Временный порядок выпуска сертификатов ключей проверки электронной подписи кредитным организациям для использования в Единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации

«СОГЛАСОВАНО»
Министерство цифрового развития,
связи и массовых коммуникаций
Российской Федерации

А.А. Гатчинов

«___» _____ 2018 г.

РАЗРАБОТАНО
ФГБУ НИИ «Восход»
Руководитель НИД4

_____ А.А. Пьянченко

«___» _____ 2018 г.

Москва 2018 г.

Доп. инв. №
Подпись и дата
Инв. № подл.

1 Назначение документа

В настоящем документе приведен временный порядок выпуска сертификатов ключей проверки электронной подписи (далее – Порядок), предназначенный для кредитных организаций при работе в Единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее – ЕБС).

2 Нормативная документация

Настоящий Порядок разработан на основании и с учетом требований следующих документов:

- 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»;
- Приказ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
- 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 25 июня 2018 года № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенных для обработки биометрических персональных данных в целях проведения идентификации».

3 Участники информационного взаимодействия

Участниками информационного взаимодействия являются:

- УФО – уполномоченный федеральный орган в сфере использования электронной подписи и осуществляющий функции головного удостоверяющего центра, которым определено Минкомсвязь России в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 976.
- ЭО – организация, эксплуатирующая ПАК «Головной удостоверяющий центр» в соответствии с государственным заданием и другими указаниями УФО, ФГБУ НИИ «Восход»;
- Кредитная организация – получатель сертификатов ключей проверки электронной подписи.

4 Выпуск сертификатов ключей проверки электронной подписи

Процедура выпуска сертификата ключа проверки электронной подписи (далее – сертификат) состоит из следующих шагов:

1. Кредитная организация формирует комплект документов на выпуск сертификата (заявку):
   - Подписанное и заверенное печатью кредитной организации заявление на создание сертификата (форма заявления представлена в приложении 1 к настоящему Порядку);
   - Заверенная доверенность на физическое лицо, которое будет выступать от имени Кредитной организации (форма доверенности представлена в приложении 2 к настоящему Порядку);
   - Копия паспорта физического лица, заверенная Кредитной организацией.
   - Выписка из Единого государственного реестра юридических лиц, полученную не ранее чем за один месяц до момента направления заявки на выпуск сертификата[1].
2. Кредитная организация направляет заявку в Минкомсвязь России по адресу: 125375, г. Москва, ул. Тверская, д. 7.
3. Минкомсвязь России в десятидневный срок с момента получения и регистрации заявки рассматривает заявку, принимает решение о выпуске сертификата и направляет ответ в Кредитную организацию. В случае принятия

[1] Предоставляется по желанию Кредитной организации

положительного решения по выпуску сертификата копия решения направляется в ЭО.

4. При положительном решении о выпуске сертификата Кредитная организация:

   а) Осуществляет доступ уполномоченного лица, данные которого будут внесены в сертификат, на портал Федерального ситуационного центра электронного правительства (далее – СЦ) в соответствии с Инструкцией по обеспечению доступа в личный кабинет СЦ (опубликована по адресу https://sc.minsvyaz.ru).

   б) Формирует файл запроса на сертификат[2] с учетом требований Приказа ФСБ России №795 от 27.12.2011 в формате pkcs#10 (форма запроса приведена в Приложении 3 Порядка). В случае повторного направления запроса на сертификат такой запрос дополнительно подписывается на ранее выданном на средствах ГУЦ сертификате с не истекшим сроком действия. Сформированные файлы архивируются в zip-архив.

   в) Уполномоченное лицо идентифицируется через Единую систему идентификации и аутентификации (ЕСИА) как представитель зарегистрированной в ЕСИА Кредитной организации для работы в личном кабинете СЦ по адресу: https://sc.minsvyaz.ru/.

   г) Формирует заявку в СЦ на выпуск сертификата в следующем порядке:
      - выбрать кнопку «Добавить запрос»,
      - в разделе «Соглашение/Услуга» выбрать «Поддержка ГУЦ»,
      - в категории запроса указать «Выпуск и регистрация сертификата ЕБС»,
      - в наименовании «Тема» указать тему запроса «Выпуск сертификата для ЕБС»,
      - в описании заявки в свободной форме указывается ее суть, прикладывается сформированный zip-архив и отправляется на рассмотрение в СЦ (кнопка «Сохранить»).

5. ЭО в десятидневный срок обрабатывает запрос на выпуск сертификата и при отсутствии замечаний осуществляет выпуск сертификата. При этом:

---

[2] Файл запроса формируется с использованием средств электронной подписи Кредитной организации класса КВ2

5.1 В случае первичного выпуска сертификата подтверждение указанных в сертификате данных осуществляется путем подписания кредитной организации (ее представителя) сертификата открытого ключа на бумажном носителе по адресу г.Москва, ул. Удальцова, д.85. После подтверждения данных производится выпуск сертификата и его размещение в личном кабинете СЦ Кредитной организации, о чем она оповещается при выполнении заявки по электронной почте. Срок действия сертификата составляет 3 года. После этого заявка на выпуск сертификата считается исполненной, а сертификат передан Кредитной организации.

5.2 В случае повторного получения сертификата подтверждение указанных в сертификате данных осуществляется путем подписания кредитной организации запроса на сертификат на ранее выданном на средствах ГУЦ сертификате (см. п. 4б). Выпущенный сертификат размещается в личном кабинете СЦ Кредитной организации, о чем она оповещается при выполнении заявки по электронной почте. Срок действия сертификата составляет 3 года. После этого заявка на выпуск сертификата считается исполненной, а сертификат передан Кредитной организации.

