РГП «КАЗАХСТАНСКИЙ ЦЕНТР МЕЖБАНКОВСКИХРАСЧЕТОВ НАЦИОНАЛЬНОГО БАНКА РЕСПУБЛИКИ КАЗАХСТАН»
(РГП «КЦМР НБ РК»)

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

ПОЛИТИКА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РГП «КЦМР НБ РК» (CERTIFICATE POLICY)

_____

Нормативный документ

2014 г.

РГП «КАЗАХСТАНСКИЙ ЦЕНТР МЕЖБАНКОВСКИХРАСЧЕТОВ НАЦИОНАЛЬНОГО БАНКА РЕСПУБЛИКИ КАЗАХСТАН»
(РГП «КЦМР НБ РК»)

Утверждена приказом

РГП «КЦМР НБ РК»

от 15 сентября 2014 года

№ 44-П

ПОЛИТИКА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РГП «КЦМР НБ РК» (CERTIFICATE POLICY)

Нормативный документ

Лист утверждения

Согласовано
Заместитель генерального
директора
_____Инкаров Б.Б.
«____»_____2014г.

Заместитель генерального
директора
_____Минникаев М.Н.
«____»_____2014г.

2014 г.

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Республиканское государственное предприятие на праве хозяйственного ведения «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан» (далее – РГП «КЦМР НБ РК» или КЦМР) является самостоятельным хозяйствующим субъектом, организацией, осуществляющей отдельные виды банковских операций. РГП «КЦМР НБ РК» – оператор межбанковской системы переводов денег, основным видом деятельности которого является проведение межбанковских платежей и переводов денег через казахстанскую межбанковскую систему перевода денег (МСПД) и казахстанские системы розничных платежей (СРП). Учредителем и уполномоченным органом по управлению КЦМР является Национальный Банк Республики Казахстан.

В соответствии с Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года для защиты информации в информационных системах КЦМР создал Удостоверяющий центр, который удостоверяет соответствие открытых (криптографических) ключей закрытым ключам, а также подтверждает достоверность регистрационных свидетельств (сертификатов).

В данном параграфе также приводятся термины, определения и сокращения, используемые в настоящем документе. В качестве основных определений использованы понятия, введенные международными стандартами и рекомендациями, в частности сериями Сектора стандартизации Международного союза электросвязи (International Telecommunication Union Telecommunication Standardization Sector, ITU-T) и Специальной комиссии интернет-разработок (Internet Engineering Task Force, IETF). В случаях, когда один или несколько схожих терминов имеют на практике несколько схожих определений, они приводятся в скобках со ссылкой на дополнительный источник.

В тексте документа под термином «сертификат» используется понятие, определенное в рекомендациях (ITU-T) X.509, если иное не оговорено особо. Термин «регистрационное свидетельство», определенный Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи», в контексте данного документа несет это же смысловое значение.

КЦМР (РГП «КЦМР НБ РК») – Республиканское государственное предприятие на праве хозяйственного ведения «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан».

Сертификат– открытый ключ пользователя вместе с дополнительной информацией, подлинность которых удостоверена электронной цифровой подписью, сформированной закрытым ключом удостоверяющего центра, который выдал данный сертификат.

Регистрационное свидетельство - документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи».

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи.

Электронная цифровая подпись (ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания.

Средства электронной цифровой подписи (средства ЭЦП) – совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи.

Открытый ключ – в криптосистемах с открытым ключом, тот ключ ключевой пары пользователя, который известен публике.

Открытый ключ электронной цифровой подписи (открытый ключ ЭЦП) – последовательность электронных цифровых символов, доступная любому лицу и

предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе.

Закрытый ключ – в криптосистемах с открытым ключом, тот ключ ключевой пары пользователя, который известен только пользователю.

Закрытый ключ электронной цифровой подписи (закрытый ключ ЭЦП) – последовательность электронных цифровых символов, известная владельцу регистрационного свидетельства и предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи.

Владелец регистрационного свидетельства (сертификата) – физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство (сертификат), правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве.

Заявитель – физическое или юридическое лицо, желающее стать владельцем регистрационного свидетельства (сертификата).

Политика сертификатов – озаглавленный набор правил, которые определяют применимость сертификата в определенной общности и/или классе приложений с общими требованиями безопасности.

Положение о практике сертификатов – нормативный документ о практике, которую имеет удостоверяющий центр для выпуска, управления, отзыва и обновления сертификатов или их ключей.

Подписывающее лицо – физическое или юридическое лицо, правомерно владеющее закрытым ключом электронной цифровой подписи и обладающее правом на ее использование на электронном документе.

Участник – физическое или юридическое лицо, которое в данной инфраструктуре открытых ключей играет роль подписчика (клиента), доверяющей стороны, удостоверяющего центра, центра регистрации, владельца сертификата или уполномоченного посредника.

Участник системы электронного документооборота - физическое или юридическое лицо, государственный орган или должностное лицо, участвующие в процессах сбора, обработки, хранения, передачи, поиска и распространения электронных документов.

Идентификация – процесс проверки идентичности физического или юридического лица, показывающий, что данное лицо является конкретным вполне определенным лицом. В контексте инфраструктуры открытых ключей, процесс идентификации состоит из двух этапов:

1) установление соответствия предъявленного лицом имени реально существующей идентичности лица;

2) установление того, что лицо, обращающееся за доступом или ищущее доступ к чему-либо от определенного имени, на самом деле являются поименованным лицом.

Аутентификация – процесс проверки того, что лицо или предмет является тем, кем (чем) себя объявляет. Этот процесс совпадает со вторым этапом, составляющим идентификацию, как раскрыто выше. Аутентификацией может также называться сервис безопасности, который гарантирует, что лицо или предмет является тем, кем (чем) себя объявляет или, что сообщение или иные данные исходят от определенного лица или устройства.

Инфраструктура открытых ключей (ИОК) – инфраструктура, способная обеспечить управление открытыми ключами, посредством которых можно реализовать сервисы аутентификации, шифрования, контроля целостности и доказательности действий.

Данные активации – любые данные, за исключением ключей, которые необходимы для функционирования криптографических модулей и требуют защиты (например, персональные идентификационные номера (PIN), парольные фразы или физически хранимые части ключа).

Квалификатор политики – информация, зависящая от политики, которая может сопровождать идентификатор Политики сертификатов в сертификате X.509. Такая информация может включать в себя URL-ссылку на применимое Положение о практике сертификатов или Соглашение с доверяющей стороной. Она также может включать в себя текст или ссылку на текст, который содержит условия использования сертификата или иную правовую информацию.

Соглашение с доверяющей стороной – соглашение между удостоверяющим центром и доверяющей стороной, которое обычно устанавливает права и ответственность между этими сторонами, касающуюся проверки цифровых подписей и других применений сертификатов (в контексте настоящей Политики соглашением с доверяющей стороной является Договор о предоставлении услуг Удостоверяющего центра КЦМР).

Соглашение с подписчиком – соглашение между УЦ и подписчиком, которое устанавливает права и ответственность сторон, касающуюся выпуска и управления сертификатами (в контексте настоящей Политики соглашением с подписчиком является Договор о предоставлении услуг Удостоверяющего центра КЦМР).

Цепочка сертификатов – упорядоченная последовательность сертификатов, которая может быть обработана для получения открытого ключа последнего объекта цепочки от открытого ключа первого объекта цепочки.

Ключевая пара и сертификат первичной инициализации – ключевая пара и сертификат с ограниченно коротким периодом действия, которые используются новым подписчиком, успешно прошедшим процедуру первоначальной проверки идентичности, для самостоятельного формирования постоянной ключевой пары.

Компрометация ключей – утрата владельцем ключей уверенности в том, что используемые ключи обеспечивают безопасность информации.

Список отозванных сертификатов (СОС) – список, отражающий набор сертификатов, которые более не считаются действительными выпустивших им удостоверяющим центром.

Средства криптографической защиты информации (СКЗИ) – средства, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами.

Носитель ключевой информации – электронное устройство, которое может хранить электронные данные и содержит ключевую информацию (например: токен, дискета, CD-ROM, DVD-ROM, Смарт карты, Флэш карты, Touch Memory, e-Token, USB Flash drive и другие).

Токен – физическое устройство, выдаваемое авторизованному пользователю вычислительных ресурсов в целях упрощения процедур аутентификации.

Объектный идентификатор – упорядоченный список целочисленных значений от корня к узлу дерева международных объектных идентификаторов, который однозначно идентифицирует этот узел.

Дерево международных объектных идентификаторов – особая форма иерархического дерева регистрации имен, корень которого соответствует международным рекомендациям (ITU-T) X.660, а узлы – органам регистрации, ответственным за выделение ветвей от родительского узла.

СОБС - система обмена банковскими сообщениями.

МСПД - межбанковская система перевода денег.

ФАСТИ – система транспорта информации.

1.1. Обзор

Настоящая Политика применения регистрационных свидетельств удостоверяющего центра КЦМР определяет порядок применения (политику) сертификатов, выпускаемых удостоверяющим центром КЦМР для участников обслуживаемых им информационных систем (далее – Политика сертификатов).

Настоящая Политика сертификатов устанавливает для участников систем правовые и технические требования, необходимые для выпуска, использования, управления и отзыва сертификатов, обеспечения связанных с ними сервисов доверия. Политика сертификатов обеспечивает безопасность и целостность информации в информационных системах и представляет собой единый набор норм, которые применяются в них, обеспечивая тем самым гарантию определенного уровня доверия.

Настоящий документ, в частности, определяет виды сертификатов, выпускаемых УЦ КЦМР, сферы их применения, а также связанные с ними процедуры проверки. Сертификат связывает значение открытого ключа с информацией, которая идентифицирует подписчика УЦ, использующего соответствующий закрытый ключ. Сертификаты применяются доверяющими сторонами, которым необходимо использовать открытый ключ из сертификата. Степень доверия к сертификату определяется следующими факторами:

правилами, которым следует УЦ при аутентификации подписчика и выпуске сертификата;

правилами функционирования, определяющими управление безопасностью УЦ;

обязательствами по отношению к подписчику УЦ;

правами и обязанностями УЦ, установленными действующим законодательством Республики Казахстан, Положением о практике сертификатов УЦ КЦМР.

Настоящая Политика сертификатов адресована:

Подписчикам, которым необходимо понимание того, как они аутентифицируются, каким образом допускается использовать сертификаты и соответствующие ключевые пары, в чем состоят их обязанности как подписчиков, и как они защищены в системе;

Доверяющим сторонам, которым необходимо понимание того, насколько целесообразно доверять сертификатам системы или электронным цифровым подписям, использующим эти сертификаты;

Владельцам сертификатов, которые используют сертификаты для работы с подписчиками и также нуждаются в понимании того, в чем состоят их обязанности, вытекающие из использования сертификатов.

Настоящий документ разработан в соответствии с рекомендациями (IETF) RFC 3647 для структуры Политики сертификатов и Положения о практике сертификатов.

Настоящая Политика сертификатов сама по себе не является юридическим соглашением между КЦМР и участниками обслуживаемых им информационных систем. Обязательства между ними устанавливаются заключаемыми договорами. Вместе с тем, договоры, устанавливающие отношения между КЦМР и участниками указанных систем, имеют ссылку на настоящую Политику сертификатов, так как она детализирует содержание этих договорных отношений.

1.2. Наименование и идентификация документа

Наименование документа: «Политика применения регистрационных свидетельств удостоверяющего центра РГП «КЦМР НБ РК» (Certificate Policy)».

Редакция документа: 1.2.

Введен в действие приказом КЦМР__ № 2014 года.

Действующая редакция настоящего документа публикуется на официальном информационном ресурсе КЦМР по адресу: http://www.kisc.kz/ca/doc/PolicyKISC.pdf.

КЦМР как организация, ответственная за содержание настоящей Политики сертификатов, назначила ряд расширений значений объектных идентификаторов (OID) для сертификатов, используемых в системах КЦМР. Для обозначения сертификатов подписчиков этих систем используются следующие значения объектных идентификаторов:

политика сертификатов подписчиков МСПД (межбанковская система перевода денег) – (1.2.398.3.5.2.7);

политика сертификатов подписчиков систем розничных платежей – (1.2.398.3.5.2.8);
политика сертификатов подписчиков СОБС (система обмена банковскими сообщениями)– (1.2.398.3.5.2.9);
политика сертификатов подписчиков ФАСТИ (система транспорта информации) – (1.2.398.3.5.2.10);
политика сертификатов подписчиков системы «Авангард Plat» – (1.2.398.3.5.2.11);
политика сертификатов первичной инициализации – (1.2.398.3.5.2.12).

Полный перечень объектных идентификаторов сертификатов, назначенных УЦ КЦМР, опубликован на официальном информационном ресурсе КЦМР в сети Интернет по адресу http://www.kisc.kz/ca/policy.html.

Каждый из вышеперечисленных объектных идентификаторов может быть далее расширен в целях определения дополнительных положений политики, охватывающих конкретные виды сертификатов. Расширенный объектный идентификатор, в этом случае, должен быть определен в соответствующем Положении о практике сертификатов.

1.3. Участники инфраструктуры открытых ключей

1.3.1. Удостоверяющий центр

Удостоверяющий центр (УЦ) – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства, выполняющее все свои функции в соответствии с настоящей Политикой сертификатов.

1.3.2. Центры регистрации

Центр регистрации (ЦР) – структурное подразделение удостоверяющего центра, ответственное за выполнение операций по идентификации, аутентификации, проверке полномочий владельцев при изготовлении и выдаче регистрационного свидетельства.

1.3.3. Подписчики

Подписчик – субъект (или объект), для которого УЦ КЦМР выпустил сертификат.

В большинстве случаев подписчиками являются юридические лица в лице своих уполномоченных представителей (физических лиц) или непосредственно физические лица. Вместе с тем, в роли подписчиков могут выступать технические средства, например, платежные терминалы, серверы и т.п., при этом в некоторых случаях под подписчиком подразумевается юридическое или физическое лицо, которое правомерно владеет и пользуется данным техническим средством.

С учетом данной оговорки под подписчиком можно, в частности, понимать подписывающее лицо, то есть физическое или юридическое лицо, правомерно использующее ключевую пару, открытый ключ которой удостоверен сертификатом, выпущенным УЦ КЦМР.

1.3.4. Доверяющие стороны

Доверяющие стороны (пользователи сертификатов) – подписчики УЦ КЦМР или владельцы сертификатов, выпущенных УЦ КЦМР.

Использование термина «доверяющие стороны (пользователи сертификатов)» обусловлено тем, что они действуют, полагаясь на сертификаты, выпущенные УЦ КЦМР, и/или электронные цифровые подписи, проверяемые с помощью этих сертификатов.

1.3.5. Другие участники

1.3.5.1. Владельцы сертификатов

Владельцы сертификатов – юридические или физические лица, имеющие договорные отношения с КЦМР о праве собственности на выпущенные УЦ КЦМР сертификаты.

В ряде случаев владельцем сертификата является соответствующий подписчик. В остальных случаях владельцем сертификата является заинтересованное юридическое лицо, имеющее договорные отношения с КЦМР о праве собственности на эти сертификаты.

1.3.5.2. Уполномоченные посредники

Уполномоченные посредники – юридические лица, вошедшие в договорные отношения с КЦМР, которые могут выполнять операции по идентификации и аутентификации заявителей при выпуске и отзыве сертификатов УЦ КЦМР.

