**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 (далее – владелец сертификата, пользователь ГУЦ; 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.

[1] Кредитная организация вправе по собственной инициативе представить копию документа, содержащего сведения из указанного документа.

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 положительного решения по выпуску сертификата копия решения направляется в ЭО.

4. При положительном решении о выпуске сертификата Кредитная организация:

   а) Осуществляет доступ представителя Кредитной организации 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 (рекомендации по формированию запроса приведены в Приложении 4 Порядка). В случае повторного направления запроса на сертификат такой запрос дополнительно подписывается с использованием валидного на момент подписания сертификата, ранее полученного в ГУЦ, с не истекшим сроком действия. Сформированные файлы архивируются в zip-архив.

   в) Представитель Кредитной организации проходит процедуру авторизации через Единую систему идентификации и аутентификации (далее – 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[3] в следующем порядке:

      – выбрать кнопку «Добавить запрос»,
      – в разделе «Выбор типа запроса» в поле «Соглашение/Услуга» выбрать «Поддержка ИС ИЭП»,
      – в разделе «Выбор типа запроса» в категории тип запроса указать «Регламентная процедура»,
      – В разделе «Описание запроса» выбрать в качестве информационной системы «ФГИС ГУЦ»,

[2] Файл запроса формируется с использованием средств электронной подписи Кредитной организации класса КВ2.
[3] Кредитная организация может сформировать несколько заявок в СЦ в зависимости от количества запросов на сертификат, при этом одна заявка на выпуск сертификата в СЦ должна содержать один запрос на выпуск сертификата.

- В разделе «Описание запроса» в категории «Тип регламентной процедуры» указать «Выпуск и регистрация сертификата для 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:

5.1 Вопросы, связанные с корректностью полей в запросе на выпуск сертификата, а также организационные вопросы согласно п 5.2 Порядка решаются в рамках взаимодействия между ЭО и Кредитной организацией по сформированной в СЦ заявке (п.п. «г» ч.4 раздела 4 Порядка).

5.2. В случае первичного выпуска сертификата удостоверение указанных в сертификате данных и факт его получения осуществляется путем заверения владельцем сертификата открытого ключа на бумажном носителе (форма приведена в Приложении 5 Порядка) в следующем порядке:

а) ЭО изготавливает сертификат в электронном виде, а также копии (два экземпляра) сертификата открытого ключа на бумажном носителе,

б) ЭО приостанавливает заявку на выпуск сертификата в СЦ с целью согласования даты и времени заверения Кредитной организацией изготовленной ЭО копии сертификата открытого ключа на бумажном носителе; предлагаемая ЭО дата и время заверения копии сертификата на бумажном носителе не должна превышать регламентный срок обработки заявки на выпуск сертификата открытого ключа для ЕБС в СЦ,

в) в установленную дату и время владелец сертификата или физическое лицо на основании заверенной доверенности на получение сертификата ключа проверки электронной подписи (далее – доверенное лицо; форма доверенности приведена в Приложении 3 Порядка) является по адресу г. Москва, ул. Удальцова д. 85 с основным документом, удостоверяющий личность. После заверения копий

сертификата представителем ЭО и владельцем сертификата по одному экземпляру заверенной копии передается каждой из сторон. В случае получения копии сертификата на бумажном носителе доверенным лицом, один экземпляр копии сертификата подписывает доверенное лицо и передает ЭО, а два экземпляра копии сертификатов, заверенные ЭО, передаются для подписи и заверения владельцу сертификата. Далее подписанный и заверенный владельцем сертификата экземпляр копии сертификата направляется в ЭО посредством почтового отправления или курьерской службой по адресу 119607, г. Москва, ул. Удальцова д. 85.

г) после подтверждения указанных данных на бумажном носителе производится размещение сертификата открытого ключа 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.

5.3. В случае повторного получения сертификата подтверждение указанных в сертификате данных осуществляется путем подписания владельцем сертификата запроса на сертификат с использованием валидного на момент подписания сертификата, ранее полученного в ГУЦ, с не истекшим сроком действия. 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 ИС ИЭП»,
- в категории «Тип запроса» указать «Регламентная процедура»,
- в разделе «Описание запроса» в качестве системы выбрать «ФГИС ГУЦ», а в типе запроса указать «Отзыв сертификата для ЕБС»,
- наименовании «Тема» указать тему запроса «Отзыв сертификата для ЕБС»,
- в описании заявки в свободной форме указывается причина отзыва сертификата, серийный номер сертификата на отзыв и отправляется на рассмотрение в СЦ (кнопка «Сохранить»).

2. ЭО осуществляет отзыв сертификата.

