

УТВЕРЖДЕН

Приказом

от 26.04.2022г. № 3-1-100/000818-22

ПОРЯДОК
реализации АО «Торговый дом
«ПЕРЕКРЕСТОК» функций аккредитованного
удостоверяющего центра и исполнения его
обязанностей

Владелец	Начальник Управления криптографии Департамента информационной безопасности
Введен в действие	01.01.2023 г.
Срок действия	действует с даты введения в действие и до даты издания распорядительного документа, отменяющего действие
Проверка актуальности	1 раз в год

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	3
2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УЦ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)	3
3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	4
4. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ	6
5. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УЦ.....	10
6. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	11
7. ТЕРМИНЫ И СОКРАЩЕНИЯ	17
8. СВЯЗАННЫЕ ДОКУМЕНТЫ	20
Приложение 1. Форма Заявления на выдачу КСКПЭП.....	21
Приложение 2. Форма Заявления на прекращение действия КСКПЭП	23
Приложение 3. Форма Заявления на подтверждение подлинности ЭП в электронном документе	24
Приложение 4. Форма Заявления на получение информации о статусе КСКПЭП.....	25
Приложение 5. Руководство по обеспечению безопасности использования квалифицированной ЭП и средств квалифицированной ЭП.....	26

История изменений

Версия	Дата	Описание изменений	Разработчик
1.0	19.03.2020	Исходная версия	Корчинская Е.
2.0		Переработан в соответствии с Требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденными приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13.11.2020 № 584 и решением рабочей группы X5 Group по аккредитации от 10.11.2021	Корчинская Е.

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Предмет регулирования
 - 1.1.1. Порядок реализации АО «Торговый дом «ПЕРЕКРЕСТОК» функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее – Порядок) разработан в соответствии с Требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденными приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13.11.2020 № 584, является локальным нормативным документом АО «Торговый дом «ПЕРЕКРЕСТОК» и определяет процедуру выполнения АО «Торговый дом «ПЕРЕКРЕСТОК» функций УЦ, а также его права и обязанности.
 - 1.1.2. АО «Торговый дом «ПЕРЕКРЕСТОК» осуществляет функции УЦ непосредственно и через доверенных лиц в соответствии с пунктом 4 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».
 - 1.1.3. Термины, используемые в Порядке, применяются в значениях, определенных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
 - 1.1.4. Электронная версия Порядка размещается на официальном сайте УЦ в информационно-телекоммуникационной сети "Интернет" по адресу <http://cdp.x5.ru/> (далее – официальный сайт УЦ в сети «Интернет»).
- 1.2. Сведения об УЦ
 - 1.2.1. Информация о месте нахождения и графике работы УЦ размещена на официальном сайте УЦ в сети "Интернет".
- 1.3. Порядок информирования о предоставлении услуг УЦ
 - 1.3.1. УЦ осуществляет информирование заявителей о предоставлении услуг по телефону, электронной почте, через официальный сайт УЦ в сети «Интернет».
 - 1.3.2. Справочный телефон УЦ: +7(495)662-88-88.
 - 1.3.3. Электронная почта УЦ: uc@x5.ru .
 - 1.3.4. Официальный сайт УЦ в сети «Интернет»: <http://cdp.x5.ru/> .
- 1.4. Стоимость услуг УЦ
 - 1.4.1. Стоимость услуг УЦ, сроки и порядок расчетов за оказание услуг УЦ определяются согласованным Договором на оказание услуг УЦ.

2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УЦ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

- 2.1. УЦ в соответствии с частью 1 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» выполняет следующие функции:
 - 2.1.1. создает и выдает КСКПЭП;
 - 2.1.2. осуществляет подтверждение владения заявителем ключом электронной подписи (далее - ключ ЭП), соответствующим ключу проверки электронной подписи (далее - ключ проверки ЭП), указанному им для получения КСКПЭП;
 - 2.1.3. устанавливает сроки действия КСКПЭП;
 - 2.1.4. аннулирует КСКПЭП;

- 2.1.5. выдает по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП;
 - 2.1.6. ведет реестр выданных и аннулированных КСКПЭП (далее – реестр КСКПЭП);
 - 2.1.7. создает по обращениям заявителей ключи ЭП и ключи проверки ЭП;
 - 2.1.8. проверяет уникальность ключа проверки ЭП в реестре КСКПЭП;
 - 2.1.9. осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
 - 2.1.10. осуществляет иную связанную с использованием электронной подписи деятельность.
- 2.2. Доверенные лица УЦ в соответствии с частью 4 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» выполняют следующие функции:
- 2.2.1. принимают заявления на выдачу КСКПЭП (далее – заявление на КСКПЭП);
 - 2.2.2. вручают КСКПЭП от имени УЦ;
 - 2.2.3. идентифицируют заявителя при его личном присутствии.

3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

- 3.1. УЦ в соответствии с частью 4 статьи 13 и частью 4 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» вправе:
- 3.1.1. наделять третьих лиц (доверенных лиц) полномочиями по приему заявлений на КСКПЭП и вручению КСКПЭП от имени УЦ;
 - 3.1.2. выдавать КСКПЭП как в форме электронных документов, так и в форме документов на бумажном носителе
- 3.2. УЦ в соответствии с частями 2, 6 статьи 13, частью 7 статьи 14, частями 1, 2.1, 3, 4 статьи 15, частями 1, 2.2, 3, 4 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» обязан:
- 3.2.1. информировать заявителей об условиях и порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;
 - 3.2.2. обеспечивать актуальность информации, содержащейся в реестре КСКПЭП, её защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
 - 3.2.3. предоставлять безвозмездно любому лицу в соответствии с Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации от 22.08.2017 № 436, информацию, содержащуюся в реестре КСКПЭП;
 - 3.2.4. обеспечивать конфиденциальность созданных ключей ЭП;
 - 3.2.5. отказать заявителю в создании и выдаче КСКПЭП, если:
 - 3.2.5.1. не подтверждена достоверность представленных сведений;
 - 3.2.5.2. не подтверждено владение ключом ЭП, соответствующим ключу проверки ЭП;
 - 3.2.5.3. не подтверждена уникальность ключа проверки ЭП;

