Приложение
к приказу № ОРД-П/3500-23-000128
от 29.08.2023

УТВЕРЖДАЮ
Генеральный директор
АО «Северсталь-инфоком»
_____ С.В. Дунаев
_____28 августа 2023 г

РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
АО «СЕВЕРСТАЛЬ-ИНФОКОМ»

Череповец, 2023

96001378318

Лист согласования

К ОРД № от 00.00.0000
Вид документа: Приказ
Наименование документа: «Об утверждении регламента УЦ»
Инициатор: Попова Нина Васильевна

Дата выполнения	ФИО	Статус
01.08.2023 16:13:32	Веселова Любовь Алексеевна, Управление по обеспечению бизнеса	Согласовано
01.08.2023 16:30:59	Бовыкин Сергей Владиславович, Управление по обеспечению бизнеса	Согласовано
01.08.2023 17:07:17	Леонтьев Эдуард Николаевич, Административная группа (виртуальная)	Согласовано
25.08.2023 11:32:59	Кудряшов Евгений Игоревич, Управление по обеспечению бизнеса	Согласовано

Инициатор _____ Попова Нина Васильевна

Содержание

1 Перечень сокращений 5

2 Термины и определения 6

3 Введение 8

3.1 Идентификация Регламента 8

3.2 Область применения Регламента 8

3.3 Контактная информация 9

Общие положения 10

3.4 Назначение Удостоверяющего Центра 10

3.5 Деятельность Удостоверяющего Центра 10

3.6 Подразделение эксплуатации Удостоверяющего Центра 11

3.7 Пользователи услуг Удостоверяющего Центра 12

3.8 Разрешение споров 12

3.9 Ответственность 12

3.10 Прекращение деятельности 12

3.11 Порядок утверждения и внесения изменений в Регламент 13

4 Права и обязанности 14

4.1 Права Удостоверяющего Центра 14

4.2 Права пользователей УЦ 14

4.3 Обязательства Удостоверяющего Центра 15

4.3.1 Ключ подписи уполномоченного лица Удостоверяющего Центра 15

4.3.2 Регистрация пользователей УЦ 16

4.3.3 Изготовление закрытых и открытых ключей пользователей УЦ 16

4.3.4 Изготовление сертификатов открытых ключей 16

4.3.5 Отзыв сертификатов открытых ключей 17

4.3.6 Приостановление действия сертификатов открытых ключей 17

4.3.7 Возобновление действия сертификатов открытых ключей 17

4.3.8 Уведомления 17

4.3.9 Реестр сертификатов открытых ключей 18

4.4 Обязательства пользователей УЦ 18

4.4.1 Обязанности владельцев сертификатов открытых ключей 19

5 Процедуры и механизмы реализации функционала удостоверяющего центра 20
5.1 Регистрация пользователей УЦ 20
5.1.1 Процедура регистрации внутренних пользователей 20
5.1.2 Процедура регистрации внешних пользователей 22
5.2 Процедуры работы с сертификатами и ключами шифрования 23
5.2.1 Создание ключей и сертификатов Центра сертификации 23
5.2.2 Обновление ключей и сертификатов Центров сертификации 23
5.2.3 Создание ключей и сертификатов внутренних пользователей 24
5.2.4 Приостановление действия и отзыв сертификатов внутренних пользователей 26
5.2.5 Создание ключей и сертификатов внешних пользователей 27
5.2.6 Журнал учета изданных сертификатов 27
5.3 Процедуры работы со списками отозванных сертификатов 28
5.4 Работа с носителями ключевой информации 28
5.4.1 Все выданные носители с ключевой информацией подлежат обязательному учету. Хранение ключевых носителей 28
5.4.2 Права и обязанности пользователей 28
6 Восстановление УЦ после аварий 30
6.1 Восстановление после аварий 30
7 Обслуживание УЦ 32

1 Перечень сокращений

IETF	Internet Engineering Task Force
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
ИОК	Инфраструктура открытых ключей
ОС	Операционная система
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
УЦ	Корпоративный Удостоверяющий Центр АО «Северсталь-инфоком» в г. Череповец
ЦС	Центр Сертификации
ЭП	Электронная подпись

2 Термины и определения

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Закрытый ключ - криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной цифровой подписи и/или шифрования данных.

Запрос на сертификат - сообщение, содержащее необходимую информацию для получения сертификата.

Запрос на отзыв сертификата - сообщение, содержащее необходимую информацию для отзыва сертификата.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Каталог ИТ-услуг (ИТ-каталог) – главный источник информации о предоставляемых ИТ-услугах, который объединяет в себе различные сервисы. Позволяет пользователю в круглосуточном режиме самостоятельно создавать новые заявки и инциденты, отслеживать статус их выполнения.

Ключ (криптографический ключ) - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Ключевая пара - открытый и закрытый ключи.

Ключевой носитель - носитель, содержащий один или несколько ключей.

