ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание седьмое, 2015

Часть 12. Инфраструктура открытых ключей для МСПД

Утверждено Генеральным секретарем и опубликовано с его санкции

Международная организация гражданской авиации

ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание седьмое, 2015

Часть 12. Инфраструктура открытых ключей для МСПД

Утверждено Генеральным секретарем и опубликовано с его санкции

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***
ISBN 978-92-9249-946-4

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

ИСПРАВЛЕНИЯ		
№	Дата	Кем внесено

ОГЛАВЛЕНИЕ

Страница

Страница

1. СФЕРА ПРИМЕНЕНИЯ

В седьмом издании документа Doc 9303 изменена структура спецификаций ИКАО для машиносчитываемых проездных документов. Без внесения принципиальных изменений в конкретные технические требования данное новое издание Doc 9303 скомпоновано в виде свода спецификаций машиносчитываемых официальных проездных документов размера 1 (ПД1), машиносчитываемых официальных проездных документов размера 2 (ПД2) и машиносчитываемых проездных документов размера 3 (ПД3), а также виз. Такой комплект спецификаций состоит из различных самостоятельных документов, в которых сгруппированы общие, т. е. применимые ко всем МСПД, спецификации, а также технические требования, относящиеся к конкретному формату МСПД.

Настоящая часть 12 документа Doc 9303 основана на шестом издании тома 2 *"Спецификации на электронные паспорта со средствами биометрической идентификации"* части 1 *"Машиносчитываемые паспорта"* документа Doc 9303 (2006) и на третьем издании тома 2 *"Спецификации на электронные МСПД со средствами биометрической идентификации"* части 3 *"Машиносчитываемые официальные проездные документы"* документа Doc 9303 (2008).

В части 12 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 CRL. Кроме того, устанавливаются требования в отношении принимающих государств и их систем проверки, которые валидируют эти сертификаты и CRL.

Часть 12 документа Doc 9303 следует рассматривать вместе с:

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

В части 12 документа Doc 9303 изложены спецификации профиля PKI электронных МСПД, 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

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

- **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) лиц, 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.

- **Лица, подписывающие документы (DS).** Лицо, подписывающее документы, подписывает в цифровой форме данные, подлежащие хранению на электронных МСПД; эта подпись хранится в объекте защиты документа.

- **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 документов, 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 лиц, подписывающих документы.

CSCA каждого государства или организации выдачи играет роль предмета 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 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 лиц, подписывающих документы (C_{DS}), других сертификатов и списков CRL.

Сертификаты национального сертифицирующего полномочного органа с правом подписи (C_{CSCA}) используются для валидации сертификатов лиц, 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.

3.2 Лицо, подписывающее документы

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

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

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

Каждый сертификат лица, 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 лица, подписывающего документы, применительно к каждому электронному МСПД.

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

3.3 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 произвести валидацию пути сертификации, как указано в разделе 6.

3.4 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.

3.5 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.

4. УПРАВЛЕНИЕ КЛЮЧАМИ

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

- пара ключей подписывающегося CA страны и
- пара ключей лиц, подписывающих документы.

Государство или организация выдачи МОГУТ иметь дополнительные типы ключей:

- пара ключей органа, подписывающего мастер-списки, и
- пара ключей органа, подписывающего списки отклонений.

Пары ключей подписывающегося CA страны, лиц, подписывающих документы, органа, подписывающего мастер-списки, и органа, подписывающего списки отклонений, выпускаются с использованием сертификатов формата [X.509]. Содержащиеся в сертификатах CSCA открытые ключи используются для верификации подписи CSCA на выпущенных сертификатах (лицо, подписывающее документ; орган, подписывающий мастер-список; орган, подписывающий список отклонений и CSCA) и на выпущенных CRL. Открытые ключи, содержащиеся в сертификатах лица, подписывающего документы, используются для верификации цифровых подписей, созданных с помощью соответствующего закрытого ключа субъектом лица, подписывающего документы, на объектах защиты документа (SO_D). Открытые ключи, содержащиеся в сертификатах органа, подписывающего мастер-списки, используются для верификации цифровой подписи на мастер-списках. Открытые ключи, содержащиеся в сертификатах органа, подписывающего списки отклонений, используются для верификации цифровой подписи на списках отклонений (указанных в части 3 документа Doc 9303).

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 применяемостью закрытого ключа и сроком действия открытого ключа, как указано в таблице 1.

Таблица 1. Применяемость и сроки действия ключей

	Использование закрытого ключа	***Срок действия открытого ключа (предположительный срок действия паспорта 10 лет)***
Подписывающийся CA страны	3–5 лет	13–15 лет
Лицо, подписывающее документы	До 3 мес[1]	Приблизительно 10 лет
Орган, подписывающий мастер-списки	По усмотрению государства или организации выдачи	По усмотрению государства или организации выдачи
Орган, подписывающий списки 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` (применяемость закрытого ключа) сертификата DS, может быть несколько более длинным для обеспечения перекрываемости или в силу производственных требований.

4.1 Ключи и сертификаты лиц, подписывающих документы

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

4.1.1 Период действия открытого ключа лиц, подписывающих документы

Срок службы (т. е. период действия сертификата) лица, 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 лица, 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.