- 3.2.6. вносить информацию о прекращении действия или аннулировании КСКПЭП в реестр КСКПЭП;
- 3.2.7. хранить в течение всего периода осуществления функций УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, следующую информацию:
 - 3.2.7.1. реквизиты основного документа, удостоверяющего личность владельца КСКПЭП;
 - 3.2.7.2. сведения, подтверждающие ознакомление заявителя с содержанием КСКПЭП;
- 3.2.8. использовать усиленную квалифицированную ЭП, основанную на КСКПЭП, выданном головным удостоверяющим центром;
- 3.2.9. обеспечивать круглосуточную доступность реестра КСКПЭП в сети «Интернет», за исключением периодов технического обслуживания;
- 3.2.10. при принятии решения о прекращении выполнения функций аккредитованного удостоверяющего центра:
 - 3.2.10.1. сообщить об этом в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, определенный постановлением Правительства Российской Федерации от 28.11.2011 № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи» (далее - уполномоченный федеральный орган), не позднее чем за один месяц до даты прекращения выполнения функций аккредитованного удостоверяющего центра;
 - 3.2.10.2. передать в уполномоченный федеральный орган в соответствии с Порядком передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного удостоверяющего центра, утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.08.2017 № 416, реестр КСКПЭП, информацию, подлежащую хранению в УЦ;
 - 3.2.10.3. уведомить в письменной форме владельцев КСКПЭП, срок действия которых не истек, не менее чем за один месяц до даты прекращения осуществления своих функций;
- 3.2.11. при обращении за созданием и выдачей КСКПЭП:
 - 3.2.11.1. идентифицировать заявителя;
 - 3.2.11.2. получить от заявителя подтверждение правомочия обращаться за получением КСКПЭП;
 - 3.2.11.3. осуществить проверку достоверности документов и сведений, представленных заявителем, с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие действующих и создаваемых информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (далее - инфраструктура);
 - 3.2.11.4. ознакомить заявителя с информацией, содержащейся в КСКПЭП, под расписку, в том числе посредством использования квалифицированной электронной подписи при наличии действующего сертификата;

- 3.2.11.5. предоставить заявителю руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

4. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ

4.1. Процедура создания ключей ЭП и ключей проверки ЭП.

4.1.1. Создание ключа ЭП и ключа проверки ЭП осуществляется:

4.1.1.1. с использованием средств ЭП, имеющих подтверждение соответствия требованиям, установленным приказом ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требованиям к средствам удостоверяющего центра»;

4.1.1.2. в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с ФСБ России в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 09.02.2005 № 66, следующими способами:

4.1.1.2.1. самостоятельно заявителем на его автоматизированном рабочем месте (далее – АРМ);

4.1.1.2.2. оператором УЦ по обращению заявителя на АРМ оператора УЦ.

4.2. Планы, основания, процедуры, сроки и порядок смены ключей ЭП УЦ, а также порядок информирования владельцев КСКПЭП об осуществлении такой смены.

4.2.1. Смена ключа ЭП, используемого для подписания КСКПЭП, осуществляется УЦ в связи с истечением срока его действия (далее - плановая смена ключа ЭП).

4.2.2. Плановая смена ключа ЭП производится не позднее 10 рабочих дней до дня истечения периода его использования для создания КСКПЭП, установленного эксплуатационной документацией на средство УЦ. УЦ в рамках плановой смены ключа ЭП осуществляется создание ключа ЭП и запроса на КСКПЭП, который направляется в головной удостоверяющий центр.

4.2.3. Информирование владельцев КСКПЭП о плановой смене ключа ЭП, в том числе указание доверенного способа получения сертификата УЦ, осуществляется путем размещения соответствующей информации на официальном сайте УЦ в сети «Интернет».

4.3. Порядок осуществления смены ключей ЭП УЦ в случаях нарушения их конфиденциальности.

4.3.1. Смена ключа ЭП, используемого для подписания КСКПЭП, осуществляется УЦ в случаях нарушения его конфиденциальности, угрозы нарушения его конфиденциальности (далее - внеплановая смена ключа ЭП). Со дня установления факта нарушения конфиденциальности ключа ЭП УЦ прекращает его использование.

4.3.2. Внеплановая смена ключа ЭП осуществляется не позднее одного рабочего дня со дня установления факта нарушения его конфиденциальности, угрозы нарушения его конфиденциальности.

4.3.3. К угрозам нарушения конфиденциальности ключа ЭП относятся:

4.3.3.1. применение в отношении программных средств УЦ, имеющих доступ к ключу ЭП УЦ, вредоносного программного обеспечения;

4.3.3.2. нарушение правил хранения и эксплуатации ключа ЭП УЦ;