Компрометация ключа - утрата доверия к тому, что используемые ключи недоступны посторонним лицам, или подозрение, что ключи были временно доступны неуполномоченным лицам. К событиям, связанным с компрометацией ключа, относятся (включая, но не ограничиваясь):

- физическая утеря ключевого носителя;
- передача ключа по открытым каналам связи или не надежная защита ключа при его передаче;
- доступ постороннего лица в место физического хранения ключевого носителя, к устройству хранения ключа или подозрение, что данные факты имели место (срабатывание сигнализации, повреждение устройств контроля

несанкционированного доступа (слепков печатей), повреждение замков, взлом учётной записи пользователя и т. п.);

- перехват информации вредоносным программным обеспечением;
- перехват ключа при распределении ключей;
- сознательная передача ключа постороннему лицу;
- увольнение сотрудников, имевших доступ к ключу юридического лица.

Открытый ключ - криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен другим пользователям системы и предназначен для проверки электронной цифровой подписи и шифрования. При этом открытый ключ не позволяет вычислить закрытый ключ.

Плановая смена ключей - смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Сертификат открытого ключа (сертификат) - цифровой документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью его издателя. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует. Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 и рекомендациях IETF 1999 года RFC 2459.

Список отозванных сертификатов - созданный УЦ список сертификатов, отозванных до окончания срока их действия.

Средство электронной подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной подписи в электронном документе, создание закрытых и открытых ключей электронных подписей.

Внутренние пользователи – сотрудники компаний группы «Северсталь».

Внешние пользователи – сотрудники внешних по отношению к компаниям группы Северсталь организаций.

3 Введение

Настоящий Регламент определяет порядок, механизмы и условия предоставления и использования услуг Корпоративного Удостоверяющего Центра АО «Северсталь-инфоком» в г. Череповец, включая обязанности пользователей (пользователей сертификатов открытых ключей), подразделения эксплуатации УЦ (далее - администраторов УЦ), протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы Удостоверяющего центра.

Содержание Регламента соответствует положениям Федерального закона от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».

Сервисы УЦ АО «Северсталь-инфоком» в г. Череповец предоставляются пользователям информационной системы компаний группы «Северсталь» и «Севергрупп», а также внешним пользователям, работающим в интересах указанных выше компаний, для реализации следующих сервисов информационной безопасности:

- строгая (усиленная) аутентификация;
- обеспечение контроля целостности данных;
- обеспечение конфиденциальности данных;
- обеспечение неотказуемости от авторства.

Использование данных сервисов основано на применении сертификатов открытых ключей и ассоциированных с ними открытых и закрытых ключей.

3.1 Идентификация Регламента

Наименование документа: «Регламент Удостоверяющего центра АО «Северсталь-инфоком» в г. Череповец.

3.2 Область применения Регламента

Настоящий Регламент служит соглашением, налагающим обязательства на все вовлеченные стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

Данный Регламент предназначен для установления норм и принципов работы с криптографическим материалом, используемым для защиты информации, не составляющей государственную тайну.

Регламент УЦ предназначен для обслуживающего персонала и пользователей УЦ. Обслуживающий персонал должен руководствоваться настоящим документом для эксплуатации УЦ. Пользователи УЦ должны руководствоваться настоящим документом при работе с закрытыми ключами и сертификатами.

Конфликты, возникающие в процессе работы УЦ и применения пользователями сертификатов, могут быть решены согласно настоящему Регламенту.

3.3 Контактная информация

Подразделение эксплуатации УЦ (из состава специалистов АО «Северсталь-инфоком») располагается на объекте информатизации центрального офиса АО «Северсталь-инфоком» в г. Череповец ул. Ленина, 123а и на производственной площадке г. Череповец ул. Мира, 30, Инфоком А (ЦТД).

Контакты:

Адрес электронной почты: pki@stalcom.com.

Общие положения

3.4 Назначение Удостоверяющего Центра

УЦ предназначен для предоставления возможности участникам информационной системы использовать сервисы по защите информации, базирующиеся на сертификатах открытых ключей. Участникам ИС предоставляются следующие возможности:

- использование электронной цифровой подписи для аутентификации авторов электронных документов и почтовых сообщений;
- контроль целостности информации, представленной в электронном виде, передаваемой в процессе обмена участников информационной системы;
- контроль целостности информации, представленной в электронном виде, передаваемой в процессе обмена участников почтового документооборота между внешними и внутренними пользователями;
- аутентификация участников информационных систем при доступе к информационным ресурсам;
- конфиденциальность информации, представленной в электронном виде, передаваемой в процессе обмена участников информационной системы;
- конфиденциальность и (или) контроль целостности информации, представленной в электронном виде, передаваемой в процессе обмена участников почтового документооборота между внешними и внутренними пользователями.

3.5 Деятельность Удостоверяющего Центра

В процессе деятельности УЦ осуществляет:

1) внесение в реестр УЦ регистрационной информации о пользователях;
2) предоставление ключевых носителей;
3) формирование закрытых и открытых ключей по обращениям пользователей с записью их на ключевой носитель;
4) изготовление сертификатов открытых ключей пользователей в электронной форме;
5) ведение реестра изготовленных сертификатов открытых ключей пользователей;
6) отзыв сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;

7) приостановление и возобновление действия сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
8) предоставление пользователям сведений об аннулированных и приостановленных сертификатах открытых ключей.

