Приложение №1 к Договору об организации защищенного
шифрованного соединения с использованием СКЗИ «Континент TLS VPN»

Регламент Удостоверяющего Центра ООО «НКО «Вестерн Юнион ДП Восток».

1. Введение

1.1. Краткий обзор

Настоящий документ определяет:

- регламент применения сертификатов ключей проверки электронной подписи (далее сертификатов), выпущенных удостоверяющим центром общества с ограниченной ответственностью «Небанковская кредитная организация «Вестерн Юнион ДП Восток» (далее Оператор), включая обязанности владельцев СКП;
- регламент работы сервисов удостоверяющего центра Оператора;
- принятые форматы данных и протоколы взаимодействия с удостоверяющим центром Оператора;
- основные организационно-технические мероприятия, необходимые для безопасной работы удостоверяющего центра Оператора.

Данный документ составлен с учетом нормативных документов Российской Федерации (см. Приложение 1) и в соответствии с рекомендациями RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. Структура Регламента соответствует рекомендациям RFC 3647, поэтому некоторые разделы могут состоять только из фразы «Нет условий», означающей, что Оператор не вводит каких-либо условий для данного раздела. Такая структура документа позволяет упростить понимание Регламента УЦ и сравнение его положений с положениями регламентов иных удостоверяющих центров.

1.2. Идентификация

Полное наименование документа: «Регламент применения сертификатов ключей проверки электронной подписи удостоверяющего центра общества с ограниченной ответственностью «Небанковская кредитная организация «Вестерн Юнион ДП Восток».

Сокращенное наименование документа: Регламент УЦ.

Текущая версия: 1.0

Дата издания: Январь 2016.

1.3. Участники ИОК

Инфраструктура открытых ключей Оператора включает в себя:

- Удостоверяющий центр (далее УЦ);
- Уполномоченное лицо УЦ;
- Администратора УЦ;
- владельцев сертификатов;
- пользователей сертификатов.

В состав УЦ входят:

- Корневой Центр Сертификации (далее Корневой ЦС);
- Выпускающий Центр Сертификации для сегмента. ru (далее Выпускающий ЦС сегмента. ru);
- Выпускающий Центр Сертификации для сегмента .net (далее Выпускающий ЦС сегмента .net);
- WEB-сервисы:
  - Веб-интерфейс Выпускающего ЦС сегмента. ru (далее Веб-интерфейс. ru);
  - Веб-интерфейс Выпускающего ЦС сегмента .net (далее Веб-интерфейс .net);
  - Точки распространения COC (далее CDP);
  - Веб-портал сегмента. ru (далее Веб-портал. ru);

- Веб-портал сегмента .net (далее Веб-портал .net);
- АРМ администрирования УЦ.

1.3.1. Корневой Центр Сертификации

Корневой ЦС предназначен для выпуска и обеспечения жизненного цикла сертификатов Выпускающего ЦС сегмента. ru и Выпускающего ЦС сегмента .net (далее Выпускающие ЦС).

Корневой ЦС расположен на автономном сервере и не взаимодействует ни с какими другими компонентами УЦ.

На Корневом ЦС находится эталонная база всех изготовленных сертификатов Выпускающих ЦС.

К функциям Корневого ЦС относятся:

- генерация ключей и сертификатов уполномоченного лица УЦ;
- смена ключей и сертификатов уполномоченного лица УЦ;
- выпуск сертификатов Выпускающим УЦ по запросам, полученным от Уполномоченного лица УЦ;
- ведение базы данных сертификатов Выпускающих ЦС;
- изменение базы данных сертификатов Выпускающих ЦС по запросам, полученным от Уполномоченного лица УЦ. Включает в себя выполнение следующих операций:
  - аннулирование (отзыв) сертификатов Выпускающих ЦС;
  - приостановление действия сертификатов Выпускающих ЦС;
  - возобновление действия сертификатов Выпускающих ЦС;
- формирование СОС по запросам Уполномоченного лица УЦ;
- ведение архива всех выпущенных СОС в автоматическом режиме;
- обеспечение уникальности следующей информации в сертификатах, Выпускающих ЦС:
  - ключ проверки электронной подписи;
  - серийный номер сертификата;
- протоколирование работы Корневого ЦС.

1.3.2. Выпускающий Центр сертификации сегмента. ru

Выпускающий ЦС сегмента. ru предназначен для выпуска и обеспечения жизненного цикла сертификатов российским кредитным организациям, являющимся операторами по переводу денежных средств, присоединившихся к Правилами Платежной Системы Вестерн Юнион (далее Правила) и оказывающая Услуги своим клиентам – физическим и юридическим лицам – в соответствии с законодательством Российской Федерации и Правилами (далее Участники).

Выпускающий ЦС сегмента. ru взаимодействует только со следующими серверами и АРМ по отдельному сегменту локальной сети с использованием защищенного сетевого протокола:

1. сервер, на котором развернут Веб-интерфейс. ru;
2. сервер, на котором развернут контроллер домена Оператора;
3. АРМ администрирования УЦ.

На Выпускающем ЦС сегмента. ru находится эталонная база всех изготовленных сертификатов Участников.

К функциям Выпускающего ЦС сегмента. ru относятся:

- генерация ключей Выпускающего ЦС сегмента. ru;
- формирование запросов на выпуск сертификата Выпускающего ЦС сегмента. ru для последующей обработки данного запроса на Корневом ЦС;

- выпуск сертификатов Участникам по запросам, поступившим через Веб-интерфейс. ru;
- ведение базы данных сертификатов Участников с предоставлением доступа к ней контроллеру домена Оператора;
- изменение базы данных сертификатов Участников по запросам, полученным от Администратора УЦ. Включает в себя выполнение следующих операций:
  - аннулирование (отзыв) сертификатов Участников;
  - приостановление действия сертификатов Участников;
  - возобновление действия сертификатов Участников;
- формирование СОС по запросам Администратора УЦ;
- формирование СОС в автоматическом режиме с периодичностью, заданной в расписании;
- ведение архива всех выпущенных СОС в автоматическом режиме;
- обеспечение уникальности следующей информации в сертификатах Участников:
  - ключ проверки электронной подписи;
  - серийный номер сертификата;
- протоколирование работы Выпускающего ЦС сегмента. ru.

1.3.3. Выпускающий Центр сертификации сегмента .net

Выпускающий ЦС сегмента .net предназначен для выпуска и обеспечения жизненного цикла сертификатов российским кредитным организациям, являющимся операторами по переводу денежных средств, присоединившихся к Правилами Платежной Системы Вестерн Юнион (далее Правила) и оказывающая Услуги своим клиентам – физическим и юридическим лицам – в соответствии с законодательством Российской Федерации и Правилами (далее Участники).

Выпускающий ЦС сегмента .net взаимодействует только со следующими серверами и АРМ по отдельному сегменту локальной сети с использованием защищенного сетевого протокола:

4. сервер, на котором развернут Веб-интерфейс .net;
5. сервер, на котором развернут контроллер домена Оператора;
6. АРМ администрирования УЦ.

На Выпускающем ЦС сегмента. ru находится эталонная база всех изготовленных сертификатов Участников.

К функциям Выпускающего ЦС сегмента. ru относятся:

- генерация ключей Выпускающего ЦС сегмента .net;
- формирование запросов на выпуск сертификата Выпускающего ЦС сегмента .net для последующей обработки данного запроса на Корневом ЦС;
- выпуск сертификатов Участникам по запросам, поступившим через Веб-интерфейс .net;
- ведение базы данных сертификатов Участников с предоставлением доступа к ней контроллеру домена Оператора;
- изменение базы данных сертификатов Участников по запросам, полученным от Администратора УЦ. Включает в себя выполнение следующих операций:
  - аннулирование (отзыв) сертификатов Участников;
  - приостановление действия сертификатов Участников;
  - возобновление действия сертификатов Участников;
- формирование СОС по запросам Администратора УЦ;
- формирование СОС в автоматическом режиме с периодичностью, заданной в расписании;
- ведение архива всех выпущенных СОС в автоматическом режиме;
- обеспечение уникальности следующей информации в сертификатах Участников:

- ключ проверки электронной подписи;
- серийный номер сертификата;

– протоколирование работы Выпускающего ЦС сегмента .net.

1.3.4. Веб-интерфейс Выпускающего ЦС для сегмента. ru

Веб-интерфейс. ru предназначен для выполнения формирования запросов на выпуск сертификатов Участниками.

Веб-интерфейс. ru взаимодействует с Выпускающим ЦС сегмента. ru по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

Веб-интерфейс. ru является точкой входа Участников, использующих для подключения к Платежной Системе Вестерн Юнион сеть общего пользования Интернет.

1.3.5. Веб-интерфейс Выпускающего ЦС для сегмента .net

Веб-интерфейс .net предназначен для выполнения формирования запросов на выпуск сертификатов Участниками.

Веб-интерфейс .net взаимодействует с Выпускающим ЦС сегмента .net по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

Веб-интерфейс .net является точкой входа Участников, использующих для подключения к Платежной Системе Вестерн Юнион выделенное сетевое подключение.

1.3.6. Веб-портал сегмента .ru

Веб-портал. ru предназначен для обеспечения доступа Участникам к репозиторию УЦ с помощью сети общего пользования Интернет (подробнее про репозиторий УЦ см. Раздел 2).

URL-адрес Веб-портала .ru в сети общего пользования Internet: https://gostca.westernunion.ru/

Комплексом организационно-технических мер обеспечивается требуемые показатели доступности Веб-портала. ru.