4.1.2 Период, на который выдается закрытый ключ лицам, подписывающим документы

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

Государство или организация могут назначить одного или более лиц, подписывающих документы (с парой собственных уникальных ключей у каждого), которые будут обеспечивать соответствующие функции в любое данное время.

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

- устанавливать очень короткий период применяемости закрытого ключа; и/или
- назначить одновременно несколько лиц, подписывающих документы, которые будут функционировать в одно и то же время, причем у каждого будет свой собственный уникальный закрытый ключ и сертификат открытого 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 от момента выдачи электронного МСПД до момента, когда он становится действительным.

Государство или организация выдачи, которые выдают небольшое число электронных МСПД в день, могут принять решение о назначении одного лица, подписывающего документы, и им может также оказаться удобным установить несколько более продолжительный период применяемости закрытого ключа.

Независимо от количества электронных МСПД, выпускаемых ежедневно, или количества одновременно функционирующих лиц, которые подписывают документы, РЕКОМЕНДУЕТСЯ, чтобы максимальный период использования любого закрытого ключа лица, 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.

4.2 Ключи и сертификаты CSCA

Период применяемости закрытого ключа CSCA гораздо короче, чем период действия сертификата для соответствующего открытого ключа.

4.2.1 Период действия открытого ключа подписывающегося CA страны

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

- продолжительность применения соответствующего закрытого ключа CSCA для подписания сертификатов лиц, подписывающих документы (C_{DS});
- срок службы сертификатов открытых ключей лиц, подписывающих документы (см. п. 4.1.1).

4.2.2 Период, на который выдается закрытый ключ подписывающемуся CA страны

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

- В маловероятном случае компрометации закрытого ключа подписывающегося CA государства или организации выдачи действительность всех электронных МСПД, выданных с использованием ключей лица, подписывающего документы, чьи сертификаты были подписаны скомпрометированным закрытым ключом CSCA, подвергается сомнению. В этой связи государства или организации выдачи МОГУТ пожелать устанавливать довольно короткий срок применяемости ключа.
- Однако поддержание очень короткого периода применяемости в определенный момент приведет к одновременному наличию очень большого количества 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.

4.2.3 Замена ключа подписывающегося CA страны

Ключи CSCA являются предметами доверия во всей системе, без которых система разрушится. Поэтому государствам или организациям выдачи СЛЕДУЕТ тщательно планировать замену своей пары ключей CSCA. По истечении первоначального периода применяемости 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 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 сертификатов, включая сертификаты лиц, подписывающих документы, а также для подписания списков CRL государства или организации выдачи ДОЛЖНЫ использовать самый новый закрытый ключ CSCA.

4.3 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, подписы-

вающего 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.

4.3.1 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 подписывающегося CA страны" в разделе 4.2), отзыв старого сертификата CSCA также влечет за собой ОТЗЫВ нового сертификата CSCA.

Если необходимо отозвать сертификат CSCA, 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.

4.3.2 Отзыв других сертификатов

Когда государство или организация выдачи решают отозвать сертификат лица, подписывающего документы; органа, подписывающего мастер-списки; органа, подписывающего списки отклонений, или средств связи, им не надо ждать до тех пор, пока истечет очередной период обновления текущего CRL. Новый CRL РЕКОМЕНДУЕТСЯ выпускать в течение 48 ч с момента уведомления об отзыве.

4.4 Криптографические алгоритмы

Государство или организация выдачи ДОЛЖНЫ поддерживать один и тот же алгоритм для использования в своих CSCA и ключах подписи документов, несмотря на то, что могут потребоваться различные размеры ключей в зависимости от выбранного алгоритма.

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 государство или организация выдачи ПОДДЕРЖИВАЮТ один из нижеуказанных алгоритмов.

4.4.1 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 [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.

4.4.2 Алгоритм цифровой подписи (DSA)

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

4.4.3 DSA на основе эллиптической кривой (ECDSA)

Государства или организации выдачи, применяющие алгоритм ECDSA для генерирования или верификации подписи, ИСПОЛЬЗУЮТ стандарт [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].

4.4.4 Алгоритмы хэширования

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

5. МЕХАНИЗМЫ РАССЫЛКИ

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.

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

- сертификаты CSCA;
- сертификаты лиц, подписывающих документы;
- списки CRL (null (пустые) и non-null (не пустые));
- сертификаты органа, подписывающего мастер-списки; мастер-списки;
- сертификаты органа, подписывающего списки отклонений.

Механизмы рассылки, используемые в инфраструктуре PKI электронных МСПД, включают следующее:

- ДОК;
- двусторонний обмен;
- 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 2.

Таблица 2. Первичный и вторичный механизмы рассылки

	Сертификаты CSCA	***Сертификаты лица, подписывающего документы***	***CRL (Null и Non-null) (пустые и не пустые)***	***Сертификаты органа, подписывающего мастер-списки***	***Мастер-списки***	***Сертификаты органа, подписывающего списки отклонений***
Первичный	Двусторонний	Бесконтактная ИС электронных МСПД	Двусторонний	Мастер-списки	ДОК/ двусторонний	Списки отклонений
Вторичный	Мастер-списки	ДОК	ДОК			

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 лиц, 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 лиц, подписывающих документы (C_{DS}), путем включения таких сертификатов в объекты защиты документов (SO_D). Им следует ожидать, что сертификаты лиц, подписывающих документы (C_{DS}), опубликованные в ДОК, также будут рассылаться пограничным пунктам в течение 48 ч.

