

**РГП «КАЗАХСТАНСКИЙ ЦЕНТР МЕЖБАНКОВСКИХ РАСЧЕТОВ
НАЦИОНАЛЬНОГО БАНКА РЕСПУБЛИКИ КАЗАХСТАН»
(РГП «КЦМР НБ РК»)**

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

**ПРАВИЛА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
РГП «КЦМР НБ РК» (CERTIFICATE PRACTICE STATEMENT)**

Утверждены приказом
РГП КЦМР НБ РК
от “15” сентября 2014 года
№ 44-П

Нормативный документ

2014 г.

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ	7
1.1. ОБЗОР	10
1.2. НАИМЕНОВАНИЕ И ИДЕНТИФИКАЦИЯ ДОКУМЕНТА	11
1.3. УЧАСТНИКИ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ.....	11
1.3.1. Удостоверяющий центр	11
1.3.2. Центры регистрации	11
1.3.3. Подписчики	11
1.3.4. Доверяющие стороны.....	12
1.3.5. Другие участники.....	12
1.3.5.1. Владельцы сертификатов	12
1.3.5.2. Уполномоченные посредники.....	12
1.3.6. Другие участники.....	12
1.4. ИСПОЛЬЗОВАНИЕ СЕРТИФИКАТОВ	12
1.4.1. Допустимое использование сертификата	12
1.4.2. Ограничения на использование сертификата	12
1.5. УПРАВЛЕНИЕ ДОКУМЕНТОМ	13
1.5.1. Организация, ответственная за содержание документа	13
1.5.2. Контактное лицо.....	13
1.5.3. Утверждающая инстанция.....	13
1.5.4. Процедура утверждения изменений и дополнений	13
1.6. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ	13
2. ОТВЕТСТВЕННОСТЬ ЗА ПУБЛИКАЦИЮ И ХРАНИЛИЩЕ	14
2.1. ХРАНИЛИЩЕ	14
2.2. ПУБЛИКАЦИЯ ИНФОРМАЦИИ О СЕРТИФИКАТАХ	14
2.3. ПЕРИОДИЧНОСТЬ ПУБЛИКАЦИИ.....	14
2.4. КОНТРОЛЬ ДОСТУПА К ХРАНИЛИЩУ	15
3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ	15
3.1. НАЗНАЧЕНИЕ ИМЕН.....	15
3.1.1. Типы имен	15
3.1.2. Требование значимости имен	16
3.1.3. Анонимность подписчиков и использование псевдонимов	16
3.1.4. Правила интерпретации различных форм имен	16
3.1.5. Уникальность имен	16
3.1.6. Распознавание, аутентификация и роль торговых марок.....	16
3.2. ПЕРВОНАЧАЛЬНАЯ ПРОВЕРКА ИДЕНТИЧНОСТИ.....	17
3.2.1. Способ доказательства факта владения закрытым ключом	17
3.2.2. Процедура аутентификации юридического лица	17
3.2.3. Процедура аутентификации физического лица	18
3.2.4. Не подвергающиеся проверке сведения о заявителе	18
3.2.5. Проверка полномочий.....	18
3.2.6. Критерии взаимодействия	18
3.3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ЗАЯВЛЕНИЙ О СМЕНЕ КЛЮЧЕЙ В СЕРТИФИКАТАХ	18
3.3.1. Идентификация и аутентификация при плановой (очередной) смене ключей	19
3.3.2. Идентификация и аутентификация при внеплановой смене ключей после отзыва сертификатов	19
3.4. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПРИ ОТЗЫВЕ СЕРТИФИКАТОВ.....	19
4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТОВ	19
4.1. ЗАЯВЛЕНИЯ НА ВЫПУСК СЕРТИФИКАТОВ	19
4.1.1. Лица, имеющие право подавать заявления на выпуск сертификата	19
4.1.2. Процедура регистрации и связанные с ней обязательства	19
4.2. ОБРАБОТКА ЗАЯВЛЕНИЙ НА ВЫПУСК СЕРТИФИКАТОВ.....	20
4.2.1. Процедуры идентификации и аутентификации	20
4.2.2. Прием или отказ в приеме заявления на выпуск сертификатов	20
4.2.3. Срок рассмотрения заявлений на выпуск сертификатов	20

4.3.	ВЫПУСК СЕРТИФИКАТОВ	20
4.3.1.	Действия удостоверяющего центра в ходе выпуска сертификатов	20
4.3.2.	Уведомление подписчиков удостоверяющим центром о выпуске сертификатов	20
4.4.	ПРИНЯТИЕ СЕРТИФИКАТОВ.....	21
4.4.1.	Поведение, означающее принятие сертификатов.....	21
4.4.2.	Публикация сертификата удостоверяющим центром	21
4.4.3.	Уведомление удостоверяющим центром других сторон о выпуске сертификатов	21
4.5.	ИСПОЛЬЗОВАНИЕ СЕРТИФИКАТОВ И КЛЮЧЕВЫХ ПАР	21
4.5.1.	Использование закрытых ключей и сертификатов подписчиками	21
4.5.2.	Использование открытых ключей и сертификатов доверяющими сторонами	21
4.6.	ОБНОВЛЕНИЕ СЕРТИФИКАТОВ.....	22
4.7.	СМЕНА КЛЮЧЕЙ СЕРТИФИКАТОВ.....	22
4.8.	ИЗМЕНЕНИЕ СЕРТИФИКАТОВ	23
4.9.	ОТЗЫВ И ПРИОСТАНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТОВ.....	23
4.9.1.	Основания для отзыва сертификатов	23
4.9.2.	Лица, имеющие право подавать заявления на отзыв сертификатов	24
4.9.3.	Процедуры отзыва сертификата	24
4.9.4.	Срок подачи заявлений на отзыв сертификата	24
4.9.5.	Срок рассмотрения заявлений на отзыв сертификата	24
4.9.6.	Требования о проверке отзыва сертификата для доверяющих сторон	24
4.9.7.	Частота выпуска списков отозванных сертификатов	24
4.9.8.	Максимальная задержка списков отозванных сертификатов	25
4.9.9.	Требование доступности онлайн-проверки отзыва и информации о статусе	25
4.9.10.	Требования онлайн-проверки отзыва	25
4.9.11.	Иные формы объявления об отзыве	25
4.9.12.	Особые требования, касающиеся компрометации ключей	25
4.9.13.	Основания приостановления действия сертификата	25
4.9.14.	Лица, имеющие право запрашивать приостановление действия сертификатов	26
4.9.15.	Процедуры рассмотрения заявления на приостановление	26
4.9.16.	Предельный срок приостановления	26
4.10.	СЕРВИСЫ СТАТУСА СЕРТИФИКАТОВ	27
4.10.1.	Эксплуатационные характеристики	27
4.10.2.	Режим работы сервисов	27
4.10.3.	Дополнительные возможности	27
4.11.	ОКОНЧАНИЕ ПОДПИСКИ.....	27
4.12.	ДЕПОНИРОВАНИЕ И ВОССТАНОВЛЕНИЕ КЛЮЧА	27
5.	КОНТРОЛЬ ОБЪЕКТОВ, УПРАВЛЕНИЯ И ФУНКЦИОНИРОВАНИЯ.....	27
5.1.	ФИЗИЧЕСКИЙ КОНТРОЛЬ.....	27
5.1.1.	Размещение и конструкция здания	27
5.1.2.	Физический доступ	27
5.1.3.	Электропитание и кондиционирование воздуха	28
5.1.4.	Влияние водной стихии	28
5.1.5.	Предотвращение и защита от пожаров	28
5.1.6.	Хранение носителей информации	28
5.1.7.	Утилизация	28
5.1.8.	Внешнее резервирование	28
5.2.	ПРОЦЕДУРНЫЙ КОНТРОЛЬ	29
5.2.1.	Распределение ролей	29
5.2.2.	Численность персонала, необходимого для отдельной задачи	29
5.2.3.	Идентификация и аутентификация каждой роли	29
5.2.4.	Функции, требующие разделения обязанностей	30
5.3.	КОНТРОЛЬ ПЕРСОНАЛА	30
5.3.1.	Требования к опыту и квалификации	30
5.3.2.	Процедуры фоновой проверки	30
5.3.3.	Требования к подготовке, переподготовке и повышению квалификации	30
5.3.4.	Требование к частоте подготовки, переподготовки и повышения квалификации	30
5.3.5.	Последовательность и частота перемещений по службе	30
5.3.6.	Ответственность за несанкционированные действия	30
5.3.7.	Требования к независимым контракторам	31
5.3.8.	Документация, раскрываемая персоналу	31