1.3.7. Веб-портал сегмента .net

Веб-портал .net предназначен для обеспечения доступа Участникам к репозиторию УЦ с помощью выделенного сетевого подключения (подробнее про репозиторий УЦ см. Раздел 2).

URL-адрес Веб-портала .net в сети общего пользования Internet: https://gostca.westernunion.ru/

Комплексом организационно-технических мер обеспечивается требуемые показатели доступности Веб-портала. net.

1.3.8. АРМ администрирования УЦ

АРМ администрирования УЦ предназначен для выполнения Администратором УЦ организационно-технических мероприятий, связанных с выполнением процедур управления жизненным циклом Участников.

АРМ администрирования УЦ взаимодействует с Выпускающим ЦС сегмента .ru, Выпускающим ЦС сегмента .net (далее Выпускающие ЦС), а так же с Веб-интерфейсом .ru и Веб-интерфейсом .net (далее Веб-интерфейсы) по протоколу HTTP(S) с односторонней аутентификацией.

К основным функциям АРМ администрирования УЦ относятся:

– обеспечение взаимодействия Администратора УЦ с Выпускающими ЦС и Веб-интерфейсами;
– обеспечение возможности проверки и одобрения запроса на выпуск сертификатов Участников, поступающих от Участников через Веб-интерфейс .ru или Веб-интерфейс .net (далее Веб-интерфейсы);

- организация просмотра информации из Базы Данных Выпускающего ЦС, относящейся к Участнику, зарегистрированному в УЦ;
- распечатка сертификатов Участников на бумажном носителе;
- создание запросов на отзыв сертификатов Участников;
- создание запросов на приостановление действия сертификатов Участников;
- создание запросов на возобновление действия сертификатов Участников;
- распечатка сертификатов Корневого ЦС и Выпускающих ЦС на бумажном носителе;
- сохранение СОС на отчуждаемом носителе в виде файла;
- сохранение сертификатов Корневого ЦС и Выпускающих ЦС на отчуждаемом носителе в виде файла;
- просмотр журналов Выпускающих ЦС и Веб-интерфейсов;
- публикация СОС Выпускающих ЦС.

1.3.9. Уполномоченное лицо УЦ

Сотрудник Оператора, наделенный правами и обязанностями по выполнению процедур управления жизненным циклом (выпуск, приостановка действия, возобновление действия и отзыв) сертификатов Выпускающих УЦ. Уполномоченное лицо УЦ имеет доступ к закрытому ключу Корневого ЦС и использует этот ключ для формирования электронной подписи на сертификатах, Выпускающих ЦС и СОС Корневого ЦС.

1.3.10. Владелец сертификата

Владельцем сертификата является Участник, на имя которого выпущен сертификат.

1.3.11. Пользователи сертификатов

Пользователями сертификатов являются субъекты, применяющие выпущенные согласно настоящему Регламенту УЦ сертификаты, и которые действуют, доверяя сертификату Корневого ЦС и/или любой ЭП Уполномоченного лица ЦС.

1.4. Использование сертификатов

1.4.1. Допустимое использование

Сертификаты, которые выпускаются Выпускающими ЦС, могут быть использованы только в следующих целях:

1. аутентификация Участников при подключении к Платежной Системе Вестерн Юнион;
2. шифрование канала передачи данных между Участником и Платежной Системой Вестерн Юнион.

1.4.2. Запрещенное использование

Запрещается использовать сертификаты в целях, не указанных в п. 1.4.1. настоящего Регламента.

1.5. Управление регламентом

1.5.1. Организация, управляющая Регламентом УЦ

ООО «НКО «Вестерн Юнион ДП Восток»
125171, г. Москва, Ленинградское шоссе, д. 16а, строение 1
Телефон/факс: +7 495 797-2195
url: www.westernunion.ru
e-mail: Moscow.infosec@westernunion.com

1.5.2. Контактное лицо

Менеджер Регламента УЦ - Руководитель органа криптографической защиты информации ООО «НКО «Вестерн Юнион ДП Восток».

1.5.3. Лицо, определяющее соответствие Регламента УЦ политикам применения сертификатов

Соответствие Регламента УЦ политикам применения сертификатов определяет Менеджер Регламента УЦ.

1.5.4. Процедура утверждения Регламента УЦ

Исправления и дополнения настоящего Регламента осуществляются Менеджером Регламента УЦ.

Утверждение настоящего Регламента осуществляются Президентом ООО «НКО «Вестерн Юнион ДП Восток».

Исправления и/или дополнения Регламента УЦ публикуются в Репозитории УЦ в виде исправленной и/или дополненной новой версии документа.

1.6. Определения и акронимы

1.6.1. Определения

Аутентификация — процесс, устанавливающий, что субъект является тем за кого себя выдает.

Данные активации — закрытые данные, отличные от ключей, требуемые для управления ключевым носителем.

Домен доверия — несколько доменов ИОК, между которыми установлены отношения доверия. В частном случае один домен ИОК так же является доменом доверия.

Домен ИОК — совокупность субъектов ИОК, в вершине цепочки сертификации которых находится один и тот же Центр сертификации.

Ключ электронной подписи — уникальная последовательность символов, предназначенная для создания электронной подписи.

Заявитель — Участник, подписавший со своей стороны Заявление о присоединении к «Регламенту применения сертификатов ключей проверки электронной подписи удостоверяющего центра общества с ограниченной ответственностью «Небанковская кредитная организация «Вестерн Юнион ДП Восток» и подавший заявление на выпуск сертификата.

Идентификация — процесс, устанавливающий однозначное соответствие субъекта отличительным признакам.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Инфраструктура открытых ключей или (ИОК) — архитектура, организация, методики, способы и процедуры, которые обеспечивают управление и применение криптографической системы, основанной на сертификатах ключей проверки электронной подписи.

Участник – российская кредитная организация, являющаяся оператором по переводу денежных средств, присоединившаяся к Правилам Платежной Системы Вестерн Юнион и оказывающая Услуги своим клиентам – физическим и юридическим лицам – в соответствии с законодательством Российской Федерации и Правилами.

Ключевая пара - ключ электронной подписи и соответствующий ему ключ проверки электронной подписи.

Компрометация ключа электронной подписи – результат действий физического лица, повлекший за собой разглашение ключа электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Политика применения сертификатов (Certificate Policy) или ППС — набор правил, определяющий использование сертификата некоторым сообществом и/или классом приложений с заданными требованиями безопасности.

Пользователь — субъект, применяющий выпущенный согласно настоящему Регламенту УЦ сертификат, и который действует доверяя этому сертификату и/или любой ЭП проверенной с использованием этого сертификата.

Правила - Правила Платежной Системы Вестерн Юнион.

Путь (цепочка) сертификации — упорядоченная последовательность сертификатов, которая может быть обработана вместе с ключом проверки электронной подписи начального объекта для признания ключа проверки электронной подписи конечного объекта.

Регламент удостоверяющего центра (Certification Practice Statement) или Регламент УЦ — это документ, содержащий описание процедур и действий, которые УЦ использует при выпуске, управлении, отзыве и обновлении сертификатов.

Сертификат ключа проверки электронной подписи (Сертификат) - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Список аннулированных (отозванных) сертификатов или СОС - электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, содержащий список серийных номеров сертификатов, которые в определенный момент времени были отозваны, либо действие которых было приостановлено. Сертификаты, чьи номера присутствуют в списке файла СОС, являются отозванными из обращения Удостоверяющим центром.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Электронный документ - форма подготовки, отправления, получения или хранения информации с помощью электронных технических средств, зафиксированная на магнитном диске, магнитной ленте, лазерном диске и ином электронном материальном носителе.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

PKCS#10 (RFC 2986) – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.

Terminal ID -

1.6.2. Акронимы

CDP CRL Distribution Point (Точка доступа к СОС);
CRL Certificate Revocation List (Список аннулированных (отозванных) сертификатов);
PKCS Public-Key Cryptography Standard;
PKI Public Key Infrastructure (Инфраструктура ключа проверки электронной подписи);
RFC Request For Comments;
DN Distinguished Name (Отличительное имя);

ИОК Инфраструктура открытых ключей;
ПО Программное обеспечение;
СОС Список аннулированных (отозванных) сертификатов;
СКЗИ Средства криптографической защиты информации;
УЦ Удостоверяющий центр;
ЦС Центр сертификации;
ЭП Электронная подпись.

2. Публикация и ответственность за актуальность информации в репозитории

2.1. Репозиторий

УЦ поддерживает в актуальном состоянии репозиторий. В качестве репозитория используются выделенные директории на Веб-портале. ru и Веб-портале .net.

2.2. Публикация информации

Публикации подлежит:
- сертификат Корневого ЦС;
- сертификаты центров сертификации Выпускающих ЦС;
- списки аннулированных сертификатов Корневого ЦС и Выпускающих ЦС;
- Регламент УЦ;
- шаблон заявления на выпуск сертификата;
- шаблон заявления о присоединении к Регламенту УЦ;
- шаблон соглашения с пользователем;
- сведения об аттестации и аккредитации УЦ;
- сопутствующая информация, уведомления, обновления и исправления.

2.3. Время и частота публикаций

Публикация информации осуществляется, как только она становится доступной и с частотой необходимой для поддержания ее в актуальном состоянии.

2.4. Управление доступом к репозиториям

Вся публикуемая информация является общедоступной для пользователей сертификатов. Администратор УЦ использует различные механизмы для предотвращения неавторизованного изменения, дополнения и/или удаления опубликованной информации.