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 (C_{DS}), 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 лица, подписывающего документы (C_{DS}), 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.

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. Мастер-списки ДОЛЖНЫ удовлетворять спецификациям, изложенным в разделе 8.

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 существует 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, 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 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 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

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 (C_{CSCA}), используются для верификации цифровых подписей на сертификатах (включая сертификаты лица, подписывающего документы, органа, подписывающего мастер-списки, и органа, подписывающего списки отклонений) 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, доверительную копию сертификата CSCA (C_{CSCA}) 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 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 в расширении "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.

6.2 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 доку-

менте 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].

7. ПРОФИЛИ СЕРТИФИКАТОВ И CRL

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 разделе 7.1 для следующих типов сертификата:

- подписывающийся CA страны;
- лицо, подписывающее 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 подписаывающегося CA страны, лица, подписывающего документы, и органа, подписывающего мастер-списки CSCA, определяются в разделе 3. Объект органа, подписывающего списки отклонений, определяется в части 3 документа Doc 9303.

Профиль CRL определяется в разделе 7.2.

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.

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 Профили сертификатов

В таблице 3 определены предусмотренные профилем сертификата требования к полям основной части сертификата. В таблице 4 указаны требования к расширениям сертификата.

Таблица 3. Профиль полей сертификата

Компонент сертификата	***Присутствие***	***Замечания***
Сертификат	m	
Сертификат TBS	m	См. следующую часть таблицы
Алгоритм подписи	m	Вводимые здесь значения зависят от выбранного алгоритма
значение подписи	m	Вводимые здесь значения зависят от выбранного алгоритма
Сертификат TBS		
версия	m	ДОЛЖНА быть v3
серийный номер	m	ДОЛЖНО быть положительное целое число и максимум 20 октетов. ДОЛЖНО применяться шифрование с использованием дополнительного кода и номер ДОЛЖЕН представляться наименьшим количеством октетов
подпись	m	Вводимое здесь значение ДОЛЖНО быть таким же, как в компоненте "алгоритм подписи" последовательности "сертификат"
выдающий	m	Название страны и серийный номер, если таковые присутствуют, ДОЛЖНЫ быть печатаемой строкой. Другие атрибуты, имеющие синтаксис строки каталога, ДОЛЖНЫ быть либо печатаемой строкой, либо строкой формата UTF8. Название страны ДОЛЖНО состоять из прописных букв. Информация по соглашениям об именовании приводится в п. 7.1.1

Компонент сертификата	*Присутствие*	*Замечания*
срок действия	m	Данные ДОЛЖНЫ заканчиваться буквой Z. Элемент "секунды" ДОЛЖЕН присутствовать. Сроки вплоть до 2049 года ДОЛЖНЫ указываться в формате времени UTC. Время UTC ДОЛЖНО быть представлено в виде YYMMDDHHMMSSZ. Сроки после 2050 года ДОЛЖНЫ указываться в обобщенном формате времени. Обобщенный формат времени НЕ ДОЛЖЕН содержать долей секунд. Обобщенный формат времени ДОЛЖЕН быть представлен в виде YYYYMMDDHHMMSSZ
субъект	m	Название страны и серийный номер, если таковые присутствуют, ДОЛЖНЫ быть печатаемой строкой. Другие атрибуты, имеющие синтаксис строки каталога, ДОЛЖНЫ быть лицо печатаемой строкой, либо строкой формата UTF8. Название страны ДОЛЖНО состоять из прописных букв. Название страны в поле "выдающий" и в поле "субъект" ДОЛЖНО совпадать. Информация по соглашениям об именовании приводится в п. 7.1.1
Информация об открытом ключе субъекта	m	
уникальный идентификатор выдающего	x	
уникальный идентификатор субъекта	x	
расширения	m	См. следующую таблицу, где указано, какие расширения следует включать. Значения по умолчанию для расширений НЕ ДОЛЖНЫ шифроваться

Таблица 4. Профиль расширения сертификата

Название расширения	***Самоподписанные исходные серти-фикаты CSCA***		***Связующие сертификаты CSCA***		***Лицо, подписыва-ющее документы***		***Орган, подписывающий мастер-списки, и орган, подписывающий списки отклонений***		***Средства связи***		***Замечания***
	Присутствие	***Критичность***	***Присутствие***	***Критичность***	***Присутствие***	***Критичность***	***Присутствие***	***Критичность***	***Присутствие***	***Критичность***	
Идентификатор ключа полномочного органа	**o**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	
идентификатор ключа	m		m		m		m		m		
лицо, выдающее сертификат полномочного органа			o		o		o		o		
Серийный номер сертификата полномочного органа	o		o		o		o		o		
Идентификатор ключа субъекта	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
Идентификатор ключа субъекта	m		m		m		m		m		
Применяемость ключа	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	
цифровая подпись	x		x		m		m		o		Некоторые сертификаты средств связи (например, сертификаты TLS) преду-сматривают, чтобы биты поля "Применяемость ключа" устанавливались в соответствии с конкретным используемым набором шифров. Некоторые наборы шифров требуют установки битов цифровой подписи, а некоторые не требуют
неотказуемость	x		x		x		x		x		
шифрование ключа	x		x		x		x		o		
шифрование данных	x		x		x		x		x		
согласование ключей	x		x		x		x		o		
подпись сертификата ключа	m		m		x		x		x		
подпись CRL	m		m		x		x		x		
только шифратор	x		x		x		x		x		
только дешифратор	x		x		x		x		x		