- 4.3.3.3. несанкционированный доступ в помещения, в которых располагаются средства УЦ, на которых осуществляется хранение и использование ключа ЭП УЦ.
- 4.3.4. В связи с внеплановой сменой ключа ЭП прекращается действие КСКПЭП, созданных с использованием ключа ЭП УЦ, с занесением сведений в реестр КСКПЭП.
- 4.3.5. Информирование владельцев КСКПЭП о внеплановой смене ключа ЭП, в том числе указание доверенного способа получения сертификата УЦ, исключающего уничтожение, модифицирование, блокирование при передаче и иные неправомерные действия с сертификатом УЦ, осуществляется путем размещения соответствующей информации на официальном сайте УЦ в сети "Интернет" не позднее одного рабочего дня со дня установления факта нарушения конфиденциальности ключа ЭП или угрозы нарушения его конфиденциальности.
- 4.4. Порядок смены ключа ЭП владельца КСКПЭП
- 4.4.1. Смена ключа ЭП по инициативе владельца КСКПЭП осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».
- 4.4.2. Смена ключа ЭП осуществляется на основании заявления на КСКПЭП.
- 4.4.3. В заявлении на КСКПЭП указываются:
- 4.4.3.1. Фамилия, имя, отчество (при наличии) владельца КСКПЭП;
 - 4.4.3.2. Реквизиты основного документа, удостоверяющего личность;
 - 4.4.3.3. Идентификационный номер налогоплательщика;
 - 4.4.3.4. Страховой номер индивидуального лицевого счёта;
 - 4.4.3.5. Адрес электронной почты (при наличии).
- 4.4.4. Заявление на КСКПЭП подписывается заявителем.
- 4.4.5. Создание КСКПЭП осуществляется при условии:
- 4.4.5.1. Идентификации заявителя;
 - 4.4.5.2. Подтверждения достоверности представленных сведений с использованием инфраструктуры;
 - 4.4.5.3. Подтверждения владения заявителем ключом ЭП, соответствующим ключу проверки ЭП;
 - 4.4.5.4. Подтверждения уникальности ключа проверки ЭП.
- 4.4.6. КСКПЭП создаётся в течение 5 рабочих дней со дня подачи заявления.
- 4.4.7. КСКПЭП выдаётся в форме документа на бумажном носителе после идентификации заявителя и ознакомления с информацией, содержащейся в КСКПЭП.
- 4.4.8. Одновременно с КСКПЭП выдаётся Руководство по обеспечению безопасности использования усиленной электронной подписи.
- 4.5. Процедура создания и выдачи КСКПЭП.
- 4.5.1. Создание КСКПЭП осуществляется на основании заявления на КСКПЭП, которое формируется в месте выдачи КСКПЭП УЦ по месту нахождения заявителя на бумажном носителе.
- 4.5.2. В заявлении на выдачу КСКПЭП указывается:
- 4.5.2.1. Фамилия, имя, отчество (при наличии) заявителя;
 - 4.5.2.2. Реквизиты основного документа, удостоверяющего личность;

- 4.5.2.3. Идентификационный номер налогоплательщика;
- 4.5.2.4. Страховой номер индивидуального лицевого счёта;
- 4.5.2.5. Адрес электронной почты (при наличии).
- 4.5.3. Заявление на КСКПЭП подписывается заявителем.
- 4.5.4. Одновременно с заявлением на сертификат представляется документ, удостоверяющий личность заявителя, реквизиты которого указаны в заявлении на КСКПЭП.
- 4.5.5. Создание КСКПЭП осуществляется при условии:
 - 4.5.5.1. Идентификации заявителя;
 - 4.5.5.2. Подтверждения достоверности представленных сведений с использованием инфраструктуры;
 - 4.5.5.3. Подтверждения владения заявителем ключом ЭП, соответствующим ключу проверки ЭП;
 - 4.5.5.4. Подтверждения уникальности ключа проверки ЭП.
- 4.5.6. Идентификация осуществляется при личном присутствии по следующим документам:
 - 4.5.6.1. гражданина Российской Федерации по основному документу, удостоверяющему личность;
 - 4.5.6.2. иностранного гражданина по паспорту гражданина иностранного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;
 - 4.5.6.3. беженца, лица без гражданства по документу, установленному законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.
- 4.5.7. КСКПЭП создаётся в течение 5 рабочих дней со дня подачи заявления. Срок создания КСКПЭП может быть увеличен до 30 рабочих дней в случае несвоевременного получения сведений, находящихся в распоряжении государственных органов, иных органов, необходимых для создания КСКПЭП. Срочное создание и выдача КСКПЭП не осуществляется.
- 4.5.8. КСКПЭП выдаётся в форме документа на бумажном носителе после идентификации заявителя и ознакомления с информацией, содержащейся в КСКПЭП.
- 4.5.9. Одновременно с КСКПЭП выдаётся Руководство по обеспечению безопасности использования усиленной электронной подписи.
- 4.6. Подтверждение действительности ЭП, использованной для подписания электронных документов.
 - 4.6.1. Подтверждение действительности ЭП, использованной для подписания электронных документов, осуществляется в отношении ЭП, созданной с использованием сертификата УЦ.
 - 4.6.2. Подтверждение действительности ЭП осуществляется на основании заявления, подаваемого в УЦ.
 - 4.6.3. В заявлении указываются:
 - 4.6.3.1. фамилия, имя и отчество (при наличии) лица, подающего заявление;
 - 4.6.3.2. уникальный серийный номер КСКПЭП;
 - 4.6.3.3. фамилия, имя и отчество (при наличии) владельца КСКПЭП, с использованием которого создана ЭП, действительность которой требуется проверить;

- 4.6.3.4. дата и время, на момент наступления которых требуется установить подлинность ЭП;
- 4.6.3.5. адрес, на который необходимо направить результаты проверки действительности ЭП.
- 4.6.4. Одновременно с заявлением предоставляется электронный документ с ЭП, действительность которой необходимо проверить, на съемном носителе информации.
- 4.6.5. Подтверждение действительности ЭП, использованной для подписания электронного документа, осуществляется в течение 5 рабочих дней со дня поступления заявления/
- 4.6.6. Проверка действительности ЭП, использованной для подписания электронного документа, включает проверку соответствия формы КСКПЭП Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденным приказом ФСБ России от 27.12.2011 № 795, действительности КСКПЭП, включенных в последовательность проверки от КСКПЭП, соответствующего проверяемой ЭП, до сертификата УЦ, выданного ему головным удостоверяющим центром, а также списков аннулированных КСКПЭП и меток доверенного времени, а также действительность на момент создания проверяемых КСКПЭП подтверждения соответствия средств ЭП и средств удостоверяющего центра, с использованием которых созданы указанные КСКПЭП.
- 4.6.7. Результаты проверки действительности ЭП, использованной для подписания электронного документа, направляются по адресу, указанному в заявлении на подтверждение действительности ЭП.
- 4.7. Процедуры, осуществляемые при прекращении действия и аннулировании сертификата.
 - 4.7.1. Прекращение действия сертификата осуществляется в случаях, установленных частью 6 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».
 - 4.7.2. Аннулирование сертификата осуществляется в случаях, установленных частью 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».
 - 4.7.3. Прекращение действия КСКПЭП по инициативе владельца КСКПЭП осуществляется на основании заявления, которое может быть подано на бумажном носителе в месте выдачи КСКПЭП УЦ.
 - 4.7.4. В заявлении владелец КСКПЭП указывает:
 - 4.7.4.1. уникальный серийный номер КСКПЭП;
 - 4.7.4.2. фамилию, имя, отчество (при наличии);
 - 4.7.4.3. причину прекращения действия КСКПЭП.
 - 4.7.5. Заявление подписывается владельцем КСКПЭП.
 - 4.7.6. Действие КСКПЭП прекращается при условии:
 - 4.7.6.1. идентификации владельца КСКПЭП;
 - 4.7.6.2. подтверждения достоверности сведений, указанных в заявлении.
 - 4.7.7. Информация о прекращении действия КСКПЭП или аннулировании КСКПЭП вносится в реестр КСКПЭП в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов, когда стало известно или должно было стать известно о наступлении таких обстоятельств в соответствии с Порядком ведения реестра КСКПЭП.

