Министерство
социальной политики Нижегородской области

П Р И К А З

15.10.2015. № 602

г. Нижний Новгород

Об утверждении Временного регламента работы Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области

В соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» и на основании приказа министерства социальной политики Нижегородской области от 07.08.2015 №488 «О создании Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области»

п р и к а з ы в а ю:

1. Утвердить Временный регламент работы Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области согласно приложению к настоящему приказу.
2. Контроль за исполнением приказа оставляю за собой.

И.о. министра С.Н.Кошелева

Приложение
к приказу министерства социальной политики
Нижегородской области
от «15» октября 2015 года №602

ВРЕМЕННЫЙ РЕГЛАМЕНТ РАБОТЫ

Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области

1. Перечень сокращений и определений, используемых в рамках настоящего Регламента.

1.1. ЭД (электронный документ) – документ, зафиксированный на электронном носителе (в виде набора символов, звукозаписи или изображения) и предназначенный для передачи во времени и пространстве с использованием средств вычислительной техники и электросвязи с целью хранения и(или) использования.

1.2. ЭП (электронная подпись) – информация в электронной форме, полученная в результате криптографического преобразования информации с использованием закрытого ключа ЭП, которая присоединена к ЭД или иным образом связана с ЭД и позволяющая идентифицировать владельца сертификата открытого ключа ЭП, а также установить отсутствие искажения информации в ЭД.

1.3. Закрытый ключ ЭП – уникальная последовательность символов, известная владельцу сертификата открытого ключа ЭП и предназначенная для создания в ЭД ЭП с использованием средств ЭП (подписание ЭД). Закрытый ключ ЭП действует на определенный момент времени (действующий закрытый ключ ЭП). Закрытый ключ ЭП действует, если:

1.3.1. Наступил момент времени ввода в действие закрытого ключа ЭП.

1.3.2. Срок действия закрытого ключа ЭП не истек.

1.3.3. Сертификат открытого ключа ЭП, соответствующий данному закрытому ключу ЭП не аннулирован (не отозван) и действие его не приостановлено.

1.4. Открытый ключ ЭП – уникальная последовательность символов, соответствующая закрытому ключу ЭП, предназначенная для подтверждения с использованием средств ЭП подлинности ЭП в ЭД.

1.5. Сертификат ключа ЭП – ЭД с ЭП уполномоченного лица УЦ или бумажный документ, подписанный уполномоченным лицом УЦ, подтверждающий соответствие между закрытым ключом ЭП и информацией, идентифицирующей владельца ключа ЭП. Содержит информацию о владельце ключа ЭП, сведения об открытом ключе ЭП, его назначении и области применения, название УЦ и другие сведения. Сертификат ключа ЭП действует на определенный момент времени (действительный сертификат ключа ЭП). Сертификат ключа ЭП действует если:

1.5.1. Наступил момент времени ввода в действие сертификата ключа ЭП.

1.5.2. Срок действия сертификата ключа ЭП не истек.

1.5.3. Сертификат ключа ЭП не аннулирован (не отозван) и действие его не приостановлено.

1.6. СОС (список отзыва сертификатов ключей ЭП) – ЭД с ЭП уполномоченного лица УЦ, включающий в себя список серийных номеров сертификатов ключей подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

1.7. Ключевой дистрибутив – зашифрованный на парольном ключе файл, формируемый УКЦ для зарегистрированных пользователей УЦ. Включает в себя необходимую первичную ключевую информацию для обеспечения защищенного взаимодействия с УЦ, первичный закрытый ключ ЭП и сертификат ключа ЭП пользователя, сертификат ключа ЭП уполномоченного лица УЦ, другие файлы, необходимые для реализации функций ЭП.

1.8. Ключевой носитель – носитель данных с ключевым дистрибутивом, содержащим ключевую и парольную информацию пользователя УЦ включая:

1.8.1. Открытый и закрытый ключи ЭП.

1.8.2. Сертификат ключа ЭП.

1.8.3. СОС УЦ и доверенных УЦ.

1.9. Подразделение ЗИ – подразделение, обеспечивающее информационную безопасность (в том числе защиту персональных данных за исключением сведений, составляющих государственную тайну) в министерстве социальной политики Нижегородской области (далее – Министерство) и подведомственных Министерству учреждениях (далее – Учреждения).

1.10. ЗКСПД – защищенная корпоративная сеть передачи данных Министерства.

1.11. АРМ (Автоматизированное рабочее место) – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.12. НСД (несанкционированный доступ к информации) – доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации, а также получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей;

1.13. Компрометация ключевой информации — факт доступа постороннего лица к ключевой информации, а также подозрение на факт доступа постороннего лица к ключевой информации, а именно:

1.13.1. Постороннему лицу мог стать доступным файл ключевого дистрибутива.

1.13.2. Существует подозрение на получение пароля доступа к ключам пользователя постороннему лицу.

1.13.3. Постороннему лицу мог стать доступным съемный носитель с ключевой информацией.

1.13.4. Постороннее лицо могло получить неконтролируемый физический доступ или доступ по локальной сети к ключевой информации, хранящейся на АРМ пользователя УЦ.

1.14. ПО – программное обеспечение.

1.15. СКЗИ (Средства криптографической защиты информации) – программные или программно-аппаратные средства, осуществляющие криптографическое преобразование информации.

1.16. Средства ЭП – программные или программно-аппаратные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

1.16.1. Подписание ЭД с использованием закрытого ключа ЭП.

1.16.2. Подтверждение с использованием открытого ключа ЭП подлинности ЭП в ЭД.

1.16.3. Создание закрытых и открытых ключей ЭП.

1.17. УЦ (Удостоверяющий центр) – подразделение, осуществляющие функции по созданию и выдаче системы открытых и закрытых ключей ЭП, а также иные функции, в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

1.18. ЦУС (центр управления сетью) – программное обеспечение, предназначенное для конфигурирования и управления ЗКСПД;

1.19. УКЦ (удостоверяющий и ключевой центр) — программное обеспечение, которое выполняет функции формирования и хранения первичной ключевой информации (мастер-ключи шифрования и межсетевые мастер-ключи), формирования ключей шифрования, выполнения процедур смены мастер-ключей и смены ключей при компрометации, формирования персональных ключей защиты пользователей и криптографически надежных парольных фраз (паролей), а также записи персональных ключей пользователей на аппаратные носители ключей.

1.20. Оператор УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное полномочиями в соответствии с Положением и Регламентом.

1.21. Администратор УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное полномочиями в соответствии с Положением и Регламентом.

1.22. Администратор безопасности УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное полномочиями в соответствии с Положением и Регламентом.

1.23. Уполномоченное лицо УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное УЦ полномочиями по заверению сертификатов ключей ЭП и СОС, а также наделенное полномочиями в соответствии с Положением и Регламентом.

1.24. Пользователь УЦ – физическое лицо, зарегистрированное в УЦ.

1.25. Владелец сертификата ключа ЭП – Пользователь УЦ, на имя которого УЦ выдал сертификат ключа ЭП и которое владеет соответствующим закрытым ключом ЭП, позволяющим с помощью средств ЭП создавать ЭП в ЭД (подписывать ЭД).

1.26. Внешняя организация – юридическое лицо, не входящее в структуру Министерства, осуществляющее с ЗКСПД информационное взаимодействие.

1.27. Доверенный УЦ – УЦ внешней организации, с которым УЦ установил доверенные отношения на основании Соглашения о взаимодействии и взаимном признании сертификатов ключей ЭП уполномоченных лиц УЦ (Приложение 4).

1.28. Кросс-сертификат ключа ЭП – сертификат ключа ЭП уполномоченного лица доверенного УЦ, передаваемый в УЦ с открытым ключом ЭП уполномоченного лица доверенного УЦ и ЭП уполномоченного лица доверенного УЦ. Обеспечивает признание ЭП, сертификат ключа ЭП которой выдан в доверенном УЦ.

1.29. Плановая смена ключей – смена ключей, не вызванная компрометацией ключей, осуществляемая в соответствии с документацией на СКЗИ.

1.30. Срок действия сертификата ключа ЭП – 1 год с момента введения в действие ключа ЭП.