Название расширения	*Самоподписанные исходные сертификаты CSCA*		*Связующие сертификаты CSCA*		*Лицо, подписывающее документы*		*Орган, подписывающий мастер-списки, и орган, подписывающий списки отклонений*		*Средства связи*		*Замечания*
Период применяемости закрытого ключа	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	
не ранее	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
не позднее	o		o		o		o		o		
Политика применения сертификата	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
информация о политике	m		m		m		m		m		
Идентификатор политики	m		m		m		m		m		
Квалификаторы политики	o		o		o		o		o		
Соответствие политик	**x**		**x**		**x**		**x**		**x**		См. примечание 1
Альтернативное имя субъекта	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	См. п. 7.1.2
Альтернативное имя выдающего	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	См. п. 7.1.2
Атрибуты каталога субъекта	**x**		**x**		**x**		**x**		**x**		
Основные ограничения	**m**	**c**	**m**	**c**	**x**		**x**		**x**		
CA	m		m		x		x		x		
ограничение длины пути	m		m		x		x		x		Всегда ДОЛЖНО быть ‘0’
Ограничения в отношении имени	**x**		**x**		**x**		**x**		**x**		См. примечание 1
Ограничения в отношении политики	**x**		**x**		**x**		**x**		**x**		См. примечание 1
Расширенная применяемость ключей	**x**		**x**		**x**		**m**	**c**	**m**	**c**	См. п. 7.1.3
Пункты распределения CRL	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	
пункт распределения	m		m		m		m		m		ДОЛЖНЫ использоваться ldap, http или https См. п. 7.1.4
причины	x		x		x		x		x		
орган, выпускающий CRL	x		x		x		x		x		
Любая политика запрета	**x**		**x**		**x**		**x**		**x**		См. примечание 1
Самый свежий CRL	**x**		**x**		**x**		**x**		**x**		См. примечание 2

Название расширения	***Самоподписанные исходные сертификаты CSCA***		***Связующие сертификаты CSCA***		***Лицо, подписывающее документы***		***Орган, подписывающий мастер-списки, и орган, подписывающий списки отклонений***		***Средства связи***		***Замечания***
Частное расширение в Интернете	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	См. примечание 3
Изменение имени	**o**	**nc**	**o**	**nc**	**x**		**x**		**x**		См. п. 7.1.5
Тип документа	**x**		**x**		**m**	**nc**	**x**		**x**		См. п. 7.1.6
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, выпущенных 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 применяемость 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 Требования в отношении полей выдающего органа и субъекта

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 [ИСО 3166-1];
- поле "обычное название" ДОЛЖНО присутствовать.

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

7.1.2 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.

7.1.3 Требования расширения "расширенная применяемость ключей"

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

Идентификатором объекта (OID), который должен быть включен в расширение "расширенная применяемость 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).

7.1.4 Требования расширения "пункты распределения 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

