

# Памятка по созданию двухкомпонентных ключей электронной подписи с помощью ПО SBERSIGN

## 1. Настройка параметров ПО «SberSign» и создание двухкомпонентных ключей электронной подписи

Двухкомпонентные ключи электронной подписи (ЭП) изготавливаются их владельцами самостоятельно с помощью ПО «SberSign».

### 1.1 Настройка параметров ПО «SberSign» для формирования ключей ЭП

Прежде чем приступить к созданию (генерации) ключей ЭП следует скопировать главный ключ и узел замены (файлы gk.db3 и uz.db3) в корневой каталог флэш-накопителя и осуществить необходимые настройки ПО «SberSign». Для этого запустите приложение «Параметры SberSign»: ПУСК->Все программы ->SberSign ->Параметры SberSign (см. Рисунок 1).

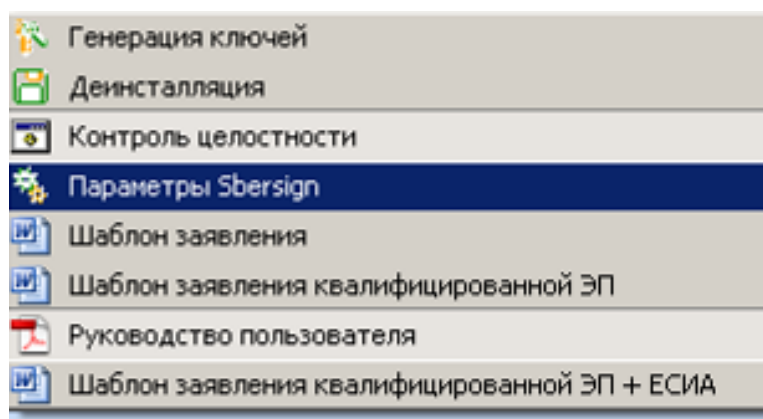
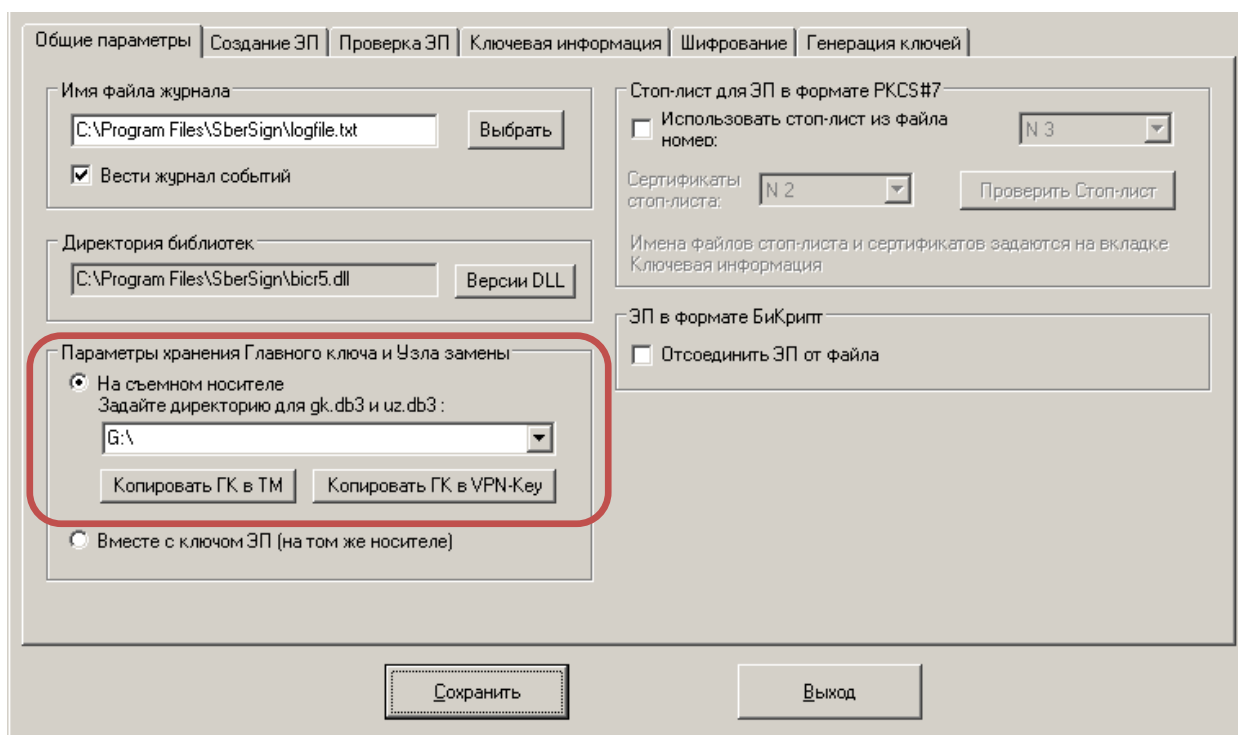