3. Идентификация и аутентификация

3.1. Присваивание имен

3.1.1. Типы имен

В качестве имени в сертификате используется отличительное имя согласно стандарту X.500.

3.1.2. Требования к интерпретации имен

Имена, содержащиеся в сертификатах, однозначно идентифицируют субъектов (владельцев сертификатов). В качестве имени в сертификате указывается Terminal ID владельца сертификата.

3.1.3. Анонимные или владельцы с псевдонимами

Выпуск сертификатов для анонимных владельцев недопустим. Использование псевдонимов разрешено.

3.1.4. Правила интерпретации различных форм имен

Нет условий.

3.1.5. Уникальность имен

Возможно существование нескольких сертификатов с одинаковыми отличительными именами, владельцем которых является один и тот же Участник. При этом УЦ гарантирует уникальность издаваемых сертификатов.

3.1.6. Признание, аутентификация и роль торговых марок

Нет условий.

3.2. Первоначальное подтверждение подлинности

3.2.1. Метод доказательства обладания ключом электронной подписи

Методом доказательства обладания ключом электронной подписи являться криптографическая демонстрация эквивалентности или документальное подтверждение обладания ключом электронной подписи.

Если ключевая пара создается с помощью Веб-интерфейса, то доказательство не требуется.

3.2.2. Проверка идентификационной информации организации

Проверка идентификационной информации организации (Заявителя) проводится в порядке, предусмотренным в Правилах.

3.2.3. Проверка личной идентификационной информации

Нет условий.

3.2.4. Непроверяемая информация

Сертификат не может содержать непроверяемую информацию.

3.2.5. Проверка полномочий

Нет условий.

3.2.6. Критерии взаимодействия с другими УЦ

Нет условий.

3.3. Аутентификация и идентификация при обновлении ключей

3.3.1. Аутентификация и идентификация при плановой замене ключей

Аутентификация и идентификация субъекта при плановой замене ключей осуществляется по действительному сертификату, либо по документально подтвержденному запросу на выпуск нового сертификата.

3.3.2. Аутентификация и идентификация при обновлении ключей после отзыва

Аутентификация и идентификация субъекта при обновлении ключей после отзыва осуществляется по документально подтвержденному запросу на выпуск нового сертификата.

3.4. Аутентификация и идентификация при подаче запроса на отзыв

Аутентификация и идентификация субъекта в случае подачи запроса на отзыв может осуществляться по действительному сертификату, либо по документально подтвержденному запросу на отзыв сертификата.

4. Функциональные требования жизненного цикла сертификата

В настоящем разделе описываются условия и порядок представления услуг удостоверяющим центром Участникам, права, обязательства и ответственность удостоверяющего центра и владельцев сертификатов.

Удостоверяющий центр предоставляет Участникам следующие виды услуг:

- внесение в реестр Удостоверяющего центра регистрационной информации об Участнике;
- создание (выпуск) сертификатов в электронной форме;
- изготовление копии сертификатов на бумажном носителе;
- ведение реестра изготовленных Удостоверяющим центром сертификатов;
- предоставление сертификатов в электронной форме из реестра изготовленных сертификатов, по запросам пользователей;
- аннулирование (отзыв) сертификатов по обращениям владельцев сертификатов;
- приостановление и возобновление действия сертификатов по обращениям владельцев сертификатов;
- предоставление пользователям сведений об аннулированных (отозванных) сертификатах и сертификатах с приостановленным сроком действия;
- подтверждение подлинности электронной подписи уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах по запросу пользователей;
- распространение средств электронной подписи.

4.1. Заявление на выпуск сертификат

4.1.1. Кто может подать заявление на выпуск сертификата

Заявление на выпуск сертификата может подать Участник.

4.1.2. Процесс регистрации и требования

Процесс регистрации Участника состоит из следующих процедур:

- регистрация Заявителя в предусмотренном Правилами порядке;
- подписание Заявителем со своей стороны Договора о присоединении к Регламенту УЦ и заявления на выпуск сертификата;
- регистрация Заявителя в реестре Выпускающего центра Администратором УЦ.

4.1.3. Перечень документов, представленных Заявителем для проведения процедуры его регистрации

Заявитель, желающий пройти процедуру регистрации в Удостоверяющем центре, должен предоставить:

- подписанный со своей стороны Договор о присоединении к Регламенту УЦ;
- подписанное со своей стороны заявление на выпуск сертификата;
- адрес электронной почты;

- контактные телефоны;
- данные для удаленной идентификации владельца сертификата (ключевая фраза длиной до 64 символов).

Если от имени Заявителя действует физическое лицо, наделенное полномочиями представлять интересы Заявителя, то дополнительно к вышеуказанному перечню требуется представить:

- доверенность на предоставление документов, необходимых для выпуска сертификата.

4.2. Обработка заявления на выпуск сертификата

4.2.1. Выполнение функций аутентификации и идентификации

Аутентификация и идентификация осуществляется в соответствии с требованиями раздела 3.2. настоящего Регламента.

4.2.2. Принятие или отклонение заявления навыпуск сертификата

УЦ может отклонить заявление на выпуск сертификата в следующих случаях:

- заявление на выпуск сертификата было передано способом, не соответствующим требованиям Регламента УЦ, или в не соответствующем формате;
- данные, указанные в заявлении не соответствуют действительности;
- данные, указанные в заявлении не подтверждены соответствующими документами;
- Заявитель не подтвердил факт обладания ключом подписи;
- Заявитель нарушил каким-либо образом Договор о присоединении к Регламенту УЦ;
- Заявитель не прошел процедуру аутентификации и идентификации.

Заявление на выпуск сертификата принимается, если отсутствуют вышеперечисленные причины для его отклонения.

4.2.3. Срок обработки заявления на выпуск сертификата

Администратор УЦ должен начать обработку заявления на выпуск сертификата в течение одного рабочего дня с момента его получения. Однако настоящий Регламент УЦ не устанавливает ограничения времени обработки заявления, если таковое не содержится в соглашении между сторонами. Заявление считается активным до момента его принятия или отклонения.

Временем передачи заявления считается:

- при вручении лично – время вручения;
- при передаче по электронной почте – время передачи сообщения на почтовый сервер Оператора;
- при передаче иным способом - время получения заявления Администратором УЦ.

После рассмотрения заявления на выпуск сертификата Администратор УЦ должен вынести решение о его принятии, либо отклонении, о чем Заявитель должен быть проинформирован.

4.3. Выпуск сертификата

4.3.1. Действия удостоверяющего центра во время выпуска сертификата

УЦ выпускает сертификаты по одобренным заявлениям. Сертификат выпускается в соответствии с настоящим Регламентом УЦ и информацией указанной в заявлении.

Выпуск сертификата для Участника осуществляется в соответствии со следующим алгоритмом действий:

- Заявитель формирует ключевую пару собственными средствами или с помощью Веб-интерфейса;

- Заявитель формирует запрос на выпуск сертификата с помощью Веб-интерфейса Заявителем;
- Администратор УЦ проверяет обладание Заявителем закрытом ключом в случае формирования ключевой пары собственными средствами Заявителя;
- Администратор УЦ выпускает сертификат в электронном виде на основании запроса Заявителя и изготавливает его дубликат на бумажном носителе.

4.3.2. Оповещение Заявителя о выпуске сертификата

УЦ оповещать Заявителя о выпуске сертификата по телефону или электронной почте. Заявитель так же может проверить состояние запроса на выпуск сертификата с помощью Веб-интерфейса.

4.4. Признание сертификата

4.4.1. Действия по признанию сертификата

Признанием сертификата является следующие действия Заявителя:

- использование сертификата Заявителем.

Кроме того, если УЦ не получает в течение 1 рабочего дня уведомления от Заявителя об отклонении сертификата, сертификат так же считается признанным.

4.4.2. Публикация сертификата удостоверяющим центром

УЦ не публикует выпущенные сертификаты Участников.

4.4.3. Уведомление третьей стороны о выпуске сертификата удостоверяющим центром

Нет условий.

4.5. Использование сертификата и ключевой пары

4.5.1. Использование сертификата и ключевой пары владельцем

Владелец сертификата может использовать собственный сертификат после его признания и в соответствии с требованиями Регламента УЦ и иных руководящих документов. Владелец сертификата должен защищать ключ электронной подписи от компрометации.

4.5.2. Использование сертификата и ключа проверки электронной подписи пользователями

Перед использованием сертификата пользователь обязан:

- ознакомиться с Регламентом УЦ, в соответствии с которым выпущен сертификат;
- проверить статус используемого сертификата и сертификата УЦ.

Пользователь может использовать только действительный сертификат.

4.6. Обновление сертификата

Обновление сертификата является выпуском нового сертификата без изменения ключа проверки электронной подписи или другой информации в сертификате.

4.6.1. Обстоятельства обновления сертификата

УЦ не осуществляет обновление сертификатов.

4.6.2. Кто может подать запрос на обновление сертификата

Нет условий.

4.6.3. Обработка запросов на обновление сертификатов

Нет условий.

4.6.4. Оповещение клиента о выпуске нового сертификата

Нет условий.

4.6.5. Действия по признанию обновленного сертификата

Нет условий.

4.6.6. Публикация обновленного сертификата администратором Сервера безопасности

Нет условий.

4.6.7. Уведомление третьей стороны о выпуске сертификата Удостоверяющим центром

Нет условий.

4.7. Обновление ключей

Данный раздел описывает выпуск нового сертификата в случае обновления ключей.

4.7.1. Обстоятельства обновления ключей

Обновление ключей возможно в случае компрометации ключа электронной подписи, а так же в случае истечения срока действия сертификата. Генерация ключей совершается владельцем сертификата собственными средствами или с помощью Веб-интерфейса.