4.8. Порядок ведения реестра КСКПЭП

- 4.8.1. Реестр КСКПЭП ведётся в соответствии с Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минкомсвязи России от 22.08.2017 № 436.
- 4.8.2. Информация о прекращении действия или аннулировании сертификата вносится в реестр сертификатов в соответствии с пунктом 4.7.7 Порядка.

4.9. Порядок технического обслуживания реестра КСКПЭП.

- 4.9.1. Срок проведения технического обслуживания реестра КСКПЭП не может превышать 12 часов.
- 4.9.2. Уведомление о проведении технического обслуживания размещается на официальном сайте УЦ в сети «Интернет».

5. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УЦ

5.1. Информирование заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

- 5.1.1. Информирование владельца КСКПЭП об условиях и о порядке использования средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности средств ЭП, осуществляется посредством предоставления ему одновременно с выдачей КСКПЭП в соответствии с частью 4 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» Руководства по обеспечению безопасности использования усиленной электронной подписи.

5.2. Выдача по обращению заявителя средств ЭП.

- 5.2.1. Выдача средств ЭП, эксплуатационной и технической документации к ним во временное пользование производится по обращению заявителя в УЦ.
- 5.2.2. Выдаваемые средства ЭП должны обеспечивать техническую возможность проверки всех ЭП, в том числе если в состав электронных документов лицом, подписавшим электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные ЭП, или если электронный документ подписан несколькими ЭП.
- 5.2.3. В случае прекращения использования средств ЭП, эксплуатационная документация и средства ЭП возвращаются в УЦ.

5.3. Обеспечение актуальности информации, содержащейся в реестре КСКПЭП, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

- 5.3.1. Актуализация информации, содержащейся в реестре КСКПЭП, и обеспечение ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий осуществляются техническими средствами УЦ.

5.4. Обеспечение доступности реестра КСКПЭП в сети «Интернет»

- 5.4.1. Доступность актуального реестра КСКПЭП обеспечивается УЦ в круглосуточном режиме, за исключением периодов технического обслуживания.

5.5. Порядок обеспечения конфиденциальности созданных УЦ ключей ЭП.

- 5.5.1. Конфиденциальность ключей ЭП, создаваемых на АРМ УЦ, обеспечивается УЦ в соответствии с требованиями пунктов 26, 27, 29, 30 Инструкции 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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152.

5.5.2. УЦ не осуществляет временного хранения и уничтожения ключей ЭП, созданных на АРМ УЦ.

5.6. Осуществление регистрации КСКПЭП в федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»

5.6.1. При выдаче КСКПЭП в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» сведения о выданном КСКПЭП направляются в ЕСИА.

5.7. Осуществление по желанию лица, которому выдан КСКПЭП, безвозмездной регистрации указанного лица в ЕСИА.

5.7.1. При выдаче КСКПЭП в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» УЦ по желанию владельца КСКПЭП безвозмездно осуществляет его регистрацию в ЕСИА с проведением идентификации владельца при его личном присутствии.

5.8. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре КСКПЭП, включая информацию о прекращении действия КСКПЭП или об аннулировании КСКПЭП, в том числе путем публикации перечня прекративших свое действие (аннулированных) КСКПЭП.

5.8.1. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре КСКПЭП, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов Предоставление доступа к информации, содержащейся в реестре КСКПЭП, включая информацию о прекращении действия КСКПЭП или об аннулировании КСКПЭП, осуществляется безвозмездно с использованием сервиса УЦ.

5.8.2. Перечень прекративших свое действие и аннулированных КСКПЭП в соответствии с пунктом 3.2 Порядка публикуется на официальном сайте УЦ в сети «Интернет».

5.8.3. Актуализация перечня прекративших свое действие и аннулированных КСКПЭП, размещенного на официальном сайте УЦ в сети «Интернет», осуществляется два раза в сутки.

6. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Общие положения.

6.1.1. Порядок не является договором присоединения в смысле статьи 428 Гражданского кодекса Российской Федерации.

6.1.2. Порядок определяет форматы данных, основные организационно-технические мероприятия, направленные на обеспечение деятельности УЦ.

6.1.3. В случае вступления в силу изменений в законодательство или иные нормативные правовые акты, указанные изменения вступают в силу с момента, указанного в законодательстве или иных нормативных правовых актов, независимо от внесения

изменений в Порядок. УЦ инициирует приведение Порядка в соответствие с принятыми изменениями в законодательство или иные нормативные правовые акты.