7.1.5 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}
```

7.1.6 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(1..2)

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

7.2 Профиль CRL

В таблице 5 определены требования к профилю полей основной части CRL. В таблице 6 определены требования к профилю расширений CRL и записей CRL.

Таблица 5. Профили полей CRL

Компоненты списка сертификатов	***CSCA CRL***	***Замечания***
Список сертификатов	m	
список сертификатов TBS	m	См. следующую часть таблицы
Алгоритм подписи	m	Вводимое здесь значение зависит от выбранного алгоритма
значение подписи	m	Вводимое здесь значение зависит от выбранного алгоритма
Список сертификатов TBS		
версия	m	ДОЛЖНА быть v2
подпись	m	Вводимое здесь значение ДОЛЖНО быть таким же, как в компоненте "алгоритм подписи" последовательности "список сертификатов"
выдающий	m	Название страны и серийный номер, если таковые присутствуют, ДОЛЖНЫ быть печатаемой строкой. Другие атрибуты, имеющие синтаксис строки каталога, ДОЛЖНЫ быть либо печатаемой строкой, либо строкой формата UTF8. Название страны ДОЛЖНО состоять из прописных букв
Текущее обновление	m	Данные ДОЛЖНЫ заканчиваться буквой "Z". Элемент "секунды" ДОЛЖЕН присутствовать. Сроки вплоть до 2049 года ДОЛЖНЫ указываться в формате времени UTC. Время UTC ДОЛЖНО быть представлено в виде YYMMDDHHMMSSZ.

Компоненты списка сертификатов	*CSCA CRL*	*Замечания*
		Сроки после 2050 года ДОЛЖНЫ указываться в обобщенном формате времени. Обобщенный формат времени НЕ ДОЛЖЕН содержать долей секунд. Обобщенный формат времени ДОЛЖЕН быть представлен в виде YYYYMMDDHHMMSSZ
следующее обновление	m	Данные ДОЛЖНЫ заканчиваться буквой "Z". Элемент "секунды" ДОЛЖЕН присутствовать. Сроки вплоть до 2049 года ДОЛЖНЫ указываться в формате времени UTC. Время UTC ДОЛЖНО быть представлено в виде YYMMDDHHMMSSZ. Сроки после 2050 года ДОЛЖНЫ указываться в обобщенном формате времени. Обобщенный формат времени НЕ ДОЛЖЕН содержать долей секунд. Обобщенный формат времени ДОЛЖЕН быть представлен в виде YYYYMMDDHHMMSSZ
Отозванные сертификаты	m	Если таковые имеются, этот компонент НЕ ДОЛЖЕН быть пустым
Расширения CRL	m	См. следующую таблицу, где указано, какие расширения следует включать. Значения по умолчанию для расширений НЕ ДОЛЖНЫ шифроваться

Таблица 6. Профиль расширений CRL и записей CRL

Название расширения	*CSCA CRL*	*Критич-ность*	*Замечания*
Расширения CRL			
Идентификатор ключа полномочного органа	**m**	**nc**	ДОЛЖЕН быть таким же, как значение в поле "идентификатор ключа субъекта" в сертификате органа выдачи CRL
идентификатор ключа	m		
лицо, выдающее сертификат полномочного органа	o		
Серийный номер сертификата полномочного органа	o		

Название расширения	*CSCA CRL*	*Критич-ность*	*Замечания*
Альтернативное имя органа выдачи	**o**	**nc**	См. примечание 1
Номер CRL	**m**	**nc**	ДОЛЖЕН быть неотрицательным целым числом длиной максимум 20 октетов. ДОЛЖНО применяться шифрование с использованием дополнительного кода и номер ДОЛЖЕН представляться в формате наименьшего количества октетов
Индикатор дельта-списка CRL	**x**		
Выдающий пункт распределения	**x**		
Самый свежий CRL	**x**		
Расширения записей CRL			
Код причин	**x**		
Код временного приостановления действия сертификата	**x**		
Дата утраты валидности	**x**		
Орган выдачи сертификата	**x**		

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 "название страны" 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 названием страны. 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 "альтернативное имя выдающего органа" в CRL.

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

8. СТРУКТУРА МАСТЕР-СПИСКА CSCA

Мастер-списки реализуются как конкретные образцы типа "информация о содержании", определенные в документе [RFC 5652]. Информация о содержании ДОЛЖНА содержать единственный конкретный образец "подписанные данные" нижеуказанного профиля. Никакие другие типы данных в поле "информация о содержании" не включаются. Все мастер-списки ДОЛЖНЫ составляться в формате DER для сохранения целостности содержащихся в них подписей.

8.1 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 7. Мастер-список

Значение		*Замечания*
Подписываемые данные		
версия	m	Значение = v3
алгоритмы представления в краткой форме	m	
информация об инкапсулированном содержании	m	
тип электронного содержания	m	id-icao-cscaMasterList
электронное содержание	m	Зашифрованное содержание поля мастер-списка CSCA
сертификаты	m	ДОЛЖЕН быть включен сертификат органа, подписывающего мастер-списки, и СЛЕДУЕТ включить сертификат CSCA, который может быть использован для верификации подписи в поле "информация о подписавшемся"
crls	x	
информация о подписавшихся	m	Государствам РЕКОМЕНДУЕТСЯ включать в это поле только одну единицу информации о подписавшемся

Значение		***Замечания***
информация о подписавшемся	m	
версия	m	Значение этого поля диктуется полем sid. См. правила, касающиеся этого поля, в документе [RFC 5652]
sid	m	
Идентификатор ключа субъекта	r	РЕКОМЕНДУЕТСЯ, чтобы поддерживалось это поле, а не поле "орган выдачи и порядковый номер"
алгоритм представления в краткой форме (digest)	m	Алгоритмный идентификатор алгоритма, используемого для выдачи хэш-значения над инкапсулированным содержанием и подписанными атрибутами. См. примечание 1
подписанные атрибуты	m	Могут быть включены дополнительные атрибуты. Однако они должны обрабатываться принимающими государствами только для верификации значения подписи. Поле "подписанные атрибуты" ДОЛЖНО включать время подписания (см. [PKCS #9])
алгоритм подписи	m	Алгоритмный идентификатор алгоритма, используемого для выдачи значения подписи и любых связанных с ней параметров. См. примечание 1
подпись	m	Результат процесса генерации подписи
неподписанные атрибуты	o	Хотя это поле МОЖЕТ быть включено, принимающие государства могут пожелать его игнорировать

Примечание 1. Идентификаторы алгоритма представления в краткой 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 идентификаторы алгоритма представления в краткой форме при обоих условиях: при отсутствии параметров или с параметрами "NULL".

8.2 Спецификации мастер-списка формата ASN.1

