## Порядок формирования ключа аутентификации, запроса и заявки

## на издание сертификата ключа аутентификации.

## Порядок получения сертификата ключа аутентификации и его установки

*\*\*\* Сайт УФК - > ГИС -> Удостоверяющий центр -> Порядок получения сертификата ->* [*Инструкция по генерации ключа аутентификации и шифрования (для Континент-АП)*](https://ulyanovsk.roskazna.gov.ru/upload/ulyanovsk/instruktciia_kontinent_ap.docx)

*Ссылка <https://ulyanovsk.roskazna.gov.ru/gis/udostoveryayushhij-centr/poryadok-polucheniya-sertifikata/>*

1. **Термины и определения**

**Организация-заявитель** - юридическое лицо, обратившееся за получением сертификата открытого ключа аутентификации.

**Автоматизированное рабочее место** (далее - АРМ) – рабочее место, обеспечивающее возможность удаленного online взаимодействия Управления Федерального казначейства по Ульяновской области (далее - Управление) и Организации-заявителя, включая наличие в нем программного обеспечения (далее - ПО) и технических средств, в том числе средств криптографической защиты информации (далее - СКЗИ), предназначенных для работы в системе электронного документооборота Федерального Казначейства (далее - СЭДФК).

**Администратор АРМ Организации-заявителя** - сотрудник Организации-заявителя, отвечающий за обеспечение бесперебойной эксплуатации ПО, СКЗИ и технических средств АРМ Организации-заявителя, контроль мероприятий по защите информации, хранение и учет ЭД, взаимодействие с Управлением по техническим вопросам и вопросам обеспечения безопасности информации. На администратора АРМ Организации-заявителя могут возлагаться задачи по отправке/приему электронных документов и сообщений.

**Закрытый ключ аутентификации** - уникальная последовательность символов, известная владельцу сертификата открытого ключа и предназначенная для аутентификации Организации-заявителя на стороне Управления с последующим установлением защищенного (шифрованного) канала связи при информационном взаимодействии в СЭДФК с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи).

1. **Порядок работы с ключами аутентификации для организации шифрованной связи (при использовании аппаратно-программного комплекса шифрования "Континент")**
	1. СКЗИ "Континент-АП" обеспечивает доступ удаленных пользователей к ресурсам сегментов общей сети передачи данных, защищенных средствами изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.7" (далее – АПКШ "Континент"), установленного в Управлении.
	2. **Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому руководителем Организации-заявителя.** Пользователи СКЗИ обязаны выполнять требования «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13.06.2001 № 152) в части, их касающейся.
	3. Формирование ключа аутентификации и запроса на получение сертификата открытого ключа аутентификации для СКЗИ "Континент-АП" осуществляется администратором АРМ Организации-заявителя с последующей передачей запроса специалисту Управления, ответственному за выдачу сертификата открытого ключа аутентификации.
	4. Срок действия ключа аутентификации соответствующего сертификата - **один год и три месяца**.
	5. За 10 дней до окончания срока действия сертификата открытого ключа аутентификации администратор АРМ Организации-заявителя:
* осуществляет формирование нового ключа аутентификации и соответствующего запроса на получение сертификата открытого ключа аутентификации в соответствии с п. 3.1 настоящего Порядка;
* передает специалисту Управления, ответственному за выдачу сертификата открытого ключа аутентификации, документы, указанные в п. 4.1. настоящего Порядка;
* получает в электронном виде сертификат открытого ключа аутентификации.
	1. О всех случаях компрометации закрытых ключей аутентификации администратор АРМ Организации-заявителя извещает Управление по телефону 42-75-22. В этом случае формируется новый ключ аутентификации в соответствии с [п. 3.](#Par305)1 настоящего Порядка.
1. **Формирование ключа аутентификации, запроса и заявки на издание сертификата ключа аутентификации**

**ВНИМАНИЕ!**

**Перед формированием запроса на сертификат, убедитесь, что выбран криптопровайдер используемый по умолчанию: «Код безопасности» (см. рис. ниже)**

****

* 1. Ключ аутентификации и запроса на получение сертификата открытого ключа аутентификации формируются администратором АРМ Организации-заявителя.