3.6 Подразделение эксплуатации Удостоверяющего Центра

Подразделение эксплуатации УЦ предназначено для решения задач по:

- управлению деятельностью УЦ;
- взаимодействию с пользователями в части разрешения вопросов, связанных с применением средств ЭП, ключей и сертификатов открытых ключей, изготовляемых и распространяемых УЦ;
- регистрации пользователей ИОК;
- ведению реестра зарегистрированных пользователей ИОК;
- предоставлению служебных ключей и сертификатов открытых служебных ключей по обращению пользователей ИОК;
- распространению средств электронной подписи и шифрования для пользователей группы компаний «Северсталь» и «Севергрупп»;
- организации, контролю выполнения, а также непосредственно выполнению мероприятий по защите ресурсов УЦ от несанкционированного доступа со стороны внешних и внутренних злоумышленников;
- изготовлению и предоставлению криптографических ключей по обращению пользователей ИОК в соответствии с установленным порядком;
- изготовлению и предоставлению изготовленных сертификатов открытых ключей в электронной форме по обращению пользователей ИОК, в соответствии с установленным данным Регламентом порядком;
- отзыву сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей согласно установленной данным Регламентом процедуре;
- приостановлению и возобновлению действия сертификатов открытых ключей по обращению владельцев сертификатов открытых ключей, согласно установленной данным Регламентом процедуре;
- предоставлению пользователям ИОК сведений об аннулированных и приостановленных сертификатах открытых ключей;

- предоставлению копий сертификатов открытых ключей, находящихся в реестре изготовленных сертификатов, по запросам пользователей ИОК, в соответствии с установленной данным Регламентом процедурой;
- организации и выполнению мероприятий по эксплуатации программных и технических средств обеспечения деятельности УЦ.

3.7 Пользователи услуг Удостоверяющего Центра

Пользователями (потребителями) услуг или сервисов УЦ (далее по тексту - пользователи) называются зарегистрированные на УЦ лица, являющиеся владельцами сертификатов открытых ключей, изданных данным УЦ.

Проходить процедуру регистрации на УЦ, то есть быть зарегистрированным пользователем и являться владельцем сертификата может быть только физическое лицо (человек).

В тех случаях, когда сертификаты требуются для работы каких-либо устройств или программных приложений, назначается ответственное лицо, на чьё имя регистрируется сертификат.

Пользователем сертификата может быть любое лицо, устройство или программное приложение.

3.8 Разрешение споров

Сторонами в споре, в случае его возникновения, являются УЦ и пользователь.

При возникновении споров стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, должны рассматриваться в арбитражном суде в соответствии с действующим законодательством Российской Федерации.

3.9 Ответственность

УЦ не несет никакой ответственности в случае нарушения пользователями положений настоящего Регламента, а также инструкций пользователя сервисами УЦ.

3.10 Прекращение деятельности

Деятельность УЦ может быть прекращена по решению владельца в порядке, установленном законодательством Российской Федерации.

3.11 Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент утверждается приказом Генерального директора АО «Северсталь-инфоком».

Изменения в Регламент вносятся в порядке, предусмотренном для его утверждения.

4 Права и обязанности

4.1 Права Удостоверяющего Центра

УЦ имеет право:

- предоставлять заинтересованным лицам копии сертификатов открытых ключей в электронной форме, находящихся в реестре Удостоверяющего Центра;
- не проводить регистрацию лиц, обратившихся по вопросу представления копий сертификатов открытых ключей в электронной форме, находящихся в реестре УЦ;
- отказать в предоставлении услуг по регистрации пользователям, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;
- отказать в изготовлении сертификата открытого ключа зарегистрированным пользователям, подавшим заявление на изготовление сертификата открытого ключа, с указанием причин отказа;
- отказать в отзыве сертификата, в приостановлении или возобновлении действия сертификата открытого ключа владельцу сертификата, подавшему заявление на отзыв сертификата, в случае если истек установленный срок действия закрытого ключа, соответствующего открытому ключу в сертификате;
- отозвать сертификат открытого ключа пользователя в случае установленного факта компрометации соответствующего закрытого ключа, без уведомления владельца отозванного сертификата открытого ключа, или уведомив его с указанием обоснованных причин;
- приостановить действие сертификата открытого ключа пользователя, без уведомления владельца приостановленного сертификата открытого ключа, или уведомив его с указанием обоснованных причин.

4.2 Права пользователей УЦ

Пользователи – владельцы сертификатов открытых ключей имеют следующие права:

- получить список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный УЦ;

- получить копию сертификата открытого ключа уполномоченного лица Удостоверяющего Центра;
- получить копию сертификата открытого ключа в электронной форме, находящегося в Реестре сертификатов открытых ключей УЦ;
- применять копии сертификатов открытого ключа в электронной форме для проверки электронной цифровой подписи электронных почтовых сообщений в соответствии со сведениями, указанными в сертификате открытого ключа подписи.
- применять список аннулированных (отозванных) и приостановленных сертификатов открытых ключей, изготовленный УЦ, для проверки статуса сертификатов открытых ключей подписи.
- обратиться в УЦ для внесения в реестр УЦ регистрационной информации о пользователе, с целью в дальнейшем стать владельцем сертификата открытого ключа;
- обратиться в УЦ на предмет получения средства электронной подписи;
- обратиться в УЦ для изготовления ключей шифрования и сертификатов открытых ключей;
- воспользоваться предоставляемыми УЦ программными средствами, чтобы передать по сети в УЦ заявление (запрос) в электронной форме на изготовление сертификата открытого ключа;
- воспользоваться предоставляемыми УЦ программными средствами, чтобы получить и установить на свое рабочее место изготовленный сертификат открытого ключа в электронной форме;
- обратиться в УЦ для отзыва, приостановления или возобновления действия сертификата открытого ключа в течение срока действия соответствующего закрытого ключа.