Уполномоченные посредники обязаны обеспечивать исполнение соответствующих требований настоящей Политики сертификатов и заключенного с УЦ КЦМР договора. Типовой договор о сотрудничестве КЦМР с уполномоченным посредником УЦ опубликован на официальном информационном ресурсе КЦМР в сети Интернет по адресу http://www.kisc.kz/ca/dog_coop.rtf.

1.4. Использование сертификатов

1.4.1. Допустимое использование сертификата

УЦ КЦМР выпускает сертификаты, различные по целям использования.

По назначению открытых ключей, которые ими удостоверяются, все сертификаты, выпускаемые УЦ КЦМР, делятся на 2 группы: сертификаты ключей для аутентификации (включая сертификаты ключей для ЭЦП) и сертификаты ключей для протоколов ключевого обмена. Разрешенное использование, согласно назначению, отражается в расширениях «keyUsage» и/или «extendedKeyUsage» каждого сертификата.

Кроме того, по области допустимого применения сертификаты разделены объектными идентификаторами политики, которые отражаются в расширении «cerificatePolicies». Например, сертификаты системы МСПД предназначены для использования только в МСПД и не предназначены для использования в системе ФАСТИ и наоборот. Полный перечень используемых объектных идентификаторов политики опубликован на официальном информационном ресурсе КЦМР в сети Интернет по адресу http://www.kisc.kz/ca/policy.html.

1.4.2. Ограничения на использование сертификата

Использование сертификатов, выпущенных УЦ КЦМР, не должно противоречить действующему законодательству Республики Казахстан.

Сертификаты, выпущенные УЦ КЦМР, не должны использоваться по окончании сроков их действия, в случае отзыва или нарушения целостности.

Сертификаты подписчиков УЦ КЦМР предназначены для работы с программным обеспечением доверяющих сторон и подписчиков и не используются как сертификаты УЦ. В свою очередь, сертификаты УЦ не используются ни для каких функций, кроме функций УЦ.

Кроме того, сертификаты, выпущенные УЦ КЦМР, запрещается использовать в информационных системах с повышенными требованиями к отказоустойчивости, например, в системах управления оборудованием, относящимся к категории источников повышенной опасности, таким как ядерное, аэронавигационное оборудование, системах контроля вооружения, воздушного движения или тому подобных. Также сертификаты, выданные УЦ КЦМР, запрещается использовать в чрезвычайных ситуациях, в которых ошибка при принятии решения о доверии, основанном на данных сертификатах, может повлечь за собой смерть, ранение персонала или серьезный ущерб окружающей среде.

1.5. Управление документом

1.5.1. Организация, ответственная за содержание документа

Республиканское государственное предприятие на праве хозяйственного ведения «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан».

050040, г. Алматы, микрорайон «Коктем-3», д. 21.

1.5.2. Контактное лицо

Начальник отдела удостоверяющего центра РГП «КЦМР НБ РК».
050040, г.Алматы, микрорайон «Коктем-3», д. 21.
+7 (727) 250-66-79; +7 (727) 250-66-64
ca@kisc.kz

1.5.3. Утверждающая инстанция

Генеральный директор РГП «КЦМР НБ РК» или лицо, его замещающее.

1.5.4. Процедура утверждения изменений и дополнений

Изменения и дополнения в Политику сертификатов готовятся отделом удостоверяющего центра КЦМР и оформляются в виде отдельного документа, содержащего либо актуальный текст Политики, либо уведомление об изменениях и дополнениях в ее актуальный текст.

Изменения проходят согласование с отделом информационной безопасности и главным юрисконсультом РГП «КЦМР НБ РК».

При этом за определение необходимости изменения объектных идентификаторов Политики сертификатов для приведения их в соответствие с измененным содержанием документа отвечает отдел удостоверяющего центра КЦМР.

Политика сертификатов и все изменения и дополнения к ней публикуются.

Публикация актуальной редакции Политики сертификатов или утвержденных уведомлений об изменениях и дополнениях к ней осуществляется на официальном информационном ресурсе КЦМР в сети Интернет по адресу: http://www.kisc.kz/ca/doc/PolicyKISC.pdf. Их публикация по указанному адресу является официальным уведомлением заинтересованных участников.

Все утвержденные изменения в Политику сертификатов вступают в силу и становятся обязательными для исполнения юридическими и физическими лицами, связанными обязательствами по ссылающимся на нее договорам, с момента их публикации, если иное особо не предусмотрено содержанием изменений.

1.6. Термины, определения и сокращения

Приведены выше, во введении.

2. ОТВЕТСТВЕННОСТЬ ЗА ПУБЛИКАЦИЮ И ХРАНИЛИЩЕ

2.1. Хранилище

УЦ КЦМР обеспечивает функционирование хранилища сертификатов, публично доступного для всех заинтересованных сторон.

2.2. Публикация информации о сертификатах

Основным протоколом работы хранилища является облегченный протокол доступа к каталогам (LDAP). Данный протокол позволяет доверяющим сторонам и подписчикам формировать онлайновые запросы, касающиеся информации о статусе сертификатов или его изменения. Вместе с тем, доступ к информации в хранилище возможен и через web-

интерфейс. Все возникающие на практике исключения к этому правилу должны быть документально оформлены и утверждены в Положении о практике сертификатов.

УЦ КЦМР предоставляет подписчикам и доверяющим сторонам информацию о том, по каким адресам находятся соответствующее хранилище и служба онлайнового протокола статуса сертификатов (OCSP).

УЦ КЦМР публикует сертификаты, которые он выпустил. В случае отзыва сертификата подписчика УЦ КЦМР удаляет этот сертификат из действующего хранилища. Кроме того, УЦ КЦМР выпускает списки отозванных сертификатов (COC) и предоставляет сервис OCSP.

В любое время на официальном информационном ресурсе КЦМР в сети Интернет доступны актуальные версии:

Политики сертификатов;

Положения о практике сертификатов;

Договора о предоставлении услуг УЦ КЦМР, одновременно играющего роль соглашения с подписчиком и соглашения с доверяющей стороной.

Кроме того, подписчикам и доверяющим сторонам в любое время в хранилище доступны действующие (неотозванные) сертификаты, а также действующие списки отозванных сертификатов.

2.3. Периодичность публикации

Информация УЦ публикуется незамедлительно по мере ее появления. УЦ КЦМР обеспечивает публикацию в хранилище списков отозванных сертификатов и работу сервисов проверки статуса сертификатов. Список отозванных сертификатов обновляется по мере появления отозванных сертификатов незамедлительно, но не реже одного раза в неделю. После того как срок действия сертификата истек, он может быть исключен из списка отозванных сертификатов.

2.4. Контроль доступа к хранилищу

УЦ КЦМР размещает в хранилище информацию, предназначенную для публичного доступа, но только для чтения. При этом УЦ КЦМР реализует меры безопасности, предотвращающие добавление, исключение или изменение данных в хранилище неавторизованными на то лицами.

УЦ КЦМР не использует на постоянной основе средства ограничения чтения данных из хранилища. Ссылки на списки отозванных сертификатов, информация о том, по каким адресам необходимо обращаться в хранилище и к службе онлайнового протокола статуса сертификатов (OCSP), доступна всем желающим на официальном информационном ресурсе КЦМР в сети Интернет.

При работе с хранилищем участники информационных систем, обслуживаемых УЦ КЦМР, также имеют возможность использовать протокол криптографической защиты соединений SSL/TLS.

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. Назначение имен

Имена, присутствующие в сертификатах подписчиков, идентифицируют подписчиков.

3.1.1. Типы имен

Сертификаты подписчиков в поле «Subject» обязательно содержат отличительные имена (DN-имена), соответствующие рекомендациям (ITU-T) X.501, которые, в свою очередь, обязательно имеют компонент общего имени (CN).

Этот компонент CN в сертификатах, выпускаемых УЦ КЦМР, отражает данные, однозначно идентифицирующие подписчика. Если подписчиком является физическое лицо или юридическое лицо в лице своего представителя, то компонент CN может содержать такие данные как индивидуальный идентификационный номер (для граждан Республики Казахстан), фамилию, имя и/или псевдоним. Если подписчиком является техническое средство, например, сервер, компонент CN может отражать его полное доменное имя, если служба – название службы и т.п.

В любом случае, содержание компонента CN в сертификате пользователя однозначно идентифицирует подписчика.

3.1.2. Требование значимости имен

Сертификаты, выпускаемые УЦ КЦМР, содержат значимые имена в смысле общеизвестности их семантики, что помогает идентифицировать соответствующих подписчиков, владельцев сертификатов и сервисы удостоверяющего центра.

3.1.3. Анонимность подписчиков и использование псевдонимов

Анонимность подписчиков не допускается. Назначение подписчику псевдонима допускается только при условии документального закрепления исключительной принадлежности этого псевдонима данному подписчику. Например, псевдоним может быть назначен данному подписчику в рамках заключенного договора владельцем сертификата или удостоверяющим центром. При этом в любом случае псевдоним должен однозначно идентифицировать подписчика.

3.1.4. Правила интерпретации различных форм имен

Не устанавливаются.

3.1.5. Уникальность имен

Вследствие требования однозначной идентификации подписчиков имена всех подписчиков являются уникальными. Вместе с тем, подписчик может иметь два и более сертификата с одним и тем же DN-именем в поле «Subject».

3.1.6. Распознавание, аутентификация и роль торговых марок

Заявители на выпуск сертификата не должны использовать в своих заявлениях имена, нарушающие права их законных правообладателей. УЦ КЦМР не несет ответственности за проверку на предмет правообладания заявителем именем, указанным в заявлении. УЦ КЦМР не обязан вступать в споры, связанные с собственностью на доменные, торговые и тому подобные имена и марки. УЦ КЦМР оставляет за собой право отклонить любое заявление на изготовление ключей и регистрационного свидетельства и/или регистрацию регистрационного свидетельства (далее – заявление на выпуск сертификата) или приостановить его рассмотрение, если подобное разбирательство является общеизвестным фактом.

3.2. Первоначальная проверка идентичности

Первоначальная проверка идентичности – это наиболее полная форма процедуры идентификации и аутентификации при выпуске сертификата, которая состоит из следующих этапов:

проверка достоверности информации о потенциальном подписчике, выполняемая уполномоченным посредником, удостоверяющим центром или заявителем по документам, предъявляемым потенциальным подписчиком при личной явке или явке уполномоченного им представителя (для юридических лиц)[1];

генерация ключевой пары подписчика;

доставка открытого ключа подписчика в УЦ КЦМР;

доказательство удостоверяющему центру факта владения подписчиком закрытым ключом, который соответствует открытому ключу, подлежащему удостоверению сертификатом.

Проведение процедуры идентификации и аутентификации в форме первоначальной проверки идентичности обязательно, если достоверность информации о заявителе или потенциальном подписчике проверяется впервые или не может быть проверена и подтверждена на основе действующих сертификатов и полномочий участников по действующим договорам.

[1] При поступлении заявления на выпуск сертификата к уполномоченному посреднику данную проверку проводит уполномоченный посредник. Удостоверяющий центр проводит данную проверку при поступлении заявления на выпуск сертификата от заявителя, одновременно выступающего потенциальным подписчиком. В остальных случаях данную проверку проводит заявитель.

3.2.1. Способ доказательства факта владения закрытым ключом

В ходе первоначальной проверки идентичности заявитель обязан продемонстрировать УЦ КЦМР факт правомерного владения потенциальным подписчиком закрытым ключом, соответствующим открытому ключу, который указан в заявлении на выпуск сертификата, то есть будет указан в сертификате.

Способом доказательства владения закрытым ключом может являться электронный документ в формате PKCS#10 или PKCS#7. Формат PKCS#10 используется только в случае, когда заявителем выступает потенциальный подписчик, процедура первоначальной проверки идентичности проводится без участия уполномоченного посредника, и сертификат подписчика выпускается без использования ключевой пары и сертификата первичной инициализации.

В остальных случаях используется формат PKCS#7 с ЭЦП, сформированной закрытым ключом, соответствующим действующему сертификату, например, закрытым ключом заявителя, уполномоченного посредника или закрытым ключом первичной инициализации потенциального подписчика. При этом в качестве подписываемых данных выступает запрос на изготовление сертификата в формате PKCS#10 с ЭЦП потенциального подписчика.

Вместе с тем, допускается, чтобы генерация ключевой пары подписчика осуществлялась в УЦ КЦМР при условиях, что такой способ выбирается при согласии подписчика и заявителя, генерация осуществляется с обязательным использованием защищенного носителя ключевой информации, исключающего возможность доступа к закрытому ключу. В данном случае иных доказательств правомерного владения закрытым ключом не требуется.

3.2.2. Процедура аутентификации юридического лица

Если заявителем на выпуск сертификата выступает юридическое лицо, его уполномоченным представителем в КЦМР или уполномоченному посреднику представляется заявление по форме, соответствующей приложению 2 к Правилам выдачи, регистрации, хранения, отзыва (аннулирования) регистрационных свидетельств, в том числе их копий на бумажном носителе и ведения регистра регистрационных свидетельств, утвержденным приказом Председателя Агентства Республики Казахстан по информатизации и связи от 8 декабря 2005 года № 457-п (http://www.kisc.kz/ca/doc/rules.rtf).

При наличии у заявителя действующего сертификата заявление на выпуск нового сертификата может быть подано в форме электронного документа. При этом сведения, содержащиеся в заявлении, подтверждаются электронной цифровой подписью заявителя.

3.2.3. Процедура аутентификации физического лица

Заявителем на выпуск сертификата – физическим лицом в КЦМР или уполномоченному посреднику представляется заявление по форме, соответствующей приложению 1 к Правилам выдачи, регистрации, хранения, отзыва (аннулирования) регистрационных свидетельств, в том числе их копий на бумажном носителе и ведения регистра регистрационных свидетельств, утвержденным приказом Председателя Агентства Республики Казахстан по информатизации и связи от 8 декабря 2005 года № 457-п (http://www.kisc.kz/ca/doc/rules.rtf).

При наличии у заявителя действующего сертификата заявление на выпуск нового сертификата может быть подано в форме электронного документа. При этом сведения, содержащиеся в заявлении, подтверждаются электронной цифровой подписью заявителя.

3.2.4. Не подвергающиеся проверке сведения о заявителе

Отсутствуют.

3.2.5. Проверка полномочий

В процессе рассмотрения заявлений на выпуск сертификата физическому лицу, уполномоченному представлять юридическое лицо, УЦ КЦМР и уполномоченный посредник действуют в соответствии с параграфом 3.2.2. Дополнительных проверок таких полномочий не проводится, так как они подтверждаются соответствующим заявлением и прилагаемыми к нему документами.

Вместе с тем, УЦ КЦМР в порядке, установленном законодательством, проверяет сведения, указанные в заявлениях на выпуск сертификата. В связи с этим, УЦ КЦМР оставляет за собой право в случаях, вызывающих сомнения при такой проверке, требовать от заявителей представления дополнительных документов, подтверждающих сведения, указанные в заявлении.

3.2.6. Критерии взаимодействия

УЦ КЦМР может обеспечивать сервисы взаимодействия своих подписчиков с подписчиками других УЦ при следующих условиях:

другой УЦ функционирует в соответствии с Положением о практике сертификатов, которое соответствует аналогичным требованиям УЦ КЦМР;

между удостоверяющими центрами заключено соответствующее соглашение и приняты необходимые организационно-технические меры.