Для создания запроса на получение сертификата:

Вставьте **чистый USB-диск**, на который будет сохранен ключ аутентификации.

* + 1. Вызовите контекстное меню пиктограммы Абонентского пункта, расположенной на панели задач Windows.
		2. В меню “Сертификаты” активируйте команду “Создать запрос на пользовательский сертификат…”.
		3. На экране появится диалоговое окно для создания запроса. Все поля обязательны для заполнения[[1]](#footnote-1).



ВНИМАНИЕ!!! Заглавные буквы в адресе электронной почты НЕ допустимы!

* + 1. Отметьте галочкой поле рядом с надписью «Бумажная форма». В полях «Электронная форма» и «Бумажная форма» укажите путь для сохранения файла запроса и файла заявки на сертификат.

(**Нажав кнопку «Подробно>>» можно поменять имя создаваемого контейнера – ключа аутентификации**:



* + 1. Нажмите кнопку “OK”
		2. Установите пароль



!!!ВНИМАНИЕ**: запишите или запомните пароль**, он вам понадобится при установке сертификата

Нажмите «ОК»

* + 1. На экране появится диалог Код Безопасности CSP с перечнем тех ключевых носителей, на которых может быть сохранена ключевая информация.



* + 1. В списке устройств выберите вставленный чистый flash-носитель (п.3.1. настоящего Порядка), например, “Дисковод, D” (буква диска может быть другая).
		2. Нажмите кнопку “OK”.
		3. На экране появится сообщение о завершении создания запроса.



* + 1. Нажмите кнопку “OK” в окне сообщения.

**Внимание!!! Убедитесь, что на flash-носителе появилась папка с наименованием «Topsecretkeys» - это и есть закрытый ключ.**

* + 1. Файл запроса имеет расширение «**\*.req»** и находится в папке, указанной в пункте 3.1.3 настоящего Порядка. Файл бумажной формы запроса (Заявка на получение в удостоверяющем центре сертификата ключа абонентского пункта, далее – Заявка) имеет расширение \*.html и находится в папке, указанной в пункте 3.1.3 настоящего Порядка.
		2. Заявка распечатывается **в двух экземплярах**, заполняется (вписывается в связи с чем производится выдача сертификата ключа аутентификации, должность руководителя Организации-заявителя, паспортные данные руководителя Организации-Заявителя, реквизиты приказа по организации «О назначении ответственных лиц»), подписывается руководителем Организации-заявителя, заверяется печатью Организации-заявителя (образец заполнения указан в Приложении 1 к настоящему Порядку).
		3. Изготовленный ключевой контейнер подлежит учету в соответствии с требованиями «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13.06.2001 № 152.
1. **Порядок получения сертификата ключа аутентификации**
	1. Для получения сертификата ключа аутентификации администратор АРМ Организации-заявителя передает уполномоченному специалисту Управления следующие документы:
* файл запроса на сертификат ключа аутентификации (файл \*.req) на съемном носителе информации, не содержащем ключей электронной подписи;
* Заявку на получение в удостоверяющем центре сертификата ключа абонентского пункта, оформленную в соответствии с п. 3.3 настоящим Порядком (образец указан в Приложении № 1).
* паспорт владельца сертификата ключа аутентификации, с предоставлением копии 2-3 страницы, заверенной в установленном порядке;
* согласие владельца сертификата открытого ключа аутентификации на обработку персональных данных (**если ранее не подавалось**, по образцу, указанному в Приложении №2);
* копию приказа «О назначении ответственных лиц», заверенную в установленном порядке, с целью контроля выполнения требований п.2.2 настоящего Порядка (примерная форма приказа указана в Приложении № 3);
* доверенность на право получения сертификатов ключей аутентификации (Приложение № 4).
	1. Место приема заявлений на получение сертификата ключа аутентификации:

