Утвержден приказом
Министерства цифрового
развития Кыргызской Республики
от «25» августа 2021 года № 100-пр

РЕГЛАМЕНТ

Главного (корневого) удостоверяющего центра

Министерства цифрового развития Кыргызской Республики

2021

1. Сокращения

Сокращение	Полное наименование
МЦР	Министерство цифрового развития Кыргызской Республики
КУЦ МЦР	Корневой удостоверяющий центр МЦР
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУЦ	Подчиненный удостоверяющий центр
СОС	Список отозванных сертификатов
УЦ	Удостоверяющий центр
ЦР	Центр регистрации
Инфраструктура открытых ключей	Совокупность сервисов для управления ключами и цифровыми сертификатами пользователей, программ и систем.

2. Общие сведения о Корневом удостоверяющем центре

2.1. Корневой удостоверяющий центр Министерства цифрового развития Кыргызской Республики является главным (корневым) удостоверяющим центром. Издателем самоподписанного сертификата ключа проверки подписи КУЦ МЦР является Министерство цифрового развития Кыргызской Республики.

2.2. КУЦ МЦР создает и выдает сертификаты ключей проверки электронных подписей для подчиненных удостоверяющих центров, находящихся на территории Кыргызской Республики.

2.3. КУЦ МЦР руководствуется в своей деятельности следующими нормативными правовыми актами:

- Закон Кыргызской Республики «Об электронной подписи» (далее - Закон);
- Закон Кыргызской Республики «Об информации персонального характера»;
- постановление Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742;
- Требования к защите информации, содержащейся в базах данных государственных информационных систем» (далее - Требования по ЗИ), утвержденные ППКР от 21 ноября 2017 года № 760;
- Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» (далее - Требования по безопасности ПД), утвержденные постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 759;
- Положение о Корневом удостоверяющем центре Министерства цифрового развития Кыргызской Республики;
- Настоящий Регламент КУЦ МЦР.

2.4. КУЦ МЦР является удостоверяющим центром верхнего уровня (root) в иерархической структуре удостоверяющих центров Кыргызской Республики, основанной на инфраструктуре открытых ключей.

2.5. Реквизиты КУЦ МЦР:

- юридический адрес: Кыргызская Республика, 720010 г. Бишкек, ул. Уметалиева, 41;
- фактическое местонахождение: Кыргызская Республика, 720010 г. Бишкек, ул. Уметалиева, 41;
- контактные телефоны: + 96 312 60 50 35, адрес электронной почты: info@ict.gov.kg.

3. Назначение Регламента

3.1. Настоящий Регламент КУЦ МЦР, в соответствии с пунктом 8 Положения о КУЦ МЦР, разработан Государственным предприятием «Инфоком» при Министерстве цифрового развития Кыргызской Республики - техническим оператором КУЦ МЦР, обеспечивающим бесперебойное функционирование КУЦ МЦР и утвержден соответствующим приказом МЦР.

3.2. Изменения в Регламент КУЦ МЦР, которые не оказывают влияние на работу ПУЦ, вносятся без оповещения ПУЦ путем обновления копий Регламента КУЦ МЦР в местах его опубликования.

3.3. Изменения в Регламент КУЦ МЦР, которые оказывают влияние на работу ПУЦ, вносятся путем обновления копий Регламента в местах его опубликования с оповещением ПУЦ.

3.4. Все изменения, вносимые в настоящий Регламент, утверждаются соответствующим приказом МЦР.

3.5. Регламент КУЦ МЦР определяет принципы эксплуатации ПАК КУЦ МЦР и функционально-техническое обеспечение работы КУЦ МЦР.

3.6. Регламент КУЦ МЦР предназначен для администраторов и пользователей удостоверяющих центров иерархической структуры удостоверяющих центров Кыргызской Республики.

3.7. Целью настоящего Регламента КУЦ МЦР является создание технологических и правовых отношений между КУЦ МЦР, подчиненными удостоверяющими центрами в Кыргызской Республике, а также другими УЦ.

3.8. Настоящий Регламент КУЦ МЦР не регулирует деятельность удостоверяющих центров банков и иных финансово-кредитных учреждений Кыргызской Республики, деятельность которых регулируется Национальным банком Кыргызской Республики.

3.9. Регламент КУЦ МЦР определяет:

- структуру иерархии удостоверяющих центров в Кыргызской Республике;
- порядок работы КУЦ МЦР;
- права и обязанности КУЦ МЦР;
- порядок взаимоотношений между КУЦ МЦР и ПУЦ;
- требования по применению электронных подписей в облачных технологиях.

3.10. Регламент КУЦ МЦР распространяется в электронном формате путем опубликования на сайте **www.ict.gov.kg** а также в бумажном формате по письменному требованию на возмездной основе.

3.11. Настоящий Регламент КУЦ МЦР вступает в силу со дня официального опубликования и действует до принятия следующей версии Регламента КУЦ или официального уведомления о прекращении его действия.

4. Термины и определения

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация.

Сертификат ключа проверки подписи - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки подписи владельцу сертификата ключа проверки подписи.

Квалифицированный сертификат ключа проверки подписи (далее - квалифицированный сертификат) - сертификат ключа проверки подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо органом исполнительной власти, уполномоченным в сфере использования электронной подписи, осуществляющим функции главного (корневого) удостоверяющего центра;

Владелец сертификата ключа проверки подписи - лицо, которому в порядке, установленном настоящим Законом, удостоверяющим центром выдан сертификат ключа проверки подписи;

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

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

Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по созданию и выдаче сертификатов ключа проверки подписи;

Аккредитация удостоверяющего центра - признание органом исполнительной власти, уполномоченным в сфере использования электронной подписи, соответствия удостоверяющего центра требованиям, установленным настоящим Законом об электронной подписи;

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

Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций создания, хранения и выдачи сертификатов ключа проверки подписи, а также ведения реестра сертификатов ключа проверки подписи;

Участники электронного взаимодействия - государственные органы, органы местного самоуправления, организации, их союзы и объединения, а также граждане, обменивающиеся информацией в электронной форме;

Подчиненный удостоверяющий центр – удостоверяющий центр, сертификат которого издан КУЦ МЦР. ПУЦ издает сертификаты ключей проверки подписи пользователям ПУЦ, а также иные функции, связанные с деятельностью УЦ.

5. Иерархия удостоверяющих центров

Иерархия удостоверяющих центров Кыргызской Республики, выдающих сертификаты ключей проверки электронной подписи строится по следующей схеме:

– Корневой удостоверяющий центр Министерства цифрового развития Кыргызской Республики (КУЦ МЦР), являющийся головным, сертификат ключа проверки подписи который является самоподписанным;

– Подчиненные удостоверяющие центры (ПУЦ), сертификаты ключей проверки подписи, которых изданы КУЦ МЦР.

6. Корневой удостоверяющий центр

КУЦ МЦР включает следующие основные функциональные компоненты на базе ПАК «Инфраструктура открытых ключей CERTEX»:

6.1. **Центр сертификации** – компонент КУЦ МЦР, обеспечивающий:

- издание, отзыв (аннулирование), приостановление и возобновление действия сертификатов ключей проверки подписи ПУЦ;
- работу со списками отозванных (аннулированных) сертификатов;
- обработку запросов на кросс сертификаты с иными УЦ;
- обработку запросов на сертификаты ключей проверки подписи ПУЦ и просмотр запросов и сертификатов ключей проверки подписи;
- экспорт и проверку сертификатов ключей проверки подписи.

Центр сертификации выполняет следующие функции:

- генерацию пары ключей для КУЦ МЦР со сроком действия 10 (десять) лет и создание запроса на издание сертификата ключа проверки подписи КУЦ МЦР со сроком действия 10 (десять) лет;
- издание сертификатов ключа проверки подписи для ПУЦ со сроком действия до 5 (пять) лет;
- отзыв (аннулирование), приостановление и возобновление действия сертификатов ключей проверки подписи ПУЦ;
- ведение реестра действующих сертификатов ключей проверки подписи ПУЦ, публикация сертификатов ключа проверки подписи КУЦ, ПУЦ и списков отозванных (аннулированных) сертификатов КУЦ и ПУЦ.