4.3 Обязательства Удостоверяющего Центра

4.3.1 Ключ подписи уполномоченного лица Удостоверяющего Центра

УЦ обязан использовать закрытый ключ уполномоченного лица Удостоверяющего Центра (корневого центра сертификации), а также закрытые ключи функциональных центров сертификации (издающих центров сертификации) только для подписи издаваемых им сертификатов открытых ключей и списков отозванных сертификатов.

УЦ обязан принять меры по защите названных закрытых ключей в соответствии с положениями настоящего Регламента.

4.3.2 Регистрация пользователей УЦ

УЦ обеспечивает достоверность регистрации пользователей по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

УЦ обязан обеспечить проверку уникальности регистрационной информации пользователей, заносимой в реестр УЦ и используемой для идентификации владельцев сертификатов открытых ключей.

УЦ обязан не разглашать (не публиковать) регистрационную информацию пользователей, за исключением информации, используемой для идентификации владельцев сертификатов открытых ключей и заносимой в изготавливаемые сертификаты.

Публикация информации, используемой для идентификации владельцев сертификатов открытых ключей, осуществляется путем включения ее в изготавливаемые сертификаты.

4.3.3 Изготовление закрытых и открытых ключей пользователей УЦ

УЦ обязан по обращению пользователя через систему ИТ-каталог изготовить закрытый и открытый ключ с использованием средств электронной подписи УЦ или предоставить пользователю специализированное программное обеспечение, позволяющее пользователю изготовить ключевую пару самостоятельно и передать запрос на изготовление сертификата в УЦ.

УЦ обязан обеспечить сохранение в тайне изготовленного закрытого ключа.

Ключ записывается на аппаратный носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства электронной подписи, выполняющего процедуру генерации ключей.

4.3.4 Изготовление сертификатов открытых ключей

УЦ обеспечивает изготовление сертификата открытого ключа зарегистрированному пользователю по обращению в системе ИТ-каталог на основании предоставленного или сформированного администратором УЦ запроса на сертификат.

4.3.5 Отзыв сертификатов открытых ключей

УЦ обязан отозвать сертификат открытого ключа во всех случаях и в порядке, установленных данным Регламентом.

УЦ обязан в течение 24 часов занести сведения об отозванном сертификате в список отозванных сертификатов с указанием даты и времени занесения и причины отзыва.

4.3.6 Приостановление действия сертификатов открытых ключей

УЦ обязан приостановить действие сертификата открытого ключа во всех случаях, установленных данным Регламентом.

УЦ обязан в течение 24 часов занести сведения о приостановленном сертификате в список отозванных сертификатов с указанием даты и времени занесения и признака приостановления.

4.3.7 Возобновление действия сертификатов открытых ключей

УЦ обязан возобновить действие сертификата открытого ключа по заявлению его владельца и в течение 24 часов исключить сведения о приостановленном сертификате из списка отозванных сертификатов.

4.3.8 Уведомления

4.3.8.1 Уведомление о факте отзыва сертификата открытого ключа

Официальным уведомлением о факте отзыва сертификата является опубликование списка отозванных сертификатов, содержащим сведения об отозванном сертификате на точку распространения списка отзыва, указанную в сертификате открытого ключа.

Временем отзыва сертификата открытого ключа признается время занесения сведений об отозванном сертификате в список отозванных сертификатов и включенное в его структуру.

Временем опубликования списка отозванных сертификатов признается время включения списка отозванных сертификатов в структуру хранилища.

4.3.8.2 Уведомление о факте приостановления действия сертификата открытого ключа

Официальным уведомлением о факте приостановления действия сертификата является опубликование списка отозванных сертификатов, содержащего сведения о

приостановленном сертификате, на точку распространения списка отзыва, указанную в сертификате открытого ключа.

Временем приостановления действия сертификата открытого ключа признается включенное в его структуру время занесения сведений о приостановленном сертификате в список отозванных сертификатов.

Временем опубликования списка отозванных сертификатов признается время включения списка отозванных сертификатов в структуру хранилища.

4.3.8.3 Уведомление о факте возобновления действия сертификата открытого ключа

Официальным уведомлением о факте возобновления действия сертификата является опубликование списка отозванных сертификатов, не содержащего сведения о приостановленном сертификате на точку распространения списка отзыва, указанную в сертификате открытого ключа. Список отозванных сертификатов должен иметь включенное в его структуру время изготовления списка отозванных сертификатов более позднее, чем приостановление действия сертификата.

Временем возобновления действия сертификата открытого ключа признается время официального уведомления о факте возобновления действия сертификата.

Осуществление удаленного подключения с использованием сертификата, который был восстановлен возможно после прохождения синхронизации данных о восстановлении сертификата в корпоративных информационных системах. Синхронизация может занимать до 2-х рабочих дней.

4.3.9 Реестр сертификатов открытых ключей

УЦ обязан вести реестр всех изготовленных сертификатов открытых ключей пользователей в течение установленного срока хранения.

Реестр сертификатов открытых ключей ведется в электронном виде.

Сертификаты открытых ключей представлены в реестре в форме электронных копий изготовленных сертификатов.