5.4.	ПРОЦЕДУРЫ КОНТРОЛЬНОГО ПРОТОКОЛИРОВАНИЯ.....	31
5.4.1.	Типы протоколируемых событий.....	31
5.4.2.	Частота анализа контрольных протоколов.....	31
5.4.3.	Срок хранения контрольных протоколов.....	31
5.4.4.	Защита контрольных протоколов.....	31
5.4.5.	Резервное копирование контрольных протоколов.....	31
5.4.6.	Система сбора контрольных протоколов.....	32
5.4.7.	Уведомление субъекта, вызвавшего событие.....	32
5.4.8.	Оценка уязвимости.....	32
5.5.	ВЕДЕНИЕ АРХИВА.....	32
5.5.1.	Типы архивируемых событий.....	32
5.5.2.	Срок хранения архива.....	32
5.5.3.	Защита архива.....	32
5.5.4.	Резервное копирование архива.....	32
5.5.5.	Требование о пометке времени на архивных записях.....	32
5.5.6.	Условия архивирования.....	32
5.5.7.	Порядок получения и проверки архивной информации.....	33
5.6.	СМЕНА КЛЮЧЕЙ УЦ.....	33
5.7.	ВОССТАНОВЛЕНИЕ ПОСЛЕ КОМПРОМЕТАЦИИ И ПРОИСШЕСТВИЙ.....	33
5.7.1.	Процедуры обработки происшествий и компрометации.....	33
5.7.2.	Повреждения вычислительных, программных ресурсов и/или данных.....	33
5.7.3.	Компрометация закрытого ключа удостоверяющего центра.....	33
5.7.4.	Возможности непрерывной деятельности после происшествий.....	34
5.8.	ПРЕКРАЩЕНИЕ РАБОТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	34
6.	КОНТРОЛЬ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ.....	35
6.1.	ГЕНЕРАЦИЯ И УСТАНОВКА КЛЮЧЕВЫХ ПАР.....	35
6.1.1.	Генерация ключевых пар.....	35
6.1.2.	Доставка закрытого ключа подписчику.....	35
6.1.3.	Доставка открытого ключа в удостоверяющий центр.....	36
6.1.4.	Передача открытого ключа удостоверяющего центра доверяющим сторонам.....	36
6.1.5.	Размеры ключей.....	36
6.1.6.	Генерация и проверка качества параметров криптографических алгоритмов.....	36
6.1.7.	Цели использования ключа (расширение «keyUsage» согласно X.509 v3).....	36
6.2.	ЗАЩИТА ЗАКРЫТОГО КЛЮЧА И ИНЖЕНЕРНЫЙ КОНТРОЛЬ КРИПТОГРАФИЧЕСКОГО МОДУЛЯ.....	36
6.2.1.	Стандарты и контроль криптографического модуля.....	37
6.2.2.	Разделение закрытого ключа между ответственным персоналом по схеме m из n	37
6.2.3.	Депонирование закрытого ключа.....	37
6.2.4.	Резервное копирование закрытого ключа.....	37
6.2.5.	Архивирование закрытого ключа.....	37
6.2.6.	Загрузка/выгрузка закрытого ключа в/из криптографического модуля.....	37
6.2.7.	Хранение закрытого ключа в криптографическом модуле.....	37
6.2.8.	Способы активации закрытого ключа.....	37
6.2.9.	Способ деактивации закрытого ключа.....	38
6.2.10.	Способ уничтожения закрытого ключа.....	38
6.2.11.	Оценка криптографических модулей.....	38
6.3.	ДРУГИЕ ОСОБЕННОСТИ УПРАВЛЕНИЯ КЛЮЧЕВЫМИ ПАРАМИ.....	38
6.3.1.	Архивирование открытых ключей.....	38
6.3.2.	Сроки действия сертификатов и использования ключевых пар.....	38
6.4.	ДАННЫЕ АКТИВАЦИИ.....	39
6.4.1.	Генерация и установка данных активации.....	39
6.4.2.	Защита данных активации.....	39
6.4.3.	Иные аспекты работы с данными активации.....	39
6.5.	КОНТРОЛЬ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ.....	39
6.5.1.	Специальные технические требования компьютерной безопасности.....	39
6.5.2.	Оценка компьютерной безопасности.....	40
6.6.	ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЖИЗНЕННОГО ЦИКЛА.....	40
6.6.1.	Контроль развития системы.....	40
6.6.2.	Контроль управления безопасностью.....	40
6.6.3.	Контроль безопасности жизненного цикла.....	40

6.7.	СРЕДСТВА УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ	40
6.8.	МЕТКИ ВРЕМЕНИ	40
7.	ПРОФИЛИ СЕРТИФИКАТОВ, СОС И OCSP	41
7.1.	ПРОФИЛЬ СЕРТИФИКАТА	41
7.1.1.	Номер версии	41
7.1.2.	Расширения сертификата	41
7.1.3.	Объектные идентификаторы алгоритмов	42
7.1.4.	Формы имен	42
7.1.5.	Ограничения на использование имен	42
7.1.6.	Объектный идентификатор политики сертификатов	42
7.1.7.	Использование расширения «policyConstraints»	42
7.1.8.	Синтаксис и семантика квалификаторов политики	42
7.1.9.	Семантика обработки критических расширений «certificatePolicies»	42
7.2.	ПРОФИЛЬ СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ	42
7.2.1.	Номер версии	43
7.2.2.	Расширения списка отозванных сертификатов	43
7.3.	ПРОФИЛЬ OCSP	43
7.3.1.	Номер версии	43
7.3.2.	Расширения OCSP	43
8.	ПРОВЕРКА ДЕЯТЕЛЬНОСТИ	43
8.1.	ЧАСТОТА ИЛИ ОСНОВАНИЯ ПРОВЕДЕНИЯ ПРОВЕРОК	44
8.2.	ИДЕНТИЧНОСТЬ И КВАЛИФИКАЦИЯ ПРОВЕРЯЮЩИХ ИНСТАНЦИЙ	44
8.3.	ОТНОШЕНИЯ МЕЖДУ УЦ КЦМР И ПРОВЕРЯЮЩИМИ ИНСТАНЦИЯМИ	44
8.4.	ТЕМАТИКА ПРОВЕРОК	44
8.5.	МЕРЫ, ПРЕДПРИНИМАЕМЫЕ ПРИ ВЫЯВЛЕНИИ НЕДОСТАТКОВ	44
8.6.	ОБРАТНАЯ СВЯЗЬ	45
9.	ПРОЧИЕ КОММЕРЧЕСКИЕ И ЮРИДИЧЕСКИЕ ВОПРОСЫ	45
9.1.	ТАРИФЫ	45
9.1.1.	Тариф за выпуск и обновление сертификатов	45
9.1.2.	Тариф за доступ к сертификатам	45
9.1.3.	Тариф за доступ к информации об отзыве или статусе сертификатов	45
9.1.4.	Тарифы за иные сервисы	46
9.1.5.	Политика возмещения	46
9.2.	ФИНАНСОВАЯ ОТВЕТСТВЕННОСТЬ	46
9.2.1.	Страховое покрытие	46
9.2.2.	Другие средства	46
9.2.3.	Страхование гарантий для клиентов	46
9.3.	КОНФИДЕНЦИАЛЬНОСТЬ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ	46
9.3.1.	Спектр конфиденциальной информации	46
9.3.2.	Информация, не рассматриваемая в качестве конфиденциальной	47
9.3.3.	Ответственность за защиту конфиденциальной информации	47
9.4.	КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ	47
9.4.1.	План конфиденциальности	47
9.4.2.	Информация, рассматриваемая в качестве персональных данных	47
9.4.3.	Информация, не рассматриваемая в качестве персональных данных	47
9.4.4.	Ответственность за защиту персональных данных	47
9.4.5.	Уведомление и согласие на использование конфиденциальной информации	48
9.4.6.	Раскрытие персональных данных судебным и административным инстанциям	48
9.4.7.	Другие основания для раскрытия персональных данных	48
9.5.	ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ	48
9.6.	ГАРАНТИИ И ЗАВЕРЕНИЯ	48
9.6.1.	Гарантии и заверения удостоверяющего центра	48
9.6.2.	Гарантии и заверения центров регистрации	49
9.6.3.	Гарантии и заверения подписчиков	49
9.6.4.	Гарантии и заверения доверяющих сторон	49
9.6.5.	Гарантии и заверения владельцев сертификатов	50
9.6.6.	Гарантии и заверения уполномоченных посредников	50

