря доверия" для обоих имен CSCA и что эти "якоря доверия" связаны с одним и тем же CSCA. Если CSCA изменил имя и включил в CRL факультативное расширение `альтернативное имя выдающего`, пользователь МОЖЕТ в факультативном порядке убедиться в том, что поле выдающего органа в сертификате идентично одному из значений в этом расширении.

Если орган, выпустивший CRL, не является CSCA, который выпустил этот сертификат, переменная "статус сертификата" задается как "НЕ ОПРЕДЕЛЕН" и обработка прекращается.

c) Валидация пути сертификации для органа, выпустившего CRL. Следует отметить, что в приложении электронного МСПД все CRL выпускаются CSCA, которые являются "якорями доверия" для соответствующих путей. В отличие от алгоритма, приведенного в документе [RFC 5280], приложение электронного МСПД не требует, чтобы "якорь доверия", используемый для пути сертификации CRL, был тем же "якорем доверия", который использовался для валидации требуемого сертификата. Однако если "якоря доверия" различные, оба они ДОЛЖНЫ быть "якорями доверия" для одного и того же CSCA. В отличие от стандарта [RFC 5280] приложение электронных МСПД имеет несколько одновременно действующих "якорей доверия" для заданного CSCA. Если путь сертификации не может быть успешно валидирован, переменная статус_сертификата задается как "НЕ ОПРЕДЕЛЕН" и обработка прекращается.

d) Верификация подписи на CRL. Если подпись не может быть успешно верифицирована, переменная статус_сертификата задается как "НЕ ОПРЕДЕЛЕН" и обработка прекращается.

e) Поиск сертификата в CRL. Если в списке найдена запись данных, совпадающих с органом выдачи и серийным номером сертификата, переменная статус_сертификата задается как "НЕ УКАЗАН".

D.1.2.4 Выходные данные

Возвращение к статусу_сертификата. Если этапы a), b), c) или d) оказались неуспешными, статус будет "НЕ ОПРЕДЕЛЕН". Если данный сертификат числится в списке CRL как отозванный, статус будет "НЕ УКАЗАН". Если валидация CRL прошла успешно и сертификат не числится в CRL, статус будет "НЕ ОТОЗВАН".

D.2 ЭТАПЫ, НЕ ТРЕБУЕМЫЕ ЭЛЕКТРОННЫМ МСПД

D.2.1 Валидация пути сертификации

Установочные данные для дополнительных вводных данных, которые не связаны с валидацией электронного МСПД, включают:

- начальные вводные данные "запрет на сравнение политик": задать запрет на сравнение политик;

- начальные вводные данные "любая политика запрета": задать запрет на обработку значения поля "любая политика";

- начальные вводные данные "разрешенные поддеревья": задать разрешение на все поддеревья;
- начальные вводные данные "исключенные поддеревья": задать неисключение каких-либо поддеревьев;
- начальные вводные данные "четко определенная политика": этот параметр НЕ следует задавать;
- "начальный набор политик для пользователя": задать специальное значение "любая политика".

Инициализация переменных параметров государства, которые не связаны с приложением электронного МСПД, включает:

- разрешенные_поддеревья: инициализировать разрешением всех поддеревьев;
- исключенные_поддеревья: инициализировать неисключением каких-либо поддеревьев;
- любая_политика_запрета: если заданы начальные вводные данные "любая политика запрета", инициализировать с установкой на "0". В противном случае установить значение 1 или любое большее значение;
- соответствие_политик: инициализировать с установкой на "0";
- четко_определенная_политика: инициализировать с установкой на "2";
- дерево_действующей_политики: инициализировать элемент действующая_политика, задав "любая политика", инициализировать элемент набор_квалификаторов, задав "пусто", а ожидаемый_набор_политик установить на "любая политика".

D.2.2 Валидация CRL

Установочные данные для дополнительных вводных данных, которые не связаны с валидацией электронного МСПД, включают:

- "использование дельта-списков": задать запрет на использование дельта-списков.

Инициализация переменных параметров государства, которые не связаны с приложением электронного МСПД, включают:

- маскирование_причин: инициализировать, задав "пустой набор";
- маскирование_промежуточных_причин: инициализировать, задав специальное значение "все причины".

D.3 МОДИФИКАЦИИ, ТРЕБУЕМЫЕ ДЛЯ ОБРАБОТКИ CRL

Система валидации CRL, удовлетворяющая требованиям процедуры валидации CRL, изложенная в документе [RFC 5280], не предназначена для поддержки среды, связанной с изменением имени CA, как это имеет место, например, в случае приложения электронного МСПД. Поэтому эти системы требуют некоторой модификации для обеспечения валидации в особом случае, описанном ниже:

a) В п. 6.3.3 на этапе a) процедуры валидации CRL, описанной в документе [RFC 5280], для обновления локальной буферной памяти с соответствующим(и) CRL используется имя в поле "пункт распределения" расширения "пункты распределения CRL" рассматриваемого сертификата. Для приложения электронного МСПД этот этап необходимо модифицировать, и следует использовать только атрибут `название страны` поля "пункт распределения", чтобы идентифицировать и получить надлежащий CRL.

b) В п. 6.3.3 на этапе f) процедуры валидации CRL, описанной в документе [RFC 5280], существует требование о том, что для валидации пути сертификации для органа выдачи CRL должен использоваться тот же самый "якорь доверия", который использовался для валидации требуемого сертификата. Применительно к приложению электронного МСПД такого требования НЕТ, поскольку для каждого открытого ключа CSCA устанавливаются независимые "якоря доверия".