6.2. **Центр регистрации** - компонент КУЦ МЦР, выполняет регистрацию УЦ, формирование запросов в Центр сертификации, изготовление ключевых носителей, выпуск сертификатов ключей проверки подписи, а также следующие основные функции:

- безопасное хранение и использование ключа подписи Администратора ЦР КУЦ МЦР;
- идентификацию, аутентификацию и регистрацию ПУЦ;
- формирование заверенного Администратором ЦР КУЦ запроса на сертификат ключа проверки подписи ПУЦ;
- выдача сертификатов ключей проверки подписи владельцам ПУЦ;
- ведение справочников запросов и изданных сертификатов ключей проверки подписи;
- формирование запросов на отзыв (аннулирование), приостановление или возобновление действия сертификатов в Центр сертификации КУЦ МЦР.

6.3. **Сервис публикации** - компонент КУЦ МЦР, осуществляет публикацию изданных сертификатов ключей проверки подписи и списков, отозванных (аннулированных) сертификатов ключей проверки подписи в общедоступных хранилищах данных и выполняет следующие функции:

- публикация сертификатов ключа проверки подписи пользователей КУЦ МЦР;
- публикация списка отозванных (аннулированных) сертификатов ключей проверки подписи КУЦ МЦР;
- получение актуальных СОС с точек распространения ПУЦ.

7. Права и обязанности КУЦ МЦР

Права:

7.1. Предоставлять копию сертификата ключа проверки подписи в электронной или бумажной форме, находящегося в реестре КУЦ МЦР по официальному запросу ПУЦ.

7.2. Отказать в изготовлении сертификата ключа проверки подписи ПУЦ, подавшим заявление на его изготовление, с указанием причин отказа.

7.3. Приостановить действие сертификата ключа проверки подписи ПУЦ с уведомлением владельца сертификата ключа проверки подписи, действие которого приостановлено, с указанием причин.

Обязанности:

7.4. Проводить периодическую внутреннюю проверку деятельности КУЦ по соблюдению требований настоящего Регламента с составлением акта, отражающим выявленные нарушения и сроки их устранения. Данная проверка должна проводиться не реже одного раза в год.

7.5. Для формирования усиленной электронной подписи использовать только сертифицированные средства электронной подписи, соответствующие требованиям нормативных актов Кыргызской Республики.

7.6. Использовать ключ подписи КУЦ МЦР только для подписания издаваемых КУЦ МЦР сертификатов ключа проверки подписи и СОС КУЦ МЦР.

7.7. Принимать необходимые меры по защите ключа подписи КУЦ МЦР от несанкционированного доступа.

7.8. Производить привязку времени сервера КУЦ МЦР к времени GMT (Greenwich Mean Time) с учетом часового пояса, а также синхронизировать по времени все программные и технические средства обеспечения деятельности КУЦ МЦР.

7.9. Осуществлять регистрацию ПУЦ в соответствии с порядком, определенным настоящим Регламентом КУЦ МЦР.

7.10. Обеспечить занесение регистрационной информации ПУЦ в реестр КУЦ МЦР.

7.11. Обеспечить уникальность регистрационной информации ПУЦ, для идентификации владельцев сертификатов ключа проверки подписи.

7.12. Не разглашать (не публиковать) регистрационную информацию ПУЦ, за исключением информации, заносимой в сертификаты ключей проверки подписи.

7.13. Изготовить сертификат ключа проверки подписи зарегистрированных ПУЦ по заявлению на изготовление сертификата ключа проверки подписи, в соответствии с настоящим Регламентом КУЦ МЦР.

7.14. Обеспечить уникальность изготовленных сертификатов ключей проверки подписи ПУЦ.

7.15. Выполнять процедуру выпуска сертификата ключа проверки подписи с использованием сертифицированного программного и/или аппаратного средства.

7.16. Отозвать (аннулировать), приостановить и возобновить действие сертификата ключа проверки подписи ПУЦ по заявлению его владельца.

7.17. Отозвать (аннулировать) сертификат ключа проверки подписи ПУЦ, если истек установленный срок, на который действие данного сертификата было приостановлено.

7.18. Отозвать (аннулировать) сертификат ключа проверки подписи ПУЦ в случае установления факта компрометации ключа подписи.

7.19. Занести сведения об отозванном (аннулированном) сертификате ключа проверки подписи в СОС в день поступления заявления с указанием даты и времени занесения.

7.20. Занести сведения о сертификате ключа проверки подписи, действие которого приостановлено, в СОС в день поступления заявления с указанием даты и времени занесения, а также признака приостановления.

7.21. Исключить из СОС сведения о сертификате ключа проверки подписи, действие которого возобновлено, в течении 24 (двадцать четыре) часов с момента поступления заявки.

7.22. Публиковать актуальный СОС. Адрес размещения СОС заносится в издаваемые КУЦ МЦР сертификаты ключей проверки подписи.

7.23. Официально уведомить о факте изготовления сертификата ключа проверки подписи его владельца. Срок уведомления – не позднее 24 (двадцать четыре) часа с момента изготовления сертификате ключа проверки подписи.

7.24. Официальным уведомлением о факте отзыва (аннулирования) сертификата ключа проверки подписи является опубликование СОС, содержащего сведения об отозванном (аннулированном) сертификате ключа проверки подписи, в точках распространения СОС. Временем отзыва (аннулирования) сертификата ключа проверки подписи признается время занесения сведений об отозванном (аннулированном) сертификате в СОС. Временем опубликования СОС признается включенное в его структуру время изготовления СОС.

7.25. Официальным уведомлением о факте приостановления действия сертификата ключа проверки подписи является опубликование СОС, содержащим сведения о сертификате ключа проверки подписи, действие которого приостановлено, в точках распространения СОС. Временем приостановления действия сертификата ключа проверки подписи признается время занесения сведений об этом сертификате в СОС. Временем опубликования СОС признается включенное в его структуру время изготовления СОС.

7.26. Официально уведомить о факте возобновления действия сертификата ключа проверки подписи его владельца. Срок уведомления – не позднее 24 (двадцать четыре) часов с момента исключения сведений о сертификате ключа проверки подписи, действие которого возобновлено, из СОС. Официальным уведомлением о факте возобновления действия сертификата является опубликование СОС, не содержащего сведений об этом сертификате, в точках распространения СОС. Этот СОС должен иметь более позднее время опубликования, чем СОС, в котором указан сертификат ключа проверки подписи, действие которого приостановлено. Временем возобновления действия сертификата ключа проверки подписи признается время официального уведомления о факте возобновления действия сертификата.

7.27. Вести реестр всех изготовленных сертификатов ключа проверки подписи ПУЦ в течение установленного срока хранения. Реестр сертификатов ключа проверки подписи ведется в электронном виде. Сертификаты ключей проверки подписи представлены в реестре в электронной форме.

7.28. Осуществлять выдачу заверенных бумажных копий сертификатов ключей проверки подписи по обращениям ПУЦ.

7.29. Публиковать выписки из реестра, позволяющие определить действительность сертификатов ключа проверки подписи ПУЦ. Выписка из реестра КУЦ МЦР предоставляется по требованию пользователя в виде списка сертификатов ключа проверки подписи и, при необходимости, СОС ключей проверки подписи в электронной форме в формате, описанном в PKCS#7 «Cryptographic Message Syntax Standard».

7.30. Уведомлять владельца сертификата ключа проверки подписи о фактах, которые стали известны КУЦ МЦР и которые существенным образом могут сказаться на возможности дальнейшего использования ключа подписи и сертификата ключа проверки подписи.

8. Права и обязанности ПУЦ

Права:

8.1. Получить список отозванных (аннулированных) и приостановленных сертификатов ключа проверки подписи, изготовленный КУЦ МЦР.

8.2. Получить сертификат ключа проверки подписи КУЦ МЦР.

8.3. Получить сертификат ключа проверки подписи в электронной форме, находящегося в реестре сертификатов ключа проверки подписи КУЦ МЦР.

8.4. Применять сертификат ключа проверки подписи КУЦ МЦР для проверки электронной подписи КУЦ МЦР в сертификатах ключа проверки подписи, изготовленных КУЦ МЦР.