1.31. Рабочий день УЦ (далее – рабочий день) – промежуток времени с 10:00 до 17:00 (время московское) каждого дня недели за исключением выходных и праздничных дней.

2. Введение.

2.1. Временный регламент работы Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области (далее – Регламент) разработан во исполнение приказа министерства социальной политики Нижегородской области от 07.08.2015 №488 «О создании Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области» в соответствии с действующим законодательством и определяет технологию эксплуатации аппаратно-программного комплекса и функционально-техническое обеспечение работы УЦ и предназначен для применения сотрудниками УЦ и пользователями УЦ.

2.2. Настоящий Регламент определяет:

- организационную структуру УЦ;
- порядок работы УЦ в рамках функционирования автоматизированной системы УЦ;
- требования к порядку применения сертификатов ключей электронной подписи в защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области;
- требования к порядку создания, использования и аннулирования сертификатов ключей ЭП;
- требования, предъявляемые к сертификатам ключей ЭП, программному и аппаратному обеспечению компонентов УЦ;
- порядок представления информации пользователям УЦ;
- обязанности и ответственность уполномоченных лиц УЦ и пользователей УЦ в соответствии с требованиями, предъявляемыми действующим законодательством Российской Федерации.

2.3. Деятельность УЦ регламентируется Федеральным законом от 06 апреля 2011 года №63-ФЗ «Об электронной подписи», Положением об Удостоверяющем центре защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области, утвержденным приказом министерства социальной политики Нижегородской области от 07.08.2015 №488 «О создании Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области» (далее – Положение), настоящим Регламентом, документами, определяющими функции, права, обязанности, ответственность должностных лиц УЦ, и квалификационными требованиями, предъявляемыми к ним, а также пакетом эксплуатационной документации на программно-аппаратный комплекс УЦ.

2.4. Настоящий Регламент распространяется в электронной форме по каналам защищенной почты ЗКСПД и на бумажном носителе.

2.5. Настоящий Регламент вступает в силу с момента его утверждения.

2.6. Действие настоящего Регламента отменяется приказом министра социальной политики Нижегородской области. УЦ уведомляет пользователей УЦ о прекращении действия настоящего Регламента.

3. Общие положения Регламента.

3.1. Назначение УЦ.

3.1.1. УЦ предназначен для решения задач и обеспечения функций, определенных Положением в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

3.2. Состав УЦ.

3.2.1. УЦ, в соответствии с Положением, осуществляет свою деятельность с использованием программно-аппаратного комплекса с установленным ЦУС и УКЦ.

3.2.2. УКЦ предназначен для выполнения следующих основных функций:

- внесение в реестр регистрационной информации о пользователях УЦ;

- изготовление сертификатов ключей ЭП пользователей УЦ в электронной форме;
- изготовление копий сертификатов ключей ЭП пользователей УЦ на бумажном носителе;
- выдача сертификатов ключей ЭП пользователю УЦ;
- формирование закрытых и открытых ключей ЭП по обращениям пользователей УЦ с возможностью записи их на ключевой носитель;
- ввод в действие, аннулирование (отзыв), приостановление или возобновление действия сертификатов ключей ЭП по обращениям пользователей УЦ;
- ведение реестра изготовленных сертификатов ключей ЭП пользователей УЦ;
- представление копий сертификатов ключей ЭП, находящихся в реестре изготовленных сертификатов ключей ЭП в электронной форме, по запросам пользователей УЦ;
- представление пользователям УЦ сведений об аннулированных и приостановленных сертификатах ключей ЭП;
- подтверждение подлинности ЭП в ЭД, по обращениям пользователей УЦ;
- подтверждение подлинности ЭП уполномоченного лица УЦ в изготовленных им сертификатах ключей ЭП по обращениям пользователей УЦ;
- распространение средств ЭП по обращениям пользователей УЦ;
- идентификация, аутентификация и регистрация пользователей УЦ в ЗКСПД с использованием ЭП;
- безопасное хранение и использование закрытого ключа ЭП уполномоченного лица УЦ.

4. Разрешение конфликтных ситуаций

4.1. Сторонами в конфликтной ситуации, в случае ее возникновения, считаются УЦ и лицо, оспаривающее ЭД, подписанный ЭП, сертификат ключа ЭП, которой выдан УЦ.

4.2. При возникновении конфликтных ситуаций, Стороны предпринимают все необходимые действия для урегулирования вопросов, которые могут возникнуть в рамках действия Регламента работы, путем совместных переговоров.

4.3. Разрешение конфликтных ситуаций проводится в соответствии с Порядком разрешения конфликтных ситуаций, возникающих при использовании электронной цифровой подписи (Приложение 1), определенным разработчиком используемого сторонами СКЗИ.

4.4. Споры между Сторонами, не урегулированные в процессе совместных переговоров, разрешаются в порядке, предусмотренном действующим законодательством Российской Федерации.

5. Порядок внесения изменений в Регламент.

5.1. Предложения пользователей УЦ по внесению изменений в Регламент в письменном виде вносятся на рассмотрение в Подразделение ЗИ.

5.2. Подразделение ЗИ рассматривает предложения в недельный срок и представляет по ним заключение в Министерство.

5.3. Министерство рассматривает представленные документы и принимает решение о подготовке проекта приказа Министерства о внесении изменений в Регламент либо об отклонении поступивших предложений.

5.4. Изменения, вносимые в Регламент, доводятся до сведения пользователей УЦ в соответствии с пункту 2.4 настоящего Регламента.

6. Процедурные положения Регламента

6.1. Регистрация пользователей УЦ и выработка открытого и закрытого ключей ЭП и сертификата ключа ЭП.

6.1.1. Пользователь лично прибывает в УЦ для удостоверения подлинности его личности. Аутентификация личности производится по паспорту или другому документу, удостоверяющему личность.

6.1.2. Пользователь оформляет пакет документов, необходимый для изготовления сертификата ключа ЭП (Приложение 2) (далее – пакет документов).

6.1.3. Оператор УЦ проверяет достоверность и правильность сведений, указанных в пакете документов и направляет пакет документов на регистрацию пользователя УЦ с проставлением отметки о дате получения пакета документов.

6.1.4. Администратор безопасности УЦ с использованием ЦУС вносит данные о пользователе (регистрирует пользователя УЦ).

6.1.5. Информация о зарегистрированном пользователе УЦ передается в УКЦ для формирования открытого и закрытого ключей ЭП и сертификата ключа ЭП.

6.1.6. Оператор УЦ изготавливает два экземпляра сертификата ключа ЭП владельца ключа ЭП на бумажном носителе (Приложение 5) и в течение 2-х дней уведомляет владельца ключа ЭП об изготовлении сертификата ключа ЭП.

6.1.7. Уполномоченное лицо УЦ заверяет сертификаты ключа ЭП пользователя УЦ на бумажном носителе своей подписью и печатью УЦ.

6.1.8. В течение 2-х недель с момента изготовления сертификата ключа ЭП на бумажном носителе владелец ключа ЭП обязан заверить собственноручной подписью оба экземпляра сертификата ключа ЭП на бумажном носителе и получить один экземпляр сертификата ключа ЭП на бумажном носителе и электронный носитель с ключевым дистрибутивом и сертификатом ключа ЭП (если имеется) у оператора УЦ с регистрацией в журнале учета выдачи ключевых дистрибутивов (Приложение 4). В журнале учета выдачи ключевых дистрибутивов также проставляется отметка о проведении инструктажа владельца ключа ЭП о правилах эксплуатации, хранения и возврата СКЗИ и ключевых носителей. Второй экземпляр сертификата ключа ЭП на бумажном носителе остается в УЦ.

6.1.9. ПО и СКЗИ, необходимые для работы с ЭП и сертификатом ключа ЭП, устанавливаются на АРМ пользователя УЦ на основании заявки, подписанной руководителем (заместителем руководителя) подразделения Министерства или руководителем (заместителем руководителя) Учреждения.

6.1.10. В случае невыполнения пункту 6.1.8 настоящего Регламента производится отзыв сертификата ключа ЭП.

6.2. Смена ключа ЭП без компрометации ключа ЭП.