9.7. ОТКАЗ ОТ ГАРАНТИЙ	50
9.8. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ	51
9.9. КОМПЕНСАЦИИ	51
9.9.1. Возмещения подписчика	51
9.9.2. Возмещения доверяющих сторон	51
9.9.3. Возмещения владельцев сертификатов	52
9.9.4. Возмещения уполномоченных посредников	52
9.9.5. Возмещения центров регистрации	52
9.10. ВСТУПЛЕНИЕ В СИЛУ И ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ.....	52
9.10.1. Вступление в силу	52
9.10.2. Прекращение действия	53
9.10.3. Правовые последствия прекращения действия	53
9.11. ИНДИВИДУАЛЬНЫЕ УВЕДОМЛЕНИЯ И СВЯЗЬ С УЧАСТНИКАМИ	53
9.12. ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ	53
9.12.1. Процедура изменения и дополнения	53
9.12.2. Механизм и сроки уведомления	53
9.12.3. Процедура изменения объектных идентификаторов	54
9.13. ПОЛОЖЕНИЯ О РАЗРЕШЕНИИ СПОРОВ	54
9.14. ПРИМЕНИМОЕ ПРАВО	54
9.15. ЮРИСДИКЦИЯ	54
9.16. РАЗНОЕ	54
9.16.1. Полнота соглашения	54
9.16.2. Передача прав	54
9.16.3. Делимость	54
9.16.4. Правоприменение (адвокатские компенсации и отказ от прав)	55
9.16.5. Форс-мажор	55
9.17. ПРОЧИЕ ПОЛОЖЕНИЯ	55
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.....	56

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, 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, подавшее документы на выпуск или отзыв регистрационного свидетельства.

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, УЦ, ЦР, владельца сертификата или уполномоченного посредника.

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 настоящих Правил роль соглашения с доверяющей стороной выполняет Заявление подписчика на выпуск регистрационного свидетельства, означающее согласие подписчика нести обязательства и выполнять требования, предусмотренные настоящим Положением о практике сертификатов и соответствующей Политикой сертификатов).

Соглашение с подписчиком – соглашение между УЦ и подписчиком, которое устанавливает права и ответственность сторон, касающуюся выпуска и управления сертификатами (в контексте настоящих Правил роль соглашения с подписчиком выполняет Заявление подписчика на выпуск регистрационного свидетельства, означающее согласие подписчика нести обязательства и выполнять требования, предусмотренные настоящим Положением о практике сертификатов и соответствующей Политикой сертификатов).

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 выпустившим их удостоверяющим центром.

Средства криптографической защиты информации (СКЗИ) – средства, реализующие 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

Настоящие Правила применения регистрационных свидетельств удостоверяющего центра КЦМР (далее – Положение о практике сертификатов) регламентируют деятельность удостоверяющего центра и детализируют для участников, обслуживаемых КЦМР информационных систем Политику применения регистрационных свидетельств Удостоверяющего центра (далее – Политика сертификатов, соответствующая Политика сертификатов).

Настоящее Положение о практике сертификатов устанавливает нормы, реализуемые УЦ КЦМР при обеспечении сервисов, которые определены Политикой сертификатов и включают в себя, но не ограничиваются выпуском, управлением и отзывом сертификатов.

Политика сертификатов устанавливает для участников информационных 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.

Если Политика сертификатов определяет требования, которым должны соответствовать все участники информационных систем, обслуживаемых УЦ КЦМР, то настоящее Положение о практике сертификатов раскрывает то, как деятельность УЦ КЦМР обеспечивает реализацию Политики сертификатов. В частности, настоящее Положение о практике сертификатов детализирует порядок, в соответствии с которым УЦ КЦМР:

обеспечивает безопасность и управление ядром инфраструктуры обслуживаемых информационных систем;

выпускает, управляет и отзывает для нее сертификаты.

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

Настоящее Положение о практике сертификатов само по себе не является юридическим соглашением между КЦМР и участниками обслуживаемых им информационных систем. Вместе с тем, оно приобретает статус такого юридического соглашения в момент подписания участником заявления на выпуск регистрационного свидетельства (сертификата) или договора, содержащих ссылку на Политику сертификатов и обязательство участника выполнять ее требования.

Настоящий документ определяет также виды сертификатов, выпускаемых УЦ КЦМР, сферы их применения, а также связанные с ними процедуры проверки.

Исчерпывающий перечень профилей сертификатов, выпускаемых удостоверяющим центром КЦМР для участников обслуживаемых им информационных систем, с указанием определяющих их критериев, приведен в следующей таблице:

Описание	Значение расширения <i>keyUsage</i>	Значение расширения <i>extendedKeyUsage</i>
1	2	3
Сертификаты для обеспечения подлинности, целостности и доказательности электронных документов с помощью электронной цифровой подписи	«c0» (в соответствии с OID 2.5.29.15)	отсутствует (расширение не используется)
Сертификаты для обеспечения конфиденциальности ключей и данных с помощью шифрования	«30» (в соответствии с OID 2.5.29.15)	отсутствует (расширение не используется)

1	2	3
Сертификаты для аутентификации клиента сервером или службой на платформе Windows или иных платформах (например, по протоколам SSL/TLS, IPSec)	«a0» (в соответствии с OID 2.5.29.15)	«OID 1.3.6.1.5.5.7.3.2» (только для TLS/SSL) или отсутствует (для IPSec и других случаев)
Сертификаты домена (DV) для протокола SSL/TLS	«f8» (в соответствии с OID 2.5.29.15)	«OID 1.3.6.1.5.5.7.3.1»
Сертификаты организации (OV) для протокола SSL/TLS	«f8» (в соответствии с OID 2.5.29.15)	«OID 1.3.6.1.5.5.7.3.1»

1.2. Наименование и идентификация документа

Наименование документа: «Правила применения регистрационных свидетельств удостоверяющего центра РГП «КЦМР НБ РК» (Certification Practice Statement)».

Редакция документа: 1.3.

Введен в действие приказом КЦМР от 26 февраля 2018 года № 12-П.

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

Сертификаты, выпускаемые УЦ КЦМР, содержат значения объектных идентификаторов, определенные соответствующей Политикой сертификатов. В связи с этим, в настоящем Положении о практике сертификатов значения объектных идентификаторов не устанавливаются. Объектные идентификаторы используются в соответствии с параграфом 7.1.6 Политики сертификатов (<http://www.kisc.kz/ca/doc/PolicyKISC.pdf>).

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 настоящими Правилами.

1.3.2. Центры регистрации

Центр регистрации (ЦР) – структурное подразделение удостоверяющего центра или действующее на основании договора с удостоверяющим центром юридическое лицо, ответственные за идентификацию заявителя, прием документов на выпуск или отзыв регистрационных свидетельств и предоставление заявителю готовых регистрационных свидетельств.

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

Уполномоченный посредник – юридическое лицо, вошедшее в договорные отношения с КЦМР, которое может выполнять операции по идентификации и аутентификации заявителей при выпуске и отзыве сертификатов УЦ КЦМР.

Уполномоченный посредник обязан обеспечивать исполнение соответствующих требований настоящей Политики сертификатов и заключенного с УЦ КЦМР договора.

1.3.6. Другие участники

Определены разделом 1.3.6 соответствующей Политики сертификатов.

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 5 профилей, перечисленных в параграфе 1.1. Разрешенное использование, согласно профилю отражается в расширениях «keyUsage» и/или «extendedKeyUsage» каждого сертификата.

Кроме того, по области допустимого применения сертификаты разделены объектными идентификаторами политики, которые отражаются в расширении «certificatePolicies». 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) 250-66-75; +7 (727) 250-66-74; +7 (727) 250-66-72

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 Положение о практике сертификатов готовятся отделом удостоверяющего центра КЦМР и оформляются в виде отдельного документа, содержащего либо актуальный текст Положения, либо уведомление об изменениях и дополнениях в его 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.