8.5. Применять СОС, опубликованный КУЦ МЦР, для установления статуса сертификатов ключа проверки подписи, изготовленных КУЦ МЦР.

8.6. Применять сертификат ключа проверки подписи КУЦ МЦР для проверки электронной подписи электронных документов.

8.7. Сформировать пару ключей электронной подписи на своем рабочем месте с использованием средства электронной подписи и программных средств, предоставляемых или рекомендуемых КУЦ МЦР.

8.8. Обратиться в КУЦ МЦР с заявлением на изготовление сертификата ключа проверки подписи.

8.9. Воспользоваться предоставляемыми КУЦ МЦР программными средствами, чтобы получить и ввести в действие на своем рабочем месте изготовленный сертификат ключа проверки подписи в электронной форме.

8.10. Обратиться в КУЦ МЦР с заявлением на отзыв (аннулирование) и приостановление действия сертификата ключа проверки подписи, владельцем которого он является, в течение срока действия соответствующего сертификата ключа проверки подписи.

8.11. Обратиться в КУЦ МЦР с заявлением на возобновление действия приостановленного сертификата ключа проверки подписи, владельцем которого он является, в течение срока действия соответствующего сертификата ключа проверки подписи и в срок, на который действие сертификата было приостановлено.

8.12. Обратиться в КУЦ МЦР с заявлением на получение информации о статусе сертификата ключа проверки подписи, выданного КУЦ МЦР.

Обязанности:

8.13. Представить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента КУЦ МЦР.

8.14. Хранить в тайне приватный ключ подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

8.15. Применять для формирования электронной подписи только действующий ключ подписи.

8.16. Не применять ключ подписи в случае его компрометации или в случае, если возникло подозрение в его компрометации.

8.17. Применять ключ подписи только в соответствии с назначениями его использования, указанными в соответствующих полях сертификата ключа проверки подписи.

8.18. Немедленно обратиться в КУЦ МЦР с заявлением на отзыв (аннулирование) сертификата ключа проверки подписи в случае потери, раскрытия, искажения приватного ключа подписи, а также в случае, если ПУЦ стало известно, что этот ключ подписи используется или использовался ранее другими лицами.

8.19. Не использовать ключ подписи, связанный с сертификатом ключа проверки подписи, заявление на отзыв (аннулирование) которого подано в КУЦ МЦР в течение времени, исчисляемого с момента подачи заявления на отзыв (аннулирование) сертификата в КУЦ МЦР по момент времени официального уведомления об отзыве (аннулировании) сертификата, либо об отказе в отзыве (аннулировании) сертификата.

8.20. Не использовать ключ подписи, заявление на приостановление действия

сертификата ключа проверки подписи, связанного с ним, подано в КУЦ МЦР, в течении времени, исчисляемого с момента подачи заявления на приостановление действия сертификата в КУЦ МЦР по момент официального уведомления о приостановлении действия сертификата ключа подписи, либо об отказе в приостановлении действия сертификата ключа подписи.

8.21. Не использовать ключ подписи, связанный с сертификатом ключа проверки подписи, который отозван (аннулирован) или действие его приостановлено.

8.22. Осуществлять запись ключа подписи ПУЦ только на защищенные ключевые носители.

9. Политика конфиденциальности

9.1. К конфиденциальной информации относятся:

- ключ подписи КУЦ МЦР;
- персональные данные должностных лиц КУЦ МЦР, за исключением сведений публикуемых в сертификатах ключей проверки подписи;
- регистрационные данные ПУЦ, за исключением сведений публикуемых в сертификатах ключей проверки подписей;
- схема конфигурации и размещение программных и аппаратных средств КУЦ МЦР;
- схемы энергоснабжения и жизнеобеспечения КУЦ МЦР;
- схемы подключения аппаратных средств и телекоммуникационного оборудования КУЦ МЦР;
- журнал учета (регистрации) КУЦ МЦР.

9.2. КУЦ МЦР не должен раскрывать конфиденциальную информацию третьим лицам за исключением случаев:

- требующих раскрытия в соответствии с действующим законодательством;
- при наличии судебного решения;
- определенных Регламентом КУЦ МЦР случаев.

9.3. Информация, не отнесенная к конфиденциальной, является информацией, доступ к которой возможно получить на сайте КУЦ МЦР. К такой информации относятся данные, включаемые в сертификаты ключей проверки подписи КУЦ МЦР и сертификаты ключей проверки подписи ПУЦ, а также публикуемые в СОС КУЦ МЦР.

10. Аккредитация и регистрация Подчиненного удостоверяющего центра

10.1. Заявление о присоединении к Регламенту КУЦ МЦР (Приложение № 1) и заявление о получении аккредитации (Приложение № 2) представляются заинтересованным юридическим лицом в Центр регистрации КУЦ МЦР (ЦР КУЦ МЦР).

10.2. К вышеуказанным заявлениям прилагаются следующие документы:

1) документ, подтверждающий наличие финансового обеспечения ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в сертификате ключа проверки электронной подписи, выданном таким ПУЦ, или информации, содержащейся в реестре сертификатов, который ведет такой ПУЦ, в сумме не менее чем полтора миллиона сомов. Таким документом может являться: банковская гарантия; договор поручительства.

В случае предоставления банковской гарантии в качестве документа, подтверждающего наличие финансового обеспечения ответственности, заявитель указывает номер лицензии на осуществление банковской деятельности кредитной организации, предоставившей банковскую гарантию;

2) актуальная выписка из бухгалтерского баланса, подтверждающая, что стоимость чистых активов ПУЦ составляет не менее чем один миллион сомов;

3) документы, выдаваемые государственным органом исполнительной власти в области обеспечения безопасности, подтверждающие соответствие используемых ПУЦ средств электронной подписи и средств ПУЦ, требованиям, установленным

государственным органом исполнительной власти в области обеспечения безопасности;

4) документы, подтверждающие право собственности ПУЦ, либо иное законное основание использования им средств электронной подписи и средств ПУЦ, указанных в подпункте 3 настоящего пункта;

5) документы, подтверждающие наличие в штате ПУЦ не менее двух работников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключей проверки электронных подписей, имеющих высшее профессиональное образование в области информационных технологий или информационной безопасности, либо высшее или среднее профессиональное образование, прошедших переподготовку или повышение квалификации по вопросам использования электронной подписи:

- копии трудовых договоров (с приложением утвержденных должностных инструкций);

- копии документов о высшем профессиональном образовании в области информационных технологий или информационной безопасности (диплом установленного государственного образца) или копии документов о прохождении переподготовки или повышения квалификации по вопросам использования электронной подписи (свидетельства установленного образца);

- копии сертификатов администратора безопасности ПУЦ;

6) схема взаимодействия модулей (компонент) удостоверяющего центра и схемы электронной подписи с данными о применяемых алгоритмах криптографических преобразований и другими исходными данными (основными требованиями) по реализации процесса формирования электронной подписи и требованиями к отдельным параметрам и удостоверяющему центру, утвержденными заявителем;

7) перечень нормативно-технических документов, утвержденных внутренним актом ПУЦ, регламентирующих:

- политику информационной безопасности удостоверяющего центра;

- регламент или правила деятельности удостоверяющего центра;

- политику применения регистрационных свидетельств;

- положение об удостоверяющем центре;

- инструкцию о действиях работников, осуществляющих работы от лица заявителя, непосредственно участвующих в работах по сопровождению, администрированию;

- выписку регистрационных свидетельств удостоверяющего центра (далее - ответственные лица) во внештатных, кризисных ситуациях;

- инструкцию о резервном копировании информационных ресурсов удостоверяющего центра;

- инструкцию по установке, настройке и использованию программного обеспечения или программно-аппаратного комплекса удостоверяющего центра;

- инструкцию по созданию, использованию, хранению, передаче и уничтожению ключевой документации;

8) учредительные документы ПУЦ, либо их надлежащим образом заверенные копии;

9) надлежащим образом заверенный перевод на государственный язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);

10) доверенность или иной документ, подтверждающий право уполномоченного лица ПУЦ, направившего указанные документы, действовать от имени ПУЦ.