```
CscaMasterList
{ 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
```

9. 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).

— — — — — — — —

Добавление A к части 12

СРОКИ СЛУЖБЫ (ИНФОРМАЦИОННОЕ)

Нижеследующие примеры иллюстрируют расчет периода применяемости 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 применяемости закрытых ключей и срок действия сертификата открытых ключей были минимальными. В этом примере минимальный период применяемости закрытого ключа для сертификатов лиц, подписывающих документы, составляет 1 мес.

Наименование	***Период применяемости/ срок действия***
Срок действия электронного МСПД	5 лет
Период применяемости закрытого ключа лица, подписывающего документы	1 мес
Срок действия сертификата лица, подписывающего документы	5 лет + 1 мес
Период применяемости 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 применяемости 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 применяемости 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 применяемости закрытых ключей и срок действия сертификата открытых ключей были средними.

Наименование	***Период применяемости/ срок действия***
Срок действия электронного МСПД	10 лет
Период применяемости закрытого ключа лица, подписывающего документы	2 мес
Срок действия сертификата лица, подписывающего документы	10 лет + 2 мес
Период применяемости 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 применяемости 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 применяемости 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 применяемости закрытых ключей и сроков действия сертификатов открытых ключей.

Наименование	***Период применяемости/ срок действия***
Срок действия электронного МСПД	10 лет
Период применяемости закрытого ключа лица, подписывающего документы	3 мес
Срок действия сертификата лица, подписывающего документы	10 лет + 3 мес
Период применяемости 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 применяемости 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 применяемости 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 8. Поля и расширения сертификатов

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
Сертификат	RFC 5280, раздел 4.1.1	
сертификат TBS	RFC 5280, раздел 4.1.1.1	
алгоритм подписи	RFC 5280, раздел 4.1.1.2	
значение подписи	RFC 5280, раздел 4.1.1.3	
Сертификат TBS	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)
серийный номер	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 серийного номера длиной до 20 октетов. CA, соблюдающие требования, НЕ ДОЛЖНЫ использовать значение серийного номера 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 алгоритма подписи в последовательности "сертификат"
`выдающий`	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 "не ранее" и "не позднее" могут шифроваться в формате времени UTC или с использованием обобщенного формата времени. CA, удовлетворяющие этому профилю, ДОЛЖНЫ всегда шифровать даты срока действия сертификата с использованием формата времени UTC вплоть до 2049 года. Сроки действия сертификатов после 2050 года ДОЛЖНЫ шифроваться с использованием обобщенного формата времени
`(если кодируется в формате времени UTC)`	X.690, п. 11.8.1	Кодировка заканчивается буквой "Z", как указано в пункте по формату времени UTC в документе ITU-T X.680 | ИСО/МЭК 8824-1

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
	X.690, п. 11.8.2	Элемент "секунды" всегда присутствует
(если кодируется с использованием обобщенного формата времени)	X.690, п. 11.7.1	Кодировка заканчивается буквой "Z", как указано в пункте по обобщенному формату времени в документе ITU-T Rec. X.680 | ИСО/МЭК 8824-1
	X.690, п. 11.7.2	Элемент "секунды" всегда присутствует
	RFC 5280, раздел 4.1.2.5.2	Значения в обобщенном формате времени НЕ ДОЛЖНЫ содержать долей секунды. Для целей этого профиля значения в обобщенном формате времени 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`
информация об открытом ключе субъекта	RFC 5280, раздел 4.1.2.7	
уникальный идентификатор выдающего	RFC 5280, раздел 4.1.2.8	CA, удовлетворяющие этому профилю, НЕ ДОЛЖНЫ генерировать сертификаты с уникальными идентификаторами
уникальный идентификатор 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
Идентификатор ключа полномочного органа	RFC 5280, раздел 4.2.1.1	Для упрощения построения пути сертификации поле идентификатора ключа расширения "идентификатор ключа полномочного органа" ДОЛЖНО включаться во все сертификаты, 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

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
идентификатор ключа		
лицо, выдающее сертификат полномочного органа		
серийный номер сертификата полномочного органа		
Идентификатор ключа субъекта	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"
идентификатор ключа субъекта		
Применяемость ключа	RFC 5280, раздел 4.2.1.3	Ограничения по применяемости ключа могут применяться в тех случаях, когда ключ, который мог бы использоваться более чем для одной операции, должен быть ограничен
цифровая подпись		Бит поля цифровой подписи 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		
шифрование ключа		
шифрование данных		
согласование ключей		
подпись сертификата ключа		Бит поля подписи на сертификате ключа задается, когда открытый ключ субъекта используется для верификации подписи на сертификатах открытых ключей