Положение о практике сертификатов и все изменения и дополнения к нему публикуются.

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

Все утвержденные изменения и дополнения в Положение о практике сертификатов вступают в силу и становятся обязательными для исполнения юридическими и физическими лицами, связанными обязательствами по ссылающимся на него 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 онлайн-запросы, касающиеся информации о статусе сертификатов или его изменения. Вместе с тем, доступ к информации в хранилище возможен и через web-интерфейс.

УЦ КЦМР предоставляет подписчикам и доверяющим сторонам информацию о том, по каким адресам находятся соответствующее хранилище и служба онлайн-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.

Сертификаты публикуются в соответствии со следующей таблицей:

Тип сертификата	Требования по доступу
Сертификаты УЦ КЦМР	<ol style="list-style-type: none">1. Доступны на официальном информационном ресурсе УЦ в сети Интернет по адресу http://www.kisc.kz/ca/crl.html;2. Вручаются доверяющим сторонам из рук в руки при успешном прохождении процедуры первичной регистрации;3. Доступны в хранилище УЦ по протоколу LDAP¹;4. Доступны как часть цепочки сертификатов, которая может быть получена вместе с сертификатом подписчика.
Сертификаты сервера OCSP	<ol style="list-style-type: none">1. Доступны в хранилище УЦ по протоколу LDAP;2. Доступны как часть любой квитанции (ответа) сервера OCSP.
Сертификаты подписчиков	Доступны в хранилище УЦ по протоколу LDAP.
Сертификаты сервера метки времени	Доступны в хранилище УЦ по протоколу LDAP.

2.3. Периодичность публикации

Изменения и дополнения к Положению о практике сертификатов публикуются в течение 5 рабочих дней со дня утверждения в соответствии с разделом 9.12. Сертификаты подписчиков публикуются незамедлительно после их выпуска. Информация о статусе

¹ Адрес для обращения в хранилище УЦ по протоколу LDAP доводится подписчикам и доверяющим сторонам по запросу после прохождения процедур первичной регистрации.

сертификатов публикуется в соответствии с нормами настоящего Положения о практике 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 онлайн-протокола статуса сертификатов (OCSP), доступны всем желающим по ссылке 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 УЦ КЦМР в полях «Issuer» и «Subject» содержат отличительное имя (DN-имя), соответствующее рекомендациям (ITU-T) X.501 и состоящее из следующих компонентов:

Компонент	Значение
Country (C) =	“KZ”
Organization (O) =	“KISC”
Common Name (CN) =	“KISC Root CA”

Остальные компоненты отличительного имени для поля «Issuer» не используются.

Сертификаты подписчиков УЦ КЦМР в поле «Subject» содержат DN-имена, соответствующие рекомендациям (ITU-T) X.501 и состоящие из следующих компонентов:

Компонент	Значение расширения <i>extendedKeyUsage</i>
1	2
Country (C) =	<i>Двухбуквенный код страны согласно стандарту ISO 3166-1</i>
Organization (O) =	<i>Название организации, в чьем ведении находится система электронного документооборота, для участия в которой выпущен сертификат</i>
¹ Organization unit (OU) =	<i>Название организации подписчика</i>
² State or Province (S) =	<i>Название области</i>
² Locality (L) =	<i>Название города</i>
Common Name (CN) =	<i>Этот компонент может содержать один или несколько из следующих пунктов: индивидуальный идентификационный номер гражданина Республики Казахстан; фамилия, имя физического лица; псевдоним подписчика, идентификатор в информационной системе [электронного</i>

¹ Данный компонент является обязательным только тогда, когда подписчиком является юридическое лицо.

² Данный компонент не является обязательным.

1	2
² Serial Number (SN) =	Этот компонент может содержать один или несколько из следующих пунктов: “ПН” <i>индивидуальный идентификационный номер гражданина Республики Казахстан;</i> “NR” <i>номер паспорта.</i>
² Unique Identification Number (UID) =	Этот компонент может содержать один или несколько из следующих пунктов: “ПН” <i>индивидуальный идентификационный номер гражданина Республики Казахстан;</i> “NR” <i>номер паспорта.</i>
¹ E-Mail Address	<i>Адрес электронной почты</i>

Поле «Subject» в сертификатах, выпускаемых УЦ КЦМР, отражает данные, однозначно идентифицирующие подписчика. Если подписчиком является физическое лицо или юридическое лицо в лице своего представителя, то поле «Subject» или расширение «Subject Alternative Name» может содержать такие данные как индивидуальный идентификационный номер (для граждан Республики Казахстан), серию и номер паспорта с указанием страны и/или псевдоним. Если подписчиком является техническое средство, например, сервер, поле «Subject» отражает его полное доменное имя, если служба – название службы и т.п.

В любом случае, содержание поля «Subject» в сертификате 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. Псевдоним назначается данному подписчику владельцем сертификата, центром регистрации или удостоверяющим центром в рамках заключенного договора. При этом в любом случае псевдоним однозначно идентифицирует 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

Заявителям на выпуск сертификата запрещается использовать в своих заявлениях имена, нарушающие права их законных правообладателей. УЦ КЦМР не проверяет, является ли заявитель правообладателем имени, указанного в заявлении. УЦ не вступает в споры, связанные с собственностью на доменные, торговые и тому подобные имена и марки. УЦ КЦМР отклоняет любое заявление на изготовление ключей и регистрационного свидетельства и/или регистрацию регистрационного свидетельства (далее – заявление на выпуск сертификата) или приостанавливает его рассмотрение, если подобное разбирательство становится 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 центром регистрации, 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.

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, процедуры идентификации и аутентификации проводятся в форме первоначальной проверки идентичности.

3.2.1. Способ доказательства факта владения закрытым ключом

В ходе первоначальной проверки идентичности заявитель демонстрирует УЦ КЦМР, центру регистрации или уполномоченному посреднику 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 центра регистрации или 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, центра регистрации, 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

¹ При поступлении заявления на выпуск сертификата в центр регистрации или к уполномоченному посреднику данную проверку проводит центр регистрации или уполномоченный посредник соответственно. Удостоверяющий центр проводит данную проверку только в отношении уполномоченных представителей своих контрагентов по двусторонним Договорам о предоставлении услуг удостоверяющего центра или по Договорам о сотрудничестве с уполномоченными посредниками. В остальных случаях данную проверку проводит заявитель.

Если заявление юридического лица на выпуск сертификата заверено собственноручной подписью, указанные в нем сведения подтверждаются при личном прибытии уполномоченного представителя заявителя в центр регистрации, к уполномоченному посреднику или в удостоверяющий центр, представлением следующих документов:

1. Свидетельство или справка о государственной регистрации (перерегистрации) юридического лица – предъявляется оригинал;

2. Паспорт или удостоверение личности уполномоченного физического лица (подписчика, на чье имя необходимо оформить сертификат) – предъявляется оригинал;

Если заявление на выпуск сертификата подано в форме электронного документа, сведения, содержащиеся в заявлении, подтверждаются ЭЦП заявителя, сформированной с использованием закрытого ключа соответствующего действующему сертификату. При этом ответственность за полноту и достоверность сведений, указанных в заявлении несет заявитель.

3.2.3. Процедура аутентификации физического лица

Сведения, указанные в заявлении физического лица на выпуск сертификата, подтверждаются при личном прибытии заявителя в центр регистрации, к уполномоченному посреднику или в удостоверяющий центр представлением следующих документов:

1. Паспорт или удостоверение личности подписчика – предъявляется оригинал;

Если заявление на выпуск сертификата подано в форме электронного документа, сведения, содержащиеся в заявлении, подтверждаются ЭЦП заявителя, сформированной с использованием закрытого ключа соответствующего действующему сертификату. При этом ответственность за полноту и достоверность сведений, указанных в заявлении несет заявитель.

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, центр регистрации 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 выпустить новый сертификат. УЦ КЦМР

требует, чтобы подписчик при этом генерировал новую ключевую пару для замены истекающей. Перед выпуском нового сертификата УЦ КЦМР, центр регистрации или/и уполномоченный посредник проверяет 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 всю процедуру первоначальной проверки идентичности, как это изложено в разделе 3.2.