УЦ обязан осуществлять выдачу копий сертификатов открытых ключей в электронной форме по обращениям пользователей.

4.4 Обязательства пользователей УЦ

Лица, проходящие процедуру регистрации в реестре УЦ, обязаны представить достоверную регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента.

4.4.1 Обязанности владельцев сертификатов открытых ключей

Пользователи – владельцы сертификатов открытых ключей обязаны:

- обеспечить сохранность ключевого носителя и недоступность закрытого ключа другим лицам, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
- обеспечить защиту ключевого носителя от копирования;
- использовать ключи только для целей, разрешенных соответствующими областями использования, определенными в сертификате, в соответствии с должностными обязанностями;
- не использовать ключи в случаях не предусмотренных должностными обязанностями;
- немедленно, в течение 1 часа, обратиться в УЦ с заявлением на отзыв сертификата открытого ключа в случае, если ему известно, что произошла компрометация ключа.

Перед тем как использовать сертификат открытого ключа, изготовленный УЦ, пользователь сертификата должен удостовериться, что его назначение, определенное соответствующими областями использования, определенными в сертификате, соответствует предполагаемому использованию. Запрещается использование ключей в случаях, не предусмотренных должностными обязанностями пользователя.

Пользователь сертификата должен самостоятельно отслеживать срок действия сертификата открытого ключа.

При завершении работ и отсутствия необходимости дальнейшего использования ключа пользователь должен обратиться в УЦ через систему ИТ-каталог для аннулирования сертификата.

5 Процедуры и механизмы реализации функционала удостоверяющего центра

5.1 Регистрация пользователей УЦ

Под регистрацией пользователей понимается внесение регистрационной информации о них в реестр Удостоверяющего Центра.

Процедура регистрации пользователей ИОК применяется в отношении физических лиц, обращающихся к услугам УЦ в части изготовления сертификатов открытых ключей пользователей и/или формирования закрытых и открытых ключей пользователей с записью их на ключевой носитель.

Регистрация пользователей ИОК на УЦ проводится на основе заявок администраторами УЦ. Заявки оформляются в системе ИТ-каталог.

Администраторы УЦ должны производить рассмотрение заявок на получение сертификатов и/или закрытых и открытых ключей в зависимости от категории заявки от 1 до 10 рабочих дней после подачи заявки.

5.1.1 Процедура регистрации внутренних пользователей

Процесс регистрации внутренних пользователей состоит из следующих процедур:

1) Заключение договора между АО «Северсталь-инфоком» и организацией на услуги УЦ.

2) Формирование заявки в электронном виде в системе ИТ-каталог, в которой указываются следующие сведения:

- Фамилия, Имя, Отчество пользователя;
- Должность, наименование подразделения;
- Телефон, адрес электронной почты;
- Имя пользователя в доменной структуре (full account name);
- Тип сертификатов (область использования сертификата):
  - для аутентификации в доменной структуре (в т.ч. для удаленного доступа);
  - для шифрования внутренней почты;
  - для обмена шифрованными сообщениями с внешними пользователями;

- для создания неквалифицированной электронной подписи на документах.
- Номер КЕ (оборудования).

3) Согласование по процедуре, установленной в информационной системе.
4) Проверка заявки администраторами УЦ на предмет правильности и полноты заполнения и принимается к выполнению или отклоняется с указанием причин отказа регистрации пользователя ИОК.
5) В случае положительного решения о регистрации пользователя ИОК на УЦ пользователю направляется сообщение электронной почты о необходимости личного присутствия пользователя для получения запрашиваемых сертификатов и ключей, в случае, если пользователь ранее не обращался в УЦ. УЦ может привлекать для проведения процедуры выдачи сертификатов и ключей пользователю ИОК сотрудников смежных подразделений при условии обязательного установления личности пользователя ИОК при выдаче. Допускается получение сертификатов и ключей представителем по доверенности.
6) В случае, если пользователь ранее уже обращался в УЦ, ему направляется инструкция с описанным порядком действий по запросу необходимых сертификатов и ключей.
7) По окончании процедуры регистрации, зарегистрированному пользователю УЦ выдаются:
   - ключи, записанные на ключевой носитель (в случае получения ключей лично);
   - сертификат открытого ключа в электронной форме, соответствующий закрытому ключу;
   - копии сертификатов открытого ключа в электронной форме уполномоченного лица Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии (цепочка Центров сертификации, вплоть до корневого издающего Центра сертификации;
   - Руководство по обеспечению безопасности использования ЭП, средств ЭП, ключевого носителя многократного использования (при первом обращении в УЦ).

Допускается отправка ключевого носителя почтовым отправлением или курьерской службой.