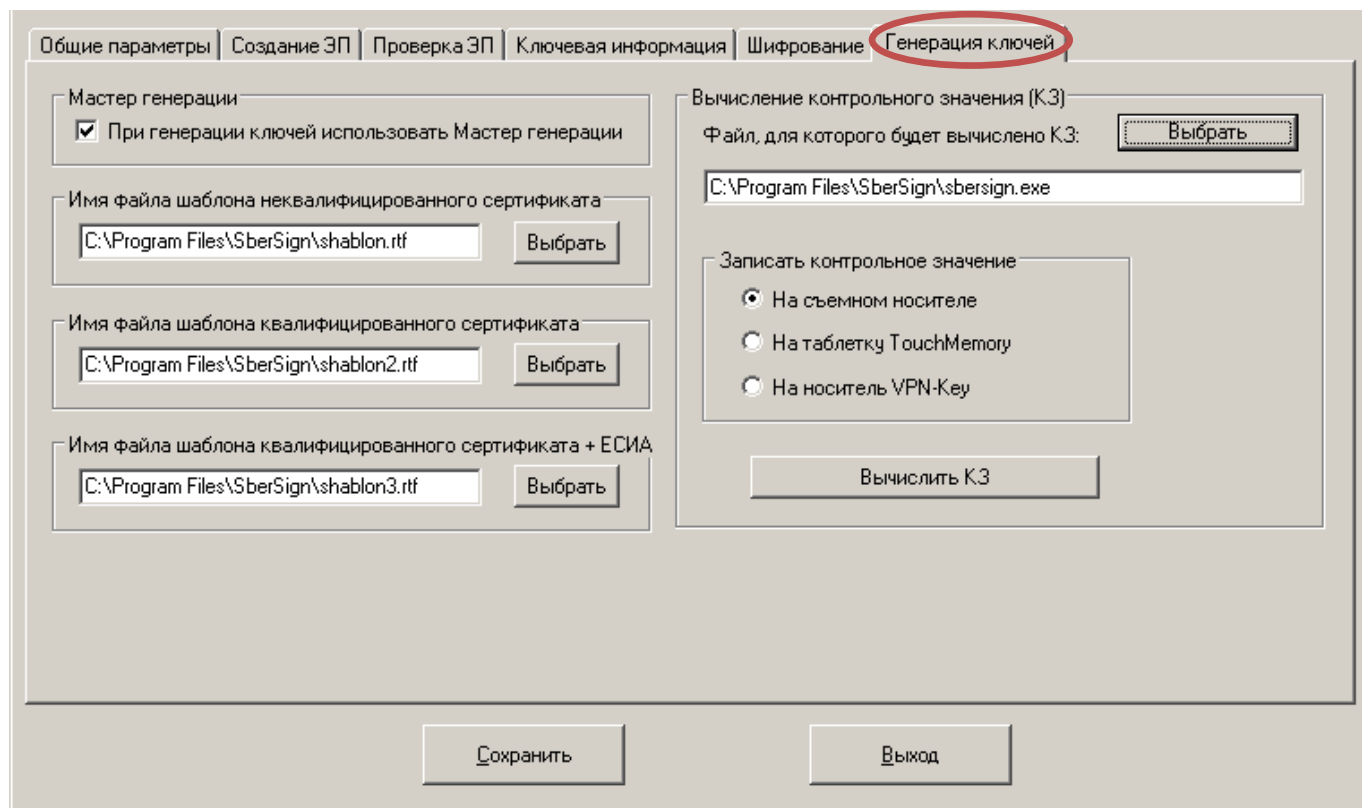
Рисунок 1 – Запуск приложения «Параметры SberSign»

Откроется окно программы «Параметры SberSign». В появившемся окне по умолчанию выбрана вкладка «Общие параметры» (см. Рисунок 2).



## Рисунок 2 – Программа настройки параметров SberSign

Выберите букву флэш-накопителя в блоке «Параметры хранения Главного ключа и Узла замены», на который предварительно были скопированы главный ключ и узел замены (файлы gk.db3 и uz.db3). Для сохранения изменений настроек нажмите кнопку «Сохранить» и перейдите на вкладку «Генерация ключей».



## Рисунок 3 – Программа настройки параметров SberSign

В разделе «Генерация ключей» (см. Рисунок 3) отметьте опцию «При генерации ключей использовать Мастер генерации». Далее необходимо указать соответствующий путь к файлу шаблона распечатки сертификата, как показано на рисунке (путь указывается по умолчанию).

Файл шаблона распечатки сертификата должен соответствовать образцу, приведённому в Приложении №1 для неквалифицированного сертификата и в Приложении №2 для квалифицированного сертификата к данной памятке.

Для сохранения изменений настроек нажмите кнопку «Сохранить» и закройте окно программы настройки параметров SberSign нажатием на кнопку «Выход».

## 1.2 Создание двухкомпонентных ключей ЭП

Ключ ЭП состоит из двух компонент, одна из которых хранится в виде файла (мастер-ключ) и зашифрована на главном ключе, а другая (основная компонента) должна быть записана на съемный носитель (флэш-накопитель или TouchMemory). С помощью ключа электронная подпись формируется под электронным документом, а с помощью ключа проверки ЭП проверяется ЭП документа.

Владелец ключа ЭП ОБЯЗАН сохранять в тайне свой ключ ЭП. Ключ проверки ЭП предназначен для передачи в места проверки ЭП.

