Регламент выпуска квалифицированных сертификатов ключей проверки электронной подписи для взаимодействия с государственной информационной системой «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»

СОГЛАСОВАНО
Письмом Минцифры России от
11.03.2024 №ОК-П24-21333

РАЗРАБОТАНО
ПАО «Ростелеком»

Москва 2024 г.

1. Настоящий Регламент устанавливает порядок выпуска квалифицированных сертификатов ключей проверки электронной подписи и их аннулирования для государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций финансового рынка, нотариусов и иных организаций на технических средствах информационной системы головного удостоверяющего центра для взаимодействия с государственной информационной системой «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (далее – Регламент) при осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных.

2. Настоящий Регламент разработан на основании приказа Минкомсвязи России от 13 апреля 2012 года № 108 «Об обеспечении осуществления Министерством связи и массовых коммуникаций Российской Федерации функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров» и с учетом требований следующих нормативно-правовых актов:
   - Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;
   - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
   - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
   - Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее – Закон № 572);
   - Приказ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» (далее – Приказ ФСБ России №795);
   - Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием

средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12 мая 2023 года № 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц».
- Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 05.05.2023 № 445 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в единой биометрической системе, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных».
- Указание Банка России от 25.09.2023 № 6540-У «О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой».

3. В настоящем Регламенте используются следующие термины и определения:
   - Единая биометрическая система (далее – ЕБС) – государственная информационная система «Единая система идентификации и аутентификации

физических лиц с использованием биометрических персональных данных», которая содержит биометрические персональные данные физических лиц, векторы единой биометрической системы и иную информацию, которая используется в целях осуществления идентификации, аутентификации с использованием биометрических персональных данных физических лиц, а также в иных правоотношениях в случаях, установленных законодательством Российской Федерации.

- Единая система идентификации и аутентификации (далее – ЕСИА) - федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
- Федеральная государственная информационная система «Федеральный ситуационный центр электронного правительства» (далее – СЦ) – федеральная государственная информационная система, предназначенная для повышения качества взаимодействия информационных систем, входящих в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, и информационных систем, использующих инфраструктуру взаимодействия, а также для обеспечения управления качеством обслуживания пользователей инфраструктуры взаимодействия, непрерывностью и доступностью услуг и сервисов инфраструктуры взаимодействия, формирования отчетности о ее работе, управления информационной безопасностью и управления инцидентами в работе инфраструктуры взаимодействия (в соответствии с постановлением Правительства Российской Федерации от 14 июля 2017 г. №839).
- Уполномоченный федеральный орган в сфере использования электронной подписи и осуществляющий функции головного удостоверяющего центра (далее – УФО) – Минцифры России (в соответствии с Постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 976).
- Уполномоченный федеральный орган осуществляющий выпуск квалифицированных сертификатов ключей проверки электронной подписи юридических лиц с указанием в качестве владельца квалифицированного

сертификата лица уполномоченного действовать без доверенности – Удостоверяющий центр Федеральной налоговой службы (в соответствии с Федеральным законом Российской Федерации от 6 апреля 2011 г. № 63-ФЗ).

– Уполномоченный федеральный орган осуществляющий выпуск квалифицированных сертификатов ключей проверки электронной подписи кредитных организаций, субъектов национальной платежной системы, указанных в Федеральном законе от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (за исключением организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, иностранных поставщиков платежных услуг), некредитных финансовых организаций и индивидуальных предпринимателей, осуществляющих указанные в части первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» виды деятельности, лиц, оказывающих профессиональные услуги на финансовом рынке, указанных в статье 76.9-5 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», саморегулируемых организаций в сфере финансового рынка, саморегулируемых организаций в сфере оказания профессиональных услуг на финансовом рынке – Удостоверяющий центр Центрального банка Российской Федерации (в соответствии с Федеральным законом Российской Федерации от 6 апреля 2011 г. № 63-ФЗ).

– Уполномоченный федеральный орган осуществляющий выпуск квалифицированных сертификатов ключей проверки электронной подписи лица, замещающего государственную должность Российской Федерации, государственную должность субъекта Российской Федерации, должностного лица государственного органа, органа местного самоуправления, должностного лица подведомственной государственному органу или органу местного самоуправления организации – Удостоверяющий центр федерального органа исполнительной власти, уполномоченного на правоприменительные функции по обеспечению исполнения федерального бюджета, казначейскому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации (в соответствии с Федеральным законом Российской Федерации от 6 апреля 2011 г. № 63-ФЗ).