6.2.1. Владельцу ключа ЭП необходимо производить периодическую (плановую) замену используемых ключей ЭП не реже заданного срока действия сертификата ключа ЭП. Процедура замены ключей ЭП проводится в соответствии с документацией СКЗИ.

6.3. Внеплановая замена ключей ЭП.

6.3.1. Внеплановая замена ключей ЭП осуществляется владельцем ключа ЭП в следующих случаях:

- компрометация ключевой информации;
- замена носителя ключевой информации в случае его выхода из строя;
- изменение регистрационных данных владельца ключа ЭП.

6.3.2. В случае компрометации ключа ЭП владелец ключа ЭП обязан незамедлительно направить в УЦ уведомление о компрометации закрытого ключа ЭП (Приложение 6) и заявление на приостановление действия сертификата ключа ЭП (Приложение 8).

6.3.2.1. Администратор безопасности УЦ приостанавливает действие сертификата ключа ЭП.

6.3.2.2. По факту компрометации ключа ЭП проводится проверка.

6.3.2.3. В случае неподтверждения акта компрометации ключа ЭП возобновляется действие сертификата ключа ЭП.

6.3.2.4. В случае подтверждения факта компрометации ключа ЭП сертификат ключа ЭП отзывается и по заявлению пользователя УЦ вырабатывается новый сертификат ключа ЭП в соответствии с пунктом 6.1 настоящего Регламента.

6.3.2.5. Администратор безопасности УЦ формирует СОС и распространяет его среди пользователей УЦ, а также обновляет СОС в публичных точках публикации. Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа ЭП является опубликование СОС, содержащего сведения об аннулированном (отозванном) сертификате ключа ЭП. Временем аннулирования

(отзыва) сертификата ключа ЭП признается время издания СОС, содержащего сведения об аннулированном (отозванном) сертификате ключа ЭП.

6.3.3. Замена носителя ключевой информации в случае его выхода из строя.

6.3.3.1. В случае выхода из строя носителя ключевой информации по заявлению владельца ключа ЭП проводятся процедуры отзыва сертификата ключа ЭП и выработки нового сертификата ключа ЭП в соответствии с пунктом 6.1 настоящего Регламента.

6.3.4. Изменение регистрационных данных владельца ключа ЭП.

6.3.4.1. В случае изменения регистрационных данных владельца ключа ЭП проводятся процедуры отзыва сертификата ключа ЭП и выработки нового сертификата ключа ЭП в соответствии с пунктом 6.1 настоящего Регламента.

6.4. Смена ключа подписи уполномоченного лица УЦ.

6.4.1. Уполномоченное лицо УЦ обязано производить периодическую (плановую) смену своих ключей подписи не ранее чем через один год после начала действия закрытого ключа ЭП уполномоченного лица УЦ и не позднее чем за один год до окончания срока действия открытого ключа ЭП. Уполномоченное лицо УЦ в соответствии с документацией на УКЦ формирует новые ключи подписи и сертификат ключа ЭП.

6.4.2. Процедура плановой смены ключей уполномоченного лица УЦ осуществляется в следующем порядке:

- уполномоченное лицо УЦ вырабатывает новый закрытый и открытый ключи ЭП;
- администратор безопасности УЦ изготавливает новый сертификат ключа подписи уполномоченного лица УЦ;
- уведомление пользователей УЦ о проведении смены ключей уполномоченного лица УЦ осуществляется в электронной форме по каналам ЗКСПД.

6.4.3. Внеплановая смена ключей уполномоченного лица УЦ при компрометации.

6.4.3.1. В случае компрометации закрытого ключа ЭП уполномоченного лица УЦ сертификат ключа ЭП уполномоченного лица УЦ аннулируется. Все сертификаты, подписанные с использованием скомпрометированного ключа ЭП уполномоченного лица УЦ, считаются скомпрометированными.

6.4.3.2. Пользователи УЦ уведомляются о компрометации закрытого ключа ЭП уполномоченного лица УЦ в электронной форме по каналам ЗКСПД.

6.4.3.3. После аннулирования сертификата ключа подписи ЭП уполномоченного лица УЦ выполняется процедура внеплановой смены ключей ЭП уполномоченного лица УЦ.

6.4.3.4. Процедура внеплановой смены ключей ЭП уполномоченного лица УЦ выполняется в порядке, определенном процедурой плановой смены ключей ЭП уполномоченного лица УЦ согласно пункту 6.4.2 настоящего Регламента.

6.4.3.5. Все подписанные с использованием скомпрометированного закрытого ключа ЭП уполномоченного лица УЦ и действовавшие на момент компрометации закрытого ключа ЭП уполномоченного лица УЦ сертификаты ключей ЭП пользователей УЦ, а также сертификаты ключей ЭП пользователей УЦ, действие которых было приостановлено, подлежат внеплановой смене.

6.5. Аннулирование (отзыв) сертификата ключа ЭП.

6.5.1. Пользователь УЦ направляет в УЦ заявление на аннулирование (отзыв) сертификата ключа ЭП (Приложение 7) (далее – заявление) в электронном виде, заверив его своей ЭП, или на бумажном носителе, заверив его собственноручной подписью.

6.5.2. Оператор УЦ при получении от пользователя УЦ заявления в электронном виде или на бумажном носителе направляет его администратору безопасности УЦ для аннулирования (отзыва) сертификата ключа ЭП.

6.5.3. Администратор безопасности УЦ после аннулирования (отзыва) сертификата ключа ЭП формирует СОС и распространяет его среди пользователей УЦ, а также обновляет СОС в публичных точках публикации.

Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа ЭП является опубликование СОС, содержащего сведения об аннулированном (отозванном) сертификате ключа ЭП. Временем аннулирования (отзыва) сертификата ключа ЭП признается время издания СОС, содержащего сведения об аннулированном (отозванном) сертификате ключа ЭП.

6.6. Приостановление действия сертификата ключа ЭП.

6.6.1. Пользователь УЦ направляет в УЦ заявление на приостановление действия сертификата ключа ЭП (Приложение 8) (далее – заявление) в электронном виде, заверив его своей ЭП, или на бумажном носителе, заверив его собственноручной подписью.

6.6.2. Оператор УЦ при получении от пользователя УЦ заявления в электронном виде или на бумажном носителе направляет его администратору безопасности УЦ для приостановление действия сертификата ключа ЭП.

6.6.3. Администратор безопасности УЦ после приостановление действия сертификата ключа ЭП формирует СОС и распространяет его среди пользователей УЦ, а также обновляет СОС в публичных точках публикации. Официальным уведомлением о факте приостановление действия сертификата ключа ЭП является опубликование СОС, содержащего сведения об приостановленном сертификате ключа ЭП. Временем приостановление действия сертификата ключа ЭП признается время издания СОС, содержащего сведения об приостановленном сертификате ключа ЭП.

6.6.4. Если в течение срока приостановления действия сертификата ключа ЭП действие этого сертификата не будет возобновлено, то сертификат ключа ЭП аннулируется (отзывается).

6.7. Возобновление действия сертификата ключа ЭП.

6.7.1. Возобновление действия сертификата ключа ЭП может быть осуществлено исключительно в период приостановления действия сертификата ключа ЭП.

6.7.2. Пользователь УЦ направляет в УЦ заявление на возобновление действия сертификата ключа ЭП (Приложение 9) (далее – заявление) в

электронном виде, заверив его своей ЭП, или на бумажном носителе, заверенное его собственноручной подписью.

6.7.3. Оператор УЦ при получении от пользователя УЦ заявления в электронном виде или на бумажном носителе направляет его администратору безопасности УЦ для возобновления действия сертификата ключа ЭП.

6.7.4. Администратор безопасности УЦ после возобновления действия сертификата ключа ЭП формирует СОС и распространяет его среди пользователей УЦ, а также обновляет СОС в публичных точках публикации. Официальным уведомлением о факте возобновления действия сертификата ключа ЭП является опубликование СОС, содержащего сведения об возобновленном сертификате ключа ЭП. Временем возобновления действия сертификата ключа ЭП признается время издания СОС, содержащего сведения об возобновленном сертификате ключа ЭП.

7. Взаимодействие УЦ и установление доверительных отношений между УЦ и УЦ внешних организаций.