подпись CRL		Бит поля подписи CRL задается, когда открытый ключ субъекта используется для верификации подписи на списке отзыва сертификатов (например, CRL, дельта-списки или ARL). Этот бит ДОЛЖЕН задаваться в сертификатах, которые используются для верификации подписи на списках CRL
только шифратор		

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
только дешифратор		
Период применяемости закрытого ключа	RFC 3280, раздел 4.2.1.4	СА, удовлетворяющие этому профилю, НЕ ДОЛЖНЫ генерировать сертификаты с расширениями, касающимися периода применяемости закрытого ключа, если только не присутствует по крайней мере один из этих двух компонентов и расширение не является критичным
не ранее		В случае их использования поля "не ранее" и "не позднее" представляются в обобщенном формате времени и ДОЛЖНЫ указываться и интерпретироваться, как изложено в разделе 4.1.2.5.2
не позднее		
Политика применения 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
информация о политике		
идентификатор политики		
квалификаторы политики		
Соответствие политик	RFC 5280, раздел 4.2.1.5	
Альтернативное имя субъекта	RFC 5280, раздел 4.2.1.6	
Альтернативное имя выдающего	RFC 5280, раздел 4.2.1.7	
Атрибуты каталога субъекта	RFC 5280, раздел 4.2.1.8	
Основные ограничения	RFC 5280, раздел 4.2.1.9	Расширение "основные ограничения" идентифицирует, является ли СА субъектом сертификата, а также максимальную глубину валидных путей сертификации, которые включает данный сертификат. СА, удовлетворяющие требованиям, ДОЛЖНЫ включать это расширение во все сертификаты СА, которые содержат открытые ключи, используемые для валидации цифровых подписей на сертификатах, и ДОЛЖНЫ помечать данное расширение в таких сертификатах как критичное

Компонент/расширение	***Ссылка***	***Соответствующие выдержки***
CA		Булеан CA указывает, принадлежит ли сертифицированный открытый ключ органу CA. Если булеан CA не задается, то бит поля "подпись сертификата ключа" в расширении применяемости ключа НЕ ДОЛЖЕН задаваться
ограничение длины пути		
Ограничение в отношении имени	RFC 5280, раздел 4.2.1.10	
Ограничение в отношении политики	RFC 5280, раздел 4.2.1.11	
Расширенная применяемость 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 "применяемость ключа"
Пункты распределения CRL	RFC 5280, раздел 4.2.1.13	
пункт распределения		
причины		
орган, выпускающий CRL		
Любая политика запрета	RFC 5280, раздел 4.2.1.14	
Самый свежий CRL	RFC 5280, раздел 4.2.1.15	
Частное расширение Интернета	RFC 5280, раздел 4.2.2	
Изменение имени		
Тип документа		
Тип сертификата браузера Netscape		
Другие частные расширения		

Таблица 9. Поля и расширения CRL

Компонент / расширение	*Ссылка*	*Соответствующие выдержки*
Список сертификатов	RFC 5280, раздел 5.1.1	
список сертификатов TBS	RFC 5280, раздел 5.1.1.1	
Алгоритм подписи	RFC 5280, раздел 5.1.1.2	
значение подписи	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 "список сертификатов"
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
текущее обновление	RFC 5280, раздел 5.1.2.4	Удовлетворяющие требованиям этого профиля органы, выпускающие CRL, ДОЛЖНЫ шифровать поле "текущее обновление" в формате времени UTC для дат до конца 2049 года. Удовлетворяющие требованиям этого профиля органы, выпускающие CRL, ДОЛЖНЫ шифровать поле "текущее обновление" в обобщенном формате времени 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 по формату времени UTC в документе ITU-T X.680 | ИСО/МЭК 8824-1
	X.690, п. 11.8.2	Элемент "секунды" всегда присутствует

Компонент / расширение	***Ссылка***	***Соответствующие выдержки***
(если кодируется в обобщенном формате времени)	X.690, п. 11.7.1	Кодировка заканчивается буквой "Z", как указано в положении по обобщенному времени в документе ITU-T Rec. X.680 | ИСО/МЭК 8824-1
	X.690, п. 11.7.2	Элемент "секунды" всегда присутствует
	RFC 5280, раздел 4.1.2.5.2	Значения в обобщенном формате времени НЕ ДОЛЖНЫ содержать долей секунды. Для целей этого профиля значения в обобщенном формате времени ДОЛЖНЫ выражаться с использованием среднего гринвичского времени и ДОЛЖНЫ включать секунды (т. е. сроки указываются как YYYYMMDDHHMMSSZ), даже если количество секунд равно нулю
следующее обновление	Раздел 5.1.2.5	Удовлетворяющие требованиям этого профиля органы, выпускающие CRL, ДОЛЖНЫ шифровать поле "следующее обновление" в формате времени UTC для дат до конца 2049 года. Удовлетворяющие требованиям этого профиля органы, выпускающие CRL, ДОЛЖНЫ шифровать поле "следующее обновление" в обобщенном формате времени 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 по формату времени UTC в документе ITU-T X.680 | ИСО/МЭК 8824-1
	X.690, п. 11.8.2	Элемент "секунды" всегда присутствует
(если кодируется в обобщенном формате времени)	X.690, п. 11.7.1	Кодировка заканчивается буквой "Z", как указано в пункте по обобщенному формату времени в документе ITU-T Rec. X.680 | ИСО/МЭК 8824-1
	X.690, п. 11.7.2	Элемент "секунды" всегда присутствует
	RFC 5280, раздел 4.1.2.5.2	Значения в обобщенном формате времени НЕ ДОЛЖНЫ содержать долей секунды. Для целей этого профиля значения в обобщенном формате времени 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

Компонент / расширение	***Ссылка***	***Соответствующие выдержки***
Расширения CRL	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
Идентификатор ключа полномочного органа	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
Альтернативное имя 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 значение номера CRL длиной до 20 октетов. Отвечающие требованиям органы, выпускающие CRL, НЕ ДОЛЖНЫ использовать значение номера CRL 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