– Оператор ЕБС – организация, осуществляющая функции оператора ЕБС. В соответствии с постановлением Правительства Российской Федерации от 16 декабря 2022 года № 2326 такие обязанности возложены на АО «Центр Биометрических технологий».

– Получатель квалифицированных сертификатов ключей проверки электронной подписи (далее – получатель сертификата) – государственные органы, органы местного самоуправления, Центральный банк Российской Федерации, организации финансового рынка, нотариусы и иные организации в целях размещения биометрических персональных данных в ЕБС, в случаях определенных федеральными законами и для осуществления идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных с использованием ЕБС.

4. Процесс получения квалифицированного сертификата для взаимодействия с ЕБС осуществляется через портал СЦ. Формирование заявки на сертификат производится в личном кабинете СЦ. Порядок доступа представителя получателя сертификата в личный кабинет СЦ приведен в «Инструкции по обеспечению доступа в личный кабинет СЦ» по ссылке:

   https://sc.digital.gov.ru/documents/-/document_library/03jzkn2sfJTq/view_file/38510.

5. Требования, предъявляемые к информационной системе Получателя квалифицированного сертификата ключа проверки электронной подписи (далее – ИС Получателя, сертификат) для возможности выпуска сертификата:

   5.1. ИС Получателя должна быть подключена к тестовым средам ЕСИА и ЕБС.

   5.2. Получатель сертификата должен иметь акцептованную оферту на сайте https://ebs.ru/.

   5.3. Получатель сертификата должен иметь сертифицированные по требованиям безопасности информации средства криптографической защиты информации для взаимодействия с ЕБС (далее – СКЗИ)

6. Порядок выпуска[1] сертификата состоит из следующих этапов:

   6.1. Получатель сертификата на своих средствах электронной подписи формирует файл запроса на сертификат с учетом требований Приказа ФСБ России № 795 в

[1] Порядок первичного выпуска сертификата и последующего выпуска сертификата идентичны

формате PKCS#10 (рекомендации по формированию запроса приведены в Приложении 1 Регламента).

Идентификация получателя сертификата проводится без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата. Таким образом, файл запроса на сертификат подписывается отсоединенной квалифицированной электронной подписью лица, действующего от имени получателя сертификата в порядке, определенном Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее - Представитель получателя сертификата).

6.2. Представитель получателя сертификата на портале СЦ (https://sc.digital.gov.ru) после авторизации в личном кабинете формирует заявку на выпуск сертификата в следующем порядке:

- в разделе «Запросы» выбрать опцию «Добавить запрос»,
- в окне «Создание запроса» в поле «Услуга» выбрать «Поддержка ИС ИЭП»,
- в окне «Создание запроса» в поле «Тип запроса» выбрать «Регламентная процедура»,
- в окне «Создание запроса» в поле «Система ИЭП» выбрать соответствующую федеральную государственную информационную систему удостоверяющего центра,
- в окне «Создание запроса» в поле «Тип регламентной процедуры» выбрать «Выпуск и регистрация сертификата для ЕБС»,
- в наименовании «Тема» указать тему запроса «Выпуск сертификата для ЕБС»,
- получатель сертификата в описании запроса в свободной форме указывает причину обращения, мнемонику ИС в ЕСИА, наименование используемого СКЗИ, прикладывает файл запроса с отсоединенной электронной подписью, сформированные ранее (п.6.1 настоящего Регламента), а также подтверждение использования для взаимодействия с ЕБС сертифицированного по требованиям безопасности информации СКЗИ и отправляется на рассмотрение в СЦ (кнопка «Создать»).

При формировании заявки на выпуск сертификата для каждого сертификата должна создаваться отдельная заявка в СЦ. Выбор приоритета при формировании

заявки на выпуск сертификата ЕБС, согласно приоритезации услуги УФО, устанавливается в «3 приоритет».

В качестве подтверждения использования для взаимодействия с ЕБС сертифицированного по требованиям безопасности информации СКЗИ к запросу прикладывается копия документа, подтверждающего права владения или пользования СКЗИ получателем сертификата (договор, акт или иное).

При указании причины обращения указывается цель взаимодействия с ЕБС (идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных; размещение биометрических персональных данных в ЕБС)

6.3. Сотрудник УФО в течение 3 рабочих дней подтверждает поступившую заявку получателя сертификата в СЦ на соответствие требованиям, описанных в пункте 5 и пункте 6 данного Регламента соответственно.