5 Отзыв сертификата

Отзыв сертификата происходит при наступлении одного из следующих событий:

- Прекращение деятельности Кредитной организации или изменении ее реквизитов, указанных в сертификате;
- Компрометация ключа электронной подписи.

Процедура отзыва сертификата состоит из следующих шагов:

1. Кредитная организация направляет запрос через СЦ на отзыв сертификата с указанием серийного номера сертификата и причины отзыва:
   - выбрать кнопку «Добавить запрос»,
   - в разделе «Соглашение/Услуга» выбрать «Поддержка ГУЦ»,
   - в категории запроса указать «Отзыв сертификата для ЕБС»,
   - в наименовании «Тема» указать тему запроса «Отзыв сертификата для ЕБС»,
   - в описании заявки в свободной форме указывается ее суть, серийный номер сертификата на отзыв, причина отзыва и отправляется на рассмотрение в СЦ (кнопка «Сохранить»).
2. ЭО осуществляет отзыв сертификата.

Приложение 1

Форма заявления на выпуск сертификата ключа проверки электронной подписи

Заявление на создание квалифицированного сертификата
ключа проверки электронной подписи

_____
Наименование юридического лица

в лице _____
Должность

_____
Фамилия Имя Отчество

действующего на основании _____
Основание

просит создать сертификат ключа проверки электронный подписи для Единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации для полномочного представителя, действующего от имени нашей организации, владельца сертификата ключа проверки электронной подписи, пользователя Головного удостоверяющего центра:

_____
Фамилия Имя Отчество

В сертификат ключа проверки электронной подписи прошу занести следующие идентификационные данные:

CommonName (CN)	Наименование организации
INN	ИНН организации
OGRN	ОГРН организации
Organization (O)	Наименование организации
Locality (L)	Город
Contry (C)	Страна = RU
State(S)	Субъект Российской Федерации
Street(STREET)	Адрес

Настоящим _____
Фамилия Имя Отчество пользователя Головного Удостоверяющего центра

Паспорт _____ _____ _____
Серия и номер Дата выдачи Код подразделения

_____

Кем выдан

соглашается с обработкой своих персональных данных ФГБУ НИИ «Восход».

Пользователь Головного Удостоверяющего центра _____

Фамилия И.О.

«____» _____ 2018 г.

_____

Должность руководителя организации

_____ _____

Наименование организации Фамилия И.О

«____» _____ 2018 г

М.П.

Приложение 2

Форма доверенности на физическое лицо, которое будет выступать от имени юридического лица

Доверенность

г. _____ _____
город дата

_____
Полное наименование организации

в лице _____
Должность

_____
Фамилия Имя Отчество

действующего на основании _____
Основание

уполномочивает _____
Фамилия Имя Отчество

Паспорт _____ _____ _____
Серия и номер Дата выдачи Код подразделения

_____
Кем выдан

действовать от имени _____
Полное наименование организации

при использовании электронной подписи электронных документов, выступать в роли Пользователя Головного Удостоверяющего центра и осуществлять действия по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, установленные для Пользователя Удостоверяющего центра

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись пользователя Головного Удостоверяющего центра _____ _____
Фамилия И.О. Подпись

подтверждаю.

_____
Должность руководителя организации

_____ _____
Наименование организации Фамилия И.О

«____» _____ 2018 г

М.П.

Приложение 3

Форма запроса сертификата PKCS10

Версия: 1
Субъект:
ИНН=001234567890
ОГРН=0001234567890
O=ФГБУ НИИ «Восход»
STREET= улица Удальцова, дом 85
L=г. Москва
S=77 Москва
C=RU
CN= ФГБУ НИИ «Восход»

Алгоритм открытого ключа:
ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001
Параметры алгоритма:
0000 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03
0010 02 02 1e 01
1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию
1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию
Длина открытого ключа: 512 бит
Открытый ключ: UnusedBits = 0
0000 01 30 86 54 4c c6 36 ac 55 2c 7e a7 f1 2d 26 d1
0010 19 49 62 72 6c 37 aa 14 3e de 37 fd b0 ae 68 aa
0020 07 dc e8 c3 a1 dc 1d 06 03 cd df aa ba 4b d6 2b
0030 1d 77 4c 59 b3 4f 2c 06 47 f3 85 9d d9 df 87 96
0040 66 77
Запрос атрибутов: 1
Атрибуты 1:

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 "КриптоПро HSM" v.2.0
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

Алгоритм подписи:
ObjectID алгоритма: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001
Параметры алгоритма: NULL
Подпись: НеиспользБит=0
0000 11 85 fa e3 14 66 5a 91 3a 3b 76 ab bd b8 85 cf
0010 2c fa 34 ec 53 aa b3 ed 39 cc 93 bf f4 f8 d6 09
0020 2c 76 06 a1 0d 88 96 42 b6 9f 61 28 ef ec 98 ce
0030 ed 10 c4 64 17 d7 93 b4 23 7d 2b 91 8b 6b 77 88
Подпись соответствует открытому ключу
Хеш ИД ключа (rfc-sha1): 44 c3 86 5c 53 7c d8 b6 5b 7e b5 5c 81 1e 44 f7 ad 3e 42 77
Хеш ИД ключа (sha1): 88 e7 30 d3 87 cb 47 6c 2e 54 0a 8c 57 8d 77 4f 3e ae 77 d8