7.1. Установление доверительных отношений между УЦ и УЦ внешних организаций является процедурой, в результате которой пользователи, получившие сертификаты ключей ЭП в одном из УЦ, получают возможность проверить подлинность ЭП пользователей, получивших сертификаты ключей ЭП в другом УЦ, а также пользователей, получивших сертификаты ключей ЭП в одном из УЦ, если другим УЦ выпущен кросс-сертификат уполномоченного лица одного из УЦ.

7.2. Установление доверительных отношений между УЦ и УЦ внешних организаций осуществляется либо напрямую на основе Соглашения о взаимном признании сертификатов ключей ЭП уполномоченных лиц УЦ и организации взаимодействия (Приложение 11), либо косвенным образом путем получения кросс-сертификатов уполномоченных лиц доверенных УЦ.

7.3. Для установления доверительных отношений на основании Соглашения каждая из Сторон оформляет на бумажном носителе список сертификатов ключей ЭП (далее – список), включающий сертификаты ключей ЭП

уполномоченных лиц УЦ и выпущенные кросс-сертификаты ключей ЭП уполномоченных лиц доверенных УЦ, которыми будут заверяться ключи ЭП пользователей, зарегистрированных в данном УЦ и в доверенных УЦ. К списку прилагаются распечатанные на бумажных носителях соответствующие сертификаты ключей ЭП. Список подписывается руководителем УЦ и руководителем УЦ внешней организации, заверяется печатями УЦ и УЦ внешней организации, и передается под расписку другой Стороне.

7.4. При изменении списка соответствующая Сторона оформляет новый список сертификатов ключей ЭП с приложенными сертификатами ключей ЭП.

7.5. Технологическое взаимодействие по установлению доверительных отношений между УЦ и УЦ внешней организации осуществляется в соответствии с технической документацией на СКЗИ.

7.6. Порядок взаимодействия доверенных УЦ в процессе формирования новых СОС и при смене (компрометации) ключей ЭП уполномоченных лиц УЦ.

7.6.1. При изменении СОС одного из доверенных УЦ, в случае отзыва (приостановления) действия сертификатов ключей ЭП пользователей, новый СОС передается в доверенный УЦ и публикуется в публичных точках публикации.

7.6.2. В случае смены (компрометации) ключей ЭП уполномоченного лица УЦ необходимо:

7.6.2.1. Немедленно сообщить о факте смены (компрометации) ключей ЭП уполномоченного лица УЦ уполномоченным лицам доверенных УЦ.

7.6.2.2. Аннулировать сертификат своего ключа ЭП и отправить новые СОС всем доверенным УЦ.

7.6.2.3. Сформировать новые ключи ЭП и сертификат ключа ЭП уполномоченного лица УЦ.

7.6.3. После выполнения действий, описанных в пункте 7.6.2, производится оформление на бумажном носителе нового списка сертификатов ключей ЭП УЦ в соответствии с пунктом 7.3 Регламента и передача новых

списков сертификатов ключей ЭП и сертификатов ключей ЭП в электронном виде доверенным УЦ.

7.6.4. Уполномоченное лицо доверенного УЦ осуществляет сравнение нового сертификата ключа ЭП уполномоченного лица УЦ с сертификатом ключа ЭП уполномоченного лица УЦ, указанного в списке.

8. Контактная информация

8.1. УЦ расположен по адресу: 603076, г. Нижний Новгород, пр-т Ленина, 54а, 3-й этаж.

Приложение 1
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Порядок разрешения конфликтных ситуаций, возникающих при использовании электронной цифровой подписи

1. Возникновение конфликтных ситуаций

1.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭП. Данные конфликтные ситуации могут возникать в следующих случаях:

1.1.1. Неподтверждение подлинности защищенных ЭД средствами проверки ЭП получателя.

1.1.2. Оспаривание факта идентификации владельца ЭП, подписавшего ЭД.

1.1.3. Заявление отправителя или получателя ЭД об его искажении.

1.1.4. Оспаривание факта отправления и (или) получения защищенного ЭД.

1.1.5. Оспаривания времени отправления и (или) получения защищенного ЭД.

1.1.6. Иные случаи возникновения конфликтных ситуаций.

1.2. В случае возникновения конфликтной ситуации пользователь, предполагающий возникновение конфликтной ситуации, должен направить администратору безопасности УЦ (непосредственно или через доверенное лицо), выдавшему ему сертификат ключа ЭП:

1.2.1. Уведомление о конфликтной ситуации с изложением обстоятельств ее возникновения.

1.2.2. ЭД, подлинность которого оспаривается. ЭД вместе с ЭП и сертификатом ключей подписи экспортируется из ПО, в котором он был получен или создан, в соответствии с руководством пользователя данного ПО.

1.2.3. При оспаривании факта доставки ЭД администратору безопасности УЦ представляются подписанные принимающей стороной извещения о доставке (прочтении) ЭД, экспортированные из ПО в виде ЭД.

1.3. Администратор безопасности УЦ обязан незамедлительно проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и в случае необходимости о мерах, принятых для разрешения возникшей конфликтной ситуации.

1.4. Конфликтная ситуация признается разрешенной в рабочем порядке в случае если уведомитель удовлетворен информацией, полученной от администратора безопасности УЦ.

1.5. В случае если уведомитель не удовлетворен полученной информацией, для разрешения конфликтной ситуации проводится техническая экспертиза.

2. Порядок проведения технической экспертизы

2.1. Экспертная комиссия созывается организацией, выполняющей функции УЦ, на основании письменного заявления (претензии) Стороны пользователя, оспаривающего ЭД. В указанном заявлении помимо реквизитов оспариваемого ЭД должны быть указаны лицо (лица), уполномоченные представлять интересы Стороны в составе экспертной комиссии.

2.2. Не позднее 10-ти рабочих дней с момента получения претензии назначается дата, место и время начала работы комиссии, о чем письменно уведомляются обе Стороны.

2.3. Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон. В состав комиссии также включается эксперт – администратор безопасности УЦ.

2.4. Экспертиза оспариваемого электронного документа осуществляется на предоставленном администратором безопасности УЦ персональном компьютере с установленным ПО СКЗИ, обеспечивающим проверку ЭП и подписание ЭД.

2.5. В случае если представители одной из Сторон по оспариваемому электронному документу не явились для участия в работе экспертной комиссии, экспертиза проводится без их участия, а об отсутствии представителей по оспариваемому ЭД составляется акт, подписываемый всеми присутствующими участниками экспертной комиссии.

2.6. Экспертиза осуществляется в три этапа:

2.6.1. Проверка оборудования и ПО и тестирование их работоспособности.

2.6.2. Контроль целостности оспариваемого ЭД путем проверки ЭП при помощи сертификата открытого ключа ЭП, представленного Стороной.

2.6.3. Проверка принадлежности, актуальности и целостности сертификата, использованного экспертной комиссией для проверки ЭП.

2.7. Проверка работоспособности оборудования и ПО проводится путем проведения в присутствии членов экспертной комиссии тестов пробной подписи и проверки подписи.

2.8. Контроль целостности оспариваемого ЭД производится посредством стандартной процедуры импорта файлов ЭД с ЭП и сертификатом в ПО СКЗИ и затем проверки ЭП импортированного ЭД в соответствии с руководством пользователя СКЗИ.

2.9. Проверка принадлежности, актуальности и целостности сертификата ключей ЭП производится путем вызова в ПО СКЗИ диалога просмотра сертификата, представленного вместе с ЭД. Просматриваемый сертификат ключа ЭП распечатывается на бумажном носителе и передается членам экспертной комиссии.

2.9.1. В случае если сертификат, используемый при проверке ЭП, издавался на основании письменного запроса пользователя, то для доказательства принадлежности актуальности и целостности сертификата,

использованного для проверки ЭП, администратором безопасности УЦ и соответствующей Стороной комиссии предъявляется сертификаты на бумажном носителе, оформленные при получении сертификата. Члены экспертной комиссии производят визуальную сверку данных сертификатов с распечатанным сертификатом, использованным при подписи оспариваемого ЭД.