3.4. Идентификация и аутентификация при отзыве сертификатов

Заявление на отзыв сертификата подаются по формам приложений 8 и 9 к Правилам выдачи, хранения, отзыва регистрационных свидетельств, и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключение корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан, утвержденным приказом Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 1231 (<http://www.kisc.kz/clients/rules.rtf>), для юридического или физического лица соответственно.

Заявление может быть подано в форме электронного документа, в этом случае оно должно быть удостоверено электронной цифровой подписью заявителя.

В противном случае, если оно исходит от имени юридического лица, то его уполномоченный представитель вместе с заявлением предоставляет УЦ КЦМР или уполномоченному посреднику:

1. Свидетельство или справка о государственной регистрации (перерегистрации) юридического лица – предъявляется оригинал;

2. Паспорт или удостоверение личности подписывающего лица, чей сертификат необходимо отозвать – предъявляется оригинал;

а если от физического лица – паспорт или удостоверение личности подписчика, чей сертификат необходимо отозвать.

4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТОВ

4.1. Заявления на выпуск сертификатов

4.1.1. Лица, имеющие право подавать заявления на выпуск сертификата

Заявление на выпуск сертификата имеют право подавать:
физические лица;
уполномоченные представители юридических лиц.

4.1.2. Процедура регистрации и связанные с ней обязательства

Центр регистрации, уполномоченный посредник или Удостоверяющий центр регистрируют заявления на выпуск сертификата после заключения заявителем договора с центром регистрации или Удостоверяющим центром. 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, центр регистрации 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, центр регистрации или уполномоченный посредник отклоняет 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;

в иных случаях, установленных законом.

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, центрами регистрации 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 создается и выпускается по факту приема УЦ КЦМР, центром регистрации 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 уведомляет подписчика о создании сертификата, способах его получения и обеспечивает ему доступ к сертификату. Уведомление осуществляется напрямую, через владельца этого сертификата, через центр регистрации 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 сертификата 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 направляет уведомление владельцу данного сертификата, центру регистрации или 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, центром регистрации 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, соответствующей Политикой сертификатов и настоящим Положением о практике сертификатов. Использование сертификата должно соответствовать содержанию 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, центром регистрации 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 соответствующими правилами (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, центры регистрации 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, центр регистрации 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, центра регистрации или владельца сертификата, который больше не использует (или не желает использовать) сертификат;

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

удостоверяющий центр, центр регистрации, 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, центр регистрации 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, центр регистрации 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 основаниям, 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, центры регистрации и уполномоченные посредники, а также их должным образом уполномоченные представители. Запрашивать отзыв сертификатов также могут уполномоченные сотрудники удостоверяющего центра.

4.9.3. Процедуры отзыва сертификата

Инициатор отзыва сертификата представляет в УЦ, в центр регистрации, владельцу сертификата или уполномоченному последнику заявление по форме, соответствующей приложениям 8 или 9 (для физических или юридических лиц соответственно) к Правилам выдачи, хранения, отзыва регистрационных свидетельств, и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключение корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан, утвержденным приказом Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 1231 (<http://www.kisc.kz/ca/doc/rules.rtf>). Заявление об отзыве может подаваться в форме электронного документа.

Перед отзывом сертификата подписчика УЦ КЦМР, центр регистрации, уполномоченный посредник или владелец сертификата проверяют, что инициатор запрашивает отзыв правомочно. При этом могут применяться все механизмы идентификации и аутентификации, которые приведены в разделе 3.2.

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 онлайн-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 онлайн-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 подать заявление в соответствии с разделом 4.9.3 в центр регистрации или уполномоченному посреднику.

Уполномоченный посредник, центр регистрации и УЦ КЦМР в этом случае принимают меры и отзывают 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 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, центр регистрации 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, центр регистрации или уполномоченный посредник подозревают и проверяют информацию об ошибочности существенного факта в заявлении на выпуск сертификата;

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

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

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

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

В последнем случае УЦ КЦМР, владелец сертификата, центр регистрации 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 только подписчики, их представители, уполномоченные должным образом, или уполномоченные сотрудники удостоверяющего центра.

4.9.15. Процедуры рассмотрения заявления на приостановление

Запросы на приостановление действия сертификатов подаются только в форме электронного документа.

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 ремонтных и регламентных 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. УЦ КЦМР также имеет возможности (запасной объект) для восстановления на случай чрезвычайных ситуаций. Запасной объект имеет многоуровневую систему физической безопасности, как и основной.

5.1.2. Физический доступ

Системы удостоверяющего центра защищены минимум тремя уровнями физической безопасности, доступ на вышестоящие уровни невозможен без корректного прохождения нижестоящих.

Доступ на каждый уровень контролируется в соответствии с прогрессивной ограничительной шкалой привилегий физического доступа. Важные эксплуатационные процедуры УЦ, в том числе любые процедуры, связанные с жизненным циклом сертификатов, такие как аутентификация, проверки, выпуск, выполняются на верхнем уровне безопасности. Для доступа на каждый уровень необходимо использовать бесконтактную карту сотрудника. Физический доступ автоматически протоколируется и контролируется видеозаписью. Передвижение по контролируемой территории УЦ КЦМР посетителей и сотрудников, не имеющих на то соответствующих полномочий, запрещено.

Система физической безопасности имеет в своем составе дополнительные уровни для безопасного управления ключами, которые защищают криптографические устройства, в том числе онлайнные, а также ключевой материал. Онлайнные криптографические устройства используются в помещениях с ограниченным доступом, остальные хранятся в сейфах, контейнерах и хранилищах. Открытие и закрытие помещений и контейнеров на этих уровнях протоколируется в контрольных целях. Доступ к криптографическим устройствам и ключевому материалу ограничен требованиями разделения обязанностей.

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

Все носители производственного программного обеспечения и данных, протоколов и резервных копий хранятся на защищенных объектах с надлежащим уровнем физического и логического контроля доступа, предусматривающего доступ ответственного персонала и защиту от случайного повреждения (вследствие пожара, наводнения или электромагнитного излучения и т.п.).

5.1.7. Утилизация

Конфиденциальные документы и материалы утилизируются, их носители перед утилизацией приводятся в нечитаемой состояние. Криптографические устройства перед утилизацией уничтожаются физически или обнуляются логически в соответствии с технической документацией на них. Тем самым исключается возможность утечки конфиденциальной информации через этот канал.

5.1.8. Внешнее резервирование

УЦ КЦМР выполняет резервное копирование важных системных данных, контрольных протоколов и другой конфиденциальной информации. Носители резервных копий хранятся на запасном объекте и защищаются физически.

5.2. Процедурный контроль

5.2.1. Распределение ролей

К разряду ответственного персонала относятся работники КЦМР, имеющие доступ или контролирующую аутентификацию и 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, выполняющим криптографические операции;
- персоналом управления безопасностью;
- персоналом системного администрирования;
- инженерным персоналом;
- управляющими инфраструктуры безопасности.

Перечисленные категории работников КЦМР считаются ответственным персоналом, занимающим ответственные участки. Претенденты на должности, относящиеся к разряду ответственного персонала, то есть на работу на ответственном участке, обязаны предоставить документы, определенные Трудовым Кодексом Республики Казахстан.

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, осуществляются одним или более чем одним ответственным работником УЦ, центра регистрации, уполномоченного посредника или заявителя с применением средств автоматизации проверки.

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

5.2.3. Идентификация и аутентификация каждой роли

Для всех работников КЦМР, претендующих на должности, входящие в разряд ответственного персонала, проводится процедура идентификации, в ходе которой при личном (физическом) присутствии претендента ответственный персонал кадровой службы или службы безопасности проверяет документы, удостоверяющие личность.

УЦ КЦМР обеспечивает, что выдаче сотруднику персональных устройств и прав доступа на соответствующие объекты, а также электронных средств для доступа и

выполнения специализированных функций в информационных системах УЦ КЦМР предшествует решение ответственного руководителя и зачисление этого сотрудника в разряд ответственного персонала.

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;
- администрированием 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 наличие 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

В необходимых случаях КЦМР привлекает на ответственные участки независимых контрактников и консультантов. Каждый такой контрактник или консультант подбирается и работает по тем же функциональным критериям и критериям безопасности, что и штатные работники соответствующих должностей.