10.3. КУЦ МЦР принимает решение об аккредитации либо об отказе в аккредитации ПУЦ в течение 30 календарных дней со дня приема заявления и приложенных документов. Рассмотрение заявления, а также полноты, целостности и содержания документов, представленных ПУЦ, осуществляется КУЦ МЦР в течение 30 календарных дней со дня приема заявления.

10.4. КУЦ МЦР проверяет достоверность сведений, содержащихся в представленных ПУЦ документах, в том числе путем согласования с уполномоченным

государственным органом в области обеспечения безопасности.

10.5. КУЦ МЦР также вправе направить запрос на получение документов, позволяющих проверить достоверность сведений, представленных ПУЦ, в иные государственные органы в соответствии с их компетенцией.

10.6. КУЦ МЦР проводит соответствующую проверку и аттестацию ПУЦ согласно требованиям, указанным в Требованиях по ЗИ.

10.7. По итогам рассмотрения заявления и прилагаемых к нему документов, а также документов, полученных от иных государственных органов (при необходимости), КУЦ МЦР в срок, не превышающий 5 дней с момента окончания рассмотрения заявления, осуществляется оформление заключения о возможности/невозможности предоставления ПУЦ аккредитации.

10.8. В течение 5 календарных дней с даты оформления заключения о возможности предоставления аккредитации КУЦ МЦР принимает решение в форме приказа о предоставлении аккредитации и об изготовлении квалифицированного сертификата с использованием средств КУЦ МЦР.

10.9. КУЦ МЦР в срок, не превышающий 10 календарных дней со дня принятия решения об аккредитации, уведомляет ПУЦ о принятом решении и выдает свидетельство об аккредитации с одновременной выдачей квалифицированного сертификата, созданного с использованием средств КУЦ МЦР. (Приложение № 9) (Приложение № 9-1) (Приложение № 10) (Приложение № 11).

Срок действия свидетельства об аккредитации составляет 5 лет, если более короткий срок не был указан в заявлении ПУЦ.

10.10. КУЦ МЦР передает уполномоченному представителю ПУЦ свидетельства об аккредитации и квалифицированный сертификат ключа проверки подписи ПУЦ.

10.11. Уполномоченный представитель ПУЦ расписывается в журнале учета выдачи свидетельства об аккредитации и квалифицированного сертификата ключа проверки ПУЦ. В журнале также проставляется отметка о проведении инструктажа о правилах эксплуатации и хранения средств криптографической защиты информации и ключевых носителей.

10.12. КУЦ МЦР изготавливает на бумажном носителе два экземпляра квалифицированного сертификата ключа проверки подписи ПУЦ, которые заверяются печатью МЦР и подписью уполномоченного лица МЦР.

10.13. Каждый экземпляр квалифицированного сертификата ключа проверки подписи ПУЦ на бумажном носителе заверяется собственноручной подписью уполномоченного представителя ПУЦ. Один экземпляр вручается уполномоченному сотруднику ПУЦ, другой экземпляр квалифицированного сертификата ключа проверки подписи ПУЦ на бумажном носителе вместе с принятыми документами хранится в КУЦ МЦР.

10.14. В течение трех рабочих дней со дня вступления приказа об аккредитации КУЦ МЦР размещает на своем официальном сайте следующую информацию:

- наименование аккредитованного ПУЦ;

-адрес местонахождения, аккредитованного ПУЦ.

10.15. В течение трех рабочих дней со дня вступления в силу приказа о квалифицированном сертификате, созданного с использованием средств КУЦ МЦР, КУЦ МЦР вносит соответствующую информацию в Реестр выданных и аннулированных КУЦ МЦР квалифицированных сертификатов.

10.16. В случае изменения наименования, места нахождения, состава руководящих органов, внесения изменений в учредительные документы аккредитованного ПУЦ, либо утраты свидетельства об аккредитации, аккредитованный ПУЦ обязан уведомить об этом КУЦ МЦР и подать заявление о переоформлении свидетельства об аккредитации в течение 20 календарных дней.

10.17. Выдача нового свидетельства об аккредитации осуществляется в течение

5 календарных дней с даты предоставления в КУЦ МЦР заявления о переоформлении свидетельства об аккредитации, с приложением документов, подтверждающих сведения об изменениях, указанных в пункте 10.13. настоящего Регламента.

11. Основания для отказа в предоставлении аккредитации

11.1. Основанием для отказа в предоставлении аккредитации является наличие в представленных ПУЦ документах недостоверной информации, а также несоответствие ПУЦ требованиям, установленным в разделе 10 настоящего Регламента.

11.2. В случае принятия решения об отказе в аккредитации ПУЦ КУЦ МЦР в срок, не превышающий 10 календарных дней со дня принятия решения об отказе в аккредитации, направляет или вручает ПУЦ уведомление о принятом решении, с указанием причин отказа, в форме документа на бумажном носителе.

11.3. ПУЦ может подать новое заявление на получение аккредитации после устранения причин, послуживших основанием для отказа в аккредитации.

12. Смена ключей подписи ПУЦ

12.1. Смену ключа подписи ПУЦ обязан производить не позднее истечения срока действия квалифицированного сертификата ключа проверки подписи.

12.2. ПУЦ заблаговременно обращается с заявлением в КУЦ МЦР на изготовление нового квалифицированного сертификата ключа проверки подписи с представлением полного пакета документов согласно раздела 10 настоящего Регламента.

12.3. По итогам выполнения действий, предусмотренных в разделе 10 настоящего Регламента, КУЦ МЦР осуществляет выдачу или отказывает в выдаче обновленного квалифицированного сертификата ключа проверки подписи ПУЦ.

13. Внеплановая смена ключей подписи ПУЦ

13.1. Внеплановая смена ключа подписи и издание обновленного квалифицированного сертификата ключа проверки подписи ПУЦ до истечения срока их действия производится ПУЦ в следующих случаях:

- компрометация ключа подписи ПУЦ или компрометация ключа подписи ПУЦ;
- выход из строя носителя ключевой информации;
- утеря носителя ключевой информации;
- изменение регистрационных данных ПУЦ;
- утеря пароля (ПИН-кода) доступа к ключевому носителю.

14. Приостановление действия и отзыв сертификата ключа проверкиподписи ПУЦ при компрометации

14.1. Ключ подписи ПУЦ считается скомпрометированным в следующих случаях:

- существует подозрение на получение пароля доступа к ключу подписи посторонними лицами;
- посторонним лицам мог стать доступным носитель с ключевой информацией;
- посторонние лица могли получить неконтролируемый физический доступ или доступ по локальной сети к ключевой информации, хранящейся на терминале ПУЦ.

14.2. В случае компрометации ключа подписи ПУЦ обязан:

- не использовать скомпрометированный ключ подписи;
- уведомить о факте компрометации ключа подписи в КУЦ МЦР по телефону (аутентификация пользователя должна осуществляться по кодовому слову, зафиксированному у Администратора ЦР КУЦ МЦР при регистрации пользователя);
- оформить и предоставить в ЦР КУЦ официальное заявление на

аннулирование (отзыв) сертификата ключа проверки подписи (Приложение № 4) на бумажном носителе, заверенное печатью и подписью уполномоченного лица ПУЦ.

14.3. При уведомлении ЦР КУЦ МЦР по телефону о компрометации ключа подписи необходимо сообщить следующую информацию:

- идентификационные данные сертификата ключа проверки подписи ПУЦ;
- данные уведомителя (ФИО, телефон/факс, кодовое слово).

14.4. После получения от ПУЦ уведомления о компрометации ЦР КУЦ МЦР обязан:

- сообщить об инциденте в КУЦ МЦР и в течение одного рабочего часа после регистрации уведомления от ПУЦ отправить в КУЦ МЦР формализованный запрос на отзыв (аннулирование) сертификата ключа проверки подписи ПУЦ;
- в течение одного рабочего часа после получения от ПУЦ заявления на отзыв сертификата ключа проверки подписи на бумажном носителе сообщить об этом в КУЦ МЦР и отправить формализованный запрос на отзыв сертификата ключа проверки подписи ПУЦ;
- переслать заявление на аннулирование (отзыв) сертификата ключа проверки подписи на бумажном носителе, заверенное собственноручной подписью уполномоченного лица ПУЦ, в КУЦ МЦР с использованием почтовой связи.