В целях безопасности в качестве носителя закрытого ключа электронной подписи рекомендуется использовать Touch Memory или VPN-Key, но программой SberSign также предусмотрена возможность использования флэш-накопителей.

В приведённом ниже примере ключи будут сформированы на флэш-накопитель.

Запустите программу «Генерация ключей», ПУСК-> Все программы -> SberSign.

В появившемся окне «Вас приветствует мастер генерации ключей ЭП» нажмите кнопку «Далее».

На первом шаге работы мастера генерации ключей необходимо выбрать тип формируемого ключа ЭП. Выбираем «Двухкомпонентный».

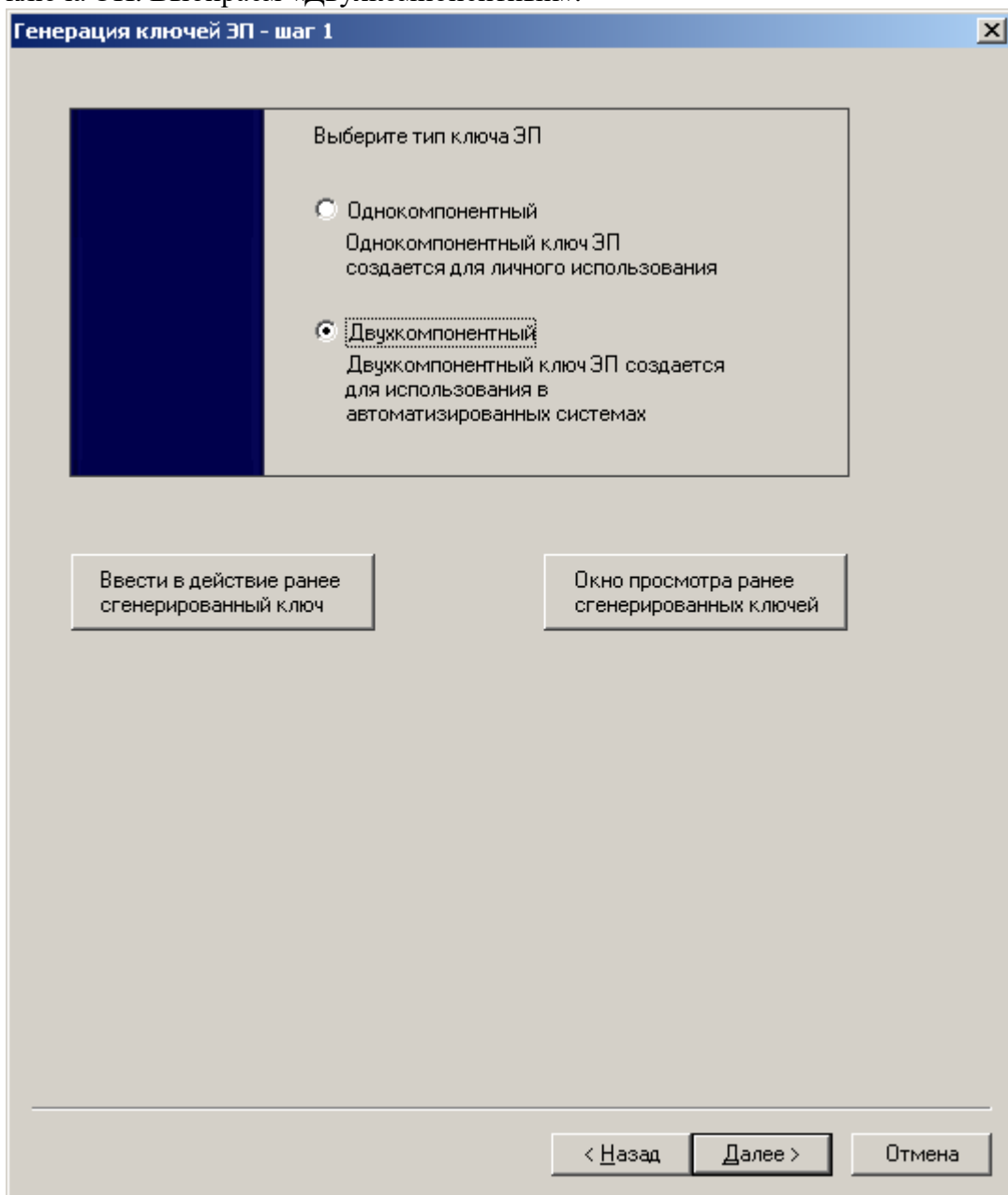


Рисунок 4 – Мастер генерации ключей ЭП – шаг 1

Нажав кнопку «Далее», перейдите на следующий этап.

Генерация ключей ЭП - шаг 2

Введите исходные данные для создания ключа ЭП

Фамилия	Иванов
Имя	Иван
Отчество	Иванович
Должность	инженер
E-Mail	ivanov@salut.ru
Наименование организации	ООО Салют
Код организации ( КУЦ )	ER5TVF
Порядковый номер ключа	02
ИНН	7736009485
ОГРН	1027707000441

Идентификатор ключа ЭП

Программой произведена попытка автоматической генерации идентификатора ключа ЭП. При необходимости можно внести вручную изменения в создаваемый идентификатор

ER5TVF02sИвановИИИинж000Салют

Запрос на квалифицированный сертификат

Создать запрос на квалифицированный сертификат

Дополнительные параметры запроса на квалифицированный сертификат

Включить в запрос данные для ЕСИА

Дополнительные параметры для ЕСИА

< Назад    Далее >    Отмена

Рисунок 5 – Мастер генерации ключей ЭП – шаг 2

На этом этапе необходимо заполнить все поля исходных данных для создания ключа ЭП и указать корректный идентификатор ключа ЭП.