3.3. Идентификация и аутентификация заявлений о смене ключей в сертификатах

Для непрерывного использования сертификатов перед истечением срока действия текущего сертификата подписчику необходимо получить новый сертификат. УЦ КЦМР требует, чтобы подписчик генерировал новую ключевую пару для замены истекающей. Перед выпуском нового сертификата УЦ КЦМР или/и уполномоченный посредник обязан проверить идентичность подписчика, который его запрашивает.

3.3.1. Идентификация и аутентификация при плановой (очередной) смене ключей

В данном случае УЦ КЦМР проверяет факт владения подписчиком закрытым ключом в том же порядке, как это изложено в параграфе 3.2.1.

3.3.2. Идентификация и аутентификация при внеплановой смене ключей после отзыва сертификатов

В данном случае подписчик повторно проходит процедуру первоначальной проверки идентичности в полном объеме, как это изложено в разделе 3.2.

3.4. Идентификация и аутентификация при отзыве сертификатов

Перед фактическим выполнением процедуры отзыва любого сертификата УЦ КЦМР проверяет тот факт, что заявление на отзыв сертификата исходит от указанного в данном сертификате подписчика, уполномоченного им лица или владельца соответствующего сертификата.

4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТОВ

4.1. Заявления на выпуск сертификатов

4.1.1. Лица, имеющие право подавать заявления на выпуск сертификатов

Заявление на выпуск сертификата имеют право подавать:

физические лица;

уполномоченные представители юридических лиц.

4.1.2. Процедура регистрации и связанные с ней обязательства

Заявления на выпуск сертификата подаются в удостоверяющий центр или уполномоченному посреднику.

Необходимым условием регистрации заявления является заключение заявителем договора о предоставлении услуг удостоверяющего центра КЦМР. Тексты договоров опубликованы на официальном информационном ресурсе УЦ КЦМР по адресу http://www.kisc.kz/ca/doc/dogovorcaps.rtf или http://www.kisc.kz/ca/doc/new/dogovorca.rtf. Заявления и гарантии данных договоров изложены ниже, в разделе 9.6.

До генерации ключевых пар подписчиков потенциальный владелец соответствующих сертификатов обязан согласовать с УЦ КЦМР необходимые атрибуты этих сертификатов.

4.2. Обработка заявлений на выпуск сертификатов

4.2.1. Процедуры идентификации и аутентификации

Любая процедура идентификации и аутентификации при выпуске сертификата выполняется в том же порядке, что и первоначальная проверка идентичности, изложенная в разделе 3.2, за исключением того, что личная явка потенциального подписчика, заявителя или их уполномоченных представителей в удостоверяющий центр или к уполномоченному посреднику не требуется, если достоверность информации о заявителе и потенциальном подписчике может быть подтверждена на основе их действующих сертификатов и полномочий участников по действующим договорам.

4.2.2. Прием или отказ в приеме заявления на выпуск сертификатов

Удостоверяющий центр или уполномоченный посредник вправе отклонить заявление на выпуск сертификата, если:

заявитель не представил всю необходимую информацию;

заявитель представил недостоверную информацию;

заявитель или потенциальный подписчик не прошел процедуру идентификации и аутентификации;

средство электронной цифровой подписи, предлагаемое к использованию заявителем, не поддерживается Удостоверяющим центром.

Удостоверяющий центр оставляет за собой право отказать в выпуске сертификата без детального разъяснения причин, в случае выявления каких-либо факторов, которые могут нанести вред его деловой репутации.

4.2.3. Срок рассмотрения заявлений на выпуск сертификатов

Заявления на выпуск сертификата рассматриваются УЦ КЦМР и уполномоченными посредниками в срок не более пяти рабочих дней с момента их поступления.

4.3. Выпуск сертификатов

4.3.1. Действия удостоверяющего центра в ходе выпуска сертификатов

Каждый сертификат подписчика создается и выпускается по факту приема УЦ КЦМР или уполномоченным посредником соответствующего заявления на выпуск сертификата. При создании и выпуске сертификата для заявителя удостоверяющий центр основывается на предварительно проверенной информации из заявления.

4.3.2. Уведомление подписчиков удостоверяющим центром о выпуске сертификатов

После создания сертификата подписчика УЦ КЦМР должен уведомить подписчика об этом, а также о способе получения сертификата. Уведомление осуществляется напрямую, через владельца этого сертификата или через уполномоченного посредника, принявшего заявление на выпуск данного сертификата.

Способами получения подписчиками своих сертификатов являются сообщения электронной почты, содержащие соответствующие сертификаты, либо загрузка сертификатов из хранилища УЦ через сеть Интернет.

Вместе с тем, по желанию подписчика сертификат может быть передан из рук в руки лично ему или уполномоченному им представителю при личной явке в КЦМР.

4.4. Принятие сертификатов

4.4.1. Поведение, означающее принятие сертификатов

Следующая реакция подписчика означает принятие им сертификата:

загрузка сертификата или установка из сообщения, к которому он прикреплен;

отсутствие возражений со стороны подписчика против принятия сертификата или его содержания.

4.4.2. Публикация сертификатов удостоверяющим центром

УЦ КЦМР размещает выпущенные сертификаты в публично доступном хранилище.

4.4.3. Уведомление удостоверяющим центром других сторон о выпуске сертификатов

О выпуске сертификата подписчика УЦ КЦМР вправе направить уведомление владельцу сертификата и уполномоченному посреднику, принявшему заявление на выпуск данного сертификата.

4.5. Использование сертификатов и ключевых пар

4.5.1. Использование закрытых ключей и сертификатов подписчиками

Использовать закрытый ключ разрешается только после того, как подписчик дал обязательство выполнять обязанности подписчика по договору с Удостоверяющим центром или владельцем соответствующего сертификата, а также требования настоящей Политики сертификатов и соответствующего Положения о практике сертификатов, УЦ в порядке, установленном действующим законодательством Республики Казахстан, выпустил сертификат соответствующего открытого ключа, и подписчик принял этот сертификат. Сертификат должен использоваться только в соответствии с действующим законодательством, договорными обязательствами, настоящей Политикой сертификатов и соответствующим Положением о практике сертификатов. Использование сертификата должно соответствовать содержанию включенных в него расширений «keyUsage» и «extendedKeyUsage». Например, если в содержании указанных расширений отсутствует значение «Цифровая подпись», то сертификат не должен использоваться в целях проверки ЭЦП.

Подписчики обязаны защищать свой закрытый ключ от несанкционированного доступа и должны прекращать его использование после истечения срока действия или отзыва соответствующего сертификата.

4.5.2. Использование открытых ключей и сертификатов доверяющими сторонами

Необходимым условием доверия к сертификатам, выпущенным УЦ КЦМР, для доверяющих сторон является принятие обязательств о выполнении обязанностей доверяющей стороны по договору с Удостоверяющим центром или владельцем соответствующего сертификата, а также требований настоящей Политики сертификатов и соответствующего Положения о практике сертификатов.

Прежде, чем предпринять любой акт, основываясь на доверии к сертификату, выпущенному УЦ КЦМР, доверяющие стороны должны самостоятельно проверить каждый соответствующий электронный документ, в частности, каждую имеющуюся на нем ЭЦП, а также связанные с этим сертификаты, метки времени, квитанции (ответы)

службы OCSP или списки отозванных сертификатов. Для проведения данной проверки доверяющей стороне следует:

1. Определить полную цепочку сертификатов, которая позволяет проверить ЭЦП, удостоверяющую сертификат ключевой пары, с помощью которой создан документ. (Данная цепочка может содержать сертификаты, выпущенные другими удостоверяющими центрами, и может не быть единственной.);

2. В случае наличия нескольких возможных цепочек сертификатов выбрать из них ту, которая в текущих обстоятельствах является оптимальной в смысле стойкости используемых криптографических алгоритмов, своей длины и т.п.;

3. Оценить соответствие использования каждого сертификата избранной цепочки:

1) требуемой сфере применения (политике), не запрещенной и не ограниченной настоящей Политикой сертификатов (например, МСПД, СОБС, ФАСТИ и т.п.);

2) содержанию полей расширения «keyUsage» и «extendedKeyUsage», включенных в сертификат (например, если не включено значение «Цифровая подпись», то на сертификат нельзя полагаться при проверке ЭЦП подписчика).

За оценку соответствия использования сертификатов доверяющими сторонами УЦ КЦМР ответственности не несет;

4. Проверить, что все сертификаты в избранной цепочке выпущены удостоверяющими центрами, уполномоченными подписывать сертификаты;

5. Используя избранную цепочку сертификатов, проверить действительность электронного документа, а также достоверность сертификата(-ов) его автора(-ов). Для этого необходимо корректно и точно выполнить криптографические операции, используя программное обеспечение и/или устройства, сертифицированные на соответствие необходимому уровню безопасности. Если при этом средствами применяемого программного обеспечения и/или устройств невозможно определить, действителен документ, или результат отрицателен, документ следует отвергнуть;

6. (При необходимости) определить дату и время создания документа. Это возможно только если документ был заверен сервером метки времени (до подписания), или метка времени была связана с ЭЦП непосредственно сразу после выработки ЭЦП документа;

7. Проверить соответствие сроков действия всех сертификатов избранной цепочки определенной дате и времени;

8. Проверить статус всех сертификатов в избранной цепочке через списки отозванных сертификатов или службу OCSP. Отзыв или приостановление любого сертификата в цепочке означает преждевременное окончание срока его действия, по сравнению с датой, когда был сформирован документ. Если хоть один из сертификатов в цепочке отозван, только доверяющая сторона ответственна за определение того, оправдано или нет полагаться на документ, сформированный подписчиком до отзыва сертификата в цепочке. Любое подобное доверие целиком относится к риску доверяющей стороны;

9. Проверить наличие соответствующих полномочий во всех сертификатах служб и серверов УЦ, задействованных при проверке.

Любое доверие к сертификату обязано быть соразмерно обстоятельствам. Если обстоятельства указывают на необходимость дополнительных гарантий, доверяющая сторона обязана получать такие гарантии, чтобы подобное доверие считалось оправданным.

4.6. Обновление сертификатов

Услуг по обновлению сертификатов УЦ КЦМР не предоставляет.

4.7. Смена ключей сертификатов

Услуг по смене ключей сертификатов УЦ КЦМР не предоставляет.

Вместе с тем, при необходимости сменить ключи подписчики и владельцы сертификатов имеют возможность инициировать выпуск нового сертификата в соответствии с разделами 4.1, 4.2 и 4.3. При этом следует учитывать, что если эта необходимость вызвана компрометацией закрытого ключа, то подписчик и владелец сертификата обязан в первую очередь инициировать отзыв сертификата, соответствующего скомпрометированному закрытому ключу.

4.8. Изменение сертификатов

Услуг по изменению сертификатов УЦ КЦМР не предоставляет.

4.9. Отзыв и приостановление действия сертификатов

4.9.1. Основания для отзыва сертификатов

Только на следующих основаниях сертификат подписчика отзывается удостоверяющим центром и публикуется в списке отозванных сертификатов:

поступило содержащее причину отзыва заявление подписчика или владельца сертификата, который больше не использует (или не желает использовать) сертификат;

удостоверяющий центр, владелец сертификата или подписчик располагает доказательствами компрометации закрытого ключа подписчика или обоснованных подозрений такой компрометации. (Договорные обязательства требуют от подписчика и владельца сертификата незамедлительного информирования УЦ КЦМР об обнаружении или обоснованном подозрении в компрометации закрытого ключа.);

удостоверяющий центр или владелец сертификата располагают доказательствами существенного нарушения подписчиком обязательства, заверения или гарантии действующего договора;

в случае смерти владельца сертификата;

утратил силу какой-либо договор, являющийся необходимым условием владения или пользования подписчиком соответствующим закрытым ключом;

удостоверяющий центр, владелец сертификата или уполномоченный посредник располагают доказательствами того, что сертификат был выпущен с существенным нарушением процедур Положения о практике сертификатов, сертификат был выпущен иному лицу, нежели указано в самом сертификате, или без аутентификации этого лица;

удостоверяющий центр, владелец сертификата или уполномоченный посредник располагают доказательствами ошибочности существенного факта в заявлении на выпуск сертификата;

удостоверяющий центр, владелец сертификата или уполномоченный посредник выявили, что при выпуске сертификата не соблюдены иные существенные условия выпуска;

информация в сертификате, за исключением непроверяемой информации, неверна или изменилась;

подписчик, владелец сертификата или уполномоченный посредник не произвел должную оплату;

по вступившему в законную силу решению суда;

продолжение использования сертификата опасно для информационных систем.

В последнем случае УЦ КЦМР, владелец сертификата или уполномоченный посредник при определении опасности использования сертификата для информационных систем среди прочего рассматривают:

количество и характер полученных жалоб;

идентичность лиц, подавших жалобы;

действующее законодательство;

иные возможные меры по исключению опасности со стороны подписчика.

Сертификаты могут отзываться по иным основания, установленным законодательством Республики Казахстан.

4.9.2. Лица, имеющие право подавать заявления на отзыв сертификатов

Подавать заявления на отзыв сертификатов имеют право подписчики, владельцы сертификатов и уполномоченные посредники, а также должным образом уполномоченные представители указанных лиц. Запрашивать отзыв сертификатов также могут уполномоченные сотрудники удостоверяющего центра.

4.9.3. Процедуры отзыва сертификата

Инициатор отзыва сертификата представляет в УЦ заявление по форме, соответствующей приложениям 4 или 5 (для юридических или физических лиц соответственно) к Правилам выдачи, регистрации, хранения, отзыва (аннулирования) регистрационных свидетельств, в том числе их копий на бумажном носителе и ведения регистра регистрационных свидетельств, утвержденным приказом Председателя Агентства Республики Казахстан по информатизации и связи от 8 декабря 2005 года № 457-п (http://www.kisc.kz/ca/doc/rules.rtf). Заявление об отзыве может подаваться в форме электронного документа. Заявление может направляться через владельца данного сертификата или уполномоченного посредника.

Перед отзывом сертификата подписчика УЦ КЦМР проверяет, что инициатор запрашивает отзыв правомочно. При этом могут применяться все механизмы идентификации и аутентификации, которые приведены в разделе 3.2.

После отзыва сертификата удостоверяющий центр по возможности уведомляет Инициатора об отзыве сертификата.

4.9.4. Срок подачи заявлений на отзыв сертификата

Заявления на отзыв сертификата должны подаваться незамедлительно с момента обнаружения соответствующих оснований.

4.9.5. Срок рассмотрения заявлений на отзыв сертификата

Заявления на отзыв сертификата рассматриваются УЦ КЦМР незамедлительно, не позднее рабочего дня, следующего за датой поступления заявления.

4.9.6. Требования о проверке отзыва сертификата для доверяющих сторон

Доверяющие стороны должны проверять статус сертификатов, на которые они желают положиться. Одним из методов, с помощью которого доверяющие стороны могут проверить статус сертификата, является обращение к действующему списку отозванных сертификатов, опубликованному УЦ КЦМР. Другими методами, с помощью которых доверяющая сторона может выполнить это требование, являются доступ в хранилище или проверка статуса сертификата по протоколу OCSP. УЦ КЦМР для проверки доверяющими сторонами статуса сертификатов обеспечивает их информацией о том, как найти соответствующий список отозванных сертификатов, интерфейс хранилища и службу OCSP.