14.5. КУЦ МЦР, в случае компрометации ключа подписи ПУЦ, обязан:

- в течение одного рабочего часа после получения от ЦР КУЦ МЦР формализованного запроса на приостановление действия сертификата ключа проверки подписи ПУЦ удовлетворить этот запрос;
- в течение одного рабочего часа после получения от ЦР КУЦ МЦР формализованного запроса на отзыв (аннулирование) сертификата ключа проверки подписи ПУЦ удовлетворить этот запрос;
- немедленно после отзыва (аннулирования) или приостановления действия сертификата ключа проверки подписи ПУЦ издать СОС;
- немедленно обновить СОС в точке публикации КУЦ МЦР. Официальным уведомлением ПУЦ о факте отзыва (аннулирования) или приостановления действия сертификата ключа проверки подписи ПУЦ является опубликование СОС, содержащего соответствующие сведения. Временем отзыва (аннулирования) или приостановления действия сертификата ключа проверки подписи ПУЦ признается время публикации СОС, содержащего соответствующие сведения.

15. Отзыв сертификата ключа проверки подписи ПУЦ

15.1. Сертификат ключа проверки подписи ПУЦ может быть отозван (аннулирован) по следующим причинам:

- изменение идентифицирующей информации или атрибутов в сертификате ключа проверки подписи ПУЦ до истечения срока действия сертификата;
- получение документов, подтверждающих реорганизацию или ликвидацию владельца сертификата, являющегося юридическим лицом, либо иные доказательства факта его реорганизации или ликвидации;
- установление неисполнения или ненадлежащего исполнения владельцем сертификата своих обязательств;
- по соответствующему акту уполномоченного государственного органа или суда.

15.2. ПУЦ направляет в ЦР КУЦ МЦР заявление на отзыв (аннулирование) сертификата ключа проверки подписи (Приложение № 4) в электронном виде, заверив его своей электронной подписью или на бумажном носителе, заверив его собственноручной подписью уполномоченного лица ПУЦ и печатью.

15.3 ЦР КУЦ МЦР при получении от ПУЦ заявления на отзыв (аннулирование) сертификата ключа проверки подписи в электронном виде или на бумажном носителе в течение одного рабочего часа направляет в КУЦ МЦР формализованный запрос на отзыв

(аннулирование) сертификата ключа проверки подписи ПУЦ.

15.4. КУЦ МЦР при получении от ЦР КУЦ МЦР формализованного запроса на отзыв (аннулирование) сертификата ключа проверки подписи ПУЦ или по соответствующему акту уполномоченного государственного органа или суда в течение одного рабочего часа удовлетворяет этот запрос.

15.5. КУЦ МЦР немедленно после удовлетворения формализованного запроса от ЦР КУЦ МЦР на отзыв (аннулирование) сертификата ключа проверки подписи ПУЦ издает СОС.

15.6. КУЦ МЦР немедленно обновляет СОС в точке публикации КУЦ МЦР. Официальным уведомлением ПУЦ о факте отзыва (аннулирования) сертификата ключа подписи ПУЦ является опубликование СОС, содержащего сведения об отзыве сертификата. Временем отзыва (аннулирования) сертификата ключа проверки подписи ПУЦ признается время публикации СОС, содержащего сведения об отозванном сертификате.

15.7. Заявление на отзыв (аннулирование) сертификата ключа проверки подписи набумажном носителе, заверенное собственноручной подписью уполномоченного лица ПУЦи печатью, и зарегистрированный в ЦР КУЦ направляется в КУЦ МЦР на хранение.

16. Приостановление действия сертификата ключа подписи ПУЦ

16.1. Действие сертификата ключа проверки подписи ПУЦ может быть приостановлено (за исключением случаев компрометации) на срок не более 45 дней.

16.2. Уполномоченное лицо ПУЦ направляет в ЦР КУЦ МЦР заявление на приостановление действия сертификата ключа проверки подписи (Приложение № 5) в электронном виде, заверив его своей электронной подписью или на бумажном носителе, заверив его собственноручной подписью и печатью.

16.3. КУЦ МЦР может приостановить действие сертификата ключа проверки подписи по соответствующему акту уполномоченного государственного органа или суда.

16.4. ЦР КУЦ МЦР при получении от ПУЦ заявления на приостановление действия сертификата ключа проверки подписи в течение одного рабочего часа направляет в КУЦ

16.5. МЦР формализованный запрос на приостановление действия сертификата ключа проверки подписи ПУЦ.

16.6. КУЦ МЦР по формализованному запросу ЦР КУЦ МЦР на приостановление действия сертификата ключа проверки подписи ПУЦ в течение одного рабочего часа удовлетворяет формализованный запрос на приостановление действия сертификата ключа проверки подписи ПУЦ.

16.7. КУЦ МЦР немедленно после удовлетворения формализованного запроса на приостановление действия сертификата ключа проверки подписи ПУЦ обновляет СОС в точке публикации КУЦ МЦР.

16.8. Официальным уведомлением ПУЦ о приостановлении действия сертификата ключа проверки подписи ПУЦ является опубликование СОС, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа проверки подписи ПУЦ признается время публикации СОС, содержащего сведения о сертификате, действие которого было приостановлено.

16.9. Зарегистрированное заявление на приостановление действия сертификата ключа проверки подписи на бумажном носителе, хранится в ЦР КУЦ.

17. Возобновление действия сертификата ключа проверки подписиПУЦ

17.1. Возобновление действия сертификата ключа проверки подписи ПУЦ может быть осуществлено исключительно в период приостановления действия сертификата

ключа проверки подписи.

17.2. Уполномоченное лицо ПУЦ представляет в ЦР КУЦ МЦР заявление на возобновление действия сертификата ключа проверки подписи (Приложение № 6) на бумажном носителе, заверив его собственноручной подписью и печатью.

17.3. ЦР КУЦ МЦР при получении от ПУЦ заявления на возобновление действия сертификата ключа проверки подписи в течение одного рабочего часа направляет в КУЦ МЦР формализованный запрос на возобновление действия сертификата ключа проверки подписи ПУЦ.

17.4. КУЦ МЦР после получения от ЦР КУЦ МЦР формализованного запроса на возобновление действия сертификата ключа проверки подписи ПУЦ в течение одного рабочего часа удовлетворяет запрос на возобновление действия сертификата ключа проверки подписи ПУЦ.

17.5. КУЦ МЦР в течение одного рабочего часа после возобновления действия сертификата ключа проверки подписи ПУЦ издает СОС.

17.6. КУЦ МЦР обновляет СОС в точке публикации КУЦ МЦР в течение одного рабочего дня (8 рабочих часов) с момента его издания. Официальным уведомлением ПУЦ о возобновлении действия сертификата ключа проверки подписи ПУЦ является опубликование СОС, не содержащего сведений о сертификате, действие которого было ранее приостановлено. Временем возобновления действия сертификата ключа проверки подписи ПУЦ признается время публикации СОС, не содержащего сведений о сертификате, действие которого было ранее приостановлено.

17.7. Зарегистрированное заявление на возобновление действия сертификата ключа проверки подписи на бумажном носителе, заверенное собственноручной подписью уполномоченного лица ПУЦ и печатью, хранится в КУЦ МЦР.

18. Смена ключа подписи КУЦ МЦР при компрометации

18.1. В случае компрометации ключа подписи КУЦ МЦР сертификат ключа проверки подписи КУЦ отзывается (аннулируется). Все сертификаты (включая кросс-сертификаты), подписанные с использованием скомпрометированного ключа подписи КУЦ МЦР, считаются отозванными (аннулированными).

18.2. После отзыва (аннулирования) сертификата ключа проверки подписи КУЦ МЦР выполняется процедура внеплановой смены ключа подписи КУЦ МЦР согласно разделу 10 настоящего Регламента.

18.3. Все подписанные с использованием скомпрометированного ключа подписи КУЦ МЦР и действовавшие на момент компрометации сертификаты подлежат внеплановой смене.

19. Основные требования к сертификату ключа проверки подписи

19.1. Сертификат ключа проверки подписи должен соответствовать международному стандарту ITU-T (сектор стандартизации в области телекоммуникаций Международного союза электросвязи) для инфраструктуры открытых ключей X.509 v3.