Идентификатор ключа ЭП не может состоять более чем из 32 символов (включая пробелы) и должен соответствовать формату: **YYYYYYNNsФИО должность организация**, где **YYYYYY** – уникальный шестизначный буквенно-цифровой код Организации - клиента ПАО Сбербанк, присваиваемый автоматизированной системой корневого Удостоверяющего центра ПАО Сбербанк, 2 последних символа которого только буквы; **NN** – уникальный для каждого Участника системы ЭДО двухзначный буквенно-цифровой порядковый номер ключа ЭП, который не должен использоваться повторно даже в случае регенерации ключа; **s** – признак принадлежности ключа ЭП организации, являющейся клиентом ПАО Сбербанк.

ПО Sbersign поддерживает создание ключа ЭП с идентификатором в формате **YYYYNNNNsФИО должность организация**, где **YYYY** – уникальный четырехзначный буквенно-цифровой код Организации - клиента ПАО Сбербанк, присваиваемый автоматизированной системой корневого Удостоверяющего центра ПАО Сбербанк; **NNNN** – уникальный для каждого Участника системы ЭДО двухзначный цифровой порядковый номер ключа ЭП, который не должен использоваться повторно даже в случае регенерации ключа; **s** – признак принадлежности ключа ЭП организации, являющейся клиентом ПАО Сбербанк.

Код Организации, закреплённый за Вашей организацией, Вы можете узнать у сотрудника ПАО Сбербанк, оформлявшего договор. Если Вы создаете первый ключ ЭП с данным кодом Организации, то он должен начинаться с 01.

Для генерации запроса на квалифицированный сертификат необходимо поставить галочку напротив «Создать запрос на квалифицированный сертификат», нажать на кнопку «Дополнительные параметры запроса на квалифицированный сертификат» и в открывшемся окне (см. Рисунок ) заполнить все поля в блоках «Информация об организации» и «Информация о владельце ключа».

Дополнительные параметры запроса на квалифицированный сертификат

Информация об организации

Страна: RU

Регион: 77 г. Москва

Населенный пункт: г. Москва

Почтовый индекс:  
(необязательно)

Адрес:  
(необязательно) ул. Вавилова, 23

Информация о владельце ключа

СНИЛС:  
(необязательно) 0000000000

Организация: ООО Салют

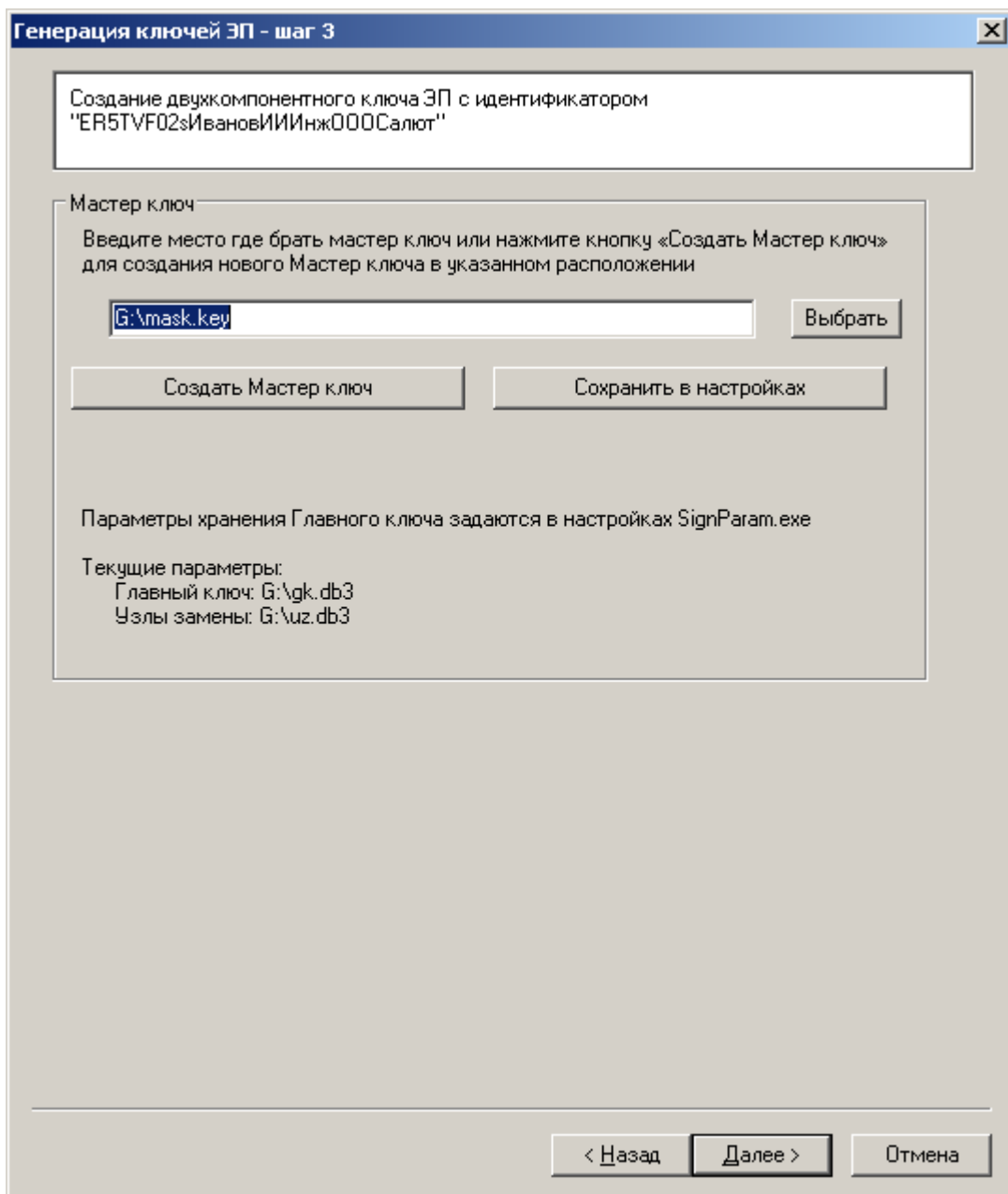
Короткое  
наименование  
организации:  
(необязательно)