5.1.2 Процедура регистрации внешних пользователей

Процесс регистрации внешних пользователей состоит из следующих процедур:

1) Заключение договора между АО «Северсталь-инфоком» и организацией или физическим лицом на услуги УЦ.
2) Создается учетная запись пользователя в корпоративном домене.
3) Формируется заявка в системе ИТ-каталог, в которой указываются следующие сведения:
   - Фамилия, Имя, Отчество пользователя;
   - Должность, наименование организации, наименование подразделения, в котором работает пользователь в рамках организации, которую он представляет;
   - Телефон, адрес электронной почты;
   - Тип сертификата;
   - Адрес доставки ключевого носителя (при необходимости).
4) Согласование по процедуре, установленной в информационной системе.
5) Проверка заявки сотрудниками подразделения эксплуатации УЦ на предмет правильности и полноты заполнения и принимается к выполнению или отклоняется с указанием причин отказа регистрации сотрудника.
6) В случае положительного решения о регистрации пользователя ИОК на УЦ пользователю направляется сообщение электронной почты о необходимости личного присутствия пользователя для получения запрашиваемых сертификатов и ключей, в случае, если пользователь ранее не обращался в УЦ. УЦ может привлекать для проведения процедуры выдачи сертификатов и ключей пользователю ИОК сотрудников смежных подразделений при условии обязательного установления личности пользователя ИОК при выдаче. Допускается получение сертификатов и ключей представителем по доверенности.
7) В случае, если пользователь ранее уже обращался в УЦ, ему направляется инструкция с описанным порядком действий по запросу необходимых сертификатов и ключей.
8) По окончании процедуры регистрации, зарегистрированному пользователю УЦ выдаются:

- ключи, записанные на ключевой носитель (в случае получения ключей лично);
- сертификат открытого ключа в электронной форме, соответствующий закрытому ключу;
- копии сертификатов открытого ключа в электронной форме уполномоченного лица Удостоверяющего Центра и вышестоящих Удостоверяющих Центров по иерархии (цепочка Центров сертификации, вплоть до корневого издающего Центра сертификации;
- Руководство по обеспечению безопасности использования ЭП, средств ЭП, ключевого носителя многократного использования (при первом обращении в УЦ).

Допускается отправка ключевого носителя почтовым отправлением или курьерской службой.

5.2 Процедуры работы с сертификатами и ключами шифрования

5.2.1 Создание ключей и сертификатов Центра сертификации

Формирование ключей Центра Сертификации производится администратором ЦС следующим образом: администратор Центра сертификации осуществляет формирование секретного ключа ЦС и сертификата открытого ключа ЦС; с секретного ключа ЦС формируется резервная копия, которая хранится у руководителя (менеджера) УЦ в сейфе. Формирование резервной копии секретного ключа ЦС возможно только для тех ЦС, сертификат которых не подписан алгоритмом ГОСТ.

5.2.2 Обновление ключей и сертификатов Центров сертификации

5.2.2.1 Плановая смена ключей Центра Сертификации

Заблаговременно (не менее чем за 1 месяц до окончания срока действия секретного ключа ЦС) администратор ЦС производит обновление сертификата ЦС, продлевая срок его действия, используя тот же секретный ключ ЦС. После этого новый сертификат ЦС необходимо распространить на все объекты инфраструктуры, в которых задействован сертификат УЦ.

Все администраторы и пользователи систем (объектов инфраструктуры) обязаны получить новый сертификат ЦС и добавить его в справочники сертификатов. Руководитель (менеджер) УЦ производит уведомление пользователей о смене сертификата ЦС. Уведомление осуществляется по электронной почте. В электронном

письме должны быть инструкции (или ссылки на инструкции), содержащие способ получения нового сертификата УЦ.

5.2.2.2 Компрометация ключей Центра Сертификации

В случае компрометации ключа Центра Сертификации вся система УЦ должна быть остановлена. Руководитель (менеджер) УЦ немедленно производит уведомление всех пользователей сертификатов открытых ключей, руководителей подразделений, в которых работают пользователи сертификатов открытых ключей, руководителя подразделения по работе с клиентами, руководителя Управления информационной безопасности, а также руководителя подразделения технической поддержки и прочих подразделений, эксплуатирующих устройства, использующих в своей работе сертификаты, выданные скомпрометированным УЦ. В оповещении указывается факт компрометации ключа Центра Сертификации, а также строгая необходимость прекращения какого-либо использования сертификатов, выданных скомпрометированным УЦ.

В том случае, если сертификат УЦ скомпрометирован, то все сертификаты, выданные УЦ, подчиненных скомпрометированному, также считаются скомпрометированными.

Для восстановления УЦ необходимо:

- удалить сертификат скомпрометированного УЦ и всех подчиненных ему УЦ со всех объектов использования;
- повторно произвести формирование ключей и сертификатов всей скомпрометированной цепочки ЦС;
- обеспечить получение сертификатов и СОС скомпрометированной цепочки ЦС всеми пользователями системы;
- произвести выпуск новых сертификатов всех пользователей, согласно процедурам, описанным в настоящем Регламенте.

5.2.3 Создание ключей и сертификатов внутренних пользователей

5.2.3.1 Процесс формирования сертификатов и ключей шифрования при личном обращении пользователя состоит из следующих процедур:

1) регистрация пользователя на УЦ на основе информации, указанной в заявке (см. п. 5.1.1);
2) администратор УЦ инициализирует ключевой носитель (токен), задав случайное значение пароля доступа к ключевому носителю, которое должно

быть в обязательном порядке сменено пользователем сертификата открытого ключа;

3) администратор УЦ выполняет генерацию ключей и запись их на ключевой носитель;
4) администратор УЦ формирует запрос к Центру сертификации на формирование сертификатов открытых ключей;
5) администратор УЦ издает сертификаты открытых ключей и публикует их в ресурсные системы (при необходимости);
6) администратор УЦ производит запись сертификатов открытых ключей пользователя и сертификатов открытых ключей УЦ на носитель (токен);
7) пользователю выдается носитель (токен) с сертификатами открытых ключей пользователя и УЦ;
8) администраторы УЦ проводят инструктаж пользователя по использованию сертификатов и ключей шифрования;
9) пользователи получают Руководство по обеспечению безопасности использования ЭП, средств ЭП, ключевого носителя многократного использования, в котором определены его обязанности и правила работы с ключевой информацией.