**г. Ульяновск, ул. Гончарова, д. 50/1, кабинет 113**, внут. тел. 210, 122

Время приема: понедельник-четверг **с 8:10 до 12:00 и с 13:30 до 16:00**

 **пятница с 8:10 до 12:00 и с 13:30 до 15:00**

* 1. После проверки комплектности, правильности оформления, наличия подтверждающих документов уполномоченный специалист Управления выдает администратору АРМ Организации-заявителя сертификат ключа аутентификации в электронном виде (user.cer), а также корневой сертификат (root.p7b).
1. **Порядок установки сертификата ключа аутентификации**

***(\*п.5 переделан на основании видеоинструкции по ссылке***

[***http://ulid.ru/index.php/know-box/school-management/198-continent-ap-nstall-cert***](http://ulid.ru/index.php/know-box/school-management/198-continent-ap-nstall-cert)***)***

**root и server установить в доверенные центры, а user через сам континент устанавливается - от Саши Загайнова. Вот то что вам дали в казначействе нужно скопировать в контейнер, и с него устанавливать потом через континент))**

5.1. Вызовите контекстное меню пиктограммы Абонентского пункта ****, расположенной на панели задач Windows.

5.2. «Установить/разорвать соединение» (если соединение установлено, то для начала его надо разорвать, потом установить).

5.3. «Сертификат» - «Импорт». Выбираем сертификат безопасности user.cer , далее «Открыть», далее выбираем ключевой контейнер сертификата пользователя, нажимаем «Ок». Сертификаты root и server устанавливаем в доверенные центры (если они не были установлены ранее).

Если все сделано правильно на экране должно появиться сообщение «Импорт пользовательского сертификата успешно завершен».

Нажимаем «Ок», выбираем новый сертификат (должен быть в самом низу выпадающего окна), нажимаем «Ок», после этого должно установиться соединение **** и значок должен стать активным.

\* пароль на контейнер не запрашивается

5.4. Для успешной установки соединения с сервера доступа Управления поле “Номер телефона” на вкладке “Общие” окна “Континент-АП Свойства”, вызываемого в меню “Настройка” пиктограммы Абонентского пункта, должно иметь значение **ksh.simtreas.ru.**

1. **Контактная информация**

Контактная информация специалистов Управления Федерального казначейства по Ульяновской области, осуществляющих прием документов на получение сертификатов ключей аутентификации:

* Специалист 1 разряда Козлов Денис Дмитриевич,
* ведущий специалист-эксперт Свиязов Александр Николаевич
* Специалист 1 разряда Ятманова Елена Александровна

Контактный телефон 8 (8422) 42-75-22

Адрес официального сайта Управления в информационно-телекоммуникационной сети "Интернет": [http://ulyanovsk.roskazna.ru](http://www.ulyanovsk.roskazna.ru)

Адрес электронной почты Управления: mashbur@simtreas.ru, адрес электронной почты Отдела режима секретности и безопасности информации Управления: ang@simtreas.ru

Приложение № 1



Приложение № 2

|  |  |
| --- | --- |
|  |  |

СОГЛАСИЕ

на обработку персональных данных

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество (при наличии) субъекта персональных данных)

проживающ\_\_ по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

документ, удостоверяющий личность: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(наименование документа, удостоверяющего личность, серия и №, сведения о дате выдачи документа и выдавшем его органе)

в соответствии с частью 4 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях получения квалифицированного сертификата ключа проверки электронной подписи даю согласие Федеральному казначейству (101000, г. Москва, Большой Златоустинский пер., д. 6, стр. 1) и Управлению Федерального казначейства по Ульяновской области, (432017, г. Ульяновск, ул. Гончарова, д. 50/1)

 (наименование и адрес территориального органа Федерального казначейства)

на обработку моих персональных данных, в том числе сведений, содержащихся в копии основного документа, удостоверяющего личность, адреса электронной почты, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение. Также даю согласие на ознакомление уполномоченного лица[[2]](#footnote-2) с информацией, содержащейся в квалифицированном сертификате ключа проверки электронной подписи[[3]](#footnote-3).

Настоящее согласие действует со дня его подписания до дня предоставления соответствующего отзыва в письменной форме.