В случае наличия замечаний по заявке представитель УФО через СЦ направляет соответствующее уведомление представителю получателя сертификата о необходимости их устранения. Согласование заявки приостанавливается представителем УФО до устранения замечаний получателем сертификата. При отсутствии устранения замечаний по заявке от получателя сертификата по истечении 10 рабочий дней с момента направления замечаний, заявка автоматически переводится в статус «закрыта».

Подтвержденная УФО заявка на выпуск сертификата в СЦ переводится на эксплуатирующую организацию для ее обработки.

6.4. Эксплуатирующая организация в течение 7 рабочих дней после поступления в СЦ подтвержденной УФО заявки на выпуск сертификата производит ее обработку и выпускает квалифицированный сертификата ключа проверки электронной подписи. Срок действия сертификата составляет 3 года.

При обработке заявки эксплуатирующая организация производит проверку запроса на выпуск сертификата на соответствие Федеральному закону от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» и приказу ФСБ России № 795. В случае наличия замечаний в запросе на выпуск сертификата эксплуатирующая организация через СЦ направляет соответствующее уведомление представителю получателя сертификата о необходимости их устранения. Обработка запроса на сертификат по заявке приостанавливается представителем эксплуатирующей организации до устранения замечаний

получателем сертификата. При отсутствии от получателя сертификата устранения замечаний по истечении 10 рабочий дней с момента направления замечаний, заявка автоматически переводится в статус «закрыта».

Выпущенный эксплуатирующей организацией квалифицированный сертификат прикладывается к заявке, статус которой в СЦ переводится эксплуатирующей организацией в «Решено».

7. Аннулирование ранее выданного получателю сертификата происходит при наступлении одного из следующих событий:
   - прекращение деятельности организации-получателя сертификата, изменение ее реквизитов, указанных в сертификате;
   - нарушение конфиденциальности ключа электронной подписи.

7.1. Процедура аннулирования сертификата состоит из следующих этапов:

7.1.1. Организация, ранее получившая сертификат в соответствии с настоящим Регламентом заполняет заявление на аннулирование своего сертификата (приведено в Приложении 2 Регламента), подписывает заявление отсоединенной квалифицированной электронной подписью лица, действующего от имени организации в порядке, определенном Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

7.1.2. Организация, аннулирующая свой сертификат, на портале СЦ (https://sc.digital.gov.ru) после авторизации в личном кабинете формирует заявку на аннулирование сертификата в следующем порядке:

- в разделе «Запросы» выбрать опцию «Добавить запрос»,
- в окне «Создание запроса» в поле «Услуга» выбрать «Поддержка ИС ИЭП»,
- в окне «Создание запроса» в поле «Тип запроса» выбрать «Регламентная процедура»,
- в окне «Создание запроса» в поле «Система ИЭП» выбрать соответствующую федеральную государственную информационную систему удостоверяющего центра,
- в окне «Создание запроса» в поле «Тип регламентной процедуры» выбрать «Аннулирование сертификата для ЕБС»,
- в наименовании «Тема» указать тему запроса «Аннулирование сертификата для ЕБС»,

– в описании запроса в свободной форме указывается причина обращения, прикладывается файл заявления с отсоединенной электронной подписью, сформированные ранее (п.7.1.1 настоящего Регламента) и отправляется на рассмотрение в СЦ (кнопка «Создать»).

7.1.3. Эксплуатирующая организация идентифицирует представителя организации, аннулирующего сертификат, без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата путем проверки электронной подписи подписанного заявления на аннулирование сертификата и осуществляет аннулирование указанного в заявлении сертификата путем его внесения в список отозванных сертификатов. Ссылка на список отозванных сертификатов публикуется на портале УФО (http://e-trust.gosuslugi.ru/MainCA). Статус заявки на аннулирование сертификата переводится представителем УФО в «Решено».

В случае если организация, направившая заявку на аннулирование сертификата для ЕБС, не проходит идентификацию, представитель эксплуатирующей организации не согласует заявку и переводит ее в статус «закрыта».

8. Оператор ЕБС для получения квалифицированного сертификата ключей проверки электронной подписи подает заявку в СЦ в соответствии с порядком выпуска сертификата (п. 6 настоящего Регламента) при условии исполнения требования по наличию СКЗИ сертифицированных по требованиям безопасности информации (п. 5.3 настоящего Регламента).