4.7.2. Кто может подать заявление на выпуск сертификата при обновлении ключей

Запрос на выпуск сертификата при обновлении ключей может подать владелец сертификата.

4.7.3. Обработка заявления на выпуск сертификата при обновлении ключей

Одобрение запроса на выпуск сертификата при обновлении ключей осуществляется в соответствии с подразделом 4.2. а выпуск сертификата в соответствии с пунктом 4.3.1.

4.7.4. Оповещение владельца о выпуске нового сертификата

Оповещение выполняется в соответствии с пунктом 4.3.2.

4.7.5. Действия по признанию нового сертификата при обновлении ключей

Признание осуществляется в соответствии с пунктом 4.4.1.

4.7.6. Публикация удостоверяющим центром нового сертификата при обновлении ключей

Публикация осуществляется в соответствии с пунктом 4.4.2.

4.7.7. Уведомление третьей стороны о выпуске удостоверяющим центром нового сертификата при обновлении ключей

Нет условий.

4.8. Изменение сертификата

Изменение сертификата является выпуском нового сертификата при необходимости изменения информации, включенной в существующий сертификат. При этом старый сертификат отзывается.

4.8.1. Обстоятельства изменения сертификата

Изменение сертификата производится в случае, если информация, содержащаяся в сертификате, становится не актуальной или при ее внесении в сертификат была допущена ошибка.

4.8.2. Кто может подать заявление на изменение сертификата

Заявление на изменение сертификата может подать владелец сертификата.

4.8.3. Обработка заявления изменение сертификата

Одобрение заявления на обновление сертификата при обновлении ключей осуществляется в соответствии с подразделом 4.2. а выпуск сертификата в соответствии с разделом 4.3.1.

4.8.4. Оповещение владельца о выпуске нового сертификата

Оповещение выполняется в соответствии с пунктом 4.3.2.

4.8.5. Действия по признанию измененного сертификата

Признание осуществляется в соответствии с пунктом 4.4.1.

4.8.6. Публикация измененного сертификата удостоверяющим центром

Публикация осуществляется в соответствии с пунктом 4.4.2.

4.8.7. Уведомление третьей стороны о выпуске измененного сертификата удостоверяющим центром

Нет условий.

4.9. Отзыв и приостановление сертификата

По истечении срока действия сертификата сертификат автоматически считается недействительным. Сертификат считается аннулированным (отозванным), приостановленным или возобновленным с момента публикации в репозитории УЦ списка аннулированных сертификатов, содержащего информацию об изменении статуса этого сертификата.

4.9.1. Обстоятельства отзыва сертификата

Сертификат может быть отозван при следующих обстоятельствах:

- при компрометации ключа электронной подписи;
- при разрыве или несоблюдении соглашений между Оператором и Участником;
- при несоблюдении владельцем сертификата требований настоящего Регламента УЦ;
- при прекращении деятельности УЦ;
- по запросу владельца сертификата.

4.9.2. Кто имеет право подать заявление на отзыв сертификата

Заявление на отзыв сертификата может быть подано:

- владельцем сертификата;
- Администратором УЦ, если он располагает достоверной информацией, требующей отзыва сертификата.

4.9.3. Процедура рассмотрения заявления на отзыв сертификата

Заявление на отзыв может быть подано в бумажной или электронной форме, либо с использованием любых средств связи, но в любом случае с аутентификацией согласно подразделу 3.4.

Заявление должно содержать следующую информацию:

- серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат;
- причину отзыва сертификата;
- необходимые комментарии.

После получения заявления от владельца сертификата Администратор УЦ производит верификацию запроса, и если таковая прошла успешно, то производит отзыв сертификата. После отзыва сертификата УЦ публикует в репозитории обновленный СОС, содержащий информацию об отозванном сертификате.

4.9.4. Срок передачи заявления на отзыв сертификата

Заявление на отзыв должно быть передано непосредственно после наступления обстоятельств отзыва сертификата.

4.9.5. Срок, за который удостоверяющий центр должен обработать заявление на отзыв сертификата

Заявление на отзыв сертификата рассматривается в течение 1 рабочего дня с момента его подачи. Временем подачи запроса считается:

- при передаче по электронной почте – время передачи сообщения на почтовый сервер УЦ;
- при вручении лично или передачей иными способами – время получения заявления на отзыв Администратором УЦ.

4.9.6. Требования к пользователям по проверке статуса сертификата

Пользователь сертификата обязан проверять его статус перед каждым использованием, используя СОС, публикуемые УЦ.

4.9.7. Частота выпуска списка аннулированных сертификатов

УЦ публикует актуальные СОС с частотой 12 часов.

Если срок действия сертификата, включенного в список аннулированных сертификатов, истекает, то он может быть удален из него после истечения срока действия сертификата.

4.9.8. Максимальное время задержки публикации списка аннулированных сертификатов

Максимальное время задержки публикации СОС составляет 5 часов.

4.9.9. Доступность онлайновой проверки отзыва/статуса сертификата

УЦ не предоставляет сервис онлайновой проверки статуса сертификата.

4.9.10. Требования к онлайновой проверке отзыва

Нет условий.

4.9.11. Другие доступные формы извещения об отзыве

Не обязательны.

4.9.12. Специальные требования, относящиеся к компрометации ключей

В случае компрометации ключа электронной подписи уполномоченного лица УЦ или ключей электронной подписи центров сертификации Выпускающих ЦС владельцы сертификатов оповещаются посредством рассылки соответствующих email-сообщений.

4.9.13. Обстоятельства приостановления действия сертификата

Действие сертификата может быть приостановлено при следующих обстоятельствах:

- по заявлению владельца сертификата;
- возникновения какого-либо разбирательства, не позволяющего на текущий момент принять решение о действительности сертификата.

4.9.14. Кто может подать заявление на приостановление действия сертификата

Заявление на приостановление действия сертификата может быть подано:

- владельцем сертификата;
- Администратором УЦ, если он располагает достоверной информацией, требующей приостановления действия сертификата.

4.9.15. Процедура рассмотрения заявления на приостановление действия сертификата

Процедура рассмотрения заявления на приостановление действия сертификата аналогична процедуре рассмотрения заявления на отзыв сертификата, приведенной в п.4.9.3.

4.9.16. Ограничение на срок приостановления действия сертификата

Ограничение на срок приостановления действия сертификата не устанавливается.

4.9.17. Обстоятельства возобновления действия сертификата

Действие сертификата может быть возобновлено:

- по заявлению владельца сертификата;
- по решению УЦ.

4.9.18. Кто может подать заявление на возобновление действия сертификата

Запрос на возобновление действия сертификата может быть подан:

- владельцем сертификата;
- Администратором УЦ, если он располагает достоверной информацией, требующей возобновления действия сертификата, либо информацией об отсутствии причин для дальнейшего приостановления действия или отзыва сертификата.

4.9.19. Процедура рассмотрения заявления на возобновление сертификата

Заявление на возобновление действия сертификата может быть подано в бумажной или электронной форме, либо с использованием любых средств связи, но в любом случае с аутентификацией согласно подразделу 3.4.

Заявление должно содержать серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат.

После получения заявления Администратор УЦ производит верификацию заявления, и если таковая прошла успешно, то производит возобновление действия сертификата. После возобновления действия сертификата владелец такового уведомляется, а СОС, не содержащий информацию о приостановлении действия сертификата, публикуется.

Заявление рассматривается в течение 1 рабочего дня с момента его подачи. Временем подачи заявления считается:

- при передаче по электронной почте – время передачи сообщения на почтовый сервер УЦ;
- при вручении лично или передачей иными способами – время получения заявления Администратором УЦ.

4.10. Сервис статуса сертификата

4.10.1. Эксплуатационные характеристики

Проверка статуса сертификатов возможна путем использования СОС, доступных в репозитории УЦ при помощи протокола HTTP.

УЦ публикует СОС по следующим URL-адресам:

https://gostca.westernunion.ru/download/ca1_wumte.crl

https://gostca.westernunion.net/download/ca1_wumte.crl

Доступность сервиса

Комплексом организационно-технических мер обеспечивается требуемые показатели доступности СОС.

4.10.2. Дополнительные возможности

Не предусмотрено.

4.11. Прекращение использования услуг

Участник может отказаться от услуг УЦ следующим образом:

- отказавшись от обновления сертификата по истечению срока его действия;
- подав заявление на отзыв своего сертификата до истечения срока действия без выдачи нового.

4.12. Депонирование и возврат ключей

УЦ не осуществляет депонирование и возврат ключей.

4.12.1. Методы и политика депонирования и возврат ключей

Не предусмотрено.

4.12.2. Методы и политика инкапсуляции и восстановления сессионного ключа

Не предусмотрено.

5. Организационные, эксплуатационные и физические меры обеспечения безопасности

В настоящем разделе описываются меры защиты информационных ресурсов УЦ, порядок эксплуатации средств защиты, а также порядок действий обслуживающего персонала УЦ.

5.1. Физические меры обеспечения безопасности

Физические меры обеспечения безопасности определяются договором аренды нежилых помещений, предусматривающим наличие поста охраны при входе в здание, в котором расположены арендуемые помещения.

5.1.1. Размещение и организация рабочей площадки

Все компоненты УЦ находятся в специализированных помещениях с ограниченным доступом, оборудованных для предотвращения и определения не авторизованного доступа, использования или раскрытия конфиденциальной информации.