Подразделение:  
(необязательно) ИТ

ОК Отмена

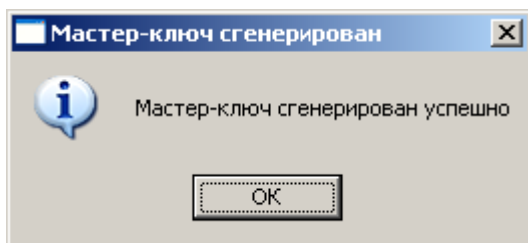
**Рисунок 6**

Для сохранения введенных данных нажмите кнопку «ОК», затем вставьте флеш – накопитель в компьютер, если этого не было сделано ранее, и нажмите кнопку «Далее» для перехода к следующему шагу (Рисунок 7).



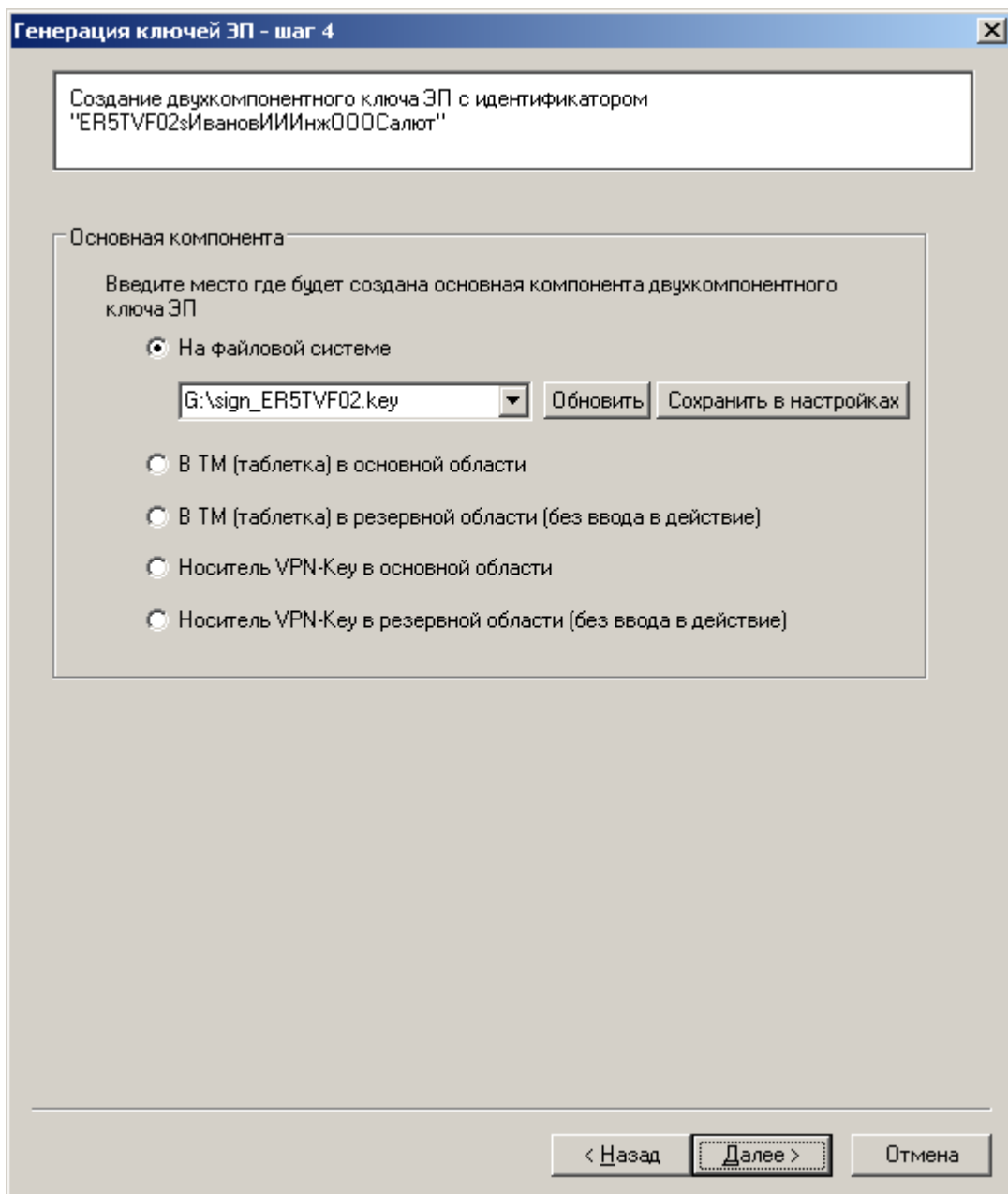
**Рисунок 7 – Мастер генерации ключей ЭП – шаг 3**