2.9.2. В случае если сертификат был издан на основании электронного запроса, подписанного ЭП с использованием ранее изданного официально оформленного сертификата, экспертной комиссии предъявляется логически связанная цепочка запросов на сертификаты и сертификаты, распечатанные на бумажных носителях, которые в совокупности подтверждают принадлежность сертификата лицу, сформировавшему ЭП. Распечатка этих запросов и сертификатов на бумажные носители производится администратором безопасности УЦ в АРМ администратора безопасности УЦ. Цепочка запросов признается действительной, а сертификат принадлежащим указанному владельцу, если выполнены следующие условия:

2.9.2.1. Цепочка логически связана, т.е. каждый следующий запрос подписан с использованием сертификата, изданного на основании предыдущего запроса.

2.9.2.2. Подпись под каждым запросом в цепочке действительна на момент издания сертификата по данному запросу.

2.9.2.3. Сертификат, которым подписан каждый запрос, действителен на момент подписания запроса.

2.9.2.4. Последним элементом в цепи является электронный сертификат (распечатывается), соответствующий (при визуальном сравнении) сертификату, используемому комиссией для проверки ЭП по оспариваемому ЭД.

2.9.2.5. Сертификат, которым заверен первый запрос в цепочке (распечатывается), соответствует (при визуальном сравнении) официально оформленному сертификату, предъявленному экспертной комиссии.

2.10. Подтверждением подлинности оспариваемого ЭД является единовременное выполнение следующих условий:

2.10.1. Проверка ЭП оспариваемого ЭД с сертификатом ключей ЭП, предъявленного Стороной, дала положительный результат.

2.10.2. Подтверждена принадлежность, актуальность и целостность сертификата ключей ЭП пользователя Стороны, с помощью которого проводится проверка ЭП оспариваемого ЭД.

2.10.3. Если у заявителя отсутствуют сомнения в принадлежности сертификата, то проверка по пункту 2.10.2 может не производится.

2.11. При необходимости подтверждения факта доставки и сроков доставки ЭД производится экспертиза извещения о доставке, представленного отправителем ЭД, и подписанного ЭП получателя ЭД. Извещение содержит контрольные суммы принятого ЭД из состава ЭП этого ЭД, однозначно идентифицирующие ЭД, на который оно сформировано. Проверка подлинности извещения производится аналогично процедурам проверки ЭД, приведенным выше.

3. Оформление результатов технической экспертизы

3.1. Результаты экспертизы оформляются в виде письменного заключения – Акта экспертной комиссии (далее – акт), подписываемого всеми членами комиссии. Акт составляется немедленно после завершения экспертизы. В акте фиксируются результаты всех этапов, проведенной экспертизы, а также все существенные реквизиты оспариваемого ЭД. Акт составляется в трех экземплярах – по одному для каждой из Сторон и УЦ. Акт является окончательным и пересмотру не подлежит.

3.2. К акту прилагаются распечатки материалов, представленных на экспертизу (сертификаты, запросы на сертификат, извещения о доставке) и результаты проверки подписи представленных ЭД.

3.3. Подтверждение подлинности ЭД, зафиксированного в акте, будет означать, что этот документ имеет юридическую силу. Неподтверждение подлинности ЭД, зафиксированное в акте, будет означать, что представленный ЭД не имеет юридической силы.

3.4. Акты, составленные экспертной комиссией, являются надлежащим доказательством при дальнейшем разбирательстве споров в суде.

_____

Приложение 2
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Перечень документов, необходимых для выработки ключа электронной подписи

- Заявление на выработку ключа электронной подписи (Приложение №3).
- Копия паспорта, заверенная работодателем.
- Копия страхового свидетельства обязательного пенсионного страхования, заверенная работодателем.
- Копия индивидуального номера налогоплательщика, заверенная работодателем.
- Копия выписки из Единого государственного реестра юридических лиц, заверенная работодателем.

_____

Приложение 3
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Заявление на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области

_____

(полное наименование организации, включая организационно-правовую форму)

в лице_____,

(должность руководителя)

_____,

(фамилия, имя, отчество руководителя)

действующего на основании_____,

просит сформировать ключи электронной подписи, записать сформированный закрытый ключ на ключевой носитель (при необходимости) и изготовить сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области

_____,

(фамилия, имя, отчество пользователя УЦ защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области)

_____ _____ _____ _____

(серия и номер паспорта, кем и когда выдан)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

Фамилия, Имя, Отчество (CN)	
Должность (T)	
E-Mail (E)	
Организация (O)	

ИНН налогоплательщика	
ИНН (INN) организации	
ОГРН(OGRN) организации	
СНИЛС(SNILS) сотрудника	
Подразделение (OU)	
Город (L)	
Область (S)	
Страна (C)	RU
Ключевая фраза	Фраза или слово, необходимые для приостановки действия сертификата по телефону:_____

Настоящим _____

(фамилия, имя, отчество пользователя УЦ защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области)

_____ _____ _____ _____

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных Удостоверяющим центром защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области _____/_____/

«___»_____201__г.

_____ _____/_____/

(Руководитель организации)

«___»_____201__г.

Уполномоченное лицо УЦ защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области _____/_____/

«___»_____201__г.

_____

Приложение 4
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Журнал учета выдачи ключевых дистрибутивов

Дата	Организация, ФИО пользователя	Идентификатор дистрибутива (пользователя)	Тип носителя	Способ передачи (лично в руки, нарочным, письмо ДП (рег. номер) в адрес…)	Отметка прохождения инструктажа	Подпись получившего (отправившего)
1	2	3	4	5	6	7

Приложение 5
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

« __»___ 2015 г. 13:35

Сертификат ключа подписи

Кому выдан:	Иванов Иван Иванович
Кем выдан:	Удостоверяющий и ключевой центр
Действителен	с 20 ноября 2015 г. по 20 ноября 2016 г.
Назначение:	▪ Подтверждает удаленному компьютеру идентификацию вашего компьютера. ▪ Защищает сообщения электронной почты.
Версия:	V3
Серийный номер:	01 C4 C6 55 2A 25 8B C0 00 00 00 00 01 3A 13 49
Алгоритм подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: Удостоверяющий и ключевой центр Организация: министерство социальной политики Нижегородской области
Действителен с:	20 ноября 2015 г. 13:35:10 (GMT+03:00)
Действителен по	20 ноября 2016 г. 13:35:10 (GMT+03:00)
Владелец:	Имя: Иванов Иван Иванович Идентификатор: 01 Должность: Главный специалист Подразделение: Сектор автоматизации Организация: УСЗН Энского района ИНН: 0909090909 Город: Энск Страна: Россия Электронная почта: big@ru.ru Почтовый адрес: 100000, г. Энск, ул. Шварценгольдта, д.19
Открытый ключ	ГОСТ Р 34.10-2001 (512 бит)

	A9 65 E4 C1 A5 1D C6 62 B2 F7 C6 2E A0 8E 9F EE
	C2 AC 98 0C C2 7F FD 50 C1 EF A5 3B AA 6A 37 BD
	A6 7E 40 BA A0 18 A2 2F 06 16 18 B3 1A E3 B9 19
	37 85 90 94 45 CC BC F9 2E 8E F3 E9 58 12 43 CD
	BC 4D 97 10 88 5B 56 12 0C 03 8D 39 4D 53 64 DB
	E0 41 31 A5 17 35 FB 11 6C 7C 46 70 CD FE 04 E4
	08 7C 2A 0B BE 6B EA DE 87 1A A6 D1 45 4A 24 21
	A2 4A AD C7 16 3C 8F 1D 2C 0E 0E 1C 97 94 10 70
Расширения сертификата X.509	
Использование ключа:	Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8)
Расширенное использование ключа	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Идентификатор ключа субъекта	22 A1 85 3A 80 0B B1 73 2C 37 94 20 2E E3 AB 14 50 1B DD 53
Идентификатор ключа центра сертификатов	Идентификатор ключа=09 08 CF AF E2 FD 75 A7 18 F9 B2 62 36 AA 4A 27 73 58 07 68 Серийный номер сертификата=01 C4 08 12 9B 04 4B 80 00 00 00 16 01 3A 00 5C
Использование ключа	Цифровая подпись, Неотрекаемость (C0)
Основные ограничения	Тип субъекта=Конечный субъект Ограничение на длину пути=Отсутствует
Информация о проверке сертификата	Статус сертификата: действителен
Время проверки:	20 ноября 2015 г. 11:44:04 (GMT+03:00)

Пользователь	Уполномоченное лицо УЦ защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области
Подпись	
	Подпись
«____»_____20 г.	«____»_____20 г.