5.1.2. Физический доступ

Физический доступ к компонентам УЦ защищен как минимум двумя уровнями доступа. На каждом уровне доступа осуществляется проверка разрешения на доступ.

5.1.3. Электропитание

Аппаратное обеспечение УЦ обеспечено источниками бесперебойного электропитания, обеспечивающими их штатное функционирование.

5.1.4. Кондиционирование и влажность

Требования по кондиционированию и влажности в помещениях соответствуют техническим условиям эксплуатации аппаратного обеспечения.

5.1.5. Пожарная безопасность

Меры пожарной безопасности соответствуют требованиям руководящего документа «Пожарная охрана предприятий. Общие требования».

5.1.6. Хранение носителей информации

Вся информация, подлежащая архивному хранению хранится в специально оборудованном архивохранилище, доступ к которому имеет ограниченный круг лиц.

5.1.7. Уничтожение информации

Все носители информации, содержащие важную информацию, после окончания срока хранения подлежат уничтожению путем физического уничтожения носителей информации.

5.1.8. Внешнее архивное хранение

Не предусмотрено.

5.2. Процессуальные меры обеспечения безопасности

5.2.1. Доверенные роли

Доверенные роли представлены как минимум следующими ролями:

- уполномоченное лицо УЦ;
- системный администратор УЦ;
- Администратор УЦ;
- администратор безопасности УЦ.

5.2.2. Количество сотрудников, требуемое для выполнения операций

Все операции, за исключением генерации ключей уполномоченного лица УЦ (ключи ЦС), могут выполняться в индивидуальном порядке и не требуют коллегиальности. Для генерации ключей Корневого ЦС и ключей центров сертификации Выпускающих ЦС необходимо участие как минимум двух сотрудников, обладающих доверенными ролями.

5.2.3. Идентификация и аутентификация для каждой роли

Первичная аутентификация и идентификация сотрудника осуществляется при приеме на работу с использованием общепринятых документов удостоверяющих личность. Доступ к программно-аппаратному обеспечению осуществляется в соответствии с полученной ролью. Аутентификация и идентификация должностных лиц производится с использованием программно-аппаратных средств аутентификации.

5.2.4. Роли, требующие разделения обязанностей

Роль администратора безопасности УЦ не может быть объединена ни с одной из ролей.

5.3. Управление персоналом

5.3.1. Требования к квалификации, опыту и допуску к секретным материалам

К персоналу, выполняющему доверенные роли, как минимум предъявляются следующие требования:

- лояльность;
- понимание и соблюдение политик безопасности;
- необходимая подготовка для выполнения своих обязанностей.

5.3.2. Процедуры проверки на соответствие общим требованиям

При назначении сотруднику доверенной роли он проходит процедуру проверки в соответствии требованиям раздела 5.3.1.

5.3.3. Требования к профессиональной подготовке

Программа подготовки сотрудников включает следующее:

- концепция PKI, в объемах необходимых для выполнения служебных обязанностей;
- должностные обязанности;
- политики и процедуры безопасности и деятельности Оператора;
- использование и эксплуатация развернутого аппаратного и программного обеспечения.

5.3.4. Требования и частота переподготовки

Переподготовка персонала осуществляется в объемах и с частотой, необходимых для поддержания и совершенствования сотрудниками их квалификации и успешного выполнения функциональных обязанностей.

5.3.5. Частота и последовательность кадровых перемещений

Нет условий.

5.3.6. Санкции за неправомочные действия

Любые неправомочные действия персонала влекут за собой санкции в соответствии с действующим законодательство Российской Федерации.

5.3.7. Требования для независимых подрядчиков

Привлечение независимых подрядчиков к выполнению доверенных ролей не допускается.

5.3.8. Обеспечение персонала документацией

УЦ обеспечивает своих сотрудников необходимой документацией для успешного выполнения их должностных обязанностей.

5.4. Процедуры регистрации событий

5.4.1. Типы регистрируемых событий

Регистрации подлежат следующие типы событий:

- события жизненного цикла ключей УЦ, включая генерацию, резервное копирование, восстановление, архивацию и уничтожение;
- события жизненного цикла сертификатов Участников, включая:
  - прием и результаты обработки всех видов заявлений, предусмотренных настоящим Регламентом УЦ;
  - выпуск, приостановление действия, возобновление действия, отзыв сертификатов;
  - выпуск и публикация СОС;

- события, влияющие на безопасность:
  - все неудачные попытки выполнить какие-либо действия с компонентами УЦ;
  - попытки доступа к компонентам УЦ каким-либо образом;
  - аварии программно-аппаратного обеспечения УЦ и другие аномалии;
  - изменение профилей защиты компонент УЦ;
  - изменения в работе межсетевых экранов.

Запись о регистрации события должна содержать следующую информацию:

- дата и время события;
- кто создал запись;
- тип события.

5.4.2. Частота обработки журналов регистрации событий

Файлы аудита проверяются администратором безопасности УЦ не реже одного раза в неделю. Так же журналы аудита просматриваются в случаях подозрительной или необычной активности, а так же при возникновении критических ситуаций. Обработка журналов аудита должна включать просмотр событий и верификацию того, что записи в журналах не были изменены или подделаны.

5.4.3. Срок хранения журналов регистрации событий

Минимальный срок хранения журналов аудита составляет 1 месяц.

5.4.4. Защита журналов регистрации событий

Доступ к журналам регистрации имеют:

- Системный администратор;
- Администратор УЦ;
- Администратор безопасности.

Журналы аудита защищаются системой регистрации событий от неавторизованного доступа, модификации, изменения, удаления или порчи.

5.4.5. Процедуры резервного копирования журналов регистрации событий

Резервное копирование журналов регистрации событий осуществляется в соответствии с общими процедурами резервного копирования, принятыми Оператором.

5.4.6. Система регистрации событий

Данные об автоматически регистрируемых событиях записываются приложениями и операционными системами. Данные о событиях, регистрируемых вручную, записываются персоналом УЦ.

5.4.7. Оповещение субъекта, явившегося причиной события

Не производится.

5.4.8. Оценка уязвимости

Оценка уязвимости систем производится в ходе проведения обработки журналов регистрации событий.

5.5. Архивные записи

5.5.1. Состав архивируемой информации

Обязательному архивному хранению подлежит:

- все виды заявлений, предусмотренных настоящим Регламентом УЦ и сопутствующая информация;

- выпущенные сертификаты Корневого УЦ, центров сертификации Выпускающих УЦ, Участников;
- журналы регистрации событий;
- реестр выпущенных СОС;
- документация удостоверяющего центра;
- внутренняя и внешняя корреспонденция персонала УЦ.

5.5.2. Срок хранения архивной информации

Для архивной информации минимальный срок хранения равен 5 годам.

После окончания срока хранения информация уничтожается путем физического уничтожения носителей информации. Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа персонала УЦ и назначаемой приказом руководителя Оператора.

5.5.3. Защита архива

Архивные документы и информация на отчуждаемых носителях хранятся в специально оборудованном помещении – архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации. Защита от модификации, удаления и разглашения архивной информации осуществляется методами и средствами ограничения доступа.

5.5.4. Процедура резервного копирования архива

Нет условий.

5.5.5. Требования к штампу времени архивных записей

Не предусмотрено.

5.5.6. Система архивного хранения

Применяется внутренняя система архивного хранения.

5.5.7. Процедура получения и верификации архивной информации

Доступ к архиву разрешен только сотрудникам, обладающим доверенной ролью. Доступ иным субъектам разрешается только по решению руководителя Оператора. При получении информации производится контроль ее целостности.

5.6. Замена ключей

УЦ при плановом обновлении ключевых пар компонент УЦ должен осуществить данную процедуру прозрачно для владельцев и пользователей сертификатов и без нарушения работоспособности системы.

5.7. Восстановление при компрометации и аварии

5.7.1. Действия при происшествии и компрометации

Все участники ИОК должны быть оповещены в случаях компрометации ключей электронной подписи компонент УЦ (Корневой ЦС, Выпускающие ЦС) или происшествий, влияющих на штатное функционирование подсистемы.

В случае компрометации УЦ в коммерчески оправданные сроки приступает к функционированию с использованием новых ключевых пар.

В случае выхода из строя по каким-либо причинам каких-либо компонент УЦ осуществляется их восстановление из резервных копий.

Резервное копирование ключей УЦ осуществляется согласно пункту 6.2.4.

5.7.2. Повреждение компьютерных ресурсов, программного обеспечения и/или данных

В случае повреждения (подозрения в повреждении) компьютерных ресурсов, программного обеспечения и/или данных УЦ восстанавливает работоспособность, используя резервные копии.

Все субъекты, на которых отражается произошедшая авария или сбой немедленно извещаются. По окончанию восстановления все субъекты, чьи интересы были затронуты аварией или сбоем оповещаются о восстановлении.

5.7.3. Порядок восстановления в случае компрометации ключей электронной подписи компонент УЦ

В случае компрометации ключа электронной подписи уполномоченного лица УЦ;

- осуществляется оповещение всех субъектов ИОК о компрометации доступными способами;
- отзыв всех сертификатов центров сертификации Выпускающих ЦС и Участников;
- публикация СОС;
- генерация новых ключевых пар и выпуск сертификатов уполномоченного лица УЦ и центров сертификации Выпускающих ЦС;
- обновление сертификатов Участников.

5.7.4. Возможность непрерывности функционирования после бедствий

Непрерывность функционирования после бедствий обеспечивается мерами, указанными в «Регламент восстановления работоспособности компонент УЦ».