Списки отозванных сертификатов, выпускаемые УЦ КЦМР, также доступны по адресу http://www.kisc.kz/ca/crl.html.

4.9.7. Частота выпуска списков отозванных сертификатов

Списки отозванных сертификатов являются едиными, в том смысле, что они содержат, при их наличии, и отозванные сертификаты УЦ, и отозванные сертификаты служб и серверов УЦ, в том числе службы OCSP и сервера метки времени, а также отозванные сертификаты подписчиков. Списки отозванных сертификатов выпускаются незамедлительно по факту отзыва какого-либо сертификата, но не реже одного раза в

неделю. После того как срок действия сертификата истек, он может быть исключен из списка отозванных сертификатов.

4.9.8. Максимальная задержка списков отозванных сертификатов

Списки отозванных сертификатов публикуются в хранилище УЦ КЦМР незамедлительно после генерации. Обычно это происходит автоматически в течение нескольких минут.

4.9.9. Требование доступности онлайновой проверки отзыва и информации о статусе

Действующий список отозванных сертификатов и служба OCSP УЦ КЦМР, дающие возможность доверяющим сторонам в режиме он-лайн получать информацию об отзыве и иных статусах сертификатов, доступны публично. УЦ КЦМР обеспечивает доверяющие стороны информацией о том, как найти действующий список отозванных сертификатов и службу OCSP. В дополнение к этому, информация о статусе сертификатов может быть получена доверяющими сторонами из хранилища по протоколу LDAP.

4.9.10. Требования онлайновой проверки отзыва

Доверяющая сторона обязана проверять статус тех сертификатов, на которые она желает положиться. Если доверяющая сторона не проверяет статус этих сертификатов с помощью опубликованного действующего списка отозванных сертификатов, она должна проверять статус сертификатов, запрашивая службу OCSP или обращаясь в хранилище УЦ КЦМР.

4.9.11. Иные формы объявления об отзыве

Отсутствуют.

4.9.12. Особые требования, касающиеся компрометации ключей

Участники информационных систем, обслуживаемых УЦ КЦМР, извещаются о компрометации или подозрении в компрометации закрытых ключей УЦ КЦМР любыми целесообразными способами.

В случае обоснованного подозрения о компрометации закрытого ключа подписчик и владелец соответствующего сертификата обязаны немедленно приостановить действие сертификата до выяснения обстоятельств.

Если факт компрометации закрытого ключа не подтвердился, то подписчик и владелец соответствующего сертификата вправе возобновить действие приостановленного сертификата, в противном случае они обязаны немедленно сообщить об этом в УЦ или уполномоченному посреднику, которые должны принять меры и отозвать сертификат.

Владелец сертификата, используемого в информационных системах КЦМР, кроме того, обязан в случае компрометации закрытых ключей или увольнения работника, имевшего доступ к закрытым ключам, отозвать соответствующие этим ключам сертификаты и для их замены запросить выпуск новых сертификатов. Новые ключевые пары и сертификаты должны быть введены в действие незамедлительно, в случае увольнения работника – не позднее дня увольнения.

4.9.13. Основания приостановления действия сертификата

Только на следующих основаниях действие сертификата подписчика приостанавливается удостоверяющим центром, и соответствующая информация публикуется в списке отозванных сертификатов:

поступило заявление подписчика или владельца сертификата, который желает временно не использовать сертификат;

удостоверяющий центр, владелец сертификата или подписчик подозревают и проверяют информацию о возможной компрометации закрытого ключа подписчика. (Договорные обязательства требуют от подписчика и владельца сертификата незамедлительного информирования УЦ КЦМР об обнаружении или обоснованном подозрении в компрометации закрытого ключа.);

удостоверяющий центр или владелец сертификата подозревают и проверяют информацию о возможном существенном нарушении подписчиком обязательства, заверения или гарантии действующего договора;

утратил силу, но находится в стадии продления (перезаключения) какой-либо договор, являющийся необходимым условием владения и пользования подписчиком соответствующим закрытым ключом;

удостоверяющий центр, владелец сертификата или уполномоченный посредник подозревают и проверяют информацию о том, что сертификат, возможно, был выпущен с существенным нарушением процедур Положения о практике сертификатов, например, иному лицу, нежели указано в самом сертификате, или без аутентификации этого лица;

удостоверяющий центр, владелец сертификата или уполномоченный посредник подозревают и проверяют информацию об ошибочности существенного факта в заявлении на выпуск сертификата;

удостоверяющий центр, владелец сертификата или уполномоченный посредник подозревают и проверяют информацию о том, что при выпуске сертификата не соблюдены иные существенные условия выпуска;

удостоверяющий центр, владелец сертификата или уполномоченный посредник подозревают и проверяют информацию о том, что данные из сертификата, за исключением непроверяемой информации, неверны или изменились;

подписчик, владелец сертификата или уполномоченный посредник не произвел должную оплату;

удостоверяющий центр, владелец сертификата или уполномоченный посредник подозревают и проверяют информацию об опасности дальнейшего использования сертификата для информационных систем.

В последнем случае УЦ КЦМР, владелец сертификата или уполномоченный посредник при определении опасности использования сертификата для информационных систем среди прочего рассматривают:

количество и характер полученных жалоб;

идентичность лиц, подавших жалобы;

действующее законодательство;

иные возможные меры по исключению опасности со стороны подписчика.

4.9.14. Лица, имеющие право запрашивать приостановление действия сертификатов

Подавать заявления на приостановление действия сертификатов имеют право подписчики, владельцы сертификатов и уполномоченные посредники, а также должным образом уполномоченные представители указанных лиц. Запрашивать приостановление действия сертификатов также могут уполномоченные сотрудники удостоверяющего центра.

4.9.15. Процедуры рассмотрения заявление на приостановление

Перед приостановлением действия сертификата подписчика УЦ КЦМР проверяет, что приостановление инициировано правомочно. Применяющиеся при этом процедуры аналогичны процедурам отзыва сертификата, которые изложены в параграфе 4.9.3.

4.9.16. Предельный срок приостановления

Предельный срок приостановления действия сертификата не устанавливается. Сертификат может находиться в состоянии приостановки до момента истечения срока его действия.

4.10. Сервисы статуса сертификатов

4.10.1. Эксплуатационные характеристики

Информация о статусе сертификатов доступна через список отозванных сертификатов, в хранилище по протоколу LDAP или на web-сайте КЦМР по адресу http://www.kisc.kz/ca/crl.html, а также через службу OCSP.

4.10.2. Режим работы сервисов

Сервисы статуса сертификатов доступны круглосуточно и непрерывно.

4.10.3. Дополнительные возможности

Не применяются.

4.11. Окончание подписки

Подписчик может отменить подписку на сертификат:
расторгнув действующий договор о подписке;
отзывая сертификат до окончания срока его действия.
Подписка на сертификат также автоматически прекращается при истечении срока его действия.

4.12. Депонирование и восстановление ключа

Процедуры депонирования закрытого ключа не применяются.

5. КОНТРОЛЬ ОБЪЕКТОВ, УПРАВЛЕНИЯ И ФУНКЦИОНИРОВАНИЯ

5.1. Физический контроль

Детальные меры физического контроля и безопасности, реализуемые в УЦ КЦМР, документально утверждены. Эти документы содержат конфиденциальную информацию КЦМР и не публикуются. Вместе с тем, общий обзор этих мер приведен в данной главе.

Кроме того, КЦМР подвергал и планирует далее регулярно подвергать выполнение этих мер независимому аудиту в соответствии с главой 8.

Для обеспечения безопасности удостоверяющего центра проводятся организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также обеспечения информационной безопасности, установлены и действуют соответствующие правила и инструкции для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

Защита информации от несанкционированного доступа осуществляется на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении регламентных и ремонтных работ.

Защита информации от несанкционированного доступа предусматривает контроль эффективности средств защиты. Этот контроль периодически выполняется администраторами безопасности на основе требований документации на средства защиты.

5.1.1. Размещение и конструкция здания

Деятельность УЦ КЦМР ведется в физически защищенных условиях, которые сдерживают, предотвращают и выявляют несанкционированное использование, доступ, раскрытие конфиденциальной информации и систем.

Эти требования выполняются, в частности, за счет создания многоуровневой системы физической безопасности. Каждый уровень является барьером защиты, который обеспечивает разрешительный контроль доступа для физических лиц и требует от лица положительного ответа для доступа к следующему участку. Каждый последующий уровень требует более строгого доступа и большей физической защищенности от вторжения или несанкционированного доступа. Кроме того, каждый уровень физической безопасности содержит следующий уровень строго внутри себя таким образом, что они не имеют общих границ. Границами внешнего уровня являются наружные стены здания.

5.1.2. Физический доступ

Доступ на каждый уровень физической безопасности контролируется таким образом, что его может получить только уполномоченный персонал.

5.1.3. Электропитание и кондиционирование воздуха

Объекты безопасности УЦ КЦМР оборудованы системами основного и резервного электропитания, обеспечивающими непрерывность электроснабжения. Они также оборудованы основными и запасными системами отопления, вентиляции и кондиционирования воздуха для контроля температуры и влажности.

5.1.4. Влияние водной стихии

Размещение объектов безопасности УЦ КЦМР сводит к минимуму риски наводнения или других вредных воздействий водной стихии.

5.1.5. Предотвращение и защита от пожаров

Объекты безопасности УЦ КЦМР размещены, оборудованы и организационно защищены средствами предотвращения и тушения пожара, вредных воздействий возгорания и задымления. Эти меры соответствуют требованиям законодательства Республики Казахстан.

5.1.6. Хранение носителей информации

УЦ КЦМР защищает используемые носители важной системной и любой другой конфиденциальной информации, системы их электропитания от пожара, наводнения, воздействия других вредных факторов, а также реализует меры сдерживания, предотвращения и выявления несанкционированного использования или доступа к этим носителям.

5.1.7. Утилизация

УЦ КЦМР реализует процедуры для утилизации отходов, предотвращающие несанкционированное использование и доступ к ним, тем самым, исключая возможность утечки конфиденциальной информации через этот канал.

5.1.8. Внешнее резервирование

УЦ КЦМР, имея безопасный внешний запасной объект, поддерживает резервное хранение и электропитание критических системных данных и любой другой конфиденциальной информации, включающей данные контроля.

5.2. Процедурный контроль

5.2.1. Распределение ролей

Работники, которым поручается управлять инфраструктурой безопасности, рассматриваются как «ответственный персонал», обслуживающий «ответственные

участки». Соискатели на роль ответственного персонала (назначения на ответственный участок) в соответствии с настоящей Политикой сертификатов должны соответствовать утвержденным типовым квалификационным требованиям к должностям работников КЦМР.

К разряду ответственного персонала относятся работники, имеющие доступ или контролирующие аутентификацию или криптографические операции, которые могут существенно влиять на:

проверку информации из заявлений на выпуск сертификатов;

прием, отказ в приеме или иную обработку заявлений на выпуск или отзыв сертификатов;

выпуск или отзыв сертификатов.

Ответственный персонал, включает в себя, но не ограничивается:

персоналом обслуживания клиентов;

персоналом системного администрирования;

инженерным персоналом;

управляющими инфраструктуры безопасности.

5.2.2. Численность персонала, необходимого для отдельной задачи

В УЦ КЦМР установлены, поддерживаются и обеспечиваются строгие процедуры контроля, гарантирующие разделение и ответственное исполнение обязанностей, выполнение наиболее важных задач несколькими ответственными лицами.

К числу наиболее важных задач, требующих выполнения несколькими лицами, относятся доступ и управление криптографическими устройствами и их ключевым материалом.

Процедуры внутреннего контроля построены так, что как минимум двое работников из числа ответственного персонала требуются для физического или логического доступа к устройству. Доступ к криптографической аппаратуре в течение всего ее жизненного цикла, от входной проверки и приемки до окончательного логического и/или физического уничтожения, осуществляется строго несколькими ответственными лицами одновременно. С момента ввода в модуль действующих ключей осуществляется дополнительный контроль для разделения физического и логического доступа к устройству. Лица, имеющие физический доступ к модулям, не хранят «частей секрета» и наоборот.

Ввод и проверка данных, необходимых для выпуска сертификата, должны осуществляться одним (или более) ответственными работниками УЦ, уполномоченного посредника или заявителя с применением средств автоматизации проверки.

Генерация сертификатов на основе введенных данных должна представлять собой автоматизированный процесс, включающий проверку полномочий инициатора.

5.2.3. Идентификация и аутентификация каждой роли

УЦ КЦМР проверяет идентичность и аутентичность всего персонала, претендующего на ответственные участки, перед выдачей им:

персональных устройств и прав доступа на соответствующие объекты;

электронных средств для доступа и выполнения специализированных функций в информационных системах УЦ КЦМР.

Идентификация выполняется ответственным персоналом кадровой службы или службы безопасности, требует личного (физического) присутствия претендентов и включает в себя проверку документов, удостоверяющих личность.

5.2.4. Функции, требующие разделения обязанностей

Функции, требующие разделения обязанностей, включают в себя, но не исчерпываются:

администрированием операционных систем серверов УЦ;

администрированием криптографических модулей;
администрированием прикладного программного обеспечения на серверах УЦ;
администрированием web-модулей интерфейса клиентов УЦ;
администрирование базы данных клиентов УЦ;
установкой, монтажом, пуско-наладкой основного оборудования.

5.3. Контроль персонала

Детальные меры контроля персонала и политики безопасности, реализуемые в УЦ КЦМР, документально утверждены. Эти документы содержат конфиденциальную информацию КЦМР и не публикуются. Вместе с тем, общий обзор этих мер приведен в данной главе.

5.3.1. Требования к опыту и квалификации

Образование, профессиональная компетентность и практический опыт претендентов на должности, входящие в разряд ответственного персонала, должны соответствовать утвержденным типовым квалификационным требованиям к должностям работников КЦМР.

5.3.2. Процедуры фоновой проверки

Претендент на должность, входящую в разряд ответственного персонала в соответствии с Трудовым Кодексом Республики Казахстан обязан подтвердить наличие базовой подготовки и образования предъявлением документа об образовании, квалификации, наличии специальных знаний или профессиональной подготовки, а практического опыта – предъявлением документа, подтверждающего трудовой стаж.

5.3.3. Требования к подготовке, переподготовке и повышению квалификации

КЦМР обеспечивает свой персонал подготовкой, переподготовкой и повышением квалификации, необходимыми для компетентного и удовлетворительного выполнения им служебных обязанностей. Тематика обучения ежегодно согласовывается менеджментом КЦМР на предмет соответствия функциям персонала и актуальности.

5.3.4. Требование к частоте подготовки, переподготовки и повышения квалификации

КЦМР проводит подготовку, переподготовку и повышение квалификации своего персонала в соответствии с Трудовым кодексом Республики Казахстан в том объеме и с той частотой, которые необходимы для функционирования и развития предприятия.

5.3.5. Последовательность и частота перемещений по службе

Специальных требований не выдвигается.