Независимым контрактникам и консультантам доступ на защищенные объекты КЦМР разрешен только в сопровождении и под постоянным контролем ответственного персонала.

5.3.8. Документация, раскрываемая персоналу

КЦМР обеспечивает свой персонал необходимым обучением и документацией, необходимой для компетентного и удовлетворительного исполнения обязанностей.

5.4. Процедуры контрольного протоколирования

5.4.1. Типы протоколируемых событий

Типы контролируемых событий, которые регистрирует УЦ КЦМР, установлены в соответствующей Политике сертификатов.

Структура записи контрольного протокола, как правило, включает в себя следующие элементы:

- дата и время записи;
- порядковый номер записи;
- идентичность сущности, вызвавшей запись;
- тип события;
- источник записи.

Структура записи событий в конкретном протоколе соответствует эксплуатационной документации программного обеспечения целевых функций удостоверяющего центра и общесистемного программного обеспечения. В случае отсутствия в протоколе какой-либо из перечисленных категорий информации, связанные с этим риски минимизируются другими техническими или организационными мерами.

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

УЦ КЦМР также осуществляет систематизацию и хранение материалов заявлений на выпуск и отзыв сертификатов, включая заявления о присоединении к публичным договорам, доверенности, уполномочивающие представителей юридических лиц, и другие материалы согласно заключенным договорам.

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 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 в архив 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 маркируются с указанием даты архивирования, информация о времени архивирования автоматически фиксируется программно-техническими средствами архивирования. Записи контрольных протоколов имеют 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 по истечении срока действия выводятся из использования. Новые ключевые пары УЦ КЦМР генерируются по мере необходимости, например, на замену выводимым из действия или в дополнение к действующим для обеспечения новых сервисов.

До истечения срока действия сертификата УЦ КЦМР проводится процедура смены ключей, которая обеспечивает плавный переход подписчиков со старой ключевой пары УЦ на новую. Процедура смены ключей УЦ состоит в следующем:

УЦ КЦМР с определенного момента, не позднее, чем за 1 год до истечения срока действия сертификата УЦ, прекращает выпускать сертификаты подписчиков, подписанные закрытым ключом, который соответствует данному сертификату УЦ;

с указанного момента по положительно рассмотренным заявлениям подписчиков выпускаются сертификаты, подписанные новой ключевой парой УЦ КЦМР.

При этом УЦ КЦМР продолжает подписывать выпускаемые списки отозванных сертификатов закрытым ключом истекающей ключевой пары до момента окончания срока действия последнего сертификата, выпущенного с его помощью.

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 выпуск и изменение статуса,

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

В случае компрометации или обоснованного подозрения в компрометации закрытых ключей УЦ уполномоченный штат КЦМР вводит в действие План восстановления функционирования, составляемый в соответствии с параграфом 5.7.4 соответствующей Политики сертификатов. Согласно указанному Плану службы безопасности и операционные службы оценивают ситуацию, корректируют План с учетом складывающейся обстановки и реализуют его с санкции ответственного руководителя КЦМР.

При необходимости отзыва сертификата УЦ КЦМР выполняются следующие процедуры:

информация об изменении статуса сертификата УЦ КЦМР (отзыве) доводится до доверяющих сторон через список отозванных сертификатов в соответствии с параграфом 4.9.7;

предпринимаются иные целесообразные меры для дополнительного уведомления об отзыве всех заинтересованных участников обслуживаемых УЦ информационных систем;

УЦ генерирует новые ключевые пары в соответствии с параграфом 6.1.1, за исключением случаев прекращения деятельности УЦ в соответствии с разделом 5.8.

5.7.4. Возможности непрерывной деятельности после происшествий

КЦМР имеет для своего удостоверяющего центра безопасный внешний запасной объект.

В КЦМР разработан, утвержден и прошел учебную проверку детальный План восстановления функционирования, нацеленный на смягчение последствий каких-либо природных или техногенных бедствий. План восстановления функционирования регулярно рассматривается с целью актуализации.

План восстановления функционирования предназначен для возобновления сервисов информационных систем и ключевых бизнес-функций. Внешний запасной объект КЦМР защищен физически и контролируется в эксплуатационном плане в соответствии с утвержденными нормативными документами в целях обеспечения безопасного и надежного резервирования работы.

КЦМР обеспечен запасным оборудованием и резервными копиями программного обеспечения систем своего УЦ на запасном объекте. Кроме того, на случай восстановления функционирования в соответствии с параграфом 6.2.4 созданы и хранятся резервные копии закрытых ключей УЦ.

УЦ КЦМР имеет на запасном объекте резервные копии важной информации, указанной в параграфе 5.7.1.

В случае стихийного бедствия или техногенной аварии, требующей временного или постоянного прекращения функционирования основного объекта УЦ, уполномоченные работники КЦМР инициируют приведение в действие Плана восстановления функционирования.

УЦ КЦМР имеет возможность возобновить и восстановить важные операции в течение 24 (двадцати четырех) часов после происшествия. При этом восстановление таких функций как выпуск и отзыв сертификатов, а также публикация сведений об отзыве сертификатов осуществляется в течение не более чем 2 (двух) часов.

Резервная и основная базы данных регулярно синхронизируются с определенной частотой. Принципы физической защиты резервного оборудования аналогичны по уровню принципам, приведенным в разделе 5.1. Не реже одного раза в год в тренировочных целях проводится пробное восстановление информации УЦ из архива.

План восстановления функционирования УЦ КЦМР, кроме того, предусматривает полное восстановление работы в течение одной недели после происшествия на основном объекте. Необходимое для этого резервное оборудование имеется, хранится и периодически испытывается на случай выхода из строя всего основного объекта КЦМР. Результаты таких испытаний рассматриваются и сохраняются для анализа и планирования.

5.8. Прекращение работы удостоверяющего центра

В случае необходимости прекращения деятельности удостоверяющего центра КЦМР предпринимает все меры, необходимые для заблаговременного уведомления об этом подписчиков, доверяющих сторон и других заинтересованных лиц. В случае принятия решения о прекращении деятельности удостоверяющего центра КЦМР разрабатывает план прекращения деятельности с целью минимизации неудобств для

клиентов, подписчиков и доверяющих сторон. План прекращения может включать в себя следующие вопросы:

уведомление с информацией о статусе УЦ для сторон, которых касается прекращение, в том числе подписчиков, доверяющих сторон и владельцев сертификатов;

оплата стоимости такого уведомления;

сохранение архивов УЦ на период, предусмотренный законодательством и соответствующей Политикой сертификатов;

продолжение сервисов поддержки подписчиков и клиентов;

продолжение сервисов отзыва, таких как выпуск списков отозванных сертификатов или поддержка онлайн-услуг проверки статуса;

отзыв действующих не отозванных сертификатов подписчиков, при необходимости;

выпуск заменяющих сертификатов удостоверяющим центром-правопреемником или, при необходимости, возврат средств тем подписчикам, чьи действующие не отозванные сертификаты отзываются в соответствии с планом прекращения;

дальнейшее местонахождение закрытых ключей УЦ и криптографических модулей, содержащих эти закрытые ключи;

положения, необходимые для передачи сервисов УЦ КЦМР его правопреемнику.

6. КОНТРОЛЬ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ

6.1. Генерация и установка ключевых пар

6.1.1. Генерация ключевых пар

Генерация ключевых пар проводится только с помощью средств криптографической защиты информации, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации¹.

Генерация ключевых пар УЦ КЦМР, кроме того, проводится только несколькими выделенными и предварительно обученными работниками из числа ответственного персонала. При этом используются криптографические модули (средства криптографической защиты информации), которые соответствуют не ниже чем второму уровню безопасности согласно указанному стандарту. По каждой процедуре генерации ключевой пары УЦ КЦМР составляется протокол, который датируется и подписывается лицами, принимавшими в ней участие. Протоколы хранятся в целях учета и контроля в течение определенного времени, установленного нормативными документами КЦМР.

6.1.2. Доставка закрытого ключа подписчику

В случае если подписчик генерирует свою ключевую пару самостоятельно, процедура доставки закрытого ключа подписчику не применима.

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

В любом случае работники или системы УЦ КЦМР не имеют доступа к закрытым ключам подписчиков.