19.2. Сертификат ключа проверки подписи должен удовлетворять требованиям Закона Кыргызской Республики «Об электронной подписи».

20. Взаимодействие КУЦ МЦР и ПУЦ

20.1. ПУЦ формируют файлы запросов на издание сертификата ключа проверки подписи ПУЦ в формате PKCS#10 или регистрационное свидетельство (P7B) в формате Base64 и отправляют их в КУЦ МЦР, используя защищенный способ передачи.

20.2. КУЦ МЦР после получения запроса от ПУЦ производит проверку файла

запроса на предмет:

- отсутствие сертификатов ключа проверки подписи ранее изданных или импортированных сертификатов с таким же ключом электронной подписи;
- соответствия данных сертификата ключа проверки подписи в запросе о принадлежности ПУЦ;
- наличия данных о точке распространения СОС в запросе;
- проверки срока действия сертификата ключа проверки подписи в запросе.

20.3. При положительном результате проверки запроса КУЦ МЦР издает сертификат ключа проверки подписи ПУЦ и отправляет его в адрес ПУЦ, используя защищенный способ передачи.

20.4. ПУЦ вводит в действие (импортирует) полученный от КУЦ МЦР квалифицированный сертификат ключа проверки подписи ПУЦ.

20.5. При возникновении конфликтной ситуации между КУЦ МЦР и ПУЦ в рамках настоящего Регламента, стороны предпринимают все необходимые меры для урегулирования спорных вопросов путем переговоров.

21. Обязанности КУЦ МЦР по поддержанию актуальности СОС

21.1. Сервис публикации КУЦ МЦР формирует и публикует СОС на официальном сайте КУЦ МЦР, откуда он доступен всем пользователям иерархической структуры КУЦ МЦР и ПУЦ.

22. Архивное хранение

22.1. Архивированию подлежит следующая документированная информация:

- реестр сертификатов ключей проверки подписи КУЦ МЦР;
- сертификаты ключей проверки подписи ПУЦ;
- журналы аудита программно-аппаратных средств обеспечения деятельности КУЦ МЦР;
- реестр зарегистрированных ПУЦ;
- заявления на изготовление сертификатов ключей проверки подписи;
- заявления на отзыв (аннулирование)сертификатов ключей проверки подписи;
- заявления на приостановление действия сертификатов ключей проверки подписи;
- заявления на возобновление действия сертификатов ключей проверки подписи;
- служебные документы КУЦ МЦР.

22.2. Архивные документы хранятся с соблюдением требований режима хранения архивных документов в соответствии с архивным законодательством Кыргызской Республики.

22.3. Документы, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов устанавливается всоответствии с архивным законодательством Кыргызской Республики.

22.4. Выделение архивных документов к уничтожению и дальнейшее уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников КУЦ МЦР, подразделений МЦР, ведающих вопросами делопроизводства

Полный состав постоянно действующей комиссии определяется приказом МЦР.

Приложение № 1
к Регламенту КУЦ МЦР

Заявление о присоединении к Регламенту КУЦ МЦР

_____
(наименование организации, включая организационно-правовую форму)

в лице_____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании_____

присоединяется к Регламенту Корневого Удостоверяющего центра Министерства цифрового развития Кыргызской Республики (КУЦ МЦР), опубликованного на сайте www.ict.gov.kg
С Регламентом КУЦ МЦР и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного Регламента.

Подпись руководителя, дата, гербовая печать организации

Заявление представил уполномоченный представитель организации:

_____ _____ _____
(фамилия) (Подпись) (Дата)

_____ _____ _____
_____

заполняется уполномоченным лицом КУЦ МЦР

Данное заявление о присоединении к Регламенту КУЦ МЦР зарегистрировано в реестре КУЦ МЦР:

Регистрационный №_____от «____»_____20____г.

Оператор Центра регистрации КУЦ МЦР_____«___» _____ 202___Г,
(Ф.И.О, подпись)

Приложение № 2
к Регламенту КУЦ МЦР

Заявление
о получении аккредитации удостоверяющего центра

_____
(полное наименование юридического лица с указанием организационно-правовой формы)

в лице _____

(должность руководителя)

_____
(фамилия, имя, отчество руководителя)

действующего на основании _____

просит обработать запрос (PKCS#10) или регистрационное свидетельство ПУЦ (P7B) в формате Base64:

_____
(тело запроса или регистрационного свидетельства)

зарегистрировать Подчиненный удостоверяющий центр, путем проведения аккредитации согласно представленным документам

_____
(наименование ПУЦ)

в Реестре КУЦ МЦР в соответствии с указанными ниже идентификационными данными иобластями использования ключа:

Наименование атрибута	**Характеристика атрибута**
CommonName	Фамилия имя отчество физического лица
serialNumber	ПИН физического лица
Неструктурированное имя	ИНН юридического лица
OrganizationName	Наименование организации
countryName	KG

МП

_____
(подпись руководителя)

«___»_____20___г.

Приложение № 3
к Регламенту КУЦ МЦР

(Форма доверенности на регистрацию УЦ)

Доверенность

г. _____ «_____»_____20____г.

_____

(полное наименование юридического лица, включая организационно-правовую форму)

в лице _____

(должность руководителя организации)

_____

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____

(должность, фамилия, имя, отчество уполномоченного представителя)

_____

(серия и номер паспорта, кем и когда выдан)

в нижеследующем:

1. Предоставить в КУЦ МЦР необходимый пакет документов, в соответствии с Регламентом КУЦ МЦР для аккредитации и регистрации Подчиненного УЦ
2. Получить сертификат ключа проверки подписи Подчиненного Удостоверяющего центра КУЦ МЦР.

Представитель наделяется правом расписываться на копии сертификата ключа подписи ПУЦ на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «____»_____20_____г.

Подпись уполномоченного представителя_____подтверждаю:

(образец подписи представителя)

МП

_____

(подпись руководителя)

«___»_____20___г.

Приложение № 4
к Регламенту КУЦ МЦР

Заявление
на аннулирование (отзыв) сертификата ключа проверки подписи
Подчиненного Удостоверяющего центра

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

в лице _____

(должность руководителя)

_____
(фамилия, имя, отчество руководителя)

действующего на основании

_____

в связи с

_____
(причина отзыва сертификата)

просит аннулировать (отозвать) сертификат ключа проверки подписи Подчиненного удостоверяющего центра:

_____
(наименование юридического лица)

содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки подписи
CommonName (CN)	Общее имя (наименование юридического лица)
E-Mail (E)	Адрес электронной почты

МП

_____
(подпись руководителя)

«__»_____20___г.

Приложение № 5
к Регламенту КУЦ МЦР

Заявление
на приостановление действия сертификата ключа проверки подписи ПУЦ

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

в лице _____

(должность руководителя)

_____
(фамилия, имя, отчество руководителя)

действующего на основании _____

просит приостановить действие сертификата ключа подписи Подчиненного удостоверяющего центра:

_____
(наименование юридического лица)

содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки подписи
CommonName (CN)	Общее имя (наименование юридического лица)
E-Mail (E)	Адрес электронной почты

Срок приостановления сертификата ключа подписи ПУЦ_____дней.
(количество дней прописью)

МП

_____
(подпись руководителя)

«__»_____20___г.

Приложение № 6
к Регламенту КУЦ МЦР

Заявление
на возобновление действия сертификата ключа проверки подписи ПУЦ

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

в лице _____
(должность руководителя)

_____
(фамилия, имя, отчество руководителя)

действующего на основании _____

просит возобновить действие сертификата ключа проверки подписи ПУЦ:

_____
(наименование юридического лица)

содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки подписи
CommonName (CN)	Общее имя (наименование юридического лица)
E-Mail (E)	Адрес электронной почты
Дата и срок приостановления сертификата	

МП

_____
(подпись руководителя)

«__»_____20___г.