5.3.6. Ответственность за несанкционированные действия

В случае обнаружения несанкционированного доступа или подозрения о нем, системный администратор вместе с сотрудником безопасности могут приостановить доступ к системам со стороны нарушителя (подозреваемого). Дальнейшие дисциплинарные санкции определяются руководством КЦМР.

5.3.7. Требования к независимым контрактникам

КЦМР оставляет за собой право привлекать на ответственные участки независимых контрактников и консультантов. Вместе с тем, такое привлечение должно осуществляться только в минимально необходимой мере, четко определенной форме и при следующих условиях:

независимый контрактник или консультант привлекается на роль ответственного сотрудника, только если для исполнения обязанностей данной роли не хватает штатных работников;

независимый контрактник или консультант проверяется в той же мере, как и штатный работник.

Если последнее условие не выполнено, то независимый контрактник или консультант допускается на защищенные объекты только в сопровождении и под постоянным контролем ответственного персонала.

5.3.8. Документация, раскрываемая персоналу

КЦМР обеспечивает свой персонал (включая ответственных работников) обучением и доступом к документации, которые необходимы для компетентного и удовлетворительного исполнения обязанностей.

5.4. Процедуры контрольного протоколирования

5.4.1. Типы протоколируемых событий

В данном параграфе устанавливаются типы контролируемых событий, которые обязан регистрировать УЦ КЦМР. Обязательные компоненты записей контрольных протоколов перечислены в Положении о практике сертификатов.

УЦ КЦМР регистрирует следующие события или данные:

события, связанные с жизненным циклом ключей УЦ, включая, но не ограничиваясь их генерацией, восстановлением и уничтожением, а также созданием, хранением и уничтожением их резервных копий;

события, связанные с жизненным циклом сертификатов, включая, но не ограничиваясь получением запросов на выпуск и изменение статуса сертификатов, генерацией и изменением статуса сертификатов, генерацией и выпуском списков отозванных сертификатов;

события, связанные с жизненным циклом криптографических модулей, включая, но не ограничиваясь их получением, вводом в эксплуатацию, использованием, сервисным обслуживанием, ремонтом, выводом из эксплуатации и уничтожением;

данные, связанные с заявлениями на выпуск сертификатов, включая вид и номер документа, идентифицирующего заявителя, данные должностного лица УЦ или уполномоченного посредника, проверившего и подтвердившего данные заявлений;

иные важные с точки зрения безопасности события, включая, но не ограничиваясь сеансами администрирования систем УЦ (дата, время, цели, в том числе, изменение профилей, доступ к контрольным протоколам и т.п.), инцидентами (сбои систем, отказы аппаратного обеспечения и другие аномалии).

Значения ключей и паролей не должны записываться в автоматические контрольные протоколы в явном виде.

5.4.2. Частота анализа контрольных протоколов

Контрольные протоколы еженедельно анализируются на предмет наличия предупреждений о нарушениях или инцидентов в работе систем. Выявленные инциденты регистрируются, устраняются и закрываются в регламентированном порядке.

5.4.3. Срок хранения контрольных протоколов

Контрольные протоколы систем УЦ ведутся в КЦМР непрерывно, подлежат ежемесячному архивированию и сдаче в архив в соответствии с разделом 5.5, где хранятся в течение регламентированного срока.

5.4.4. Защита контрольных протоколов

Контрольные протоколы защищены от несанкционированного просмотра, модификации и удаления организационными и техническими мерами.

5.4.5. Резервное копирование контрольных протоколов

Резервное копирование контрольных протоколов осуществляется ежедневно.

5.4.6. Система сбора контрольных протоколов

Не используется.

5.4.7. Уведомление субъекта, вызвавшего событие

При записи события в контрольный протокол уведомление субъекта, вызвавшего это событие, в обязательном порядке не требуется.

5.4.8. Оценка уязвимости

Оценка уязвимостей, выявленных в результате анализа контрольных протоколов, осуществляется в порядке, регламентированном для устранения инцидентов и проблем функционирования УЦ КЦМР.

5.5. Ведение архива

5.5.1. Типы архивируемых событий

Удостоверяющий центр КЦМР ведет архив:

контрольных протоколов в соответствии с разделом 5.4;

сертификатов, включая отозванные сертификаты и сертификаты с истекшим сроком действия;

информации о жизненном цикле сертификатов (заявки на изменение статуса);

списков отозванных сертификатов.

5.5.2. Срок хранения архива

Удостоверяющий центр КЦМР в ходе своей деятельности ведет архив постоянно. Данные хранятся в архиве в соответствии с регламентированными сроками. В случае прекращения деятельности УЦ КЦМР данные архива сохраняются в течение срока, установленного законодательством Республики Казахстан.

5.5.3. Защита архива

КЦМР обеспечивает хранение архивных документов в соответствии с законодательством Республики Казахстан. Доступ к архиву имеет только ответственный персонал КЦМР. Архив защищается от несанкционированного просмотра, изменений, удаления специальной системой мер.

5.5.4. Резервное копирование архива

Резервное копирование данных архива осуществляется ежемесячно, одновременно с пополнением архива данными за истекший месяц. Одна архивная копия хранится на основном объекте, вторая – на безопасном внешнем запасном объекте.

5.5.5. Требование о постановке отметки времени на архивных записях

Архивные носители должны маркироваться с указанием даты архивирования, информация о времени архивирования должна автоматически фиксироваться программно-техническими средствами архивирования. Записи контрольных протоколов должны иметь отметку о дате и времени. Сертификаты, заявки на их выпуск и изменение статуса, списки отозванных сертификатов имеют отметки о дате и времени создания, заверенные электронной цифровой подписью.

5.5.6. Условия архивирования

Удостоверяющий центр обеспечивает ведение архива в соответствии с законодательством Республики Казахстан.

5.5.7. Порядок получения и проверки архивной информации

Доступ к архиву имеет только ответственный персонал УЦ КЦМР. Проверка архивной информации регламентирована и проводится путем пробного восстановления в соответствии параграфом 5.7.4.

5.6. Смена ключей УЦ

Ключевые пары удостоверяющего центра КЦМР имеют срок действия. По окончании срока их действия закрытые ключи и их резервные копии уничтожаются по акту комиссией.

Заблаговременно до окончания срока действия администратор удостоверяющего центра организует формирование новой ключевой пары и трех соответствующих ей сертификатов (в целях обеспечения гибкости при построении цепочек сертификатов):

сертификат, содержащий новый открытый ключ, подписанный закрытым ключом истекающей ключевой пары;

сертификат, содержащий новый открытый ключ, подписанный соответствующим ему новым закрытым ключом (самоподписанный сертификат);

сертификат, содержащий истекающий открытый ключ, подписанный закрытым ключом из вновь вводимой ключевой пары.

Сформированные новые сертификаты доводятся до сведения доверяющих сторон путем публикации в хранилище.

5.7. Восстановление после компрометации и происшествий

5.7.1. Процедуры обработки происшествий и компрометации

На случай возможной компрометации или иных чрезвычайных происшествий создается и хранится на безопасном внешнем запасном объекте резервная копия следующих данных:

заявок на отзыв или изменение статуса сертификатов,

контрольных протоколов;

базы всех выпущенных сертификатов, включая отозванные сертификаты и сертификаты с истекшим сроком действия.

В соответствии с параграфом 6.2.4 создаются и хранятся резервные копии закрытого ключа УЦ.

5.7.2. Повреждения вычислительных, программных ресурсов и/или данных

Случаи повреждения вычислительных, программных ресурсов и/или данных удостоверяющего центра должны обрабатываться в порядке, регламентированном для управления инцидентами, резервного копирования, архивирования и восстановления данных.

В необходимых случаях должны вводиться в действие процедуры восстановления функционирования в соответствии с параграфом 5.7.4.

5.7.3. Компрометация закрытого ключа удостоверяющего центра

Компрометация закрытого ключа Удостоверяющего центра относится к категории чрезвычайных инцидентов и должна влечь за собой введение в действие плана восстановления функционирования в соответствии с параграфом 5.7.4. В этом случае сертификаты ключей Удостоверяющего центра в соответствии с указанным планом должны подлежать незамедлительному отзыву.

5.7.4. Возможности непрерывной деятельности после происшествий

КЦМР на случай чрезвычайных происшествий, связанных с природным или человеческим фактором имеет безопасный внешний запасной объект, разрабатывает, проверяет, обеспечивает и, в случае необходимости, реализует план восстановления функционирования. Внешний запасной объект имеет уровень физической защиты, эквивалентный основному объекту.

План определяет порядок восстановления сервисов информационных систем и основных функций удостоверяющего центра в течение 24 часов после происшествия.

При этом восстановление таких функций как:

выпуск сертификатов;

отзыв сертификатов;

публикация сведений об отзыве сертификатов

осуществляется в течение не более чем 2 (двух) часов.

В целях проверки возможностей непрерывной деятельности в случае чрезвычайных происшествий не реже одного раза в год проводится пробное восстановление информации УЦ из архива.

5.8. Прекращение работы удостоверяющего центра

Прекращение работы удостоверяющего центра КЦМР может осуществляться в соответствии с действующим законодательством Республики Казахстан. При этом удостоверяющий центр принимает все меры, необходимые для минимизации влияния указанного процесса на участников информационных систем.

В случае прекращения своей деятельности УЦ КЦМР обязан не позднее чем за 30 (тридцать) дней до даты прекращения проинформировать об этом всех подписчиков.

Начиная с этого момента, по согласованию с владельцами сертификатов решаются вопросы возможной передачи в другие удостоверяющие центры сведений, необходимых для продолжения обслуживания подписчиков. Если в течение указанных 30 дней вопросы продолжения обслуживания подписчиков другим удостоверяющим центром не решены, соответствующие сертификаты отзываются и хранятся в архиве УЦ КЦМР в соответствии с законодательством Республики Казахстан.

6. КОНТРОЛЬ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ

6.1. Генерация и установка ключевых пар

6.1.1. Генерация ключевых пар

Генерация ключевых пар должна проводиться только с использованием средств криптографической защиты информации, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации[2].

Ключевые пары УЦ КЦМР должны формироваться в криптографическом модуле УЦ КЦМР, сертифицированном на соответствие этому же стандарту, и не должны извлекаться из криптографического модуля в незащищенном виде.

Ключевые пары первичной инициализации для подписчиков могут генерировать сотрудники УЦ КЦМР, уполномоченного посредника или заявителя.

Подписчики могут доверить генерацию собственной ключевой пары другому лицу при обязательном условии создания закрытого ключа непосредственно на защищенном носителе ключевой информации, исключающем возможность доступа к закрытому ключу, его несанкционированного изменения или использования. В остальных случаях подписчики обязаны генерировать собственные ключевые пары самостоятельно.

6.1.2. Доставка закрытого ключа подписчику

Обычно подписчики генерируют свои закрытые ключи самостоятельно, в этом случае в доставке закрытого ключа подписчику нет необходимости.

---

[2] Здесь и далее по тексту роль данную роль выполняет действующий в настоящее время государственный стандарт Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования».

В противном случае в соответствии с параграфом 6.1.1 закрытый ключ генерируется непосредственно на защищенном носителе, исключающем возможность его разглашения, изменения или несанкционированного использования.

В любом случае доступ к закрытым ключам подписчиков со стороны работников или систем УЦ КЦМР должен быть исключен.

6.1.3. Доставка открытого ключа в удостоверяющий центр

При передаче открытого ключа для сертификации в удостоверяющий центр, он должен доставляться способом, исключающим возможность подмены по пути следования. При этом заявитель должен быть в состоянии подтвердить факт владения подписчиком соответствующим закрытым ключом. Приемлемым механизмом для такой доставки является запрос на подпись сертификата PKCS#10 или PKCS#7, переданный с использованием доступных каналов связи.

6.1.4. Передача открытого ключа удостоверяющего центра доверяющим сторонам

Открытый ключ УЦ КЦМР вручается доверяющим сторонам в форме сертификата на носителе, исключающем возможность его подмены или искажения. Доверяющая сторона получает этот сертификат из рук в руки в УЦ КЦМР, от уполномоченного посредника или от владельца своего сертификата. Проверка аутентичности сертификата может быть осуществлена средствами электронной цифровой подписи.

6.1.5. Размеры ключей

Ключевые пары должны иметь длину, достаточную для того, чтобы предотвратить определение закрытого ключа методами криптоанализа в период действия ключевой пары.

УЦ КЦМР регистрирует ключи, предназначенные для использования в соответствии с:

международным стандартом ГОСТ 34.310-2004 (ЭЦП), которые имеют размеры:
закрытый ключ – 256 бит;
открытый ключ – 512 бит;
алгоритмом RSA (PKCS#1) в двух вариантах:
закрытый ключ – 1536 бит;
открытый ключ – 1536 бит
или
закрытый ключ – 2048 бит;
открытый ключ – 2048 бит.

6.1.6. Генерация и проверка качества параметров криптографических алгоритмов

В части, касающейся международного стандарта ГОСТ 34.310-2004, все подписчики используют параметры схемы электронной цифровой подписи, которые предопределены УЦ КЦМР. Их качество гарантировано сертификатом соответствия средств криптографической защиты информации, в которых они реализованы, действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации.

В части, касающейся алгоритма RSA (PKCS#1), подписчики генерируют используемые параметры алгоритма самостоятельно, как и ключи. В связи с этим, генерация параметров должна проводиться только с использованием средств криптографической защиты информации, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации.

6.1.7. Цели использования ключа (расширение «keyUsage» согласно X.509 v3)

Изложено в параграфе 7.1.2.

6.2. Защита закрытого ключа и инженерный контроль криптографического модуля

6.2.1. Стандарты и контроль криптографического модуля

УЦ КЦМР должен выполнять криптографические операции на криптографических модулях, сертифицированных на соответствие действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации не ниже, чем по второму уровню безопасности.

Все закрытые ключи, которые используются в информационных системах, обслуживаемых КЦМР, должны быть защищены, поэтому обладатели закрытых ключей в соответствии с настоящей Политикой сертификатов и договорными обязательствами должны предпринимать необходимые меры, предотвращающие их потерю, разглашение, изменение или несанкционированное использование.

Подписчикам запрещается:

знакомить с закрытыми ключами посторонних лиц или передавать им носители закрытых ключей;

снимать копии с закрытых ключей за исключением разрешенных случаев резервного копирования;

выводить закрытые ключи на печать или экран монитора;

преднамеренно вносить изменения в криптографические ключи и сертификаты.

УЦ КЦМР рекомендует подписчикам в работе со своими закрытыми ключами в течение всего их жизненного цикла использовать защищенные носители ключевой информации, например, смарт-карты или аппаратные токены, которые закрытый ключ никогда не покидает.

Подписчикам сертификатов, используемых в информационных системах КЦМР, кроме того, запрещается записывать на носители закрытых ключей постороннюю информацию или иным образом применять указанные носители не по назначению. В нерабочее время носители их закрытых ключей должны находиться в личном сейфе либо в сейфе прямого начальника.

6.2.2. Разделение закрытого ключа между ответственным персоналом по схеме m из n

Контроль данных, необходимых для защиты закрытых ключей УЦ КЦМР (данные активации), должен быть регламентирован и обеспечиваться группой ответственного персонала. УЦ КЦМР должен использовать для закрытых ключей данные активации в форме разделения секрета на отдельные части, так называемые «части секрета», которые должны храниться работниками из числа ответственного персонала, так называемыми «хранителями секрета». Для восстановления закрытого ключа должно требоваться некоторое регламентированное пороговое значение частей секрета (m) из их общего числа (n).