5.8. Прекращение деятельности УЦ

В случае прекращения деятельности УЦ оповещает всех владельцев сертификатов о прекращении своей деятельности. Все претензии со стороны владельцев сертификатов принимаются в соответствии с заключенным Договором о присоединении к Регламенту УЦ.

6. Технические меры обеспечения безопасности

6.1. Генерация и инсталляция ключевых пар

6.1.1. Генерация ключевых пар

Генерация ключевых пар производиться Участником самостоятельно собственными средствами или с использованием Веб-интерфейса. Генерация ключевых пар осуществляется на ключевые носители, требования к которым приведены в разделе 6.2.1.

6.1.2. Передача ключа электронной подписи Участнику

Не предусмотрено.

6.1.3. Передача ключа проверки электронной подписи издателю сертификата

Заявитель может передать ключ проверки электронной подписи в УЦ следующими способами:

- сформировав запрос на выпуск сертификата через Веб-интерфейс;
- загрузив подписанный запрос на выпуск сертификата формата PKCS#10 в Веб-интерфейс; при этом запрос на выпуск сертификата подписывается с применением ключа электронной подписи, соответствующего ключу проверки электронной подписи, в составе запроса.

В любом случае Заявитель должен пройти аутентификацию на Веб-интерфейсе.

6.1.4. Передача ключей проверки электронной подписи центров сертификации пользователям

Ключи проверки электронной подписи ЦС содержатся в их сертификатах. Сертификаты Корневого ЦС и Выпускающих ЦС опубликованы в репозитории по URL-адресам:

https://gostca.westernunion.ru/download/root_wumte.crt
https://gostca.westernunion.net/download/root_wumte.crt
https://gostca.westernunion.ru/download/ca1_wumte.crt
https://gostca.westernunion.net/download/ca1_wumte.crt

6.1.5. Размеры ключей

Длина ключей электронной подписи следующая:

- ключ электронной подписи - 256 бит;
- ключ проверки электронной подписи - 512 бит (ГОСТ Р 34.10-2001).

Длина ключей электронной подписи, используемых для шифрования должна быть следующей:

- сессионный ключ для шифрования по ГОСТ 28147-89 - 256 бит;
- ключ электронной подписи - 256 бит;
- ключ проверки электронной подписи - 512 бит (на базе ГОСТ Р 34.10-2001).

6.1.6. Генерация параметров ключа проверки электронной подписи и проверка качества

Не применяется.

6.1.7. Цели использования ключей

В соответствии с пунктом 7.1.2.3.

6.2. Защита ключа электронной подписи и технический контроль криптографических модулей

6.2.1. Стандарты и контроль криптографических модулей

Формирование ключей электронной подписи производится на следующие типы носителей:

- процессорные карты MPCOS-EMV, российские интеллектуальные карты (РИК), интеллектуальные карты "Оскар" с использованием считывателей смарт-карт, поддерживающий протокол pS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126);
- таблетки Touch-Memory DS1993 – DS1996 с использованием устройств Аккорд 4+, электронный замок "Соболь" или устройство чтения таблеток Touch-Memory DALLAS;
- электронные ключи с интерфейсом USB;
- сменные носители с интерфейсом USB;
- реестр ОС Windows.

Создание копий ключей электронной подписи на компьютере при использовании отчуждаемого носителя для хранения ключей недопустимо.

6.2.2. Контроль ключа электронной подписи несколькими лицами

Контроль ключа электронной подписи несколькими лицами недопустим.

6.2.3. Депонирование ключа электронной подписи

Депонирование ключа электронной подписи не допустимо.

6.2.4. Резервная копия ключа электронной подписи

Резервное копирование и хранение резервных копий ключей электронной подписи компонент УЦ осуществляется с использованием методов и средств, обеспечивающих уровень защищенности не меньше уровня защищенности ключевого носителя.

6.2.5. Архивация ключа электронной подписи

УЦ обеспечивает архивное хранение ключевой пары своих компонент на протяжении минимум 5 лет после окончания их срока действия. Архивная копия ключевой пары хранится в архивохранилище. По окончании срока хранения архивная копия уничтожается в соответствии с пунктом 6.2.10.

6.2.6. Перенос ключа электронной подписи из/в криптографический модуль

Перенос ключа электронной подписи из/в криптографического модуля осуществляется методами, гарантирующими его нераспространение.

6.2.7. Хранение ключа электронной подписи в криптографическом модуле

Ключ электронной подписи ЦС хранится в криптографическом модуле в зашифрованном виде.

6.2.8. Метод активации ключа электронной подписи

Активация ключа электронной подписи может осуществляться только его владельцем.

Для активации ключа электронной подписи должны использоваться данные активации, удовлетворяющие требованиям подраздела 6.4. Активация ключа электронной подписи должна производиться на ограниченный период времени.

6.2.9. Метод деактивации ключа электронной подписи

Деактивация ключа электронной подписи должна производиться либо автоматически, либо путем отключения ключевого носителя.

6.2.10. Метод уничтожения ключа электронной подписи

После окончания срока действия или архивного хранения, если таковое осуществляется, ключ электронной подписи уничтожается методами, гарантирующими невозможность его восстановления.

6.2.11. Оценка криптографических модулей

См. раздел 6.2.1.

6.3. Другие аспекты управления ключевой парой

6.3.1. Архивация ключа проверки электронной подписи

Ключ проверки электронной подписи архивируется в составе сертификата в соответствии с подразделом 5.5.

6.3.2. Сроки действия сертификата и использования ключевой пары

Срок действия сертификата и ключевой пары составляет:

- для сертификатов Участников — 3 года;
- для сертификатов Выпускающих ЦС — 7 лет;
- для сертификатов Корневого ЦС — 14 лет.

6.4. Данные активации

6.4.1. Генерация и инсталляция данных активации

Данные активации используются для защиты ключевых носителей. Данные активации создаются перед генерацией ключевой пары.

В качестве данных активации могут быть использованы:

- пароль, PIN;
- биометрическая информация;
- системы строгой двухфакторной аутентификации.

Пароль (PIN) должен отвечать следующим требованиям:

- известен только Владельцу;
- длина не менее 8 символов;
- мощность алфавита не менее 10 символов;
- не должен содержать слов, словосочетаний, имен и т.п.

6.4.2. Защита данных активации

Данные активации должны защищаться от потери, порчи, неавторизованного использования или раскрытия.

6.4.3. Другие аспекты, относящиеся к данным активации

Передача или уничтожение данных активации должны осуществляться методами, обеспечивающими невозможность потери, кражи, разглашения, порчи, модификации или неавторизованного использования.

6.5. Средства управления безопасностью вычислительной техники

6.5.1. Особые технические требования по безопасности вычислительной техники

Используемая вычислительная техника обеспечивает сохранность и защиту данных УЦ и ключей электронной подписи от уничтожения, порчи, модификации, разглашения или неавторизованного использования.

6.5.2. Оценка безопасности вычислительной техники

Программное обеспечение, осуществляющее работу с ключевой информацией, сертифицировано ФСБ РФ.

6.6. Технические средства управления жизненным циклом

6.6.1. Средства управления разработкой системы

Нет условий.

6.6.2. Средства управления организацией безопасности

УЦ использует механизмы проверки безопасной конфигурации и целостности используемых систем.

6.6.3. Средства управления безопасностью жизненного цикла

Нет условий.

6.7. Средства управления сетевой безопасностью

УЦ использует средства сетевой безопасности, предотвращающие неавторизованный доступ к информации, и защищающие от атак.

6.8. Метки времени

Сертификаты и списки отзыва сертификатов содержат информацию о дате и времени. УЦ синхронизирует все программные и технические средства по UTC с учетом часового пояса.

7. Структура сертификатов, СОС

7.1. Структура сертификата

Все издаваемые сертификаты содержат следующие базовые поля:

- **Serial Number** - уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов УЦ;
- **Signature Algorithm** - объектный идентификатор алгоритма, используемого для подписи сертификата;
- **Issuer** - отличительное имя ЦС или идентификационные данные Уполномоченного лица УЦ;
- **Valid From** - дата начала действия сертификата;
- **Valid To** - дата окончания действия сертификата;
- **Subject** - идентификационные данные владельца сертификата;
- **Subject Public Key** - ключ проверки электронной подписи владельца сертификата;
- **Version** - версия структуры сертификата формата X.509;
- **Signature** - ЭП Уполномоченного лица УЦ.

7.1.1. Номер версии

Версия издаваемых сертификатов не ниже 3.

7.1.2. Расширения сертификата

В издаваемых сертификатах могут использоваться только перечисленные в данном разделе расширения. В случае если значение какого-либо поля (флага) перечисленных расширений не определено данным документом, УЦ вправе определить значение данного поля для издаваемых сертификатов в соответствии с требованиями X.509 и RFC 5280.

7.1.2.1. Authority Key Identifier

Данное расширение обязательно для всех сертификатов, за исключением само подписанных (сертификатов ЦС), и является некритическим. Это расширение должно обязательно содержать поле keyIdentifier, в котором содержится идентификатор ключа проверки электронной подписи издателя. Остальные поля не обязательны.

7.1.2.2. Subject Key Identifier

Данное расширение должно присутствовать во всех сертификатах, являться некритическим и содержит идентификатор ключа проверки электронной подписи владельца сертификата.

7.1.2.3. KeyUsage

Данное расширение должно присутствовать во всех сертификатах и быть критическим.