Приложение № 7
к Регламенту КУЦ МЦР

Заявление
на подтверждение подлинности электронной подписи уполномоченного лица КУЦ МЦР в сертификате ключа проверки подписи

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

в лице _____
(должность руководителя)

_____
(фамилия, имя, отчество руководителя)

Просит подтвердить подлинность электронной подписи уполномоченного лица КУЦ МЦР визданном КУЦ МЦР сертификате ключа проверки подписи и установить его статус (действует/не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки подписи прилагается к заявлению на магнитном носителе с регистрационным номером №_____;
2. Время и дата на момент наступления которых требуется установить статус сертификата: (указать час, минуту, день, месяц и год в следующем формате: ЧЧ/ММ/ДД/МЕСЯЦ/ГГГГ/)

Время и дата подачи заявления в КУЦ МЦР:
«_____:_____» «_____/_____/_____»
(час) (минута) (день) (месяц) (год)

МП

_____
(подпись руководителя)

Время и дата должны быть указаны с учетом часового пояса г. Бишкек. Если время и датане указаны, то статус сертификата устанавливается на момент времени подачи заявления в КУЦ МЦР.

Приложение 8
к Регламенту КУЦ МЦР

Требования к применению электронной подписи в облачных технологиях

Облачное хранилище и прилагаемые компоненты защиты должны обладать сертификатом соответствия, признанным на территории Кыргызской Республики, в котором также должно быть отмечено о допустимости использования указанных средств к обработке персональных данных при построении защиты информационных систем. Также, средство защиты данных должно быть поставлено в программно-аппаратном исполнении, при этом программная часть комплекса, включая средства администрирования, список пользователей и журнал регистрации должны быть размещены в энергозависимой памяти контроллера.

Идентификация/аутентификация пользователей, контроль целостности аппаратной части персональной электронно-вычислительной машины и программной среды должны выполняться контроллером комплекса вне зависимости от типа операционной среды и файловой системы до загрузки операционной системы.

Облачное хранилище должно обеспечивать:

1. Формирование закрытого ключа должно осуществляться, не покидая устройства, на котором оно должно храниться.
2. Формирование подписи должно осуществляться аппаратными криптографическими платформами, имеющими сертификаты соответствия, признанные на территории Кыргызской Республики.
3. Для защиты закрытого ключа, должен быть сформирован криптографический ключ, хранящийся на отчуждаемом аппаратном носителе, имеющим сертификацию и закреплённый за полномочным лицом.
4. Методы и алгоритмы подписи, шифрования должны соответствовать принятым на территории Кыргызской Республики криптографическим стандартам.
5. Формирование подписи должно происходить, не покидая устройства гдехранится закрытый ключ, и доступ к ключевой информации должен быть консолидированным с пользователем (владельцем электронной подписи).
6. Ввод пин-кода должен формироваться в окне, не имеющем функции сохранения или перехвата (кейлогера).
7. Обязательным должно быть информирование абонента посредством электронной подписи о применении его подписи или неудачной попытки ее применения. Персональная статистика об использовании электронной подписи должна содержать время, дату.
8. Должны быть сформированы регламентные документы, которые должны разграничивать доступ к устройствам, регламентные работы, компрометации и смены ключевой информации администратора.

Приложение 9
к Регламенту КУЦ МЦР

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

СЕРТИФИКАТ

Кому выдан: Корневой удостоверяющий центр

Кем выдан: Корневой удостоверяющий центр

Действителен с 14 сентября 2021 14:18:04 (GTM +06:00) по 12 сентября 2031 14:18:04 (GTM +06:00)

Назначение ключа	Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Версия	ITU-T X.509 V.3
Серийный номер	f3c417820b1cedb0927bf98472ebb886089d8c771fd0596f4d96f191f91efb21
Алгоритм подписи	ГОСТ 34.310-2004
Издатель	Имя: Корневой удостоверяющий центр Организация: Министерство цифрового развития Кыргызской Республики Город: Бишкек Электронная почта: pki@digital.gov.kg Страна: KG
Действителен с	14 сентября 2021 14:18:04 (GTM +06:00)
Действителен по	12 сентября 2031 14:18:04 (GTM +06:00)
Владелец	Имя: Корневой удостоверяющий центр Организация: Министерство цифрового развития Кыргызской Республики Город: Бишкек Электронная почта: pki@digital.gov.kg Страна: KG
Открытый ключ	длина ключа: 512 Бит значение: 060200003aaa000000454331000200001bfdb8cfb3af5ebaaf956 84303e6110218b64d1ea6c92e5228824076244c1643e7596cdb93ebb07a87 57ab8b1fba682e1d5d40 94d353b90856f0dbd2a72ae85b
Расширение сертификата X.509	
Использование ключа	Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Идентификатор ключа	Идентификатор ключа=f3 c4 17 82 0b 1c ed b0 92 7b f9 84 72 eb b8 86 08 9d 8c 77 1f d0 59 6f 4d 96 f1 91 f9 1e fb 21 Поставщик сертификата: Адрес каталога: C=KG L=Бишкек O=Министерство цифрового развития Кыргызской Республики CN=Корневой удостоверяющий центр E=pki@digital.gov.kg Серийный номер сертификата=f3 c4 17 82 0b 1c ed b0 92 7b f9 84 72 eb b8 86 08 9d 8c 77 1f d0 59 6f 4d 96 f1 91 f9 1e fb 21
Основные ограничения	Тип субъекта=ЦС Ограничение на длину пути=0

Результат проверки сертификата: Сертификат действителен.
Проверен 14 сентября 2021 14:18:04 (GTM +06:00)

Руководитель КУЦ **Кененбаева А.А.**

М.П. **«14» сентября 2021г.**

СӨМ ТКБнын Регламентине
9-1-тиркеме

КЫРГЫЗ РЕСПУБЛИКАСЫНЫН САНАРИПТИК
ӨНҮКТҮРҮҮ МИНИСТРЛИГИ

СЕРТИФИКАТ

Кимге берилген: Түпкү күбөлөндүрүүчү борбор
Ким чыгарган: Түпкү күбөлөндүрүүчү борбор
2022-жылдын 3-ноябрынан 15:05:20 (GTM +06:00) 2032-жылдын 3-ноябрына чейин 15:05:20 (GTM +06:00) жаракту

Ачкычтын багыты	Сертификаттарга кол коюу, чакырып алуу тизмесине (CRL) автономдуу кол коюу, чакырып алуу тизмесине кол коюу (CRL)
Версиясы	ITU-T X.509 V.3
Сериялык номери	f3 13 81 01 a7 7d 0a 42 6a 33 18 9a 2b 92 c3 c1 af 2b ef 6d
Кол коюу алгоритми	ГОСТ Р 34.10-2012
Чыгаруучу	Аталышы: Түпкү күбөлөндүрүүчү борбор Уюм: Кыргыз Республикасынын Санариптик өнүктүрүү министрлиги Бишкек шаары Электрондук почтасы: pki@digital.gov.kg Өлкөсү: KG
Жаракту	2022-жылдын 3-ноябрынан 15:05:20 (GTM +06:00) 2032-жылдын 3-ноябрына чейин 15:05:20 (GTM +06:00)
Ээси	Аталышы: Түпкү күбөлөндүрүүчү борбор Уюм: Кыргыз Республикасынын Санариптик өнүктүрүү министрлиги Бишкек шаары Электрондук почтасы: pki@digital.gov.kg Өлкөсү: KG
Ачык ачкыч	ачкычтын узундугу: 1024 Бит белгиси: 04818089db439463cebbd0a219a 843caccf8b4ff83fdfbd8c6f7d8b153b344f1ce1e184ddbd04b76788cf9dc68a 292a84e5fc76bc6b2996e57539a07c94fd187f2c7f1387a65ef5edee3c7028c 52c2f175bd582772f122b48336c78a1a1e3fe0690bed4a5974091130826 03ec681bc5f57861554e7c1fd5e899db97e738664fd809e89