6.2.3. Депонирование закрытого ключа

УЦ КЦМР не депонирует закрытые ключи.

6.2.4. Резервное копирование закрытого ключа

Резервное копирование закрытых ключей УЦ КЦМР должно производиться в регламентированном порядке в целях обеспечения возможности восстановления на случай чрезвычайных происшествий и сбоев в работе.

Резервная копия закрытых ключей УЦ КЦМР должна быть защищена от модификации и разглашения как физическими, так и криптографическими средствами. Уровень данной защиты не должен быть меньше, чем уровень защиты криптографических модулей в условиях основного и запасного объектов УЦ КЦМР.

Подписчики сертификатов, используемых в информационных системах КЦМР, должны иметь резервную копию соответствующих им закрытых ключей, которая должна храниться в личном сейфе или в запечатанном конверте в сейфе прямого руководителя с указанием на конверте подписчика.

Резервное копирование закрытого ключа подписчиками иных информационных систем, обслуживаемых КЦМР, запрещается.

6.2.5. Архивирование закрытого ключа

Закрытые ключи с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной документацией соответствующих средств криптографической защиты информации. Архивное хранение закрытых ключей не допускается.

6.2.6. Загрузка/выгрузка закрытого ключа в/из криптографического модуля

При вводе закрытого ключа УЦ КЦМР в криптографический модуль применяются механизмы, предотвращающие его утрату, хищение, изменение, разглашение, несанкционированное использование.

Изначально закрытые ключи УЦ КЦМР генерируются внутри аппаратного криптографического модуля. Необходимость их выгрузки и загрузки в него обусловлена потребностями резервного копирования и восстановления. В связи с этим, количество произведенных выгрузок не превосходит регламентированное число созданных резервных копий. Кроме того, в выгруженной форме закрытый ключ защищен криптографически, в частности, зашифрован.

Для подписчиков, использующих защищенные носители ключевой информации, например, смарт-карты или аппаратные токены, запись закрытых ключей на них также необходимо выполнять с применением механизмов, предотвращающих их утрату, хищение, изменение, разглашение и несанкционированное использование.

6.2.7. Хранение закрытого ключа в криптографическом модуле

Закрытые ключи УЦ КЦМР в криптографическом модуле хранятся только в зашифрованном виде.

6.2.8. Способы активации закрытого ключа

Участники информационных систем, обслуживаемых УЦ КЦМР, должны защищать данные активации своих закрытых ключей от потери, хищения, изменения, разглашения и несанкционированного использования.

Общим требованием для них является принятие коммерчески целесообразных мер для физической защиты своих рабочих станций, предотвращающих несанкционированное использование рабочих станций и соответствующих закрытых ключей. Рекомендуется дополнительное использование паролей в соответствии с параграфом 6.4.1 или аналогичных мер аутентификации пользователя перед активацией закрытого ключа, например, пароль на использование закрытого ключа, на вход в операционную систему, на отключение хранителя экрана или на вход в сеть.

В качестве дополнительной меры безопасности для аутентификации пользователя перед активацией закрытого ключа рекомендуется использование штатных функций аппаратных токенов, смарт-карт или биометрических устройств доступа.

В деактивированной форме закрытый ключ должен храниться только в зашифрованном виде.

Закрытые ключи УЦ КЦМР должны активироваться в криптографическом модуле пороговым числом хранителей секрета (как определено в параграфе 6.2.2), предоставивших свою часть данных активации, каждая из которых хранится на защищенном носителе. Активированный закрытый ключ остается активным до момента уничтожения.

6.2.9. Способ деактивации закрытого ключа

В целях безопасности подписчикам рекомендуется деактивировать закрытый ключ сразу же после выполнения необходимых операций с ним либо путем извлечения его защищенного носителя, либо выходом из системы, в зависимости от того, какой механизм аутентификации избран подписчиком.

6.2.10. Способ уничтожения закрытого ключа

В случае необходимости носители закрытых ключей УЦ КЦМР уничтожаются таким способом, который гарантирует отсутствие остаточной информации о ключе и исключает возможность его восстановления. Данные процедуры регламентированы и оформляются документально.

6.2.11. Оценка криптографических модулей

УЦ КЦМР использует только те типы криптографических модулей, которые успешно прошли сертификацию на соответствие требованиям действующего стандарта Республики Казахстан, определяющего общие технические требования к средствам криптографической защиты информации, не ниже чем по второму уровню безопасности.

6.3. Другие особенности управления ключевыми парами

6.3.1. Архивирование открытых ключей

Все открытые ключи, когда-либо удостоверенные УЦ КЦМР, архивируются в соответствии с разделом 5.5.

6.3.2. Сроки действия сертификатов и использования ключевых пар

Срок действия сертификатов подписчиков в информационных системах, обслуживаемых КЦМР (МСПД, системы розничных платежей, СОБС, ФАСТИ, Авангард Plat) составляет 1 (один) год. Срок действия сертификатов первичной инициализации составляет 14 (четырнадцать) суток. Срок действия остальных сертификатов подписчиков, выпускаемых УЦ КЦМР составляет 1 (один), 2 (два) или 3 (три) года по выбору подписчика. Срок действия сертификатов УЦ КЦМР составляет 20 (двадцать) лет и исчисляется с даты и времени его генерации. Действие любого сертификата заканчивается с истечением срока его действия или в случае его отзыва.

Для подписчиков сроки использования их ключевых пар совпадают со сроками использования соответствующих сертификатов, за исключением того, что они могут использоваться и дольше, в целях расшифрования или проверки электронной цифровой подписи.

УЦ КЦМР не выпускает сертификаты подписчиков, срок действия которых превышает срок действия соответствующего сертификата УЦ КЦМР, который необходимо использовать для проверки. В связи с этим, срок использования закрытого ключа УЦ КЦМР обязательно короче, чем срок действия соответствующего сертификата. В частности, срок использования закрытого ключа УЦ КЦМР не может превышать 19 (девятнадцать) лет, то есть срок действия соответствующего сертификата (20 лет) минус срок действия самого «короткого» сертификата подписчика (1 год).

По окончании периода использования ключевой пары подписчики и УЦ КЦМР обязаны прекратить любое использование этой ключевой пары. Исключение составляет вышеуказанные случаи, а также потребность УЦ КЦМР в подписи информации об отзыве

сертификатов в период до истечения срока действия последнего сертификата, который выпущен с помощью данной ключевой пары.

Для непрерывной работы в информационных системах, которые требуют наличия сертификатов, выпущенных УЦ КЦМР, пользователь должен своевременно генерировать новые ключевые пары и запрашивать выпуск новых сертификатов на замену истекающим.

6.4. Данные активации

6.4.1. Генерация и установка данных активации

Генерация и установка данных активации для закрытых ключей имеет целью защиту закрытых ключей от потери, хищения, изменения, разглашения или несанкционированного использования.

К паролям, используемым в качестве данных активации, предъявляются следующие требования:

заводская установка пароля должна быть изменена немедленно после первого подключения;

пароли не должны быть короче 6 символов;

пароли должны содержать минимум одну букву в нижнем регистре (строчную) и одну букву в верхнем регистре (заглавную);

пароли должны содержать минимум одну цифру, а также один небуквенный и нецифровой символ.

Данные активации закрытых ключей УЦ КЦМР в соответствии с настоящей Политикой сертификатов подлежат разделению секрета.

6.4.2. Защита данных активации

Участники должны защищать данные активации своих закрытых ключей от потери, хищения, изменения, разглашения или несанкционированного использования.

В соответствии с настоящей Политикой сертификатов и внутренней политикой безопасности УЦ КЦМР применяет к данным активации собственных закрытых ключей процедуры разделения секрета. УЦ КЦМР обеспечивает процедуры и средства, позволяющие хранителям секрета избежать потери, хищения, изменения, разглашения или несанкционированного использования частей секрета, которые у них находятся. Хранителям секрета запрещается:

копировать, разглашать и передавать части секрета третьим лицам или как бы то ни было несанкционированно использовать их;

разглашать посторонним лицам свой статус хранителя секрета.

В УЦ КЦМР ведется журнал, в котором регистрируется создание и передача на хранение частей секрета, а также их использование.

6.4.3. Иные аспекты работы с данными активации

При необходимости пересылки данных активации техническими методами, такая пересылка должна быть защищена от потери, хищения, модификации, разглашения, или несанкционированного использования.

Данные активации закрытых ключей УЦ КЦМР должны выводиться из использования с применением процедур, защищающих от потери, хищения, модификации, разглашения или несанкционированного использования закрытых ключей, активируемых этими данными. По истечении соответствующего срока данные активации выводятся из использования путем перезаписи или физического уничтожения.

6.5. Контроль компьютерной безопасности

6.5.1. Специальные технические требования компьютерной безопасности

УЦ КЦМР обеспечивает контроль используемых вычислительных ресурсов, программного обеспечения и данных от несанкционированного доступа с помощью систем, которые фиксируют показатели, перечисленные в параграфе 5.4.1.

Компьютеры, работающие в УЦ КЦМР, удовлетворяют следующим требованиям:

ЭВМ для подписи сертификатов изолирована от неавторизованного доступа;

операционные системы поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных и соответствующих пакетов защиты, в том числе антивирусных;

ведется мониторинг с целью обнаружения несанкционированных программных изменений;

количество запущенных системных служб сведено к минимуму.

Доступ к основным серверам разрешен только выделенным лицам, пользователи общих приложений не имеют учетных записей на основных серверах.

Основные сети, используемые для обслуживания подписчиков, логически отделены от остальных компонент. Это разделение исключает любой сетевой доступ кроме доступа через определенные прикладные процессы. УЦ КЦМР использует межсетевые экраны для защиты основных сетей от внутреннего и внешнего вмешательства и ограничивает содержание и источники сетевой активности, которая может влиять на основные системы. УЦ КЦМР устанавливает необходимость использования и требования к паролям, включая периодичность их смены. Прямой доступ к базам данных, обеспечивающим хранилище УЦ КЦМР, имеет только выделенная группа лиц из числа ответственного персонала.

Компьютеры подписчиков и доверяющих сторон должны удовлетворять следующим требованиям:

использование лицензионного программного обеспечения;

поддержание операционных систем на высоком уровне защиты, при регулярном применении всех рекомендованных и соответствующих пакетов защиты, в том числе межсетевых экранов, антивирусных программ и т.д.;

в случаях совместного использования компьютера несколькими пользователями, разграничение доступа, основанное на сложном пароле.

6.5.2. Оценка компьютерной безопасности

Средства криптографической защиты информации, которые используются участниками информационных систем, обслуживаемых УЦ КЦМР, должны быть сертифицированы на соответствие действующим в Республике Казахстан основным техническим требованиям. Специальных требований по сертификации иных компонентов используемых вычислительных систем и программного обеспечения не выдвигается.

6.6. Технический контроль жизненного цикла

6.6.1. Контроль развития системы

УЦ КЦМР выступает заказчиком используемого программного обеспечения. УЦ КЦМР самостоятельно определяет требования к его разработке, включая требования к среде разработки, корректности и качеству результирующего программного обеспечения.

6.6.2. Контроль управления безопасностью

Работоспособность и целостность технических и программных средств удостоверяющего центра должны обеспечиваться системой организационных и технических мер, основанных на разделении прав использования указанных средств,

доступа к ним, а также к техническим средствам, необходимым для доступа. Соблюдение данной системы мер должно постоянно контролироваться.

6.6.3. Контроль безопасности жизненного цикла

Специальных требований не предъявляется.

6.7. Средства управления сетевой безопасностью

Функции УЦ КЦМР должны выполняться в сетях, защищаемых в регламентированном порядке от несанкционированного доступа, вмешательства и DOS-атак.

Конфиденциальность, аутентичность, целостность и неотказумость при информационном обмене обеспечивается с помощью шифрования и цифровой подписи.

6.8. Метки времени

Сертификаты, списки отозванных сертификатов, контрольные протоколы, содержащие информацию о выпуске и изменении статуса сертификатов, должны содержать информацию о дате и времени. При этом содержащаяся в сертификатах и списках отозванных сертификатов информация о дате и времени их создания заверяется электронной цифровой подписью.

7. ПРОФИЛИ СЕРТИФИКАТОВ, COC И OCSP

7.1. Профиль сертификата

Сертификаты, выпускаемые УЦ КЦМР, соответствуют рекомендациям (ITU-T) X.509 v3 и (IETF) RFC 5280. Основные поля, содержащиеся в сертификатах, вместе с требованиями к их содержанию приведены в следующей таблице.

Название	Требования к содержанию
version	v3
serialNumber	*уникальный серийный номер сертификата*
signatureAlgorithm	*объектный идентификатор алгоритма*
issuer	C = KZ O = KISC CN = KISC Root CA
validity	*YYYYMMDDHHMMSSZ* GMT (действителен с) *YYYYMMDDHHMMSSZ* GMT (действителен по)
subject	C = KZ O = *наименование организации* (опционально) OU = *наименование подразделения* (опционально) S = *наименование области* (опционально) L = *наименование города* CN = *ИИН/ Фамилия, имя/ Псевдоним подписчика* (опционально) Serial Number = IIN*НомерИИН* или NR*НомерПаспорта* (опционально) UID = IIN*НомерИИН* или NR*НомерПаспорта* (опционально) E = *адрес электронной почты*
subjectPublicKeyInfo	*открытый ключ*
issuerSignatureAlgorithm	*объектный идентификатор алгоритма подписи сертификата, см. § 7.1.3*
signatureValue	*электронная цифровая подпись*

7.1.1. Номер версии

Все сертификаты, выпускаемые УЦ КЦМР, имеют номер версии v3.

7.1.2. Расширения сертификата

В сертификатах, выпускаемых УЦ КЦМР, используются следующие расширения:

Название	Критичность	Формат
1	**2**	**3**
authorityKeyIdentifier	FALSE	согласно OID 2.5.29.35
subjectKeyIdentifier	FALSE	согласно OID 2.5.29.14
keyUsage	TRUE	согласно OID 2.5.29.15
certificatePolicies	FALSE	согласно OID 2.5.29.32
1	**2**	**3**
subjectAlternativeName	FALSE	согласно OID 2.5.29.17
basicConstraints	TRUE	согласно OID 2.5.29.19
extendedKeyUsage	FALSE	согласно OID 2.5.29.37
cRLDistributionPoints	FALSE	согласно OID 2.5.29.31
authorityInformationAccess	FALSE	согласно OID 1.3.6.1.5.5.7.1.1 (RFC 2459)

7.1.3. Объектные идентификаторы алгоритмов

УЦ КЦМР подписывает сертификаты и списки отозванных сертификатов с помощью одного из следующих алгоритмов:

Название	Объектный идентификатор
ГОСТ 34.310-2004	{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) signature-algorithms(2) gost(2)}
SHA-1 with RSA Encryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}

7.1.4. Формы имен

Имена, которые указываются в сертификатах, выпускаемых УЦ КЦМР, соответствуют требованиям параграфа 3.1.1.

Наличие данных (о юридическом лице) в опциональном компоненте подразделения организации (OU) основного поля «subject» означает, что физическое лицо, указанное в обязательном компоненте общего имени (CN), имеет полномочия и действует от имени юридического лица OU.