На 3 шаге работы выберите место хранения мастер-ключа (флэш-накопитель или жесткий диск) и сгенерируйте его нажатием кнопки «Создать Мастер ключ». По окончании процедуры будет выведено окно с результатом (см. Рисунок ). Нажмите кнопку «ОК».



**Рисунок 8 – Окно с результатом генерации мастер ключа**

Нажмите кнопку «Далее» для перехода к следующему шагу (см. Рисунок ).



**Рисунок 9 – Мастер генерации ключей ЭП – шаг 4**

В разделе «Введите место, где будет создана основная компонента двухкомпонентного ключа ЭП» отметьте опцию «На файловой системе» и выберите из выпадающего списка букву флэш-накопителя (см. Рисунок ). Для перехода к очередному шагу нажмите кнопку «Далее».

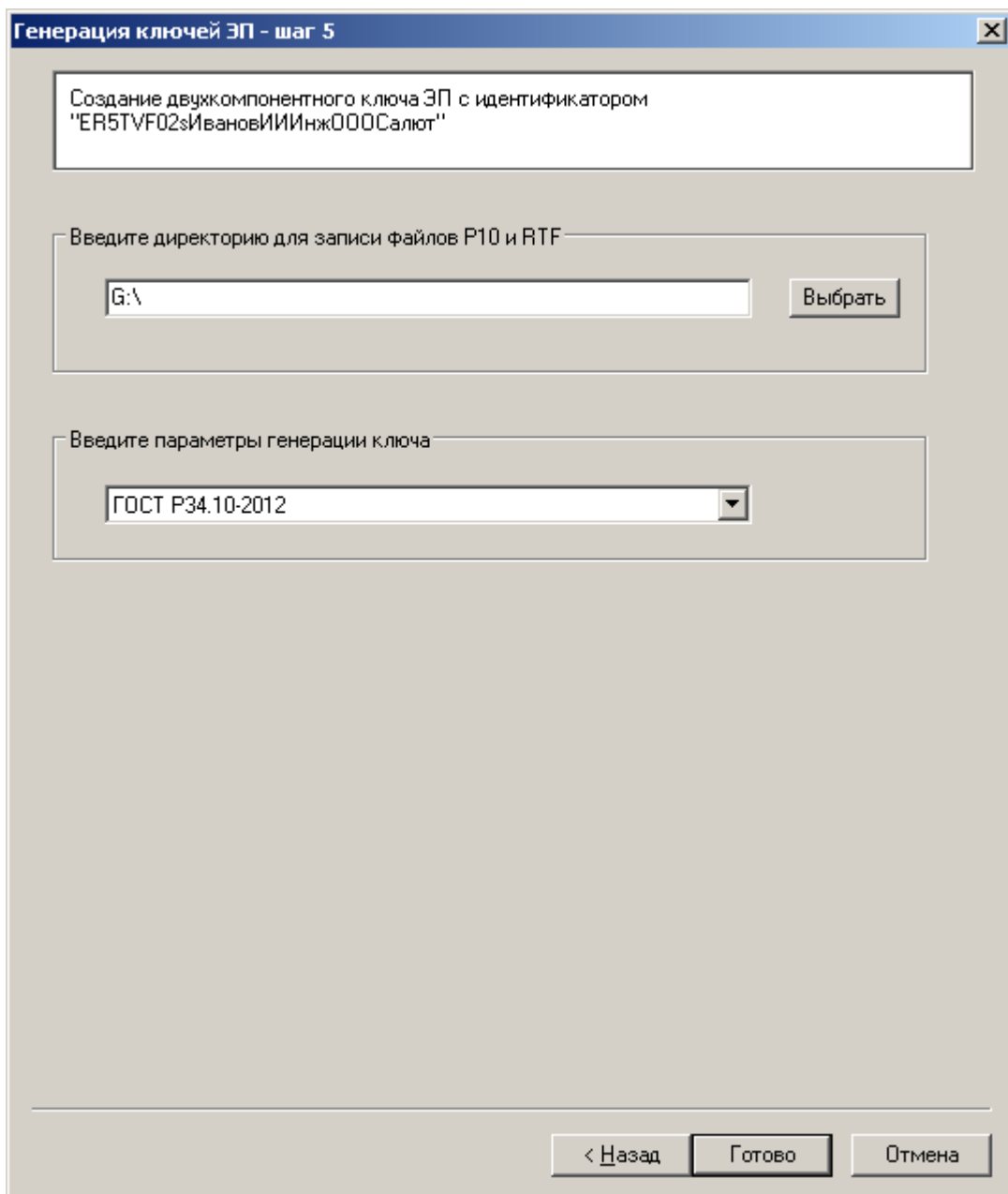


Рисунок 4 – Мастер генерации ключей ЭП – шаг 5

На шаге 5 в разделе «Введите директорию для записи P10 и RTF», нажав на кнопку «Выбрать», выберите каталог или введите его вручную в английской раскладке непосредственно в поле ввода и выберите формат, в котором он будет сохранён (см. Рисунок 4). В зависимости от выбранного на шаге 2 типа запроса на шаге 5 будет предложено сгенерировать запрос на неквалифицированный или квалифицированный