Значение полей расширения KeyUsage:

Поле	Сертификат ЦС	Сертификаты клиентов
digitalSignature	0	0/1
nonRepudiation	0	0/1
keyEncipherment	0	0/1
dataEnciphermen t	0	0/1
keyAgreement	0	0/1
keyCertSign	1	0
CRLSign	1	0
encipherOnly	0	0/1
decipherOnly	0	0/1

7.1.2.4. Certificate Policies

Не используется.

7.1.2.5. Policy Mappings

Не используется.

7.1.2.6. Basic Constraints

Расширение должно содержится сертификате ЦС и является критическим. Значение флага CA установлено в 1 (true). Расширение сертификата ЦС так же содержит поле pathLenConstraint, значение которого установлено в 0 (ноль).

7.1.2.7. Name Constraints

Используется в соответствии с разделом .

7.1.2.8. Policy Constraints

Используется в соответствии с разделом 7.1.7.

7.1.2.9. CRL Distribution Points

Данное расширение должно содержаться во всех сертификатах Участников, быть некритическим и содержать последовательность точек доступа к списку аннулированных сертификатов Выпускающих ЦС; список точек доступа приведен в разделе .

7.1.2.10. Inhibit Any-Policy

Не используется.

7.1.2.11. Authority Information Access

Расширение должно присутствовать во всех сертификатах Участников быть некритическим и содержать URL-адрес точки публикации сертификата Выпускающего ЦС в соответствии с разделом 6.1.4.

7.1.2.12. Extended Key Usage

Не используется.

7.1.3. Объектные идентификаторы криптографических алгоритмов

Все участники ИОК должны использовать в своей работе криптографические алгоритмы с объектными идентификаторами соответствующими RFC 3279, RFC 4491.

7.1.4. Формы имен

В сертификате поля идентификационных данных Уполномоченного лица Удостоверяющего центра и владельца сертификата содержат атрибуты имени формата X.500.

7.1.5. Ограничения имен

Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

Common Name:	Фамилия, имя, отчество
Organization:	Наименование организации, являющейся владельцем Удостоверяющего центра
Organization Unit:	Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего центра
Email:	Адрес электронной почты
Country:	буквенный код страны (например, RU)
State:	Субъект Федерации, где зарегистрирована организация, являющейся владельцем Удостоверяющего центра

Обязательными атрибутами поля идентификационных данных владельца сертификата, представляющего собственные интересы, являются:

Common Name:	Фамилия, имя, отчество
Email:	Адрес электронной почты
Country:	буквенный код страны (например, RU)

Обязательными атрибутами поля идентификационных данных владельца сертификата, представляющего интересы юридического лица, являются:

Common Name:	Фамилия, имя, отчество
Organization:	Наименование организации, которую представляет владелец сертификата
Organization Unit:	Наименование подразделения организации, сотрудником которого является владелец сертификата
Email:	Адрес электронной почты
Country:	буквенный код страны (например, RU)
State:	Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата

7.1.6. Объектные идентификаторы применяемых ППС

Нет условий.

7.1.7. Использование расширения Policy Constraints

Нет условий.

7.1.8. Семантика и синтаксис квалификаторов политики

Нет условий.

7.1.9. Обработка семантики критического расширения Certificate Policies

Нет условий.

7.2. Структура списков аннулированных сертификатов

Структура списков аннулированных сертификатов должна соответствовать RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Списки аннулированных сертификатов содержат следующие основные поля:

- **Version** – версия структуры СОС формата X.509;
- **Signature Algorithm** - объектный идентификатор алгоритма, используемого для подписи CRL;
- **Signature** - ЭП Уполномоченного лица УЦ.
- **Issuer** - отличительное имя ЦС или идентификационные данные Уполномоченного лица УЦ;
- **This Update** - дата и время выпуска текущего CRL;
- **Next Update** - дата и время планового выпуска следующего CRL;
- **Next Publication** - дата и время следующей плановой публикации CRL;
- **Revoked Certificates** - список аннулированных (отозванных) сертификатов, включающий серийный номер сертификата и дату отзыва. Данное поле может отсутствовать, если нет отозванных сертификатов.

7.2.1. Номер версии

Все издаваемые СОС версии 2.

7.2.2. Расширения CRL и элементов CRL

7.2.2.1. Authority Key Identifier

Идентификатор ключа Центра сертификации, которым подписан данный СОС.

7.2.2.2. CRL Number

Некритическое рекомендуемое расширение, содержащее порядковый номер СОС.

7.2.2.3. Reason Code

Некритическое рекомендуемое расширение элемента CRL, содержащее причину отзыва сертификата.

7.2.2.4. Invalidity Date

Не применяется.

8. Аудит соответствия и другие оценки

8.1. Частота и условия оценки

Аудит УЦ проводится на основании утвержденной методики аудита.

Внутренний и внешний аудит УЦ проводится по решению руководства УЦ.

8.2. Идентификация и квалификация эксперта

Внутренний аудит проводится администратором безопасности УЦ.

Внешний аудит проводится независимой организацией, соответствующей следующим требованиям:

- имеет опыт эксплуатации информационных систем на основе технологий PKI и информационной безопасности, а так же опыт в проведении аудита безопасности;
- имеет не менее двух специалистов, имеющих высшее образование или прошедших переподготовку по специальности «Защита информации».

8.3. Отношение эксперта к оцениваемому

Для проведения внешнего аудита привлекается организация организационно или юридически независимая от УЦ.

8.4. Темы, охватываемые оценкой

Область вопросов, рассматриваемая при проведении аудита:

- физическая безопасность УЦ;
- аутентификация и идентификация;
- услуги УЦ;
- безопасность программного обеспечения и доступа к сети;
- обеспечение персональной безопасности сотрудников;
- ведение журналов событий и мониторинга системы;
- процедуры архивирования и резервного копирования.

8.5. Действия, предпринимаемые в результате недостатков

Отчеты о проведенных внешних аудиторских проверках направляются руководителю УЦ.

8.6. Сообщение результатов

Нет условий.

9. Другие коммерческие и юридические вопросы

9.1. Оплата

9.1.1. Оплата выпуска или обновления сертификата

Оплата выпуска и обновления сертификата не предусмотрена.

9.1.2. Оплата доступа к сертификатам

Оплата доступа к сертификатам не предусмотрена.

9.1.3. Оплата информации об отзыве или статусе сертификата

Оплата информации об отзыве или статусе сертификата не предусмотрена.

9.1.4. Оплата других услуг

Нет условий.

9.1.5. Политика возврата платежей

Нет условий.

9.2. Финансовая ответственность

9.2.1. Страховое обеспечение

Нет условий.

9.2.2. Иные активы

Нет условий.

9.2.3. Сфера действия страхования или гарантии для клиентов

Нет условий.

9.3. Конфиденциальность коммерческой информации

9.3.1. Информация, являющаяся конфиденциальной

Конфиденциальной информацией считается:

- ключ электронной подписи;
- персональная и корпоративная информация Участников, содержащаяся в УЦ и не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи или СОС;
- информация, хранящаяся в журналах аудита УЦ;
- отчетные материалы по выполненным проверкам деятельности УЦ;
- информация о способах и порядке защиты аппаратного и программного обеспечение, способах администрирования и действий на случай непредвиденных ситуаций;
- документы с грифом «для служебного пользования» или «конфиденциально».

9.3.2. Информация, не являющаяся конфиденциальной

Информация, не являющейся конфиденциальной информацией является открытой информацией. Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации также определяется решением УЦ.

Информация, включаемая в сертификаты и СОС, издаваемые УЦ, не считается конфиденциальной. Подразумевается, что Заявитель, знает, какая информация будет содержаться в сертификате, и согласен с ее публикацией.

Вся информация, подлежащая публикации в соответствии с данным Регламентом УЦ так же не считается конфиденциальной.

9.3.3. Обязательства по защите конфиденциальной информации

Все участники должны не раскрывать и всячески препятствовать раскрытию конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев, требующих ее раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

9.4. Конфиденциальность персональной информации

9.4.1. Обеспечение конфиденциальности персональной информации

УЦ осуществляет защиту персональных данных Участников в соответствии с законодательством Российской Федерации.

9.4.2. Информация, рассматриваемая как персональная

Информация, определенная как таковая в соответствии с текущим законодательством, за исключением информации, которая должна публиковаться в соответствии с действующим законодательством в области электронной подписи.

9.4.3. Информация не рассматриваемая как персональная

Вся информация не являющаяся персональной.

9.4.4. Обязательство по защите персональных данных

УЦ защищает персональные данные сотрудников Участников и всячески препятствует их раскрытию третьим лицам.

9.4.5. Предупреждение и согласие на использование персональных данных

Любое использование персональных данных возможно только с согласия их владельца. Заявление на сертификат считается согласием на использование указанных в заявлении персональных данных в сертификате.

9.4.6. Раскрытие в соответствии с судебным или административным процессом

Раскрытие персональных данных осуществляется в соответствии с текущим законодательством Российской Федерации.

9.4.7. Иные условия раскрытия информации

Нет условий.

9.5. Права на интеллектуальную собственность

Оператор является собственником всех документов, программно-технических средств и информационных ресурсов, которые созданы за счет средств Оператора, приобретены на законных основаниях, получены в порядке дарения или наследования.

Вся продукция, в том числе и интеллектуального характера, произведенная сотрудниками Оператора при выполнении ими своих служебных обязанностей, является собственностью Оператора, если отдельным договором не предусмотрен иной режим произведенной продукции.

Оператор является обладателем исключительных прав на все созданные им объекты интеллектуальной собственности, в соответствии с законодательством Российской Федерации.

Все торговые марки, лицензии, графические символы и прочее используемое Оператором являются интеллектуальной собственностью их владельцев. Оператор согласен с возможностью отображения соответствующих логотипов и торговых марок, при предоставлении своих услуг, если этого требуют их владельцы.