Если кроме того сертификат имеет расширение «subjectAltName», оно несет в себе бизнес- идентификационный номер юридического лица-владельца сертификата.

В противном случае, владельцем сертификата является либо юридическое лицо, указанное в компоненте OU основного поля «Subject», если этот компонент не пуст, либо физическое лицо, указанное в компоненте CN поля «Subject».

7.1.5. Ограничения на использование имен

Используемые имена должны соответствовать формату DN-имен, определенных рекомендациями (ITU-T) X.501.

7.1.6. Объектный идентификатор политики сертификатов

Объектные идентификаторы Политики сертификатов, соответствующие информационным системам, в которых применяются выпущенные УЦ КЦМР сертификаты, установлены в разделе 1.2. Расширение «certificatePolicies» заполняется в соответствии с указанным разделом.

7.1.7. Использование расширения «policyConstraints»

Не применяется.

7.1.8. Синтаксис и семантика квалификаторов политики

Квалификаторы политики в сертификатах, выпускаемых УЦ КЦМР, содержат ссылку на настоящую Политику сертификатов и соответствующее ей Положение о практике сертификатов.

7.1.9. Семантика обработки критичных расширений «certificatePolicies»

Не применяется.

7.2. Профиль списка отозванных сертификатов

УЦ КЦМР формирует списки отозванных сертификатов в соответствии с рекомендациями (ITU-T) X.509 v3 и (IETF) RFC 5280. Основные поля, содержащиеся в списках отозванных сертификатов, вместе с требованиями к их содержанию приведены в следующей таблице.

Название	Требования к содержанию
1	**2**
(optional) version	v2
issuer	C = KZ O = KISC CN = KISC Root CA
thisUpdate	*YYYYMMDDHHMMSSZ* GMT
(optional) nextUpdate	*YYYYMMDDHHMMSSZ* GMT
revokedCertificates	Последовательность пар следующего вида: 1. *CertificateSerialNumber* (серийный номер сертификата); 2. *Time* (время обработки заявления на отзыв сертификата).
signatureAlgorithm	*объектный идентификатор алгоритма подписи СОС, см. § 7.1.3*
signatureValue	*электронная цифровая подпись*

7.2.1. Номер версии

Все списки отозванных сертификатов, выпускаемые УЦ КЦМР, имеют номер версии v2.

7.2.2. Расширения списка отозванных сертификатов

В списках отозванных сертификатов, выпускаемых УЦ КЦМР, используются следующие расширения:

Название	Критичность	Формат
authorityKeyIdentifier	FALSE	согласно OID 2.5.29.35
reasonCode	FALSE	согласно OID 2.5.29.14

7.3. Профиль OCSP

7.3.1. Номер версии

Для получения информации о статусе сертификатов, выпущенных УЦ КЦМР, предоставляет сервис OCSP в формате версии 1 согласно рекомендациям (IETF) RFC 2560.

7.3.2. Расширения OCSP

Предоставляемый сервис OCSP обрабатывает все расширения запросов, определенные рекомендациями (IETF) RFC 2560.

8. ПРОВЕРКА ДЕЯТЕЛЬНОСТИ

Деятельность УЦ КЦМР подлежит регулярным проверкам со стороны уполномоченного органа по управлению КЦМР в лице Национального Банка Республики Казахстан. В частности, в ходе проверок:

рассматривается актуальность и соблюдение действующих документально закрепленных требований: политики безопасности, включая требования по безопасности на объектах КЦМР, договорных обязательств. Оценивается надежность и эффективность системы внутреннего контроля;

проводится анализ вероятности потенциальных угроз для штатного режима деятельности, уязвимостей в системах обеспечения, оценка их возможных последствий, выработка мер совершенствования организации работы. Оценивается эффективность управления рисками.

Кроме того, КЦМР подвергал и планирует далее регулярно подвергать деятельность собственного удостоверяющего цента проверке независимых аудиторских компаний, имеющих лицензию на предоставление услуг по программе WebTrust для удостоверяющих центров.

8.1. Частота или основания проведения проверок

Проверки КЦМР Национальным Банком Республики Казахстан проводятся в плановом порядке 1 раз в 2 года.

КЦМР планирует приобретение услуг по проверке у независимых аудиторских компаний, имеющих лицензию на предоставление услуг по программе WebTrust для удостоверяющих центров, не реже 1 раза в год, за счет и в пределах собственных финансовых средств.

8.2. Идентичность и квалификация проверяющих инстанций

С учетом вышеизложенного, проверки деятельности УЦ КЦМР осуществляются Национальным Банком Республики Казахстан, осуществляющим функции уполномоченного органа по управлению КЦМР, и независимыми аудиторскими компаниями, имеющими лицензию на предоставление услуг по программе WebTrust.

8.3. Отношения между УЦ КЦМР и проверяющими инстанциями

Проверки УЦ КЦМР на соответствие Принципам и критериям программы WebTrust для удостоверяющих центров должны проводиться независимыми аудиторскими компаниями.

8.4. Тематика проверок

В рамках проверок со стороны Национального Банка Республики Казахстан рассматривается полнота и качество выполнения установленных требований по вопросам финансово-хозяйственной деятельности и программно-технического обеспечения.

В рамках независимых аудиторских проверок УЦ КЦМР должно проверяться соответствие деятельности УЦ КЦМР программе WebTrust для удостоверяющих центров, в том числе:

раскрытие бизнес-практик УЦ;

целостность услуг;

контроль организационного уровня.

8.5. Меры, предпринимаемые при выявлении недостатков

После получения отчета о проверке деятельности, при выявлении в ней нарушений и недостатков, составляется и реализуется план их устранения с определением сроков и должностных лиц, ответственных за выполнение мероприятий из числа руководителей структурных единиц КЦМР.

Если выявленные нарушения и недостатки представляют непосредственную угрозу безопасности и целостности информационных систем, обслуживаемых УЦ КЦМР, тогда УЦ КЦМР принимает решения о необходимости:

отзыва сертификатов и/или публикации уведомления о компрометации;

приостановления функционирования сервисов;

исключения неполноценных сервисов из сферы действия настоящей Политики сертификатов и прекращения действия соответствующих договоров.

8.6. Обратная связь

Результаты выполнения плана устранения нарушений и недостатков, выявленных в ходе проверки, УЦ КЦМР учитывает в ежегодном отчете об итогах своей деятельности, представляемом в Национальный Банк Республики Казахстан.

9. ПРОЧИЕ КОММЕРЧЕСКИЕ И ЮРИДИЧЕСКИЕ ВОПРОСЫ

9.1. Тарифы

Удостоверяющий центр КЦМР предоставляет своим клиентам следующие услуги:

выпуск сертификатов подписчиков по заявлениям юридических и физических лиц, включая:

регистрацию заявлений;

выдачу ключевых пар первичной инициализации;

создание сертификатов подписчиков;

отзыв сертификатов;

приостановление и возобновление действия сертификатов;

размещение сертификатов, Политики сертификатов, Положения о практике сертификатов и иной интересующей клиентов информации в публично доступном хранилище. Актуализация информации в хранилище;

публикация в хранилище списков отозванных сертификатов;

предоставление информации о статусе сертификатов в режиме он-лайн по протоколу OCSP (служба OCSP);

привязка данных к реальному времени в режиме он-лайн по протоколу TSP (услуги сервера метки времени);

подтверждение принадлежности, подлинности и действительности выпущенных сертификатов по заявлениям заинтересованных сторон.

9.1.1. Тариф за выпуск, изменение или смену ключей сертификатов

Оплате подлежат услуги удостоверяющего центра, связанные с выпуском сертификатов. Актуальная информация о тарифах на выпуск сертификатов постоянно доступна на информационном ресурсе КЦМР в сети Интернет по адресу http://www.kisc.kz/ca/tariff.html.

9.1.2. Тариф за доступ к сертификатам

УЦ КЦМР не взимает плату за доступность сертификатов доверяющим сторонам через хранилище или иными способами.

9.1.3. Тариф за доступ к информации об отзыве или статусе сертификатов

УЦ КЦМР не взимает плату за доступность доверяющим сторонам списков отозванных сертификатов, указанных в настоящей Политике сертификатов, через хранилище или иными способами.

УЦ КЦМР не взимает плату за доступность доверяющим сторонам службы OCSP, указанной в настоящей Политике сертификатов, или иных возможных способов получения информации о статусе сертификатов.

9.1.4. Тарифы за иные сервисы

За остальные услуги, указанные в разделе 9.1, УЦ КЦМР отдельную плату не взимает, их стоимость входит в цену договора на оказание услуг в конкретных информационных системах.

Таким образом, отдельная плата не взимается за:

отзыв сертификатов;

приостановление и возобновление действия сертификатов;

размещение сертификатов, Политики сертификатов, Положения о практике сертификатов и иной интересующей клиентов информации в публично доступном хранилище. Актуализация информации в хранилище;

публикацию в хранилище списков отозванных сертификатов;

предоставление информации о статусе сертификатов в режиме он-лайн по протоколу OCSP (служба OCSP);

привязку данных к реальному времени в режиме он-лайн по протоколу TSP (услуги сервера метки времени);

подтверждение принадлежности, подлинности и действительности выпущенных сертификатов по заявлениям заинтересованных сторон.

При этом отдельная плата не взимается за регистрацию заявлений подписчиков и выдачу им ключевых пар первичной инициализации, их стоимость включена в тариф на выпуск основного сертификата.

9.1.5. Политика возмещения

В пределах, допустимых действующим законодательством, УЦ КЦМР оставляет за собой право проводить политику возмещения, условия которой будут публиковаться на официальном информационном ресурсе в сети Интернет, включаться в Положение о практике сертификатов и Договор на предоставление услуг удостоверяющего центра.

9.2. Финансовая ответственность

9.2.1. Страховое покрытие

КЦМР несет финансовую ответственность за комплекс предоставляемых услуг по использованию информационных систем (МСПД, СОБС, ФАСТИ и др.) в рамках договора с клиентом о возможности использования конкретной системы из числа указанных. Отдельной финансовой ответственности за услуги удостоверяющего центра в комплексе услуг по использованию конкретной информационной системы КЦМР не несет.

В связи с этим, КЦМР не несет финансовой ответственности перед доверяющими сторонами, не являющимися владельцами или подписчиками сертификатов УЦ КЦМР.

9.2.2. Другие средства

Выполнение обязанностей и функций, а также риски ответственности Удостоверяющего центра перед подписчиками и доверяющими сторонами обеспечиваются финансовыми ресурсами КЦМР.

9.2.3. Страхование гарантий для клиентов

Не применяется.

9.3. Конфиденциальность коммерческой информации

9.3.1. Спектр конфиденциальной информации

Следующая информация, за исключением информации, перечисленной в параграфе 9.3.2, считается и хранится как конфиденциальная:

материалы заявлений на выпуск сертификатов;

закрытые ключи первичной инициализации;

транзакционные материалы;

контрольные протоколы;

отчеты о проверках деятельности (внутренних и аудиторских) УЦ КЦМР;

планы восстановления функционирования;

меры безопасности, контролирующие функционирование аппаратного и программного обеспечения, администрирование служб сертификатов и регистрации.

9.3.2. Информация, не рассматриваемая в качестве конфиденциальной

Участники информационных систем, обслуживаемых УЦ КЦМР, признают, что сертификаты, информация об их отзыве или иная информация о статусе сертификатов, публичная часть хранилища и содержащаяся в них информация не рассматриваются в качестве конфиденциальной информации. Информация, не перечисленная в параграфе 9.3.1, не рассматривается как конфиденциальная, если иное не предусмотрено действующим законодательством Республики Казахстан.

9.3.3. Ответственность за защиту конфиденциальной информации

Работники и подрядчики УЦ КЦМР, а также уполномоченные посредники несут ответственность за обеспечение конфиденциальности информации в соответствии с обязательствами по договорам, заключенным с КЦМР. Все работники УЦ КЦМР проходят обучение обеспечению безопасности и работе с конфиденциальной информацией.

9.4. Конфиденциальность персональных данных

9.4.1. План конфиденциальности

УЦ КЦМР в своей деятельности руководствуется действующим законодательством Республики Казахстан по вопросам защиты персональных данных. В частности, УЦ КЦМР не разглашает информацию, идентифицирующую заявителей на выпуск сертификатов, за исключением информации, перечисленной в параграфе 9.3.2. В случае прекращения деятельности данная информация передается в другой удостоверяющий центр в соответствии с разделом 5.8.

9.4.2. Информация, рассматриваемая в качестве персональных данных

Как персональные данные обрабатывается любая информация о подписчике, не доступная публично из содержания выпущенного сертификата, хранилища сертификатов и онлайнового списка отозванных сертификатов.

9.4.3. Информация, не рассматриваемая в качестве персональных данных

В качестве персональных данных не рассматривается информация, указываемая в заявлении на выпуск сертификата, публикуемая в сертификате, а также иная информация, подлежащая обязательному опубликованию в соответствии с действующим законодательством Республики Казахстан. Принятие подписчиками и владельцами сертификатов обязательства соблюдать требования настоящей Политики сертификатов означает их согласие на публикацию сведений, указываемых в сертификате.

9.4.4. Ответственность за защиту персональных данных

Все работники и подрядчики УЦ КЦМР, а также уполномоченные посредники, работающие с персональными данными, обязаны защищать их от компрометации и

разглашения третьим сторонам и несут ответственность за это в соответствии с действующим законодательством Республики Казахстан.

9.4.5. Уведомление и согласие на использование конфиденциальной информации

Персональные данные не используются без согласия стороны, которой они принадлежат, за исключением случаев, предусмотренных законодательством Республики Казахстан, настоящей Политикой сертификатов или Договором о предоставлении услуг удостоверяющего центра.

9.4.6. Раскрытие персональных данных судебным и административным инстанциям

Участники информационных систем, обслуживаемых УЦ КЦМР, признают, что КЦМР обязан раскрывать персональные данные по постановлению (решению) суда.

9.4.7. Другие основания для раскрытия персональных данных

Не применяются.

9.5. Права интеллектуальной собственности

КЦМР оставляет за собой права интеллектуальной собственности на сертификаты, которые он выпускает, и на информацию об их статусе. При этом КЦМР не запрещает копирование и распространение сертификатов на неисключительной безвозмездной основе, при соблюдении условий полноты копирования и использования сертификатов в соответствии с условиями заключенных договоров. КЦМР также не запрещает использование информации о статусе сертификатов для выполнения функций доверяющей стороны в соответствии с договором о предоставлении услуг удостоверяющего центра.

Участники информационных систем, обслуживаемых УЦ КЦМР, признают право интеллектуальной собственности КЦМР на настоящую Политику сертификатов и другую документацию КЦМР, регламентирующую деятельность УЦ.

Заявители на выпуск сертификатов сохраняют все свои права на все торговые и тому подобные марки и имена, содержащиеся в заявлениях на выпуск сертификатов и отличительные (DN-)имена в выпущенных сертификатах.

Ключевые пары, которые соответствуют сертификатам, выпущенным УЦ КЦМР, составляют собственность (в том числе интеллектуальную) владельцев сертификатов в независимости от физических носителей, на которых хранятся эти ключевые пары и которыми они защищаются. В частности, открытые ключи, сертификаты и части секрета закрытых ключей УЦ КЦМР, являются собственностью (в том числе интеллектуальной) КЦМР.