Приложение 6
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Уведомление о компрометации закрытого ключа ЭП

Пользователь_____

фамилия, имя и отчество владельца сертификата ключа подписи, должность, табельный номер

_____

организация, наименование и место нахождения организации

уведомляет Удостоверяющий центр _____

именование и место нахождения УЦ, в котором зарегистрирован пользователь

о компрометации секретного ключа ЭП, соответствующего открытому ключу подписи _____

уникальный регистрационный номер сертификата ключа подписи

Дополнительные сведения:

Наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи _____

_____ _____/_____

Должность, Ф.И.О. владельца сертификата ключа

«____» _____201__ г.

_____

Приложение 7
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Заявление на аннулирование (отзыв) сертификата ключа подписи

Пользователь_____

фамилия, имя и отчество владельца сертификата ключа подписи, должность, табельный номер

_____

организация, наименование и место нахождения организации

отзывает в Удостоверяющем центре _____

именование и место нахождения УЦ, в котором зарегистрирован пользователь

сертификат ключа подписи, соответствующего открытому ключу подписи _____

уникальный регистрационный номер сертификата ключа подписи

Дополнительные сведения:

Наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи _____

_____ _____/_____

Должность, Ф.И.О. владельца сертификата ключа

«____» _____20__ г.

_____

Приложение 8
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Заявление на приостановление действия сертификата ключа подписи

Пользователь_____

фамилия, имя и отчество владельца сертификата ключа подписи, должность, табельный номер

_____

организация, наименование и место нахождения организации

просит приостановить в Удостоверяющем центре _____

именование и место нахождения УЦ, в котором зарегистрирован пользователь

действие сертификата ключа подписи, соответствующего открытому ключу подписи _____

уникальный регистрационный номер сертификата ключа подписи

Срок приостановления действия сертификата _____ дней.

Дополнительные сведения:

Наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи _____

_____ _____/_____

Должность, Ф.И.О. владельца сертификата ключа

«____» _____20__ г.

_____

Приложение 9
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Заявление на возобновление действия сертификата ключа подписи

Пользователь_____

фамилия, имя и отчество владельца сертификата ключа подписи, должность, табельный номер

_____

организация, наименование и место нахождения организации

просит возобновить в Удостоверяющем центре _____

именование и место нахождения УЦ, в котором зарегистрирован пользователь

действие сертификата ключа подписи, соответствующего открытому ключу подписи _____

уникальный регистрационный номер сертификата ключа подписи

Срок приостановления действия сертификата _____ дней.

Дополнительные сведения:

Наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи _____

_____ _____/_____

Должность, Ф.И.О. владельца сертификата ключа

«____» _____20__ г.

_____

Приложение 10
к Временному регламенту
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Соглашение
о взаимном признании сертификатов ключей подписи уполномоченных лиц удостоверяющих центров и организации взаимодействия

г. Нижний Новгород «___» _____ 20___ г.

_____, именуемый в дальнейшем УЦ ЗКСПД, в лице _____, действующего на основании _____, с одной стороны, и _____, именуемый в дальнейшем УЦ _____, в лице _____, действующего на основании _____, с другой стороны, совместно именуемые Стороны, заключили настоящее Соглашение о нижеследующем:

1. Предмет Соглашения

1.1. Стороны договорились о сотрудничестве при взаимодействии Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области и УЦ в области организации системы электронного документооборота юридически значимыми документами между пользователями УЦ ЗКСПД и внешними организациями (далее - Система) по телекоммуникационным каналам связи с использованием средств электронной цифровой подписи (ЭП).

1.2. В качестве внешней организации понимается юридическое лицо, не входящее в структуру органов министерства социальной политики Нижегородской области, но осуществляющее с ним обмен электронными документами в рамках заключенного Соглашения.

1.3. При проведении совместных действий Стороны руководствуются Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи»,

настоящим Соглашением, Регламентом взаимодействия Удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области с удостоверяющими центрами внешних организаций, являющимся неотъемлемой частью настоящего Соглашения (Приложение 1), документацией на используемые средства защиты информации.

1.4. Стороны договорились о взаимном признании сертификатов ключей электронных подписей уполномоченных лиц удостоверяющих центров Сторон.

1.5. Стороны обеспечивают выпуск сертификатов ключей электронной подписи для пользователей, а также их обслуживание.

2. Права и обязанности Сторон

2.1. При организации взаимодействия в рамках Системы:

2.2. Стороны обязаны:

2.2.1. Осуществлять контроль за соблюдением пользователями правил пользования средствами криптографической защиты информации и ЭП.

2.3. Стороны обязуются предотвращать разглашение ставшей им известной в результате совместных действий конфиденциальной информации.

2.4. При прекращении действия Соглашения в соответствии с разделом 4 настоящего Соглашения Стороны обязаны выполнить процедуру отзыва сертификатов ключей подписи уполномоченных лиц Сторон, обслуживающих УЦ Сторон, в день прекращения действия Соглашения.

3. Ответственность сторон

3.1. Каждая из Сторон несет ответственность перед другой Стороной в размере реального ущерба, причиненного в результате неисполнения и (или) ненадлежащего исполнения своих обязательств по настоящему Соглашению, включая понесенные расходы по уплате санкций третьим лицам.

4. Сроки действия Соглашения

4.1. Настоящее Соглашение вступает в силу с момента его подписания и действует до _____ 20__г. включительно. Соглашение считается пролонгированным до 31 декабря каждого последующего года, если ни одна из Сторон не позднее, чем за месяц до истечения срока действия настоящего

Соглашения письменно не заявила другой Стороне о своем намерении прекратить действие Соглашения.

4.2. Настоящее Соглашение может быть досрочно расторгнуто по обоюдному согласию Сторон либо в одностороннем порядке при письменном уведомлении другой стороны за 30 (тридцать) календарных дней до предполагаемой даты расторжения Соглашения.

4.3. Настоящее Соглашение может быть досрочно расторгнуто по решению суда в случае грубых или преднамеренных нарушений одной из Сторон своих обязательств.

5. Обстоятельства непреодолимой силы

5.1. Стороны освобождаются от исполнения своих обязательств по настоящему Соглашению в случае действия обстоятельств непреодолимой силы, прямо или косвенно препятствующих исполнению настоящего Соглашения, то есть таких обстоятельств, которые независимы от воли Сторон, не могли быть ими предвидены в момент заключения Соглашения и предотвращены разумными средствами при их наступлении.

5.2. К обстоятельствам, указанным в пункте 5.1 Соглашения, относятся в том числе: объявленная фактическая война, гражданские волнения, эпидемии, эмбарго, санкции, пожары, землетрясения, наводнения и другие природные стихийные бедствия, а также издание актов органов государственной власти, препятствующих исполнению обязательств или делающих такое исполнение невозможным.

5.3. Сторона, подвергшаяся действию таких обстоятельств, обязана в срок не позднее 1 рабочего дня в письменном виде уведомить другую Сторону о возникновении, виде и возможной продолжительности действия соответствующих обстоятельств. Если эта Сторона не сообщит о наступлении обстоятельств непреодолимой силы, она лишается права ссылаться на него.

5.4. Наступление обстоятельств, предусмотренных в пункте 5.2 при условии соблюдения требований пункта 5.3 настоящего Соглашения, продлевает срок исполнения условий Соглашения на период, который в целом соответствует

сроку действия наступившего обстоятельства и разумному сроку для его устранения.

5.5. В случае если обстоятельства, предусмотренные пунктом 5.2 настоящего Соглашения, длятся более 6 (шести) месяцев, Стороны совместно определят дальнейшую юридическую судьбу настоящего Соглашения.

6. Заключительные положения

6.1. В случае возникновения споров и разногласий Стороны приложат все усилия, чтобы устранить их путём переговоров.