Индикатор дельта-списка	RFC 5280, раздел 5.2.4	

Компонент / расширение	***Ссылка***	***Соответствующие выдержки***
Выдающий пункт распределения	RFC 5280, раздел 5.2.5	
Самый свежий CRL	RFC 5280, раздел 5.2.6	
Код причин	RFC 5280, раздел 5.3.1	
Код временного приостановления сертификата	RFC 5280, раздел 5.3.2	
Дата утраты валидности сертификата	RFC 5280, раздел 5.3.3	
Орган выдачи 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 10. Основная часть сертификата

Компонент сертификата	***Раздел в документе RFC 3280***	***Сертификат подписывающегося CA страны***	***Сертификат лица, подписывающего документы***	***Замечания***
Сертификат	4.1.1	m	m	
сертификат TBS	4.1.1.1	m	m	См. следующую часть таблицы
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
Сертификат TBS	4.1.2			
версия	4.1.2.1	m	m	ДОЛЖНА быть v3
серийный номер	4.1.2.2	m	m	
подпись	4.1.2.3	m	m	Вводимое здесь значение СОВПАДАЕТ с OID в поле алгоритма подписи
выдающий	4.1.2.4	m	m	См. A1.5
срок действия	4.1.2.5	m	m	В вариантах реализации УКАЗЫВАЕТСЯ использование времени UTC до 2049 года, после чего используется обобщенный формат "время"
субъект	4.1.2.6	m	m	См. A1.5

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося CA страны*	*Сертификат лица, подписывающего документы*	*Замечания*
Информация об открытом ключе субъекта	4.1.2.7	m	m	
уникальный ID выдающего	4.1.2.8	x	x	
Уникальный ID субъекта	4.1.2.8	x	x	
расширения	4.1.2.9	m	m	См. следующую таблицу для получения информации о том, какие расширения СЛЕДУЕТ использовать

Таблица 11. Расширения

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося CA страны*	*Сертификат лица, подписывающего документы*	*Замечания*
Идентификатор ключа полномочного органа	4.2.1.1	o	m	Обязательное во всех сертификатах, за исключением самоподписанных сертификатов CSCA
Идентификатор ключа субъекта	4.2.1.2	m	o	
Применяемость ключа	4.2.1.3	mc	mc	Это расширение УКАЗЫВАЕТСЯ как КРИТИЧНОЕ
Период применяемости закрытого ключа	4.2.1.4	o	o	Таковым будет период, на который выдается закрытый ключ
Политика применения сертификата	4.2.1.5	o	o	
Соответствие политик	4.2.1.6	x	x	
Альтернативное имя субъекта	4.2.1.7	x	x	

Компонент сертификата	*Раздел в документе RFC 3280*	*Сертификат подписывающегося СА страны*	*Сертификат лица, подписывающего документы*	*Замечания*
Альтернативное имя выдающего	4.2.1.8	x	x	
Атрибуты каталога субъекта	4.2.1.9	x	x	
Основные ограничения	4.2.1.10	mc	x	Это расширение УКАЗЫВАЕТСЯ как КРИТИЧНОЕ
Ограничения в отношении имени	4.2.1.11	x	x	
Ограничения в отношении политики	4.2.1.12	x	x	
Расширенная применяемость ключей	4.2.1.13	x	x	
Пункты распределения CRL	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
Любая политика запрета	4.2.1.15	x	x	
Самый свежий CRL	4.2.1.16	x	x	
Частное расширение 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*
Идентификатор ключа полномочного органа	4.2.1.1			
идентификатор ключа		m	m	Если данное расширение используется, то это поле как минимум ПОДДЕРЖИВАЕТСЯ
лицо, выдающее сертификат полномочного органа		o	o	См. A1.5
серийный номер сертификата полномочного органа		o	o	
Идентификатор ключа субъекта	4.2.1.2			
Идентификатор ключа субъекта		m	m	
Применяемость ключа	4.2.1.3			
цифровая подпись		x	m	
неотказуемость		x	x	
шифрование ключа		x	x	
шифрование данных		x	x	
согласование ключей		x	x	
подпись сертификата ключа		m	x	
подпись CRL		m	x	
только шифратор		x	x	
только дешифратор		x	x	
Основные ограничения	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***
ограничение длины пути		m	x	0 – для нового сертификата CSCA, 1 – для связующего сертификата CSCA
Пункты распределения CRL	4.2.1.14			
пункт распределения		m	x	
причины		m	x	
орган, выпускающий CRL		m	x	
Политика применения сертификатов	4.2.1.5			
информация о политике				
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;

  - доверительный алгоритм открытых ключей. Если "якорь доверия" представляет собой сертификат CSCA, то доверительный алгоритм открытых ключей берется из поля "информация об открытом ключе субъекта" данного сертификата;

  - доверительный открытый ключ. Если "якорь доверия" представляет собой сертификат CSCA, то доверительный открытый ключ берется из поля "информация об открытом ключе субъекта" 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 "информация об открытом ключе субъекта" 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, соответствущий 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 "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 "открытый ключ субъекта" сертификата.

c) Если поле "информация об открытом ключе субъекта" сертификата содержит поле алгоритма с параметрами "non-null" (не пустые), задать указанные параметры переменному элементу "рабочие параметры открытого ключа". Если поле "информация об открытом ключе субъекта" сертификата содержит поле алгоритма с параметрами "null" (пустые) или параметры опущены, сравнить алгоритм в поле "открытый ключ субъекта" сертификата с "рабочим алгоритмом открытого ключа". Если алгоритм в поле "открытый ключ субъекта" 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 "открытый ключ субъекта" 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 "выдающий пункт распределения", 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 содержащится 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.

— КОНЕЦ —

ISBN 978-92-9249-946-4