¹ 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».

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, центр регистрации или уполномоченный посредник должны быть в состоянии подтвердить факт владения подписчиком соответствующим закрытым ключом. Приемлемым механизмом доставки открытого ключа подписчика в удостоверяющий центр является электронный документ в формате 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, центре регистрации, от уполномоченного посредника или от владельца своего сертификата. Сертификаты УЦ также доступны на официальном информационном ресурсе КЦМР в сети Интернет по адресу <http://www.kisc.kz/ca/crl.html>. Проверка аутентичности сертификата может быть осуществлена средствами электронной цифровой подписи.

6.1.5. Размеры ключей

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):
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

УЦ КЦМР реализует комплекс физических, логических и организационных мер, обеспечивающий безопасность собственных закрытых ключей. Подписчики обязаны по договору принимать необходимые меры, предотвращающие потерю, разглашение, изменение и несанкционированное использование своих закрытых ключей.

6.2.1. Стандарты и контроль криптографического модуля

Для генерации и хранения ключевых пар УЦ КЦМР использует криптографические модули, сертифицированные на соответствие действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации не ниже, чем по второму уровню безопасности.

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

УЦ КЦМР реализует организационно-технические меры, которые требуют для выполнения важных криптографических операций участия нескольких работников из числа ответственного персонала. УЦ КЦМР использует для закрытых ключей данные активации в форме разделения на части секрета, которые хранятся выделенными для этого работниками из числа ответственного персонала, так называемыми хранителями секрета. Для восстановления закрытого ключа требуется 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

УЦ КЦМР создает резервные копии закрытых ключей удостоверяющего центра в целях обеспечения возможности их восстановления на случай чрезвычайных происшествий и сбоев в работе. Порядок создания резервных копий регламентирован.

Резервные копии закрытых ключей УЦ КЦМР защищены от модификации и разглашения как физическими, так и криптографическими средствами. Их хранение и использование регламентировано.

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

УЦ КЦМР генерирует ключевые пары теми же аппаратными криптографическими модулями, в которых ключи будут использоваться. Вместе с тем, УЦ КЦМР осуществляет резервное копирование ключевых пар, чтобы обеспечить возможность их восстановления в случае аварии или иной нештатной ситуации. В ходе резервного копирования ключевые пары выгружаются из аппаратных криптографических модулей в зашифрованном виде, а в ходе восстановления – зашифрованные ключевые пары загружаются в них.

6.2.7. Хранение закрытого ключа в криптографическом модуле

Закрытые ключи УЦ КЦМР в криптографических модулях 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 активируются 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. В любом случае, в соответствии с настоящим Положением о практике сертификатов подписчики обязаны должным образом защищать свой закрытый ключ.

В КЦМР процедура деактивации закрытых ключей удостоверяющего центра не применяется в связи с непрерывностью функционирования.

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. В частности, используется штатная функция криптографических модулей, удаляющая ключи. 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

Период использования сертификата заканчивается при истечении срока его действия или отзыве. Период использования ключевой пары совпадает с периодом использования, соответствующего сертификата, за тем исключением, что она может и далее использоваться в целях расшифрования или проверки электронной цифровой подписи.

Срок действия сертификатов УЦ КЦМР составляет 20 (двадцать) лет и исчисляется с даты и времени его генерации. Срок действия сертификатов подписчиков в информационных системах, обслуживаемых КЦМР (МСПД, системы розничных платежей, СОБС, ФАСТИ, Авангард Plat) составляет 1 (один) год, за исключением сертификатов аутентификации сервера, срок действия которых не должен превышать 3

(трех) лет. Срок действия сертификатов первичной инициализации не превышает 30 (тридцать) суток. Срок действия остальных сертификатов подписчиков, выпускаемых УЦ КЦМР составляет 1 (один), 2 (два) или 3 (три) года по выбору подписчика. Вместе с тем, УЦ КЦМР не выпускает сертификаты подписчиков, срок действия которых превышает срок действия соответствующего сертификата УЦ КЦМР, который необходимо использовать для проверки.

Подписчики не должны использовать свои ключевые пары после истечения срока их действия никак кроме указанных выше случаев.

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

6.4. Данные активации

6.4.1. Генерация и установка данных активации

Данные активации закрытых ключей УЦ КЦМР в соответствии с Политикой сертификатов подлежат разделению секрета. Части секрета генерируются в соответствии с требованиями параграфа 6.2.2 настоящего Положения о практике сертификатов. Создание и передача частей секрета протоколируется.

Пароли, используемые в качестве данных активации:

должны генерироваться пользователями;

не должны быть короче 6 символов;

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

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

УЦ КЦМР настоятельно рекомендует подписчикам использовать для активации закрытых ключей комбинированные механизмы аутентификации, например пароль и аппаратный токен, токен и биометрический принцип, биометрический принцип и пароль.

6.4.2. Защита данных активации

Хранители секрета УЦ КЦМР подписывают соглашение, устанавливающее их ответственность, и обязаны защищать доверенные им части секрета.

УЦ КЦМР настоятельно рекомендует подписчикам хранить закрытые ключи в зашифрованном виде и защищать их с помощью аппаратных токенов и/или сильных паролей. Приветствуется использование подписчиками комбинированных механизмов аутентификации, например пароля и аппаратного токена, токена и биометрического принципа, биометрического принципа и пароля.

6.4.3. Иные аспекты работы с данными активации

Данные активации закрытых ключей УЦ КЦМР выводятся из использования с применением процедур, защищающих от потери, хищения, модификации, разглашения или несанкционированного использования закрытых ключей, активируемых этими данными. Не подлежащие дальнейшему хранению 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 защиту используемых вычислительных ресурсов, программного обеспечения и данных от несанкционированного доступа с помощью систем, которые контролируются по показателям, перечисленным в параграфе 5.4.1 соответствующей Политики сертификатов.

Компьютеры, работающие в УЦ КЦМР, удовлетворяют следующим требованиям:

ЭВМ для подписи сертификатов изолирована от несанкционированного 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 участников, 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.

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 обеспечивается 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 постоянно контролируется.

6.6.3. Контроль безопасности жизненного цикла

Специальных требований не предъявляется.

6.7. Средства управления сетевой безопасностью

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

Конфиденциальность, аутентичность, целостность и неотказность 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, содержат 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, СОС И ОССП

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
1	2
Version	v3
serialNumber	<i>уникальный серийный номер сертификата</i>
signatureAlgorithm	<i>объектный идентификатор алгоритма, см. § 7.1.3</i>
Issuer	C = KZ O = KISC CN = KISC Root CA
Validity	YYYYMMDDHHMMSSZ GMT (действителен с) YYYYMMDDHHMMSSZ GMT (действителен по)
Subject	C = KZ O = <i>наименование организации</i> (опционально) OU = <i>наименование подразделения</i> (опционально) S = <i>наименование области</i> (опционально) L = <i>наименование города</i> CN = <i>ИИН/ Фамилия, имя/ Псевдоним подписчика</i> (опционально) Serial Number = <i>ПИННомерИИН</i> или <i>NRНомерПаспорта</i> (опционально) UID = <i>ПИННомерИИН</i> или <i>NRНомерПаспорта</i> (опционально) E = <i>адрес электронной почты</i>
subjectPublicKeyInfo	<i>открытый ключ</i>
issuerSignatureAlgorithm	<i>объектный идентификатор алгоритма подписи сертификата, см. § 7.1.3</i>
signatureValue	<i>электронная цифровая подпись</i>

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
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
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-256 with RSA Encryption	{iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) Sha256WithRSAEncryption(11)}

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 соответствующей Политики сертификатов. 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 ссылки на нестоящее Положение о практике сертификатов и соответствующую Политику сертификатов через перечень всех используемых УЦ КЦМР объектных идентификаторов политики.

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
(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. <i>CertificateSerialNumber</i> (серийный номер сертификата); 2. <i>Time</i> (время обработки заявления на отзыв сертификата).
signatureAlgorithm	<i>объектный идентификатор алгоритма подписи СОС, см. § 7.1.3</i>
signatureValue	<i>электронная цифровая подпись</i>

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

рассматриваться актуальность и соблюдение действующих документально закреплённых требований: политики безопасности, включая требования по безопасности на объектах КЦМР, договорных обязательств. Может оцениваться 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 подвергать деятельность собственного удостоверяющего центра проверке независимых аудиторских компаний, имеющих лицензию на предоставление услуг по программе WebTrust для удостоверяющих центров.