- 6.1.4. Изменения и (или) дополнения в Порядок вносятся УЦ в одностороннем порядке. Указанные изменения и (или) дополнения в виде новой редакции Порядка, вступают в силу в порядке и в сроки, определенные УЦ.
- 6.1.5. Все приложения к Порядку являются его составной и неотъемлемой частью.
- 6.1.6. При необходимости УЦ по письменному запросу Пользователя предоставляет ему:
 - 6.1.6.1. копии документов, на основании которых УЦ осуществляет свою деятельность, заверенные подписью Уполномоченного лица УЦ и оттиском печати УЦ;
 - 6.1.6.2. копию действующего Порядка на бумажном носителе, заверенную подписью Уполномоченного лица УЦ и оттиском печати УЦ;
 - 6.1.6.3. копию документа (выписку из документа) УЦ о наделении Уполномоченного лица УЦ полномочиями на подписание КСКПЭП, Списков отозванных КСКПЭП и иных документов в соответствии с Порядком, заверенную подписью Уполномоченного лица УЦ и оттиском печати УЦ.
- 6.1.7. Запрос на КСКПЭП должен быть сформирован в письменном виде, подписан руководителем или иным уполномоченным лицом юридического лица, заключившего Договор с УЦ, и заверен оттиском печати (при наличии печати).

6.2. УЦ имеет право:

- 6.2.1. Запрашивать у Заявителя документы для подтверждения информации, содержащейся в заявлении на создание КСКПЭП.
- 6.2.2. Не принимать от Заявителя документы, не соответствующие требованиям законодательства и иных нормативных правовых актов.
- 6.2.3. Отказать в регистрации Пользователя и создании КСКПЭП в случае ненадлежащего оформления заявления на КСКПЭП.
- 6.2.4. Отказать в прекращении действия КСКПЭП Пользователя УЦ в случае ненадлежащего оформления соответствующего заявления на прекращение действия КСКПЭП.
- 6.2.5. Отказать в прекращении действия КСКПЭП в случае, если истек установленный срок действия ключа ЭП, соответствующего КСКПЭП.
- 6.2.6. В одностороннем порядке вносить изменения в Порядок УЦ.
- 6.2.7. Выпускать дополнительные инструкции и положения, соблюдающие процедуры, связанные с получением и применением КСКПЭП.
- 6.2.8. Осуществлять смену ключей ЭП УЦ в случаях нарушения их конфиденциальности.
- 6.2.9. Воспользоваться иными правами, предусмотренными Порядком, Федеральным законом от 06.04.2011 № 63 ФЗ «Об электронной подписи», другими федеральными законами и иными нормативными правовыми актами.

6.3. Представление информации.

- 6.3.1. УЦ вправе запросить, а Сторона, заключившая Договор, обязана предоставить УЦ документы, установленные Порядком, а также дополнительные документы по усмотрению УЦ;
- 6.3.2. К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами, и апостиль.

6.4. Ответственность сторон.

- 6.4.1. УЦ в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате: неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг, неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
- 6.4.2. УЦ несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», иными федеральными законами и иными нормативными правовыми актами, а также Порядком.
- 6.4.3. УЦ имеет финансовое обеспечение ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в КСКПЭП, выданном УЦ, или информации, содержащейся в Реестре КСКПЭП, который ведет УЦ, в определенной Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» сумме.
- 6.4.4. Пользователь УЦ принимает на себя все риски и несет ответственность за возникшие негативные последствия и убытки, в случае:
- 6.4.4.1. нарушения конфиденциальности своих ключей ЭП, ключевой фразы;
 - 6.4.4.2. утери ключевых носителей;
 - 6.4.4.3. несвоевременного уведомления УЦ о компрометации ключа ЭП;
 - 6.4.4.4. несвоевременной смены своих ключей ЭП в случае наступления событий, влекущих компрометацию ключей ЭП;
 - 6.4.4.5. неисполнения или ненадлежащего исполнения обязанностей или требований Порядка, Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иных нормативных правовых актов.
- 6.4.5. УЦ не несет ответственность за невозможность использования КСКПЭП в случае, если такая невозможность возникла после создания КСКПЭП и вызвана изменением требований информационных систем или законодательства Российской Федерации, иных нормативных правовых актов.
- 6.4.6. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по Порядку, если это неисполнение явилось следствием форс-мажорных обстоятельств.

6.5. Структура КСКПЭП и сроки действия ключевых документов.

- 6.5.1. Формат КСКПЭП, создаваемых УЦ, соответствует требованиям приказа ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи», иным нормативным правовым актам и рекомендациям IETF RFC 5280.

6.5.2. Структура корневого сертификата УЦ

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer	Издатель сертификата	CN = Минкомсвязь России ИНН = 007710474375 ОГРН = 1047702026701 O = Минкомсвязь России

		STREET = улица Тверская, дом 7 L = г. Москва S = 77 Москва C = RU E = dit@minsvyaz.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = Акционерное общество "Торговый дом "ПЕРЕКРЕСТОК" O = АО "Торговый дом "ПЕРЕКРЕСТОК" OU = Удостоверяющий центр STREET = ул. Средняя Калитниковская, д. 28, стр. 4 L = Москва S = 77 г.Москва C = RU ИНН = 007728029110 ОГРН = 1027700034493
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2012 256 бит)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
Дополнения сертификата		
CRL Distribution Point	Точки распространения списков отзыва (CRL)	Список точек распространения списка отзыва
Key Usage	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего Центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SubjectType (Тип владельца сертификата) =ЦС Path Length Constraint (Ограничение на длину пути – ограничивает количество уровней иерархии при создании подчиненных удостоверяющих центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	V0.0
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

6.5.3. Структура КСКПЭП физического лица, создаваемого УЦ.