Сертификатты кеңейтүү X.509

Ачкычты колдонуу	Сертификаттарга кол коюу, чакырып алуу тизмесине (CRL) автономдуу кол коюу, чакырып алуу тизмесине кол коюу (CRL)
Ачкыч идентификатору	Ачкыч идентификатору=f3 c4 17 82 0b 1c ed b0 92 7b f9 84 72 eb b8 86 08 9d 8c 77 1f d0 59 6f 4d 96 f1 91 f9 1e fb 21 Сертификат берүүчү: Каталогдун дареги: C=KG L=Бишкек O= Кыргыз Республикасынын Санариптик өнүктүрүү министрлиги CN= Түпкү күбөлөндүрүүчү борбор E=pki@digital.gov.kg Сертификаттын сериялык номери= f3 13 81 01 a7 7d 0a 42 6a 33 18 9a 2b 92 c3 c1 af 2b ef 6d
Негизги чектөөлөр	Субъектинтин тиби=CT Жолдун узундугуна чектөө =0

Сертификатты текшерүүнүн жыйынтыгы: Сертификат жаракту.
Текшерилген күнү: 2022-жылдын 3-ноябры, 17: 52:05 (GTM +06: 00)

ТКБнын жетекчиси **Шаршенова И.Ж.**

М.О. **2022-жылдын 4-октябры.**

Приложение 9-1
к Регламенту КУЦ МЦР

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

СЕРТИФИКАТ

Кому выдан: Корневой удостоверяющий центр

Кем выдан: Корневой удостоверяющий центр

Действителен с 3 ноября 2022 г. 15:05:20 (GTM +06:00) по 3 ноября 2032 г. 15:05:20 (GTM +06:00)

Назначение ключа	Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Версия	ITU-T X.509 V.3
Серийный номер	f3 13 81 01 a7 7d 0a 42 6a 33 18 9a 2b 92 c3 c1 af 2b ef 6d
Алгоритм подписи	ГОСТ Р 34.10-2012
Издатель	Имя: Корневой удостоверяющий центр Организация: Министерство цифрового развития Кыргызской Республики Город: Бишкек Электронная почта: pki@digital.gov.kg Страна: KG
Действителен с	3 ноября 2022 г. 15:05:20 (GTM +06:00)
Действителен по	3 ноября 2032 г. 15:05:20 (GTM +06:00)
Владелец	Имя: Корневой удостоверяющий центр Организация: Министерство цифрового развития Кыргызской Республики Город: Бишкек Электронная почта: pki@digital.gov.kg Страна: KG
Открытый ключ	длина ключа: 1024 Бит значение: 04818089db439463cebbd0a219a 843caccf8b4ff83fdfbd8c6f7d8b153b344f1ce1e184ddbd04b76788cf9dc68a 292a84e5fc76bc6b2996e57539a07c94fd187f2c7f1387a65ef5edee3c7028c 52c2f175bd582772f122b48336c78a1a1e3fe0690bed4a5974091130826 03ec681bc5f57861554e7c1fd5e899db97e738664fd809e89

Расширение сертификата X.509

Использование ключа	Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Идентификатор ключа	Идентификатор ключа=f3 c4 17 82 0b 1c ed b0 92 7b f9 84 72 eb b8 86 08 9d 8c 77 1f d0 59 6f 4d 96 f1 91 f9 1e fb 21 Поставщик сертификата: Адрес каталога: C=KG L=Бишкек O=Министерство цифрового развития Кыргызской Республики CN=Корневой удостоверяющий центр E=pki@digital.gov.kg Серийный номер сертификата= f3 13 81 01 a7 7d 0a 42 6a 33 18 9a 2b 92 c3 c1 af 2b ef 6d
Основные ограничения	Тип субъекта=ЦС Ограничение на длину пути=0

Результат проверки сертификата: Сертификат действителен.

Проверен 3 ноября 2022 года 17:52:05 (GTM +06:00)

Руководитель КУЦ **Шаршенова И.Ж.**

М.П. **«04» октября 2022г.**

Приложение 10
к Регламенту КУЦ МЦР

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

СЕРТИФИКАТ

Кому выдан: Корневой удостоверяющий центр
Кем выдан: Корневой удостоверяющий центр
Действителен с 14 сентября 2021 14:25:45 (GTM +06:00) по 12 сентября 2031 14:25:45 (GTM +06:00)

Назначение ключа	Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Версия	ITU-T X.509 V.3
Серийный номер	736dc81e87867bdd9c21b8d3d8c3b558df6706f0
Алгоритм подписи	sha256RSA
Издатель	Имя: Корневой удостоверяющий центр Организация: Министерство цифрового развития Кыргызской Республики Город: Бишкек Электронная почта: pki@digital.gov.kg Страна: KG
Действителен с	14 сентября 2021 14:25:45 (GTM +06:00)
Действителен по	12 сентября 2031 14:25:45 (GTM +06:00)
Владелец	Имя: Корневой удостоверяющий центр Организация: Министерство цифрового развития Кыргызской Республики Город: Бишкек Электронная почта: pki@digital.gov.kg Страна: KG
Открытый ключ	длина ключа: RSA 2048 Бит значение: 3082010a0282010100d0c1dc9f254217c5ea24b261f49884606b584235 e73d2cb46654e792101b5f8873e98ecc69b8d8a86de08064f0a25bdc36e3b21113c6 3d778141429214ceaf04d82dc91784dcd0330aff1414e555f9fd63ef5efe9a363a525834e7 371ee2d3924cab542beda585a89c64dd64c35db68e3318bce043357d5de5c951 bfdab6d239f1d253ea5ad81e01c694e1f31a0f39fcfeda3bf715aa93a70aba4a61596 84f4df5d5fca82d8e5ddc88257bb8adc5eead671fd948fae3ce267574f5b1937d6f6856 be49a5a099fa8eb8c6346025862ec6ca86332943660bb1e4ee0aff9fe3f03ff7c66269eae 2c99aa8c7346d5fb8aa57e94b964a5a38fe0d30710340824a3b7f02 03010001

Расширение сертификата X.509

Использование ключа	Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Идентификатор ключа	Идентификатор ключа=f3 6d c8 1e 87 86 7b dd 9c 21 b8 d3 d8 c3 b5 58 df 67 06 f0 Поставщик сертификата: Адрес каталога: C=KG L=Бишкек O=Министерство цифрового развития Кыргызской Республики CN=Корневой удостоверяющий центр E=pki@digital.gov.kg Серийный номер сертификата=73 6d c8 1e 87 86 7b dd 9c 21 b8d3 d8c3b558df6706f0
Основные ограничения	Тип субъекта=ЦС Ограничение на длину пути=0

Результат проверки сертификата: Сертификат действителен.
Проверен 14 сентября 2021 14:18:04 (GTM +06:00)

Руководитель КУЦ Кененбаева А.А.

«14» сентября 2021г.

СӨМ ТКБнын Регламентине
11-тиркеме

Кыргыз Республикасынын
Санариптик өнүктүрүү министрлиги

Күбөлөндүрүүчү борборду аккредитациялоо жөнүндө
КҮБӨЛҮК

Каттоо № __ **20__-ж. «__» _____**

Бул күбөлүк менен
баш ийген күбөлөндүрүүчү борбордун

_____

_____
(юридикалык жактын толук аталышы, ИСН, КН)

ИСН _____

КН _____

_____
(юридикалык жактын дареги, жайгашкан жери)

Кыргыз Республикасынын 2017-жылдын 19-июлундагы № 128 «Электрондук кол тамга жөнүндө» Мыйзамынын талаптарына шайкештиги тастыкталат

Кыргыз Республикасынын Санариптик өнүктүрүү министрлигинин 2021-жылдын 25-августундагы № 100-б буйругунун негизинде аккредитация 20__-ж. «___» «_____» чейинки мөөнөткө берилет.

Министр **Т.О. Иманов**

Приложение 11
к Регламенту КУЦ МЦР

Министерство цифрового развития
Кыргызской Республики

СВИДЕТЕЛЬСТВО
об аккредитации удостоверяющего центра

Регистрационный № __ **«__» _____ 20__ г.**

Настоящим Свидетельством подтверждается соответствие подчиненного удостоверяющего центра

_____

_____
(полное наименование юридического лица, ИНН, РН)

ИНН _____

РН _____

_____
(адрес, место нахождения юридического лица)

требованиям Закона Кыргызской Республики
«Об электронной подписи»
от 19 июля 2017 года № 128

Аккредитация предоставлена на срок до «__» _____20__ года включительно на основании приказа Министерства цифрового развития Кыргызской Республики от 25 августа 2021 года № 100-пр.

Министр **Т.О. Иманов**