сертификат. Файл с запросом сохранится в виде файла в указанной Вами папке на жёстком диске или флэш-накопителе. Данный файл предназначен для передачи Вами в Удостоверяющий Центр ПАО Сбербанк для выпуска неквалифицированного сертификата. После нажатия кнопки «Готово» при отсутствии на вашем съёмном носителе ключа датчика случайных чисел (ДСЧ) может быть инициирована процедура его создания. Нажимайте кнопку «ОК» для продолжения.

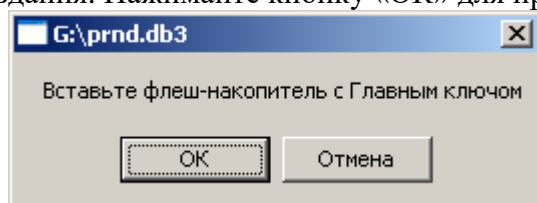


Рисунок 5 – Диалог создания ключа ДСЧ – 1



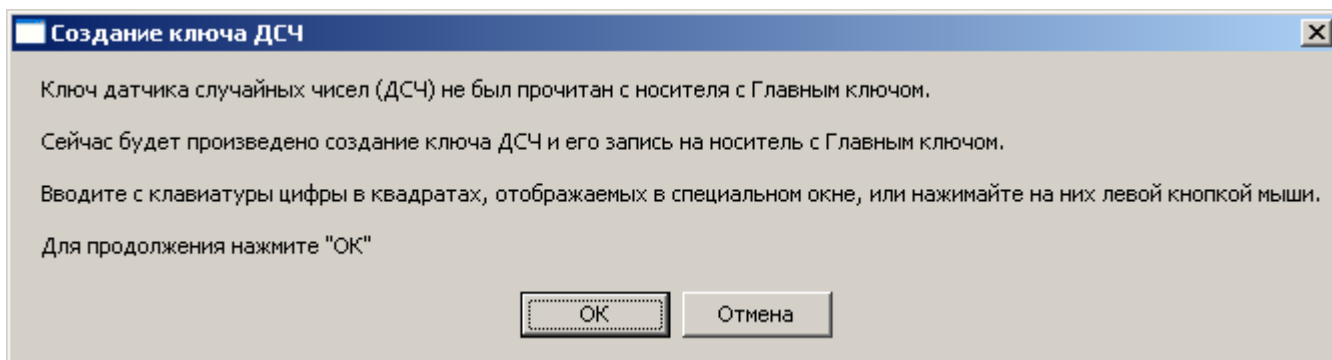


Рисунок 6 – Диалог создания ключа ДСЧ – 2

Для генерации ключа ДСЧ следует выполнить ввод цифр в квадратах, отображаемых в специальном прямоугольном окне (см. Рисунок 7), при помощи клавиатуры или нажатия на них левой кнопки мыши (приблизительно 32 нажатия для 32 – хразрядных систем и 64 нажатия для 64 – хразрядных систем). По окончании операции ключ ДСЧ будет записан на флэш – накопитель.

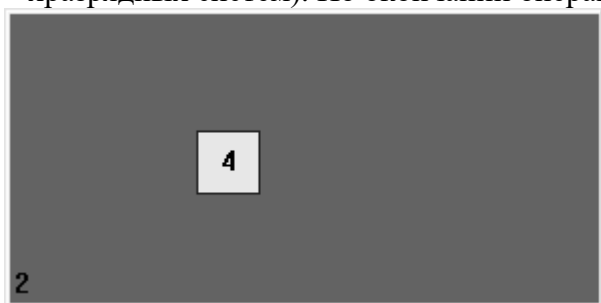


Рисунок 7 – Экран генерации ключа датчика случайных чисел (ДСЧ)

После окончания процедуры создания ключей ЭП нажмите на кнопку «ОК» в появившемся окне (см. Рисунок 8).