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012 256 бит

Issuer	Издатель сертификата	CN = Акционерное общество "Торговый дом "ПЕРЕКРЕСТОК" O = АО "Торговый дом "ПЕРЕКРЕСТОК" OU = Удостоверяющий центр STREET = ул. Средняя Калитниковская, д. 28, стр. 4 L = Москва S = 77 г.Москва C = RU INN = 007728029110 OGRN = 1027700034493
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество SurName = Фамилия GivenName = Имя и Отчество (если имеется) StreetAddress = Адрес Locality = Город State = Субъект Федерации (с двухзначным кодом) Country = Страна = RU Email = Электронная почта INN = ИНН физического лица SNILS = СНИЛС
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора закрытого ключа Уполномоченного лица Удостоверяющего центра, с

		использованием которого издан сертификат и список отозванных сертификатов
		Конкретный перечень используемых расширений устанавливается Удостоверяющим центром
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

6.5.4. Структура списка отозванных сертификатов (CRL) УЦ.

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = Акционерное общество "Торговый дом "ПЕРЕКРЕСТОК" O = АО "Торговый дом "ПЕРЕКРЕСТОК" OU = Удостоверяющий центр STREET = ул. Средняя Калитниковская, д. 28, стр. 4 L = Москва S = 77 г.Москва C = RU ИНН = 007728029110 ОГРН = 1027700034493
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reason Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего центра

- 6.5.5. Сроки действия ключевых документов.
- 6.5.5.1. Срок действия ключа ЭП УЦ составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности УЦ, и для средства ЭП, с использованием которого данный ключ ЭП был сформирован.
- 6.5.5.2. Начало периода действия ключа ЭП УЦ исчисляется с даты и времени генерации ключа ЭП УЦ.
- 6.5.5.3. Срок действия сертификата УЦ не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата УЦ и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.
- 6.5.6. Срок действия ключа ЭП физического лица – 12 месяцев.
- 6.5.7. Начало периода действия ключа ЭП физического лица исчисляется с даты и времени начала действия соответствующего сертификата.
- 6.5.8. Срок действия КСКПЭП физического лица соответствует сроку действия ключа ЭП физического лица. Время начала периода действия КСКПЭП физического лица и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

6.6. Конфиденциальность информации.

6.6.1. Типы конфиденциальной информации

- 6.6.1.1. Ключ ЭП, соответствующий КСКПЭП, является конфиденциальной информацией лица, зарегистрированного в УЦ. УЦ не осуществляет хранение ключей ЭП пользователей УЦ.
- 6.6.1.2. Персональная и корпоративная информация о лицах, зарегистрированных в УЦ, содержащаяся в Реестре КСКПЭП, не подлежащая непосредственной рассылке в качестве части КСКПЭП, считается конфиденциальной.

6.6.2. Типы информации, не являющейся конфиденциальной.

- 6.6.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.
- 6.6.2.2. Информация, включаемая в КСКПЭП и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной.
- 6.6.2.3. Персональные данные, включаемые в КСКПЭП, издаваемые УЦ, относятся к общедоступным персональным данным.
- 6.6.2.4. Информация, содержащаяся в Порядке, не считается конфиденциальной.

6.6.3. Исключительные полномочия УЦ.

- 6.6.3.1. УЦ имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации

7. ТЕРМИНЫ И СОКРАЩЕНИЯ

№	Термин / сокращение	Определение
1.	АРМ	Автоматизированное рабочее место
2.	ЕСИА	Единая система идентификации и аутентификации
3.	ИС	Информационная система
4.	ОС	Операционная система
5.	ПО	Программное обеспечение
6.	ЦС	Центр регистрации
7.	ФИО	Фамилия, имя, отчество

8.	<i>Аккредитация удостоверяющего центра</i>	признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»
9.	<i>Аннулированный сертификат ключа проверки электронной подписи</i>	не действующий сертификат, аннулированный УЦ в соответствии с Порядком
10.	<i>Владелец сертификата ключа проверки электронной подписи</i>	лицо, которому Удостоверяющим центром в соответствии с законодательством Российской Федерации и Порядком выдан сертификат ключа проверки электронной подписи
11.	<i>Доверенные лица УЦ</i>	третьи лица, наделённые УЦ полномочиями по приёму заявлений на выдачу КСКПЭП, а также вручению КСКПЭП от имени УЦ
12.	<i>Договор</i>	договор на оказание услуг Удостоверяющего центра АО «Торговый дом «ПЕРЕКРЕСТОК»
13.	<i>Заявитель Удостоверяющего центра (Заявитель)</i>	физические и юридические лица. В случае, когда Заявителем выступает юридическое лицо, его интересы представляет физическое лицо, являющееся уполномоченным представителем юридического лица, заключившего Договор.
14.	<i>Квалифицированный сертификат ключа проверки электронной подписи (КСКПЭП)</i>	сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи
15.	<i>Ключ проверки электронной подписи</i>	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки действительности электронной подписи
16.	<i>Ключ электронной подписи</i>	уникальная последовательность символов, предназначенная для создания электронной подписи
17.	<i>Ключевой документ</i>	физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию
18.	<i>Копия сертификата ключа проверки электронной подписи</i>	документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие работником удостоверяющего центра и заверенный печатью удостоверяющего центра. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи
19.	<i>Пользователь удостоверяющего центра (пользователь УЦ)</i>	физическое лицо, зарегистрированное в УЦ, а также владелец сертификата ключа проверки электронной подписи
20.	<i>Реестр удостоверяющего центра (Реестр УЦ)</i>	набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию: – реестр заявлений на регистрацию в УЦ»; – реестр зарегистрированных пользователей УЦ; – реестр заявок на изготовление сертификатов в УЦ; – реестр заявлений на изготовление сертификатов ключа проверки ЭП;