Получение носителей сертификатов и ключей шифрования осуществляется при личном присутствии пользователя в УЦ с предъявлением документа, подтверждающего личность. УЦ может привлекать для проведения процедуры выдачи сертификатов и ключей пользователю сотрудников смежных подразделений при условии обязательного установления личности пользователя при выдаче. Пользователь расписывается в ведомости выданных носителей ключевой информации и журнале учёта СКЗИ.

5.2.3.2 Обновление ключей и сертификатов внутренних пользователей

Обновление ключей и сертификатов внутренних пользователей производится либо по истечении срока действия ключей или сертификатов, либо в случае отзыва сертификатов.

Процедура обновления сертификатов открытых ключей идентична процедуре первоначального выпуска сертификатов открытых ключей пользователей ИОК, за исключением прохождения процедуры регистрации пользователя. По окончании процедуры обновления пользователю УЦ на его персональный ключевой носитель производится запись «обновленного» сертификата открытого ключа.

УЦ обязан опубликовать «обновленный» сертификат открытого ключа пользователя в реестр сертификатов открытого ключа согласно процедурам,

выполняемым при публикации первично выдаваемого сертификата пользователя в данный реестр.

5.2.4 Приостановление действия и отзыв сертификатов внутренних пользователей

Процедура приостановления действия сертификатов пользователя выполняется администраторами УЦ в случае блокировки учетной записи пользователя в домене. После восстановления УЗ, создается заявка в ИТ-каталоге и действие его сертификата возобновляется.

Процедура отзыва сертификатов выполняется администраторами УЦ в следующих случаях:

- компрометация или подозрение на компрометацию закрытого ключа (в том числе потеря ключа);
- изменение идентифицирующей информации или атрибутов в сертификате пользователя до истечения срока действия сертификата;
- невыполнение пользователем сертификата правил использования инфраструктуры открытых ключей и требований Руководства по обеспечению безопасности использования ЭП, средств ЭП, ключевого носителя многократного использования;
- другие обоснованные причины (в случае увольнения сотрудника, разрыва отношений – для внешних пользователей организаций-клиентов и т.п).

Процедура отзыва сертификатов пользователей может быть выполнена по инициативе следующих лиц:

- внутренний пользователь ИОК;
- сотрудники Управления информационной безопасности;
- руководитель (менеджер) УЦ.

Все отозванные сертификаты и сертификаты с приостановленным действием помещаются сотрудниками подразделения эксплуатации УЦ в списки отозванных сертификатов (СОС).

Сертификаты, подлежащие процедуре приостановления, не позднее 48 часов, помещаются в списки отозванных сертификатов как сертификаты с приостановленным действием на основании заявки от перечисленных выше лиц по заявке, оформленной в ИТ-каталоге.

В случае подачи заявки на приостановление сертификата по телефону необходимо в течение суток оформить заявку в ИТ-каталоге на приостановление

сертификата и передать ее сотрудникам отдела эксплуатации УЦ. Формат заявки на приостановление сертификата совпадает с форматом заявки на отзыв. В заявке на отзыв (приостановление) сертификата указываются следующие сведения:

- фамилия, имя, отчество пользователя;
- должность, наименование организации;
- телефон, адрес электронной почты;
- зарегистрированный номер сертификата;
- причина отзыва сертификатов (для приостановленных сертификатов устанавливается значение – сертификат приостановлен).

Сотрудниками подразделения эксплуатации УЦ должны поместить сертификат в списки отозванных сертификатов не позднее 48 часов после получения заявки.

Отозванные сертификаты пользователей не возобновляются. Новые сертификаты пользователь может получить только после того, как будет получена заявка на отзыв старого сертификата.

Отозванные сертификаты в обязательном порядке сохраняются в реестре УЦ, а также в локальной базе УЦ. Отозванные сертификаты подлежат архивированию до окончания срока их действия (конечной даты, указанной в сроке действия сертификата).

После отзыва сертификатов пользователь должен предоставить в УЦ носитель сертификатов для уничтожения ключей.

5.2.5 Создание ключей и сертификатов внешних пользователей

Процесс формирования сертификатов и ключей внешних пользователей аналогичен процедурам, описанным для внутренних пользователей.

5.2.6 Журнал учета изданных сертификатов

Все выданные сертификаты пользователей подлежат обязательному учету. Учет выданных сертификатов ведется средствами JMS и ИТ-каталога. При выдаче ключей и сертификатов пользователя ИОК, записанных на отчуждаемый ключевой носитель, данные о выдаче заносятся в журнал учета изданных сертификатов. Сотрудники УЦ и смежных подразделений, привлекаемых УЦ для выдачи сертификатов и ключей пользователей ИОК, ведут журналы учёта выдачи ключей и сертификатов. Пользователь ИОК получает ключевой носитель проставив личную подпись в соответствующей графе журнала.