6.2. Любые изменения и дополнения к Соглашению действительны, если они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон.

6.3. Соглашение составлено в 2-х (двух) экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

6.4. В вопросах, не закрепленных настоящим Соглашением, Сторонам надлежит руководствоваться действующим законодательством Российской Федерации.

7. Адреса и реквизиты Сторон

_____	_____
Адрес:	Адрес:
Телефон	Телефон
Факс:	Факс:

8. Подписи и печати Сторон

_____/_____ _____/_____

_____

Приложение 1
к Соглашению о взаимном
признании сертификатов ключей
подписи уполномоченных лиц
удостоверяющих центров и
организации взаимодействия
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области

Регламент взаимодействия удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области с удостоверяющими центрами внешних организаций

1. Общие положения

1.1. Регламент взаимодействия удостоверяющего центра защищенной корпоративной сети передачи данных министерства социальной политики Нижегородской области (далее – УЦ ЗКСПД) с удостоверяющими центрами внешних организаций (далее – Регламент) предназначен для организации защищенного обмена информацией и установления отношений доверия между УЦ ЗКСПД и удостоверяющими центрами внешних организаций, оказывающими услуги по организации защищенного от несанкционированного доступа электронного документооборота (ЭДО) пользователей ЗКСПД с внешними организациями и выдаче сертификатов ключей подписи пользователям внешних организаций.

1.2. Целью настоящего Регламента является создание условий для организации защищенного от несанкционированного доступа ЭДО пользователей ЗКСПД с внешними организациями через открытые и (или) защищенные каналы связи и правовых условий использования электронной подписи (далее – ЭП) в электронных документах (далее – ЭД), при соблюдении которых ЭП в ЭД признается равнозначной собственноручной подписи в документе на бумажном

носителе в соответствии с Федеральным законом от 06 апреля 2011 года №63-ФЗ «Об электронной подписи».

1.3. Регламент разработан с учетом требований законодательства Российской Федерации, нормативных документов Федеральной службы безопасности Российской Федерации, других федеральных органов исполнительной власти Российской федерации и министерства социальной политики Нижегородской области.

1.4. Настоящий регламент является неотъемлемой частью Соглашения между УЦ ЗКСПД и удостоверяющим центром внешней организации о взаимном признании сертификатов ключей подписи уполномоченных лиц удостоверяющих центров и организации взаимодействия.

1.5. Подписание Соглашения означает, что Стороны:

1.5.1. Признают сертификаты ключей подписи уполномоченных лиц УЦ каждой из Сторон.

1.5.2. Проводят все необходимые процедуры, предусмотренные Регламентом и обеспечивающие подтверждение подлинности ЭП в ЭД, если сертификат ключа подписи подписавшего ЭД заверен ЭП уполномоченного лица УЦ любой из Сторон.

1.5.3. Проводят все необходимые процедуры, предусмотренные Регламентом и обеспечивающие подтверждение подлинности ЭП в ЭД, если сертификат ключа подписи подписавшего ЭД заверен ЭП уполномоченного лица УЦ другой Стороны или ЭП уполномоченного лица иного УЦ при наличии кросс-сертификата этого УЦ, выпущенного противоположной Стороной.

2. Термины и определения

2.1. ЭД (электронный документ) – документ, зафиксированный на электронном носителе (в виде набора символов, звукозаписи или изображения) и предназначенный для передачи во времени и пространстве с использованием средств вычислительной техники и электросвязи с целью хранения и(или) использования.

2.2. ЭП (электронная подпись) – информация в электронной форме, полученная в результате криптографического преобразования информации с использованием закрытого ключа ЭП, которая присоединена к ЭД или иным образом связана с ЭД и позволяющая идентифицировать владельца сертификата открытого ключа ЭП, а также установить отсутствие искажения информации в ЭД.

2.3. Закрытый ключ ЭП – уникальная последовательность символов, известная владельцу сертификата открытого ключа ЭП и предназначенная для создания в ЭД ЭП с использованием средств ЭП (подписание ЭД). Закрытый ключ ЭП действует на определенный момент времени (действующий закрытый ключ ЭП). Закрытый ключ ЭП действует, если:

2.3.1. Наступил момент времени ввода в действие закрытого ключа ЭП.

2.3.2. Срок действия закрытого ключа ЭП не истек.

2.3.3. Сертификат открытого ключа ЭП, соответствующий данному закрытому ключу ЭП не аннулирован (не отозван) и действие его не приостановлено.

2.4. Открытый ключ ЭП – уникальная последовательность символов, соответствующая закрытому ключу ЭП, предназначенная для подтверждения с использованием средств ЭП подлинности ЭП в ЭД.

2.5. Сертификат ключа ЭП – ЭД с ЭП уполномоченного лица УЦ или бумажный документ, подписанный уполномоченным лицом УЦ, подтверждающий соответствие между закрытым ключом ЭП и информацией, идентифицирующей владельца ключа ЭП. Содержит информацию о владельце ключа ЭП, сведения об открытом ключе ЭП, его назначении и области применения, название УЦ и другие сведения. Сертификат ключа ЭП действует на определенный момент времени (действительный сертификат ключа ЭП). Сертификат ключа ЭП действует если:

2.5.1. Наступил момент времени ввода в действие сертификата ключа ЭП.

2.5.2. Срок действия сертификата ключа ЭП не истек.

2.5.3. Сертификат ключа ЭП не аннулирован (не отозван) и действие его не приостановлено.

2.6. СОС (список отзыва сертификатов ключей ЭП) – ЭД с ЭП уполномоченного лица УЦ, включающий в себя список серийных номеров сертификатов ключей подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

2.7. Ключевой дистрибутив – зашифрованный на парольном ключе файл, формируемый УКЦ для зарегистрированных пользователей УЦ. Включает в себя необходимую первичную ключевую информацию для обеспечения защищенного взаимодействия с УЦ, первичный закрытый ключ ЭП и сертификат ключа ЭП пользователя, сертификат ключа ЭП уполномоченного лица УЦ, другие файлы, необходимые для реализации функций ЭП.

2.8. Ключевой носитель – носитель данных с ключевым дистрибутивом, содержащим ключевую и парольную информацию пользователя УЦ включая:

2.8.1. Открытый и закрытый ключи ЭП.

2.8.2. Сертификат ключа ЭП.

2.8.3. СОС УЦ и доверенных УЦ.

2.9. Подразделение ЗИ – подразделение, обеспечивающее информационную безопасность (в том числе защиту персональных данных за исключением сведений, составляющих государственную тайну) в министерстве социальной политики Нижегородской области (далее – Министерство) и подведомственных Министерству учреждениях (далее – Учреждения).

2.10. ЗКСПД – защищенная корпоративная сеть передачи данных Министерства.

2.11. АРМ (Автоматизированное рабочее место) – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

2.12. НСД (несанкционированный доступ к информации) – доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих

разрешения на доступ к этой информации, а также получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей;

2.13. Компрометация ключевой информации — факт доступа постороннего лица к ключевой информации, а также подозрение на факт доступа постороннего лица к ключевой информации, а именно:

2.13.1. Постороннему лицу мог стать доступным файл ключевого дистрибутива.

2.13.2. Существует подозрение на получение пароля доступа к ключам пользователя постороннему лицу.

2.13.3. Постороннему лицу мог стать доступным съемный носитель с ключевой информацией.

2.13.4. Постороннее лицо могло получить неконтролируемый физический доступ или доступ по локальной сети к ключевой информации, хранящейся на АРМ пользователя УЦ.

2.14. ПО – программное обеспечение.

2.15. СКЗИ (Средства криптографической защиты информации) – программные или программно-аппаратные средства, осуществляющие криптографическое преобразование информации.

2.16. Средства ЭП – программные или программно-аппаратные средства, обеспечивающие реализацию хотя бы одной из следующих функций:

2.16.1. Подписание ЭД с использованием закрытого ключа ЭП.

2.16.2. Подтверждение с использованием открытого ключа ЭП подлинности ЭП в ЭД.

2.16.3. Создание закрытых и открытых ключей ЭП.