9.6. Заявления и гарантии

9.6.1. Заявления и гарантии УЦ

УЦ гарантирует:

- что его деятельность соответствует требованиям законодательства Российской Федерации;
- отсутствие каких-либо искажений или ошибок по вине сотрудников УЦ в выпущенных сертификатах и СОС;
- предоставление доступа к репозиторию и услуг аннулирования (отзыва) в соответствии с настоящим Регламентом УЦ.

Договор о присоединении к Регламенту УЦ может включать дополнительные заявления и гарантии.

9.6.2. Заявления и гарантии Центра сертификации

См. пункт 9.6.1.

9.6.3. Заявления и гарантии Участника

Участник гарантирует, что:

- вся информация, переданная клиентом в Заявлении на выпуск сертификата, является достоверной;
- ключ электронной подписи хранится в тайне и неавторизованный доступ к нему невозможен;
- сертификат используется только по назначению и в соответствии с требованиями настоящего Регламента УЦ;
- немедленно оповестит УЦ при компрометации ключа электронной подписи.

Договор о присоединении к Регламенту УЦ может включать дополнительные заявления и гарантии.

9.6.4. Заявления и гарантии пользователя

Используя сертификаты, пользователь сертификата гарантирует, что:

- использование сертификата осуществляется в соответствии с назначением, указанным в сертификате и требованиями настоящего Регламента УЦ;
- использование сертификата осуществляется только после проведения проверки ЭП сертификата и его статуса, показавшей его действительность.

9.6.5. Заявления и гарантии других участников

Нет условий.

9.7. Отказ от гарантий

Нет условий.

9.8. Ограничение ответственности

УЦ не несет ответственность за неисполнение своих обязательств по независящим от него причинам.

УЦ не несет ответственности в случае нарушения пользователями и владельцами сертификатов требований настоящего Регламента УЦ и Договора о присоединении к Регламенту УЦ.

Ответственность и ее пределы владельцев сертификатов и пользователей должны быть включены в Договор о присоединении к Регламенту УЦ.

9.9. Возмещение ущерба

В рамках текущего законодательства УЦ может потребовать от владельца сертификата возмещение ущерба в следующих случаях:

- преднамеренного или случайного искажения или указания ложной информации клиентом в Заявлении на выпуск сертификата;
- компрометации ключа электронной подписи клиента;
- использования владельцем сертификата имен или других объектов интеллектуальной собственности нарушающих права интеллектуальной собственности третьей стороны.

Договор о присоединении к Регламенту УЦ может включать дополнительные обязательства возмещения ущерба.

9.10. Период и прекращение

9.10.1. Период

Данный документ и его изменения считаются действующими с момента публикации до момента прекращения его действия.

9.10.2. Прекращение

Данный документ периодически исправляется и дополняется, оставаясь действующим до публикации новой версии или уведомления о прекращении его действия.

9.10.3. Результат прекращения действия и долговечность

После завершения действия данного документа его требования продолжают действовать для всех участников, использующих сертификаты УЦ, выпущенные в период действия данного документа, в течение всего срока действия таких сертификатов.

9.11. Индивидуальные уведомления и связь с участниками

Участники ИОК могут использовать любые способы связи между собой, если каким-либо соглашением не определено иное.

9.12. Изменения

9.12.1. Процедура изменения

Изменения в данный регламент могут быть внесены Менеджером Регламента УЦ. Изменения могут быть оформлены в виде измененного документа либо в виде обновления. Изменения и обновления публикуются.

9.12.2. Период и механизм оповещения

Оператор и Менеджер Регламента УЦ оставляют за собой право внести несущественные изменения в Регламент УЦ без оповещения, например в случае исправления опечаток, ошибок, URL или изменения контактной информации. Решение о существенности или несущественности изменений выносится Менеджером Регламента УЦ по его усмотрению.

В случае если Менеджер Регламента УЦ считает, что необходимо немедленное существенное изменение Регламента УЦ для предотвращения или остановки нарушения безопасности ИОК или любой его части, он может сделать это и опубликовать Регламент УЦ, после чего оповестить участников.

9.12.3. Обстоятельства, при которых OID должен быть изменен

Нет условий.

9.13. Условия разрешения споров

При возникновении споров стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего документа, путем переговоров. Споры между сторонами, связанные с положениями Регламента УЦ и Договора о присоединении к Регламенту УЦ и не урегулированные в процессе переговоров, должны рассматриваться в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

9.14. Применяемое законодательство

Для определения законности, толкования, интерпретации и исполнения положений данного документа любой субъект права должен использовать законодательство Российской Федерации, вне зависимости от договорных отношений установленных или нет на территории Российской Федерации.

9.15. Соответствие применяемому законодательству

Все участники должны руководствоваться законодательством Российской Федерации, а так же руководящими документами контролирующих организаций в области ЭП,

шифрования и экспорта/импорта программно-аппаратных средств и технической информации.

9.16. Разнообразные положения

9.16.1. Полнота соглашения

Нет условий.

9.16.2. Передача прав и обязанностей

Нет условий.

9.16.3. Делимость

В случае если по решению суда какие-либо положения данного документа будут признаны не имеющими юридической силы, оставшиеся положения все равно остаются действительными.

9.16.4. Правоприменение

Нет условий.

9.16.5. Форс-мажор

В рамках используемого законодательства, соглашения с клиентом и пользователем должны включать форс-мажорные условия для защиты УЦ.

9.17. Другие положения

Нет условий.

Приложение №1 к Регламенту. Перечень руководящих документов

1. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
2. Федеральный Закон РФ от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
3. Гражданский Кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (принят Государственной Думой РФ 21.10.1994) (действующая редакция);
4. Гражданский Кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (принят Государственной Думой РФ 22.12.1995) (действующая редакция);
5. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993г.).
6. Положение о порядке разработки, производства, реализации и использования шифровальных (криптографических) средств защиты информации. (ПКЗ-2005) (Утверждено Приказом ФСБ РФ от 09.02.2005 № 66);
7. Протокол координационного совещания по вопросам создания и развития системы удостоверяющих центров, г. Москва, 25 июня 2004 г.;
8. Декларация о сотрудничестве в составе объединения удостоверяющих центров;
9. Требования к заявителю на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню "С", утверждены руководством ФАПСИ 05.01.97;
10. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. (Утверждено приказом ФАПСИ от 13.06.2001 №152);
11. RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
12. RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
13. RFC 5280 Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile;
14. RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
15. RFC 4191 Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile;
16. ITU-T Recommendation X.509;
17. ITU-T Recommendation X.521.

Приложение №2 к Регламенту. Формы заявительных документов

Заявление
на аннулирование (отзыв) сертификата ключа проверки электронной подписи

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

в связи с _____
(причина отзыва сертификата)

Просит аннулировать (отозвать) сертификат ключа проверки электронной подписи, содержащий следующий серийный номер:

Серийный номер сертификата ключа проверки электронной подписи	

Владелец сертификата _____
(подпись) (фамилия, инициалы)

Руководитель организации _____
(подпись) . (фамилия, инициалы)

«____»_____ 20____ г. М.П

Заявление
на приостановление действия сертификата ключа проверки электронной подписи

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие сертификата ключа проверки электронной подписи, содержащего следующий серийный номер:

Серийный номер сертификата ключа проверки электронной подписи	

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Владелец сертификата _____ _____
(подпись) (фамилия, инициалы)

Руководитель организации _____ _____
(подпись) . (фамилия, инициалы)

«____»_____ 20____ г. М.П

Заявление
на возобновление действия сертификата ключа проверки электронной подписи

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие сертификата ключа проверки электронной подписи
подписи, содержащего следующий серийный номер:

Серийный номер сертификата ключа проверки электронной подписи	

Владелец сертификата _____ _____
(подпись) (фамилия, инициалы)

Руководитель организации _____ _____
(подпись) . (фамилия, инициалы)

«____»_____ 20____ г. М.П

Заявление
на выпуск сертификата ключа проверки электронной подписи

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность, фамилия, имя, отчество)

действующего на основании _____

_____

_____

просит изготовить сертификат ключа проверки электронной подписи для работы с ПЛАТЕЖНОЙ СИСТЕМОЙ ВЕСТЕРН ЮНИОН.

сообщаю следующие данные:

Сокращенное наименование организации в соответствии с выпиской из ЕГРЮЛ	
Наименование АИС (при необходимости)	
Юридический адрес	
Код региона/Наименование региона	
ИНН ОГРН	
Наименование средства ЭП	
Класс средства ЭП	

Кодовое словосочетание:

Подтверждаю, что указанное кодовое словосочетание является паролем для экстренной связи в случае компрометации секретного (закрытого) ключа, и обязуюсь обеспечивать сохранение конфиденциальности данного пароля.

Подтверждаю, что имеющиеся в наличии средства электронной подписи соответствуют указанному классу защиты.

С «Регламентом применения сертификатов ключей проверки электронной подписи удостоверяющего центра общества с ограниченной ответственностью «Небанковская кредитная организация «Вестерн Юнион ДП Восток» ознакомлен. В случае выявления факта компрометации личного секретного (закрытого) ключа, соответствующего выпускаемому на мое имя сертификату, обязуюсь немедленно об этом событии проинформировать своего работодателя и ООО "Небанковская кредитная организация «Вестерн Юнион ДП Восток».

Руководитель организации _____ _____

(подпись) М.П. (фамилия, инициалы)

«____» _____ 201_ г.

М.П