5.3 Процедуры работы со списками отозванных сертификатов

Список отозванных сертификатов должен выпускаться немедленно после отзыва сертификата. Публикация СОС в точки распространения списков отзыва, указанные в сертификатах открытых ключей, производится в течение 1 часа после формирования СОС.

Частота обновления СОС издающего УЦ в случае, если ни один сертификат за этот период не был отозван - 2 дня.

Администраторы корпоративных инфраструктурных сервисов и информационных систем должны регулярно обновлять СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств.

5.4 Работа с носителями ключевой информации

5.4.1 Все выданные носители с ключевой информацией подлежат обязательному учету. Хранение ключевых носителей

Личные ключевые носители пользователей рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение своих ключевых носителей.

5.4.2 Права и обязанности пользователей

Пользователь, которому в соответствии с его должностными функциями выдан ключевой носитель, обязан:

- лично получить ключевой носитель, чтобы быть уверенным в том, что содержание его ключевого носителя не компрометировано или в случае получения ключевого носителя почтовым отправлением убедиться, что конверт не был вскрыт;
- в случае порчи ключевого носителя пользователь обязан сделать соответствующую заявку в ИТ-каталоге и передать его сотруднику УЦ.

Пользователю запрещается:

- передавать свой персональный ключевой носитель другим лицам (кроме как для хранения ответственному за информационную безопасность или сотрудникам УЦ);
- оставлять персональный ключевой носитель без личного присмотра на рабочем месте и где бы то ни было;

- делать копии ключевого носителя, распечатывать или переписывать с неё файлы на иной носитель информации, вносить изменения в файлы, находящиеся на ключевом носителе;
- использовать персональный ключевой носитель на заведомо неисправном персональном компьютере.

Пользователь имеет право обращаться к сотрудникам УЦ за консультациями по вопросам использования ключевого носителя и по вопросам обеспечения информационной безопасности технологического процесса ИОК.

Пользователь несет персональную ответственность за сохранность и правильное использование вверенной ему персональной ключевой информации. Нарушения данных требований является основанием для применения к пользователю административных мер наказания.

6 Восстановление УЦ после аварий

Под авариями, которым может быть подвержен УЦ, рассматриваются следующие нештатные ситуации:

- События, повлекшие временную неработоспособность ПО УЦ:
  - сбои ПО УЦ;
  - сбои системного ПО;
  - выход из строя компонентов серверов УЦ;
- события, повлекшие потерю информации и неработоспособность ПО УЦ:
  - вирусные атаки;
  - сбои ПО УЦ;
  - сбои системного ПО;
  - выход из строя компонентов серверов УЦ.

Ответственность за обеспечение работоспособности УЦ и восстановление УЦ после сбоев несет руководитель (менеджер) УЦ. В обязанности администраторов УЦ по восстановлению УЦ после сбоев входит выполнение следующих процедур:

- определение неисправности;
- замена неисправных компонентов аппаратных платформ;
- установка и настройка системного ПО и ПО УЦ;
- восстановление информации из резервных копий.

В рамках процедур по восстановлению УЦ администраторы УЦ могут привлекать сотрудников подразделений технической поддержки предприятия клиентов и принимать во временное пользование дополнительные технические средства.

6.1 Восстановление после аварий

Восстановление после аварий, повлекших временную неработоспособность ПО УЦ и не повлекших потерю информации, выполняют администраторы УЦ собственными силами путем перезапуска, перенастройки системного программного обеспечения и программного обеспечения УЦ, а также замены компонентов серверов УЦ.

Время восстановления работоспособности УЦ после аварий повлекшие временную неработоспособность ПО УЦ и не повлекших потерю информации не должно превышать 4 часов.

Восстановление после аварий, сопровождающихся временной неработоспособность ПО УЦ и потерей информации, выполняют администраторы УЦ

как собственными силами, так и с привлечением специалистов подразделений технической поддержки путем восстановления данных из резервных копий, ПО – с дистрибутивных дисков программного обеспечения, баз данных – из резервных копий баз данных. Замена неисправных компонентов серверов УЦ может производиться с использованием временно предоставленных подразделением технической поддержки технических средств.

Восстановление УЦ производится в следующем порядке:

- Восстановление работоспособности серверов ЦС:
  - замена неисправных компонентов серверов УЦ;
  - установка системного ПО и ПО УЦ;
  - восстановление из резервных копий данных УЦ.

Приоритет должен быть отдан возможности отзыва сертификатов и выпуска СОС.

Время восстановления работоспособности УЦ после аварий повлекшие потерю информации и неработоспособность ПО УЦ не должно превышать 1 дня.

7 Обслуживание УЦ

Обслуживание УЦ АО «Северсталь-инфоком» в г. Череповец выполняется подразделением эксплуатации УЦ. В обязанности сотрудников подразделения эксплуатации УЦ входит:

- проведение мероприятий, направленных на обеспечение безопасности УЦ;
- поддержание работоспособности УЦ:
  - аудит журналов ОС и ПО УЦ, в части системных событий и событий, влияющих на безопасность;
  - периодическое резервное копирование информации УЦ;
  - проверка работоспособности программных и аппаратных средств УЦ.

Поддержка инфраструктуры аппаратных и программных средств обеспечения деятельности УЦ в обязанности сотрудников подразделения эксплуатации УЦ не входит.