		<p>–реестр заявлений на аннулирование (прекращение действия) сертификатов ключа проверки ЭП;</p> <p>–реестр заявлений на приостановление/возобновление действия сертификатов ключа проверки ЭП;</p> <p>–реестр заявлений на подтверждение подлинности ЭП в электронном документе;</p> <p>Реестр сертификатов.</p>
21.	<i>Сертификат ключа проверки электронной подписи (сертификат)</i>	электронный документ, выданный УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП
22.	<i>Система межведомственного электронного взаимодействия (СМЭВ)</i>	инфраструктура, обеспечивающая информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме
23.	<i>Список отозванных сертификатов (СОС, CRL)</i>	электронный документ с электронной подписью Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на определенный момент времени были аннулированы или действие которых было прекращено
24.	<i>Средство криптографической защиты информации (СКЗИ)</i>	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, шифрование и расшифрование информации
25.	<i>Средство электронной подписи (Средство ЭП)</i>	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. Средства электронной подписи должны иметь подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом. УЦ поддерживает использование сертифицированных средств ЭП производства ООО «КРИПТО-ПРО»
26.	<i>Стороны Договора (стороны)</i>	Акционерное общество «Торговый дом «ПЕРЕКРЕСТОК», физическое или юридическое лицо, заключившие договор на оказание услуг Удостоверяющего центра
27.	<i>Удостоверяющий центр (УЦ)</i>	Акционерное общество «Торговый дом «ПЕРЕКРЕСТОК», осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»
28.	<i>Уполномоченный федеральный орган</i>	Федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи - цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)
29.	<i>Формат сертификата ключа проверки электронной подписи (списка отозванных сертификатов)</i>	упорядоченный набор допустимых полей данных сертификата ключа проверки ЭП (списка отозванных сертификатов)

30.	<i>Электронная подпись (ЭП)</i>	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
31.	<i>Электронный документ</i>	информация, которая создается, хранится, предоставляется и распространяется в виде электрических сигналов в форме, пригодной для восприятия человеком, в том числе по информационно-телекоммуникационным сетям или в информационных системах, и подписанная электронной подписью в соответствии с законодательством Российской Федерации
32.	<i>Cryptographic Message Syntax (CMS)</i>	стандарт, определяющий формат и синтаксис криптографических сообщений

8. СВЯЗАННЫЕ ДОКУМЕНТЫ

№	Наименование документа
Внешние документы (источники права, стандарты и др.)	
1.	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2.	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
3.	Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»
4.	Приказ Минцифры России от 13.11.2020 N 584 «Об утверждении Требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей»
5.	Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»
6.	Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и требованиям к средствам удостоверяющего центра»
Внутренние документы	
1.	Порядок применения электронной подписи в Системе электронной подписи АО «Торговый дом «ПЕРЕКРЕСТОК» на базе Программно-аппаратного комплекса «КриптоПро DSS»
2.	Руководство по обеспечению безопасности использования усиленной электронной подписи

Приложение 1. Форма Заявления на выдачу КСКПЭП

ФИО:

Фамилия Имя Отчество полностью

Паспорт: серия _____

№ _____

Дата выдачи: _____

Выдан:

Наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ

на выдачу квалифицированного сертификата ключа проверки электронной подписи

Прошу зарегистрировать меня в качестве пользователя аккредитованного удостоверяющего центра АО «Торговый дом «ПЕРЕКРЕСТОК», сформировать ключи электронной подписи и создать квалифицированный сертификат ключа проверки электронной подписи (КСКПЭП) в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName(CN)	Фамилия, имя, отчество
Surname	Фамилия
GivenName	Имя, отчество
INN	ИНН
SNILS	СНИЛС
E-Mail (E)	Адрес электронной почты

С Порядком реализации функций аккредитованного удостоверяющего центра АО «Торговый дом «ПЕРЕКРЕСТОК» и исполнения его обязанностей, опубликованном по адресу <https://cdp.x5.ru/QUCReg.pdf>, ознакомлен(-на), согласен(-на), обязуюсь соблюдать.

Я ознакомился(-ась) с информацией по использованию усиленных электронных подписей и условиях признания квалифицированной электронной подписи, определенных в федеральном законе «Об электронной подписи», а также с требованиями Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, опубликованного по адресу <https://cdp.x5.ru/SignSec.pdf>, получил(-а). Обязуюсь по настоящему заявлению ознакомиться с информацией, содержащейся в квалифицированном сертификате, об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, опубликованных на сайте <https://cdp.x5.ru>.

Я, (ФИО владельца КСКПЭП полностью), паспорт серии (серия паспорта), № (номер паспорта), выдан (орган выдавший паспорт), дата выдачи (дата выдачи паспорта), зарегистрированный(ая) по адресу: (адрес по месту регистрации):

- даю согласие на обработку АО «Торговый дом «ПЕРЕКРЕСТОК» (ОГРН 1027700034493) и его доверенным лицам (далее — Оператор) своих персональных данных, а именно: фамилии, имени и отчества, контактном(ых) телефоне(ах), адресе электронной почты, СНИЛС, ИНН, пола, паспортных данных (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), фотографии с правом осуществления действий (операций) с персональными данными в целях создания квалифицированного сертификата ключа проверки электронной подписи и обслуживания в Удостоверяющем центре АО «Торговый дом «ПЕРЕКРЕСТОК», включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение;

- даю согласие на передачу фамилии, имени, отчества, СНИЛС, ИНН, сведений о поле, паспортных данных (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта), серийный номер квалифицированного сертификата ключа проверки электронной подписи в единую систему идентификации и аутентификации в целях выполнения требований Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» и требований Министерства связи и массовых коммуникаций Российской Федерации;

- даю согласие на включение фамилии, имени, отчества, ИНН, адреса электронной почты, СНИЛС в общедоступные источники персональных данных, которыми являются квалифицированный сертификат ключа проверки электронной подписи и реестр сертификатов ключей проверки электронной подписи;

- ознакомлен и согласен с тем, что Оператор вправе хранить предоставленные копии документов (паспорт, СНИЛС), а также фотографию субъекта персональных данных, и обрабатывать персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы;
- передача персональных данных иным лицам или иное их разглашение может осуществляться только с письменного согласия субъекта персональных данных. Согласие на обработку персональных данных действует с момента подписания настоящего Заявления субъектом персональных данных бессрочно и может быть отозвано им в порядке, установленном Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Владелец КСКПЭП

(субъект персональных данных)

_____ (Ф.И.О.)

_____ (подпись)

« ____ » _____ 202__ г.