"\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись субъекта персональных данных)

Приложение № 3

**Оформляется ТОЛЬКО в случае, когда заявка формируется не на имя Руководителя организации**

**П Р И К А З**

\_\_\_.\_\_\_.201\_\_\_г. № \_\_

**О назначении ответственных лиц**

На основании Договора об обмене электронными документами с Управлением Федерального казначейства по Ульяновской от \_\_.\_\_.201\_ № \_\_\_/201\_ и в целях реализации приказа Федеральной агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», п р и к а з ы в а ю:

1. Назначить администратором автоматизированного рабочего места обмена электронными документами (далее – АРМ ЭД), отвечающим за обеспечение бесперебойной эксплуатации программного обеспечения и технических средств АРМ ЭД, контроль мероприятий по защите информации, хранение и учет электронных документов, взаимодействие с Управлением Федерального казначейства по Ульяновской области по техническим вопросам и вопросам обеспечения безопасности информации, сотрудника:

|  |  |
| --- | --- |
|  |  |
| Ф.И.О. полностью | должность |

в его отсутствие

|  |  |
| --- | --- |
|  |  |
| Ф.И.О. полностью | должность |

1. Допустить к эксплуатациисредств криптографической защиты информации (далее - СКЗИ) «Континент-АП» и «КриптоПро CSP» и возложить персональную ответственность за эксплуатацию СКЗИ в соответствии с техническими условиями:

|  |  |
| --- | --- |
|  |  |
| Ф.И.О. полностью | должность |
|  |  |
| Ф.И.О. полностью | должность |
|  |  |
| Ф.И.О. полностью | должность |
|  |  |
| Ф.И.О. полностью | должность |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Должность руководителя |  | Подпись |  | Фамилия И.О. |

Приложение № 4

|  |  |
| --- | --- |
| (оформляется на бланке Заявителя) | Примерная форма |

**ДОВЕРЕННОСТЬ**

|  |  |  |
| --- | --- | --- |
|  |  | «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_г. |
| *(наименование населенного пункта)* |  | *(дата, месяц, год)* |
| Настоящей доверенностью |  |
|  |
| *(полное наименование организации)* |
| в лице |  |
| *(должность руководителя, ФИО)* |
| действующего на основании |  |
| *(учредительный документ)* |
|  |
| уполномочивает |  |
| *(должность, ФИО получателя сертификата)* |
|  |
| паспорт серия |  |  | № |  | выдан |  |
|  |
| *(кем и когда выдан)* |

совершать следующие действия:

1. Представлять в Региональный центр регистрации Удостоверяющего центра Федерального казначейства Управления Федерального казначейства по Ульяновской области комплект документов и сведений, необходимых для создания сертификата ключа абонентского пункта.
2. Получать под расписку в Региональном центре регистрации Удостоверяющего центра Федерального казначейства Управления Федерального казначейства по Ульяновской области файл сертификата ключа абонентского пункта и экземпляр на бумажном носителе.

**Настоящая доверенность выдана по** «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г. **без права передоверия.**

|  |
| --- |
|  / / |
|  *(должность руководителя) (подпись) (Фамилия И.О.)* |

|  |  |
| --- | --- |
|  М.П.\* |  |

*\*Печать ставится при наличии*

1. В поле **«Имя сотрудника» -** Фамилия Имя Отчество **руководителя Организации-заявителя**.

 В поле **«Описание»** - полное официальное наименование Организации-заявителя.

 В поле **«Организация»** - краткое официальное наименование Организации-заявителя. Длина поля не более 64 символа.

В поле **«Подразделение»** - наименование структурного подразделения (отдела) в Организации-заявителе (в случае отсутствия ввести значение **buh**).

Знаки препинания «. , : ; ! ? / \ ( ) \_» и кавычки в заполняемых полях недопустимы**.** [↑](#footnote-ref-1)
2. 1 По тексту применяются термины, используемые в Регламенте Удостоверяющего центра Федерального казначейства, утвержденном приказом Федерального казначейства от 14.09.2018 № 261. [↑](#footnote-ref-2)
3. 2 Включается в согласие при необходимости в соответствии с пунктом 5.2 Регламента Удостоверяющего центра Федерального казначейства, утвержденного приказом Федерального казначейства от 14.09.2018 № 261. [↑](#footnote-ref-3)