"Якорь доверия", используемый для валидации органа выдачи CRL, будет тем самым "якорем доверия" для открытого ключа CSCA, который соответствует закрытому ключу, использованному для подписания CRL. "Якорь доверия", используемый в целях валидации пути сертификации для требуемого сертификата, может быть тем, который применялся для более ранней пары ключей CSCA.

— — — — — — — —

Добавление E к части 12

ПРИМЕР LDS2 (ИНФОРМАЦИОННОЕ)

Пример, приводимый ниже, иллюстрирует взаимодействие между различными компонентами подписи и авторизации LDS2 с использованием PKI.

Для иллюстрации взаимодействия и проводимых предварительных мероприятий, необходимых для реализации характерного бизнес-сценария, рассмотрим сценарий, в рамках которого страна Dystopia выразила желание вносить путевые отметки в паспорта граждан страны Utopia. Позднее страна Atlantis выразила желание считывать путевые отметки, внесенные страной Dystopia в паспорта граждан страны Utopia.

Предварительные мероприятия заключаются в следующем:

- Для внесения проездных отметок Utopia установила на своих паспортах приложение LDS2.
- Dystopia и Utopia разработали собственные системы авторизации LDS2 с использованием PKI.
- Для выдачи сертификатов органам, подписывающим LDS2, Dystopia разработала свои подписи LDS1 с использованием PKI.
- На каком-то этапе Utopia и Dystopia на доверительной основе обменялись сертификатами CVCA и сертификатами клиентов и серверов SPOC (вследствие чего появилась возможность обмена новыми сертификатами CVCA и SPOC непосредственно через SPOC).
- На каком-то этапе Utopia и Atlantis на доверительной основе обменялись сертификатами CVCA и сертификатами клиентов и серверов SPOC (вследствие чего появилась возможность обмена новыми сертификатами CVCA и SPOC непосредственно через SPOC). Если приложение LDS2, предназначенное для внесения путевых отметок, открыто для считывания, т. е. любая страна может считывать проездные отметки LDS2 (разрешение требуется только для внесения информации), то этот этап можно пропустить.
- На каком-то этапе Dystopia и Atlantis на доверительной основе обменялись сертификатами CSCA.

Периодический процесс, обеспечивающий возможность внесения Dystopia электронных отметок в электронные МСПД граждан Utopia, заключается в следующем:

- Dystopia запрашивает у Utopia сертификат DV.
- Для инициирования соединения SPOC-SPOC Dystopia использует свой сертификат клиента SPOC и сертификат сервера SPOC Utopia. Затем DV Dystopia формирует запрос и направляет его из одного SPOC другому SPOC. Получив запрос, Utopia оформляет сертификат зарубежного DV, предоставляющий доступ Dystopia к считыванию/внесению информации, и этот сертификат возвращается в рамках взаимодействия между соответствующими SPOC.

- После получения сертификата DV от своего SPOC DV Dystopia оформляет сертификаты терминалов для терминалов, используемых на ее границах. Взаимодействуя с паспортом ИС, встроенные в паспорта граждан Utopia, проверяют соответствие сертификата Dystopia с сертификатом DV Dystopia и сертификата DV Dystopia с сертификатом CVCA Utopia. Затем ИС предоставляет терминалу Dystopia доступ к приложению LDS2 для считывания/внесения электронных путевых отметок в электронные МСПД.

Процесс внесения электронных отметок в электронные МСПД заключается в следующем:

- Dystopia формирует электронную путевую отметку и подписывает ее закрытым ключом, соответствующим открытому ключу, хранимому в сертификате органа, подписывающего LDS2 (путевая отметка) с использованием PKI, подписывающей LDS2 Dystopia. Сертификат органа, подписывающего LDS2, хранится на бесконтактной ИС паспорта гражданина Utopia.

При обработке паспорта гражданина Utopia на границе Atlantis:

- Если считывание путевых отметок с паспортов граждан Utopia требует наличия сертификата терминала с доступом к считыванию, запрос из Atlantis в Utopia направляется посредством взаимодействия между соответствующими SPOC. При получении запроса Utopia оформляет для Atlantis сертификат зарубежного DV с доступом к считыванию и направляет этот сертификат в Atlantis в рамках взаимодействия соответствующих SPOC. Используя сертификат DV, Atlantis формирует для терминалов Atlantis сертификаты терминалов с доступом к считыванию паспортов граждан Utopia. Если путевые отметки в паспорте гражданина Utopia можно считывать любым терминалом, то этот этап можно пропустить.

- Для верификации путевой отметки в паспортах, внесенных страной Dystopia, Atlantis использует LDS1, подписанную с помощью PKI. Хранимый в паспорте сертификат органа Dystopia, подписывающего LDS2, используется для верификации путевой отметки. Затем создается цепочка, т. е. сертификат органа Dystopia, подписавшего LDS2, верифицируется с использованием предварительно полученного сертификата CSCA Dystopia.

— КОНЕЦ —

ISBN 978-92-9275-569-0