Я, (ФИО владельца КСКПЭП, полностью), с Порядком реализации функций аккредитованного удостоверяющего центра АО «Торговый дом «ПЕРЕКРЕСТОК» и исполнения его обязанностей ознакомлен.

Владелец КСКПЭП

_____ (Ф.И.О.)

_____ (подпись)

« ____ » _____ 202__ г.

Приложение 2. Форма Заявления на прекращение действия КСКПЭП

ФИО:

Фамилия Имя Отчество полностью

Паспорт: серия

№

Дата выдачи:

Выдан:

Наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ

на прекращение действия сертификата ключа проверки электронной подписи

Прошу прекратить действие сертификат ключа проверки электронной подписи, содержащий следующие поля:

Серийный номер сертификата	
Ф.И.О.	
Организация	

_____ (собственноручная подпись) _____ (расшифровка подписи в формате «Фамилия И.О.»)

«___» _____ 20___ г.
(число) (месяц) (год)

Приложение 3. Форма Заявления на подтверждение подлинности ЭП в электронном документе

ФИО:

Фамилия Имя Отчество полностью

Паспорт: серия

№

Дата выдачи:

Выдан:

Наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ

на подтверждение подлинности электронной подписи в электронном документе

Прошу подтвердить подлинность электронной подписи в электронном документе на основании следующих данных

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № _____;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи, на прилагаемом к заявлению носителе – рег. № _____
3. Время, на момент наступления которого требуется подтвердить подлинность электронной подписи: _____

_____ (собственноручная подпись)

_____ (расшифровка подписи в формате «Фамилия И.О.»)

«___» _____ 20___ г.
(число) (месяц) (год)

Приложение 4. Форма Заявления на получение информации о статусе КСКПЭП

ФИО:

Фамилия Имя Отчество полностью

Паспорт: серия _____

№ _____

Дата выдачи: _____

Выдан:

Наименование органа, выдавшего документ

ЗАЯВЛЕНИЕ

на получение информации о статусе квалифицированного сертификата ключа проверки электронной подписи

Прошу предоставить информацию о статусе квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром АО «Торговый дом «ПЕРЕКРЕСТОК» и содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName(CN)	Наименование организации
Surname	Фамилия должностного лица
GivenName	Имя и отчество должностного лица

Время¹ (период времени) на момент наступления которого требуется установить статус сертификата:

с «_____» по «_____».

(собственноручная подпись)

(расшифровка подписи в формате «Фамилия И.О.»)

«__» _____ 20__ г.
(число) (месяц) (год)

¹ Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром. Порядок реализации АО «Торговый дом «ПЕРЕКРЕСТОК» функций аккредитованного удостоверяющего центра и исполнения его обязанностей

Приложение 5. Руководство по обеспечению безопасности использования квалифицированной ЭП и средств квалифицированной ЭП

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

- 1.1. Обеспечить конфиденциальность ключей электронных подписей.
- 1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.
- 1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
- 1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.
- 1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
- 1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
- 1.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
- 1.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено.
- 1.9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
- 1.10. Обратиться в Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, с заявлением о подтверждении подлинности электронной подписи в электронном документе в случае возникновения конфликтной ситуации.

2. Порядок применения средств квалифицированной электронной подписи

- 2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.
- 2.2. При эксплуатации средств квалифицированной электронной подписи должны использоваться только квалифицированные сертификаты ключей проверки электронной подписи, выпущенные аккредитованным Удостоверяющим центром.
- 2.3. Средства квалифицированной электронной подписи должны использоваться с сертифицированными средствами антивирусной защиты.
- 2.4. Инсталляция средств квалифицированной электронной подписи на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.
- 2.5. При установке и использовании средств квалифицированной электронной подписи должна быть обеспечена защита аппаратного и программного обеспечения от несанкционированного доступа в

соответствии с Руководством администратора безопасности из состава эксплуатационной документации на средство квалифицированной электронной подписи.

2.6. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства вычислительной техники с установленными средствами квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, средства вычислительной техники, на которых эксплуатируются средства квалифицированной электронной подписи, и защищаемую информацию.

2.7. На средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, должно использоваться только лицензионное программное обеспечение фирм - изготовителей и не должны устанавливаться средства разработки программного обеспечения и отладчики.

2.8. Программное обеспечение, устанавливаемое на средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- не санкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

2.9. Для идентификации пользователя при входе в операционную систему и BIOS на технических средствах, предназначенных для работы со средствами квалифицированной электронной подписи, необходимо использовать паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля не должна превышать 6 месяцев.

2.10. Средствами BIOS должна быть исключена возможность работы на средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, если во время начальной загрузки не проходят встроенные тесты.

2.11. ЗАПРЕЩАЕТСЯ:

- оставлять без контроля средства вычислительной техники, на которых эксплуатируются средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств электронной подписи;
- осуществлять копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;
- записывать на ключевые носители постороннюю информацию;
- изменять настройки, установленные программой установки средства электронной подписи или администратором;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами квалифицированной электронной подписи.

3. Правила использования ключевых носителей

3.1. Хранить ключ квалифицированной электронной подписи необходимо исключительно на защищенном ключевом носителе.

3.2. На ключевой носитель должен быть установлен индивидуальный PIN-код доступа (отличный от установленного по умолчанию).

3.3. Владелец ключа квалифицированной электронной подписи обязан обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц (хранить и использовать носитель таким образом, чтобы исключался несанкционированный доступ к нему других лиц) и сохранять в конфиденциальности PIN-код доступа. Владелец ключа несет персональную ответственность за хранение личных ключевых носителей.

3.4. В случае утери ключевого носителя или наличия оснований подозревать о получении к нему несанкционированного доступа сторонних лиц владелец ключа электронной подписи обязан обратиться в Удостоверяющий центр с заявлением о прекращении действия сертификатов ключей проверки электронной подписи, ключи электронной подписи которых хранятся на носителе.