2.17. УЦ (Удостоверяющий центр) – подразделение, осуществляющие функции по созданию и выдаче системы открытых и закрытых ключей ЭП, а также иные функции, в соответствии с Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

2.18. ЦУС (центр управления сетью) – программное обеспечение, предназначенное для конфигурирования и управления ЗКСПД;

2.19. УКЦ (удостоверяющий и ключевой центр) — программное обеспечение, которое выполняет функции формирования и хранения первичной ключевой информации (мастер-ключи шифрования и межсетевые мастер-ключи), формирования ключей шифрования, выполнения процедур смены мастер-ключей и смены ключей при компрометации, формирования персональных ключей защиты пользователей и криптографически надежных парольных фраз (паролей), а также записи персональных ключей пользователей на аппаратные носители ключей.

2.20. Оператор УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное полномочиями в соответствии с Положением и Регламентом.

2.21. Администратор УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное полномочиями в соответствии с Положением и Регламентом.

2.22. Администратор безопасности УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное полномочиями в соответствии с Положением и Регламентом.

2.23. Уполномоченное лицо УЦ – физическое лицо, являющееся сотрудником УЦ и наделенное УЦ полномочиями по заверению сертификатов ключей ЭП и СОС, а также наделенное полномочиями в соответствии с Положением и Регламентом.

2.24. Пользователь УЦ – физическое лицо, зарегистрированное в УЦ.

2.25. Владелец сертификата ключа ЭП – пользователь УЦ, на имя которого УЦ выдал сертификат ключа ЭП и которое владеет соответствующим закрытым ключом ЭП, позволяющим с помощью средств ЭП создавать ЭП в ЭД (подписывать ЭД).

2.26. Внешняя организация – юридическое лицо, не входящее в структуру Министерства, осуществляющее с ЗКСПД информационное взаимодействие.

2.27. Доверенный УЦ – УЦ внешней организации, с которым УЦ установил доверенные отношения на основании Соглашения о взаимодействии и взаимном признании сертификатов ключей ЭП уполномоченных лиц УЦ (Приложение 4).

2.28. Кросс-сертификат ключа ЭП – сертификат ключа ЭП уполномоченного лица доверенного УЦ, передаваемый в УЦ с открытым ключом ЭП уполномоченного лица доверенного УЦ и ЭП уполномоченного лица доверенного УЦ. Обеспечивает признание ЭП, сертификат ключа ЭП которой выдан в доверенном УЦ.

2.29. Плановая смена ключей – смена ключей, не вызванная компрометацией ключей, осуществляемая в соответствии с документацией на СКЗИ.

2.30. Срок действия сертификата ключа ЭП – 1 год с момента введения в действие ключа ЭП.

2.31. Доверенный способ передачи информации – способ передачи информации, определенный и используемый двумя или несколькими юридическими или физическими лицами на основе взаимной договоренности, и обеспечивающий требуемую степень ее защищенности.

3. Установление доверительных отношений между УЦ ЗКСПД и УЦ внешней организации

3.1. Установление доверительных отношений между двумя УЦ Сторон является организационно – технической процедурой, в результате которой участники ЭДО, получившие сертификаты ключей подписи в одном УЦ, получают возможность проверить подлинность ЭП в ЭД участников ЭДО, получивших сертификаты в другом УЦ.

3.2. Для установления доверительных отношений каждая из Сторон (УЦ ЗКСПД и УЦ внешней организации) оформляет на бумажном носителе список сертификатов ключей подписи удостоверяющего центра (Приложение 1), включающий сертификаты ключей подписи уполномоченных лиц УЦ и выпущенные кросс-сертификаты ключей подписи уполномоченных лиц доверенных УЦ, которыми будут заверяться ключи подписи пользователей,

зарегистрированных в данном УЦ и в доверенных УЦ. К списку прилагаются распечатанные на бумажных носителях соответствующие сертификаты ключей подписи, указанные в списке. Список подписывается руководителем УЦ ЗКСПД и руководителем УЦ внешней организации, заверяется печатями УЦ ЗКСПД и УЦ внешней организации и передается под расписку другой Стороне.

3.3. Список отозванных сертификатов и сертификаты ключей подписи уполномоченных лиц УЦ внешней организации в электронном виде передаются в УЦ ЗКСПД, а сертификаты ключей подписи уполномоченных лиц УЦ ЗКСПД и СОС ЗКСПД в электронном виде передаются в УЦ внешней организации.

3.4. В каждом из УЦ Сторон производится сравнение электронных сертификатов ключей подписи уполномоченных лиц УЦ другой Стороны с распечатанными сертификатами на бумажных носителях и ввод их в действие. При этом сертификаты заверяются ЭП уполномоченного лица соответствующего УЦ.

3.5. При любом изменении в списке сертификатов ключей подписи уполномоченных лиц УЦ соответствующая Сторона оформляет в соответствии с пунктом 3.2 Регламента новый список с приложенными сертификатами уполномоченных лиц УЦ и передает его другой Стороне.

4. Организация защищенного взаимодействия между УЦ ЗКСПД и УЦ внешней организации

4.1. Защищенное взаимодействие между УЦ ЗКСПД и УЦ внешней организации осуществляется на основании технической документации к СКЗИ Сторон.

5. Порядок взаимодействия УЦ Сторон при формировании новых списков отозванных сертификатов, при смене ключей подписи уполномоченных лиц УЦ

5.1. При изменении СОС в случае отзыва или приостановки действия сертификатов ключей подписи пользователей УЦ новый СОС высылается в УЦ каждой из Сторон. Полученные СОС подписываются уполномоченным лицом УЦ и размещаются в точках публикации УЦ.

5.2. Уполномоченные лица УЦ каждой из Сторон обязаны производить периодическую (плановую) замену своих ключей подписи не реже заданного срока действия ключа подписи. В целях обеспечения действительности сертификатов ключей подписи пользователей УЦ, заверенных подписью уполномоченного лица соответствующего УЦ, замена ключей подписи уполномоченного лица УЦ должна быть произведена до окончания его срока действия не менее чем за срок действия сертификатов пользователей УЦ.

5.3. В случае компрометации ключей подписи уполномоченное лицо УЦ обязано:

5.3.1. Немедленно сообщить об этом ответственным лицам УЦ другой Стороны.

5.3.2. Аннулировать сертификат ключа подписи и отправить новые СОС в УЦ другой Стороны.

5.3.3. Сформировать новые ключи подписи и сертификат ключа подписи.

5.4. После выполнения действий, описанных в пункте 5.3, производится оформление на бумажном носителе нового списка сертификатов ключей подписи УЦ в соответствии с разделом 3.2 Регламента и передача новых сертификатов уполномоченного лица УЦ в электронном виде в УЦ другой Стороны.

5.5. Уполномоченное лицо УЦ осуществляет сравнение новых электронных сертификатов уполномоченных лиц УЦ другой Стороны с сертификатами, распечатанными на бумажных носителях и вводит их в действие.

_____

Приложение 1
к Регламенту взаимодействия
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области с
удостоверяющими центрами
внешних организаций

Список сертификатов ключей подписи уполномоченных лиц
Удостоверяющего центра
(сертификаты прилагаются)

_____

Наименование и место нахождения организации Удостоверяющего центра

Уникальные регистрационные номера сертификатов ключей подписи

№ 1

...

№ N

Наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи:

_____

Перечисленные в настоящем списке сертификаты Удостоверяющего центра подтверждают полномочия сертификатов ключей подписи, заверенных приложенными сертификатами.

Руководитель УЦ _____/_____

«_____»_____ 20___ г.

_____

Приложение 2
к Регламенту взаимодействия
удостоверяющего центра
защищенной корпоративной сети
передачи данных министерства
социальной политики
Нижегородской области с
удостоверяющими центрами
внешних организаций

Список сертификатов ключей подписи
Удостоверяющего центра
(сертификаты прилагаются)

_____

Наименование и место нахождения организации Удостоверяющего центра

Уникальные регистрационные номера сертификатов ключей подписи

№ 1

...

№ N

Наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи:

_____

Перечисленные в настоящем списке сертификаты Удостоверяющего центра подтверждают полномочия сертификатов ключей подписи, заверенных приложенными сертификатами.

Руководитель УЦ _____/_____

«_____»_____ 20___ г.

_____