Приложение 1

Рекомендации по формированию запроса

Каждый запрос на квалифицированный сертификат ключа проверки электронной подписи должен содержать информацию о субъекте, информацию об открытом ключе, атрибуты, расширения сертификата и информацию о подписи запроса.

Поле «Субъект» должно содержать следующие идентификаторы:

- ИНН ЮЛ – вносится ИНН организации, строка длиной 10 символов типа «Numeric string»;
- ОГРН – вносится ОГРН организации, строка длиной 13 символов типа «Numeric string»;
- O – полное или сокращенное наименование организации;
- STREET – часть адреса места нахождения организации, включающая наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется);
- L – наименование населенного пункта по адресу регистрации организации;
- S – двухсимвольный код и наименование субъекта РФ по адресу регистрации организации;
- C – двухсимвольный код страны согласно ГОСТ 7.67-2003 (ИСО 3166-1:1997);
- CN – полное или сокращенное наименование организации.

Пример:

ИНН ЮЛ=1234567890
ОГРН=1234567890123
O=ПАО «Ростелеком»
STREET=Проспект Вернадского, д.41
L=г. Москва
S=77 Москва
C=RU
CN=ПАО «Ростелеком»

Дополнительные атрибуты и расширения должны включать:

- Параметры улучшенного ключа, вносятся следующие идентификаторы:
  - Проверка подлинности клиента (1.3.6.1.5.5.7.3.2);
  - Защищенная электронная почта (1.3.6.1.5.5.7.3.4).
- Параметры использования ключа, вносятся следующие идентификаторы:
  - Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных.
- Информацию о средствах электронной подписи владельца, вносится наименование средства электронной подписи владельца;
- Информация о сроке действия ключа подписи (2.5.29.16)[2];
- Информацию о политиках сертификата, вносятся следующие идентификаторы:

[2] Обязательный параметр с 01.09.2024 в соответствии с требованиями, предусмотренные приказом ФСБ России от 27.12.2011 №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» (в редакции Приказа ФСБ России от 02.02.2024 №50)

- 1.2.643.100.113.1 - класс средства ЭП КС 1,
- 1.2.643.100.113.2 - класс средства ЭП КС 2,
- 1.2.643.100.113.3 - класс средства ЭП КС 3,
- 1.2.643.100.113.4 - класс средства ЭП КВ 1,
- 1.2.643.100.113.5 - класс средства ЭП КВ 2.

Пример (часть запроса на сертификат с необходимыми идентификаторами):

Атрибут[0]: 1.3.6.1.4.1.311.2.1.14 (Расширения сертификатов)
Значение[0][0]:
Неизвестный тип атрибута
Расширения сертификатов: 4
2.5.29.37: Флаги = 0, Длина = 16
Улучшенный ключ
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

2.5.29.15: Флаги = 0, Длина = 4
Использование ключа
Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

1.2.643.100.111: Флаги = 0, Длина = 29
Средство электронной подписи владельца
Средство электронной подписи: ПАКМ "СКЗИ HSM"
2.5.29.32: Флаги = 0, Длина = 34
Политики сертификата
[1]Политика сертификата:
Идентификатор политики=Класс средства ЭП КС1
[2]Политика сертификата:
Идентификатор политики=Класс средства ЭП КС2
[3]Политика сертификата:
Идентификатор политики=Класс средства ЭП КС3
[4]Политика сертификата:
Идентификатор политики=Класс средства ЭП КВ1
[5]Политика сертификата:
Идентификатор политики=Класс средства ЭП КВ2

Используемый алгоритм электронной подписи:

- ГОСТ Р 34.10-2012 256 бит.

Приложение 2

Форма заявления на аннулирование квалифицированного сертификата ключа проверки электронной подписи

Заявление на аннулирование квалифицированного сертификата ключа проверки электронной подписи

_____

наименование организации, включая организационно-правовую форму

ИНН _____ ОГРН _____

просит аннулировать квалифицированный сертификат ключа проверки электронной подписи в связи с _____, содержащий следующие данные:

причина аннулирования

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Наименование организации
INNLE	ИНН организации
OGRN	ОГРН организации

_____

Должность руководителя организации или уполномоченного лица

_____ _____ /

Наименование организации Подпись ФИО

«____» _____ 20___ г.