8.1. Частота или основания проведения проверок

Частота и основания проведения проверок КЦМР со стороны Национального Банка Республики Казахстан определяются нормативными правовыми актами Национального Банка.

КЦМР планирует приобретение услуг по проверке у независимых аудиторских компаний, имеющих лицензию на предоставление услуг по программе WebTrust для удостоверяющих центров, 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

Тематика проверок КЦМР со стороны Национального Банка Республики Казахстан определяется в соответствии с нормативными правовыми актами Национального Банка.

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:

- общие практики;
- управление жизненным циклом ключей;
- управление жизненным циклом сертификатов;
- контроль организационного уровня;

целостность услуг:

- контроли жизненного цикла ключей;
- управление жизненным циклом сертификатов;

контроль организационного уровня:

- Политика и Положение о практике сертификатов;
- управление безопасностью;
- ресурсы;
- персонал;
- физическая безопасность;
- функционирование;
- управление доступом;
- разработка и поддержка систем;
- непрерывность бизнеса;
- мониторинг;
- протоколирование.

8.5. Меры, предпринимаемые при выявлении недостатков

После получения отчета о проверке деятельности, при выявлении в ней нарушений и недостатков, формы их устранения и исключения определяются в соответствии с нормативными правовыми актами Национального Банка.

Если выявленные нарушения и недостатки представляют непосредственную угрозу безопасности и целостности информационных систем, обслуживаемых УЦ КЦМР, то план

устранения недостатков составляется и реализуется в месячный срок. Для менее серьезных нарушений и недостатков в результате оценки их значимости определяется комплекс мер, который может планомерно реализовываться в течение более длительного периода времени.

8.6. Обратная связь

О результатах устранения нарушений и недостатков, выявленных в ходе проверки Национального Банка, УЦ КЦМР информирует Национальный Банк Республики Казахстан в соответствии с нормативными правовыми актами Национального Банка.

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 и обновление сертификатов

Оплате подлежат услуги удостоверяющего центра, связанные с выпуском или 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 настоящем Положении о практике сертификатов, через хранилище или иными способами.

УЦ КЦМР не взимает плату за доступность доверяющим сторонам службы OCSP, указанной в настоящем Положении о практике 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. Страхование покрытия

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

УЦ КЦМР защищает известную ему конфиденциальную информацию от компрометации и разглашения третьим сторонам. Если уполномоченный посредник или центр регистрации владеет конфиденциальной информацией, то ответственность за ее разглашение возлагается на данного уполномоченного посредника в соответствии с заключенным им договором о сотрудничестве с удостоверяющим центром или договором о предоставлении услуг удостоверяющего центра.

9.4. Конфиденциальность персональных данных

9.4.1. План конфиденциальности

УЦ КЦМР в своей деятельности руководствуются действующим законодательством Республики Казахстан по вопросам защиты персональных данных. В частности, УЦ КЦМР не разглашают 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 онлайн-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 настоящего Положения о практике сертификатов означает их согласие на публикацию сведений, указываемых в сертификате.

9.4.4. Ответственность за защиту персональных данных

Все работники и подрядчики УЦ КЦМР, центры регистрации, 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, настоящим Положением о практике 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 о предоставлении услуг удостоверяющего центра. 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 настоящее Положение о практике 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 соответствующей Политики сертификатов и настоящего Положения о практике сертификатов;

соответствие сервисов отзыва сертификатов и использования хранилища требованиям действующего законодательства Республики Казахстан, существенным требованиям соответствующей Политики сертификатов и настоящего 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 настоящего Положения о практике сертификатов.

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

9.6.2. Гарантии и заверения центров регистрации

Центры регистрации обязаны выполнять условия гарантий и заверений подписчика и доверяющей стороны, изложенные в параграфах 9.6.3 и 9.6.4 настоящего Положения о практике 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 их работниками или подписчиками вследствие халатности;

подписчики указанных сертификатов ознакомлены с настоящим Положением о практике сертификатов, соответствующей ему Политикой сертификатов, и от них центром регистрации получено письменное обязательство выполнять требования и нести ответственность, предусмотренные этими документами для подписчиков и доверяющих сторон.

Договор о предоставлении услуг между удостоверяющим центром и центром регистрации может содержать дополнительные гарантии и заверения центра регистрации.

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 соответствующей Политики сертификатов и настоящего 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 настоящего Положения о практике сертификатов.

Договор подписчика с центром регистрации и/или 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 настоящего Положения о практике сертификатов.

Договор доверяющей стороны с центром регистрации и/или владельцем сертификата могут содержать дополнительные гарантии и заверения 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 настоящего Положения о практике 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 соответствующей Политикой сертификатов, настоящим Положением о практике сертификатов, и на них владельцем сертификатов возложены обязанности 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 настоящего Положения о практике 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 настоящего Положения о практике 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 настоящего Положения о практике сертификатов ограничивается суммой прямого ущерба, но не может превышать 200 (двухсот) месячных расчетных показателей.

Ответственность подписчиков перед участниками инфраструктуры открытых ключей в рамках настоящего Положения о практике 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 настоящего Положения о практике сертификатов ограничивается суммой прямого ущерба и не может превышать 100 (ста) месячных расчетных показателей.

Ответственность уполномоченных посредников перед участниками инфраструктуры открытых ключей в рамках настоящего Положения о практике сертификатов ограничивается суммой прямого ущерба и не может превышать 200 (двухсот) 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;

использование 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 соответствующей Политикой сертификатов и настоящим 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.

9.9.5. Возмещения центров регистрации

В части, не противоречащей действующему законодательству Республики Казахстан, центры регистрации 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 предоставлении услуг удостоверяющего центра с центром регистрации может содержать дополнительные обязательства центра регистрации о возмещениях удостоверяющему центру.

9.10. Вступление в силу и прекращение действия

9.10.1. Вступление в силу

Настоящее Положение о практике сертификатов вступает в силу с момента опубликования на интернет ресурсе УЦ КЦМР. Изменения и дополнения в настоящее

Положение о практике сертификатов также вступают в силу с момента опубликования на интернет ресурсе УЦ КЦМР.

9.10.2. Прекращение действия

Настоящее Положение о практике 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 настоящего Положения о практике сертификатов участники информационных систем, обслуживаемых КЦМР, остаются связанными его 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 Положение о практике сертификатов готовятся отделом удостоверяющего центра КЦМР и оформляются в виде отдельного документа, содержащего либо актуальный текст Положения, либо уведомление об изменениях и дополнениях в его актуальный текст.

Публикация актуальной редакции Положения о практике 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/StatementKISC.pdf>.

Отдел удостоверяющего центра РГП «КЦМР НБ РК» отвечает за определение необходимости изменения объектных идентификаторов соответствующей Политики сертификатов для приведения их в соответствие с измененным содержанием Положения.

9.12.2. Механизм и сроки уведомления

УЦ КЦМР оставляет за собой право без предварительного уведомления вносить несущественные изменения и дополнения в настоящее Положение о практике 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 настоящее Положение о практике сертификатов у участников обслуживаемых информационных систем. КЦМР предварительно публикует предлагаемые существенные изменения и дополнения к настоящему Положению о практике 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 Положение о практике 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 изменениям 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 действующее Положение о практике 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 Положение о практике сертификатов требуются немедленно в целях предотвращения нарушения безопасности обслуживаемых информационных систем, КЦМР вправе внести их путем утверждения и опубликования в хранилище, тем самым вводя в действие с момента опубликования.

9.12.3. Процедура изменения объектных идентификаторов

Если в связи с внесением изменений и дополнений в настоящее Положение о практике сертификатов КЦМР определил необходимость изменения объектных идентификаторов в соответствующей Политике сертификатов, новые объектные идентификаторы для каждого класса сертификатов должны быть указаны в актуальном тексте данной Политики, который должен быть введен в действие одновременно с изменениями и дополнениями в настоящее Положение.

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 настоящего Положения о практике сертификатов, является законодательство Республики Казахстан.

9.15. Юрисдикция

Юрисдикцией для настоящего Положения о практике 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 настоящего Положения о практике 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.