9.6. Гарантии и заверения

9.6.1. Гарантии и заверения удостоверяющего центра

Удостоверяющий центр гарантирует:

отсутствие в выпущенных сертификатах умышленных искажений фактов, внесенных УЦ КЦМР или известных ему;

отсутствие в информации сертификатов случайных ошибок, допущенных УЦ КЦМР вследствие халатности при рассмотрении заявлений на выпуск или создании сертификатов;

соответствие сертификатов требованиям действующего законодательства Республики Казахстан, существенным требованиям настоящей Политики сертификатов и соответствующего Положения о практике сертификатов;

соответствие сервисов отзыва сертификатов и использования хранилища требованиям действующего законодательства Республики Казахстан, существенным требованиям настоящей Политики сертификатов и соответствующего Положения о практике сертификатов во всех существенных аспектах;

своевременное информирование заявителей на выпуск сертификатов об условиях, обязанностях и ответственности, которые влечет присоединение к договору о предоставлении услуг удостоверяющего центра.

Кроме того, удостоверяющий центр обязан выполнять условия гарантий и заверений подписчика и доверяющей стороны, изложенные в параграфах 9.6.3 и 9.6.4 настоящей Политики сертификатов.

Договор о предоставлении услуг удостоверяющего центра может содержать дополнительные гарантии и заверения удостоверяющего центра.

9.6.2. Гарантии и заверения центров регистрации

Не устанавливаются.

9.6.3. Гарантии и заверения подписчиков

Подписчики гарантируют выполнение следующих условий.

Каждая электронная цифровая подпись, сформированная с помощью закрытого ключа, который соответствует открытому ключу, указанному в сертификате, является электронной цифровой подписью подписчика, соответствующий сертификат был принят подписчиком и действует (не просрочен, не отозван и его действие не приостановлено) на момент формирования электронной цифровой подписи.

Их закрытые ключи защищены, и к ним никогда не имело доступа ни одно неуполномоченное лицо.

Все сведения, представленные подписчиком для заявления на выпуск для него сертификата, достоверны.

Вся информация, содержащаяся в сертификате подписчика, достоверна.

Сертификат используется в соответствии с действующим законодательством Республики Казахстан, существенными требованиями настоящей Политики сертификатов и соответствующего Положения о практике сертификатов.

Подписчик не является удостоверяющим центром и не использует закрытый ключ, который соответствует открытому ключу, указанному в сертификате, в целях электронной цифровой подписи каких-либо сертификатов (или любого другого формата удостоверений открытого ключа) или списков отозванных сертификатов.

Кроме того, подписчик обязан выполнять условия гарантий и заверений доверяющей стороны, изложенные в параграфе 9.6.4 настоящей Политики сертификатов.

Договор о предоставлении услуг удостоверяющего центра и договор подписчика с владельцем сертификата могут содержать дополнительные гарантии и заверения подписчика.

9.6.4. Гарантии и заверения доверяющих сторон

Доверяющие стороны гарантируют то, что они:

обладают достаточным объемом информации, чтобы принимать обоснованные решения в отношении той степени, в которой они хотят опираться на информацию из сертификата;

несут исключительную ответственность за принятие решений, опираться или не опираться на эту информацию;

принимают правовые последствия нарушений обязательств доверяющей стороны в условиях настоящей Политики сертификатов.

Договор о предоставлении услуг удостоверяющего центра и договор подписчика с владельцем сертификата могут содержать дополнительные гарантии и заверения контрагентов, касающиеся выполнения ими обязанностей доверяющей стороны.

9.6.5. Гарантии и заверения владельцев сертификатов

Владельцы сертификатов, по отношению к которым они не являются подписчиками, обязаны выполнять условия гарантий и заверений доверяющей стороны, изложенные в параграфе 9.6.4 настоящей Политики сертификатов, условия договора о предоставлении услуг удостоверяющего центра, а также гарантировать соблюдение следующих условий:

отсутствие в выпущенных сертификатах умышленных искажений фактов, внесенных их работниками или подписчиками;

отсутствие в информации сертификатов известных им случайных ошибок, допущенных подписчиком вследствие халатности;

подписчики указанных сертификатов ознакомлены с настоящей Политикой сертификатов, соответствующим ей Положением о практике сертификатов, и на них владельцем сертификатов возложены обязанности и выполнять требования и нести ответственность, предусмотренные этими документами для подписчиков и доверяющих сторон.

Владельцы сертификатов, по отношению к которым они же являются подписчиками, обязаны выполнять условия гарантий и заверений подписчика и доверяющей стороны, изложенные в параграфах 9.6.3, 9.6.4 настоящей Политики сертификатов, а также условия договора о предоставлении услуг удостоверяющего центра.

Договор о предоставлении услуг удостоверяющего центра и договор подписчика с владельцем сертификата могут содержать дополнительные гарантии и заверения владельца сертификата.

9.6.6. Гарантии и заверения уполномоченных посредников

Уполномоченные посредники гарантируют соблюдение условий договора о сотрудничестве, обязаны выполнять условия гарантий и заверений подписчика и доверяющей стороны , изложенные в параграфах 9.6.3, 9.6.4 настоящей Политики сертификатов, а также гарантировать соблюдение следующих условий:

отсутствие в принятых, проверенных и подтвержденных ими заявлениях на выпуск сертификатов умышленных искажений фактов, внесенных их работниками или заявителями;

отсутствие в информации принятых, проверенных и подтвержденных ими заявлений на выпуск сертификатов случайных ошибок, допущенных их работниками или заявителями вследствие халатности.

Договор о сотрудничестве с удостоверяющим центром может содержать дополнительные гарантии и заверения уполномоченного посредника.

9.7. Отказ от гарантий

КЦМР не несет дополнительной гарантийной ответственности, включая ответственность за товарную пригодность и соответствие, кроме той, которая включена в договоры на оказание услуг в конкретных информационных системах, если иное не предусмотрено действующим законодательством Республики Казахстан.

9.8. Ограничение ответственности

КЦМР несет финансовую ответственность за комплекс предоставляемых услуг по использованию информационных систем (МСПД, СОБС, ФАСТИ и др.) перед клиентами в рамках договоров о возможности использования конкретной системы из числа указанных.

Иная ответственность удостоверяющего центра КЦМР перед участниками инфраструктуры открытых ключей в рамках настоящей Политики сертификатов ограничивается суммой прямого ущерба, но не может превышать 200 (двухсот) месячных расчетных показателей.

Ответственность подписчиков перед участниками инфраструктуры открытых ключей в рамках настоящей Политики сертификатов ограничивается суммой прямого ущерба и не может превышать:

100 (ста) месячных расчетных показателей – для физических лиц и

200 (двухсот) месячных расчетных показателей – для юридических лиц.

Ответственность доверяющих сторон перед участниками инфраструктуры открытых ключей в рамках настоящей Политики сертификатов ограничивается суммой прямого ущерба и не может превышать 100 (ста) месячных расчетных показателей.

При этом участники инфраструктуры открытых ключей не несут ответственности за непрямой, особый, случайный, вытекающий ущерб и упущенную выгоду.

9.9. Компенсации

9.9.1. Возмещения подписчика

В части, не противоречащей действующему законодательству Республики Казахстан, подписчики обязаны возмещать расходы, связанные с:

представлением ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлении на выпуск сертификата;

сокрытием существенных фактов в заявлении на выпуск сертификата, если оно является результатом непреднамеренного или умышленного введения в заблуждение или бездействия;

непринятием мер защиты собственного закрытого ключа, приведшим к его компрометации, утере, разглашению, изменению или несанкционированному использованию;

использованием в составе своего отличительного имени названий, нарушающих права интеллектуальной собственности третьих лиц.

Договор о предоставлении услуг удостоверяющего центра и договор подписчика с владельцем сертификата могут содержать дополнительные обязательства подписчиков о возмещениях.

9.9.2. Возмещения доверяющих сторон

В части, не противоречащей действующему законодательству Республики Казахстан, доверяющие стороны обязаны возмещать расходы, связанные с:

нарушением своих договорных обязательств о выполнении обязанностей доверяющей стороны;

несоответствующим обстоятельствам доверием к сертификату;

непринятием мер по проверке сертификата с целью определения его отзыва и сроков действия.

Договор о предоставлении услуг удостоверяющего центра и договор подписчика с владельцем сертификата могут содержать дополнительные обязательства контрагентов о возмещениях, связанных с выполнением ими обязанностей доверяющей стороны.

9.9.3. Возмещения владельцев сертификатов

В части, не противоречащей действующему законодательству Республики Казахстан, владельцы сертификатов обязаны возмещать расходы, связанные с:

подтверждением ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлениях на выпуск сертификата;

сокрытием существенных фактов в заявлениях на выпуск сертификата, если оно является результатом непреднамеренного или умышленного введения в заблуждение или бездействия;

использование в составе своего отличительного имени названий, нарушающих права интеллектуальной собственности третьих лиц;

нарушением подписчиками сертификатов, принадлежащих данному владельцу, требований, предусмотренных для подписчиков и доверяющих сторон настоящей Политикой сертификатов и соответствующим Положением о практике сертификатов, если данные нарушения явились следствием неисполнения владельцем требования ознакомить подписчиков с указанными документами и возложить на них соответствующие обязанности и ответственность.

Договор о предоставлении услуг удостоверяющего центра может содержать дополнительные обязательства владельца о возмещениях.

9.9.4. Возмещения уполномоченных посредников

В части, не противоречащей действующему законодательству Республики Казахстан, уполномоченные посредники обязаны возмещать расходы, связанные:

с подтверждением ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлениях на выпуск сертификата;

с сокрытием существенных фактов в заявлениях на выпуск сертификата, если оно является результатом непреднамеренного или умышленного введения в заблуждение или бездействия.

Договор о сотрудничестве с удостоверяющим центром может содержать дополнительные обязательства уполномоченного посредника о возмещениях удостоверяющему центру.

9.10. Вступление в силу и прекращение действия

9.10.1. Вступление в силу

Настоящая Политика сертификатов вступает в силу с момента опубликования на интернет ресурсе УЦ КЦМР. Изменения и дополнения в настоящую Политику сертификатов также вступают в силу с момента опубликования на интернет ресурсе УЦ КЦМР.

9.10.2. Прекращение действия

Настоящая Политика сертификатов по мере периодического внесения изменений и дополнений остается в силе до момента замены новой редакцией.

9.10.3. Правовые последствия прекращения действия

С момента прекращения действия настоящей Политики сертификатов участники информационных систем, обслуживаемых КЦМР, остаются связанными ее условиями по всем сертификатам до момента истечения периода их действия.

9.11. Индивидуальные уведомления и связь с участниками

Участники информационных систем, обслуживаемых КЦМР, для связи друг с другом вправе использовать любые целесообразные методы, соответствующие критичности и предмету взаимодействия, если иное не определено соглашением между сторонами.

9.12. Изменения и дополнения

9.12.1. Процедура изменения и дополнения

Изменения и дополнения в Политику сертификатов готовятся отделом удостоверяющего центра КЦМР и оформляются в виде отдельного документа, содержащего либо актуальный текст Политики, либо уведомление об изменениях и дополнениях в ее актуальный текст.

Публикация актуальной редакции Политики сертификатов или уведомлений об изменениях и дополнениях к ней осуществляется на официальном информационном ресурсе КЦМР в сети Интернет по адресу: http://www.kisc.kz/ca/doc/PolicyKISC.pdf.

Отдел удостоверяющего центра КЦМР отвечает за определение необходимости изменения объектных идентификаторов Политики сертификатов для приведения их в соответствие с измененным содержанием документа.

9.12.2. Механизм и сроки уведомления

УЦ КЦМР оставляет за собой право без предварительного уведомления вносить несущественные изменения и дополнения в настоящую Политику сертификатов, включая, но не ограничиваясь исправлением опечаток, изменением адресов ссылок и контактной информации. Решения о том, являются ли данные изменения и дополнения существенными или нет, принимаются по исключительному усмотрению КЦМР.

КЦМР может запрашивать предложения о внесении изменений и дополнений в настоящую Политику сертификатов у участников обслуживаемых информационных систем. КЦМР предварительно публикует предлагаемые существенные изменения и дополнения к настоящей Политике сертификатов на своем официальном информационном ресурсе в сети Интернет, предусматривая при этом срок их рассмотрения.

Если иное не указано особо, период рассмотрения предлагаемых существенных изменений и дополнений в Политику сертификатов составляет 21 календарный день со дня опубликования. Участники информационных систем, обслуживаемых КЦМР, вправе подавать свои замечания и предложения в КЦМР в период рассмотрения.

КЦМР рассматривает все поданные замечания и предложения по предложенным изменения и дополнениям. При этом КЦМР вправе:

ввести исходные изменения и дополнения в действие в полном объеме;

составить и опубликовать новую редакцию предлагаемых изменений и дополнений;

отозвать проект изменений и дополнений в действующую Политику сертификатов.

Не отозванные и не корректировавшиеся изменения и дополнения по истечении периода их рассмотрения публикуются как вступившие в силу.

Несмотря на возможное наличие противоречий в проекте, если КЦМР считает, что существенные изменения или дополнения в Политику сертификатов требуются немедленно в целях предотвращения нарушения безопасности обслуживаемых информационных систем, КЦМР вправе внести их путем утверждения и опубликования на интернет ресурсе, тем самым вводя в действие с момента опубликования.

9.12.3. Процедура изменения объектных идентификаторов

Если КЦМР определил необходимость изменений объектных идентификаторов, указанных в настоящей Политике сертификатов, в тексте изменений и дополнений должны быть приведены новые объектные идентификаторы для каждого класса сертификатов данной Политики.

9.13. Положения о разрешении споров

Споры между участниками информационных систем, обслуживаемых УЦ КЦМР, разрешаются в соответствии с положениями действующих договоров между сторонами.

Договор о предоставлении услуг удостоверяющего центра содержит положения о разрешении споров, которые предусматривают 60-дневный срок для их решения путем переговоров в досудебном порядке. Если спор не решен таким способом он подлежит разрешению в судебном порядке.

Публикация актуальных версий договоров о предоставлении услуг удостоверяющего центра осуществляется на официальном информационном ресурсе

КЦМР в сети Интернет по адресам http://www.kisc.kz/ca/doc/dogovorcaps.rtf и http://www.kisc.kz/ca/doc/new/dogovorca.rtf.

9.14. Применимое право

Применимым правом для разрешения споров, предметом которых являются разногласия по существу настоящей Политики сертификатов, является законодательство Республики Казахстан.

9.15. Юрисдикция

Юрисдикцией для настоящей Политики сертификатов является законодательство Республики Казахстан.

9.16. Разное

9.16.1. Полнота соглашения

Не оговаривается.

9.16.2. Передача прав

Не предусматривается.

9.16.3. Делимость

В случае если часть положений настоящей Политики сертификатов будет признана неосуществимой судом или уполномоченным государственным органом, остальная ее часть сохраняет силу.

9.16.4. Правоприменение (адвокатские компенсации и отказ от прав)

Не оговаривается.

9.16.5. Форс-мажор

Договор о предоставлении услуг удостоверяющего центра имеет статью о форс-мажоре, защищающую стороны в случае возникновения обстоятельств непреодолимой силы.

9.17. Прочие положения

Не предусматриваются.