Лист регистрации изменений

| № | Дата | Изменение | Присвоенная версия |
|---|---|---|---|
| 1. | 26 августа 2018 | Первая версия | 1 |
| 2. | 8 октября 2018 | 1. Приложение «Форма запроса сертификата» изменена на «Рекомендации по формированию запроса»<br>2. Обновлена процедура получения бумажной копии сертификата в п.5.1 – 5.2.<br>3. Добавлена форма доверенности на получения сертификата<br>4. Добавлена форма копии сертификата на бумажном носителе<br>5. Внесены изменения в порядок формирования запросов на издание сертификата и на отзыв в связи с изменением каталога услуг СЦ | 1.1 |

Приложение 1

Форма заявления на выпуск сертификата ключа проверки электронной подписи

Заявление на создание квалифицированного сертификата
ключа проверки электронной подписи

_____

наименование организации, включая организационно-правовую форму

ИНН _____ ОГРН _____

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

ИНН _____ ОГРН _____

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 доверенности на получение сертификата ключа
проверки электронной подписи

Доверенность

г. _____ _____
город дата

_____
Полное наименование организации

ИНН _____ ОГРН _____

уполномочивает _____
Фамилия Имя Отчество

Паспорт _____ _____ _____
Серия и номер Дата выдачи Код подразделения

_____
Кем выдан

получить сертификат ключа проверки электронной подписи, созданного для Пользователя Головного удостоверяющего центра:

_____
Фамилия имя отчество Пользователя Удостоверяющего центра

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «___» _____ 20__ г.

Подпись представителя _____ _____
Фамилия И.О. Подпись

подтверждаю.

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

_____
должность руководителя организации

_____ _____
фамилия И.О. руководителя организации Подпись

«___» _____ 20___ г. М.П.

Приложение 4

Рекомендации по формированию запроса

Каждый запрос на 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 – вносится ИНН организации, длина 12 символов, к значению необходимо добавить 2 лидирующих нуля;
- ОГРН – вносится ОГРН организации, длина 13 символов;
- O – полное или сокращенное наименование организации;
- STREET – часть адреса места нахождения организации, включающую 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*=007712345678
*ОГРН*=1234567890123
*O*=ФГБУ НИИ «Восход»
*STREET*=улица Удальцова, дом 85
*L*=г. Москва
*S*=77 Москва
*C*=RU
*CN*= ФГБУ НИИ «Восход»

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;

– Информацию о политиках сертификата, вносятся следующие идентификаторы:

  – 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 34.10-2001;
- ГОСТ Р 34.10-2012 256 бит;
- ГОСТ Р 34.10-2012 512 бит.

Приложение 5

Форма сертификата ключа проверки электронной подписи на бумажном носителе

**Минкомсвязь России**
**125375, г. Москва, ул. Тверская, д. 7**

**Квалифицированный сертификат ключа проверки электронной подписи**

| | |
|---|---|
| Номер сертификата | ***Серийный номер сертификата*** |
| Действие сертификата | **с** ***Дата начала в формате дд.мм.гг чч.мм.сс*** **по** ***Дата окончания в формате дд.мм.гг чч.мм.сс*** |
| **Сведения о владельце сертификата** | |
| Наименование организации | ***Наименование организации*** |
| Основной государственный регистрационный номер | ***Номер ОГРН*** |
| Идентификационный номер налогоплательщика | ***Номер ИНН*** |
| Место нахождения юридического лица | ***Адрес*** |
| **Сведения об издателе сертификата** | |
| Наименование удостоверяющего центра | ***Минкомсвязь России*** |
| Место нахождения удостоверяющего центра | ***Адрес*** |
| Номер квалифицированного сертификата удостоверяющего центра | ***Номер квалифицированного сертификата*** |
| Наименование средства электронной подписи | ***Средство ЭП*** |
| Наименование средства удостоверяющего центра | ***Средство УЦ*** |
| Реквизиты заключения о подтверждении соответствия средства электронной подписи | ***Реквизиты*** |
| Класс средств удостоверяющего центра:<br>• Класс средства ЭП КС1,<br>• Класс средства ЭП КС2,<br>• Класс средства ЭП КС3,<br>• Класс средства ЭП КВ1,<br>• Класс средства ЭП КВ2,<br>• Все политики выдачи | |
| **Сведения о ключе проверки электронной подписи** | |
| Используемый алгоритм: | ***ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012*** |
| Используемое средство электронной подписи: | ***Средство электронной подписи*** |
| Класс средства электронной подписи:<br>• *Класс средства ЭП КС1,*<br>• *Класс средства ЭП КС2,*<br>• *Класс средства ЭП КС3,*<br>• *Класс средства ЭП КВ1,*<br>• *Класс средства ЭП КВ2,*<br>• *Все политики выдачи* | |
| Область использования ключа:<br>• *Проверка подлинности клиента,*<br>• *Защищенная электронная почта* | |
| Значение ключа:<br>*Значение Ключа* | |

**Электронная подпись под квалифицированным сертификатом**

Используемый алгоритм:
*Указывается применяемый ГОСТ:*
*• ГОСТ Р 34.10-2001;*
*• ГОСТ Р 34.10-2012 256 бит;*
*• ГОСТ Р 34.10-2012 512 бит*

Значение электронной подписи:
*Значение электронной подписи*

Уполномоченное лицо Удостоверяющего центра _____ / _____
Подпись ФИО
М.П «___» _____ 20_г._

Владелец квалифицированного сертификата ключа проверки электронной подписи _____ / _____
Подпись ФИО
М.П «___» _____ 20__ г.