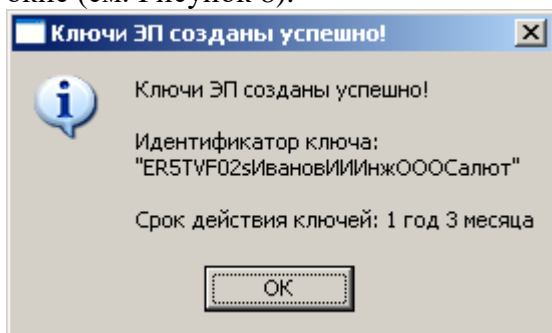


Рисунок 8 – Сообщение о создании ключей ЭП

В открывшемся окне MS Word Вы увидите проект распечатки заявления на выпуск невалифицированного (в зависимости от выбранного типа запроса на шаге 2) сертификата.

Далее этот файл должен быть распечатан в одном экземпляре, заверен соответствующими подписями, оттиском печати и передан вместе с файлом запроса (\*.p10) на выпуск сертификата в функциональное подразделение ПАО Сбербанк, заключившее с Вашей организацией договор об ЭДО. Для заявления на выпуск квалифицированного сертификата предусмотрена возможность ручного указания адреса электронной почты или мобильного телефона для регистрации заявителя в Единой системе аутентификации и идентификации (в соответствии с 33-ФЗ от 12.03.2014г.).

Если Вам необходимо сформировать несколько комплектов ключей ЭП, то для каждого комплекта Вам предстоит повторить весь процесс с момента запуска мастера генерации ключей.

## 2 Использование ключей электронной подписи

Передача подписанных ЭП электронных документов целесообразна только после получения от ПАО Сбербанк невалифицированного/квалифицированного сертификата, выпущенного на основе Вашего запроса, с отметками и печатью Удостоверяющего центра. Этот документ, в соответствии с Федеральным законом об ЭП, является для Вас гарантом того, что

Банком, в рамках договора, должны будут исполняться только поручения, подписанные ЭП, сформированной с помощью парного закрытого ключа. Со стороны Банка этот документ – гарант Вашей неотрекаемости от документа с Вашей ЭП.

Ваши ключи ЭП вступят в силу после изготовления Удостоверяющим центром электронного сертификата ключа ЭП и его регистрации в соответствующей криптосети ПАО Сбербанк.

Возможность использования Ваших новых ключей ЭП подтверждается электронным бюллетенем Удостоверяющего центра, который будет направлен Вам напрямую либо передан через функциональное подразделение ПАО Сбербанк, заключившее с Вашей организацией договор об ЭДО. Это же подразделение предоставит Вам распечатки сертификатов ключей ЭП с подписью и печатью ПАО Сбербанк.

## 2.1 Замена ключей ЭП

Срок действия Вашего ключа ЭП указан в сертификате ключа проверки ЭП, выданного Удостоверяющим центром и, как правило, не превышает одного года и трех месяцев. По истечении этого срока ключи ЭП подлежат выводу из действия. Для обеспечения непрерывности ЭДО Вам следует заблаговременно провести процедуру замены ключей ЭП.

Процедура замены ключей ЭП включает в себя все операции, изложенные в первых двух разделах настоящего документа.



00000-00000-00000-00000-13112-12855-12338-14134

**В УДОСТОВЕРЯЮЩИЙ ЦЕНТР ПАО СБЕРБАНК**  
**ЗАЯВЛЕНИЕ НА ИЗГОТОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ\***

Прошу изготовить неквалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными:

Данные заявителя				
C=SubstStrana, CN=SubstCN, O=SubstOrganizatsija, TITLE=SubstDolzhnost, EMAIL=SubstEmail, SERIALNUMBER=SubstSerialNumber, SN=SubstFamiliya, GN=SubstImyaOtchestvo				
Данные организации:	ИНН:	SubstINN	ОГРН (ОГРНИП):	SubstOGRN

Сведения о ключе проверки электронной подписи	
Значение:	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
Идентификатор:	SubstIdentifier
Используемый алгоритм:	Хэш - ГОСТ Р SubstHash, ЭП - ГОСТ Р SubstGost
Используемое средство электронной подписи:	Бикрипт 5.0

	Прошу предоставить копию сертификата ключа проверки электронной подписи в бумажной форме
--	--

**Заявитель (уполномоченный представитель):**

***Подпись и полномочия уполномоченного  
представителя удостоверяю***

\_\_\_\_\_  
Подпись

\_\_\_\_\_  
ФИО

\_\_\_\_\_  
Подпись Руководителя

\_\_\_\_\_  
ФИО Руководителя

МП

\* В заявлении используются понятия определенные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»



00000-00000-00000-00000-13112-12855-12338-14134

**В УДОСТОВЕРЯЮЩИЙ ЦЕНТР ПАО СБЕРБАНК****ЗАЯВЛЕНИЕ НА ИЗГОТОВЛЕНИЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ\***

Прошу изготовить квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными:

Данные заявителя				
C=RU, CN=SubstCN, ST=SubstRegion, L=SubstNaselennyiPunkt, O=SubstOrganizatsija, INN=SubstINN, STREET=SubstAddress, OGRN=SubstOGRN, OU=SubstPodrazdelenie, TITLE=SubstDolzhnost, SN=SubstFamiliya, GN=SubstImyaOtchestvo, SNILS=SubstSNILS, EMAIL=SubstEmail				
Данные организации:	ИНН:	SubstINN	ОГРН (ОГРНИП):	SubstOGRN

Сведения о ключе проверки электронной подписи	
Значение:	12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
Идентификатор:	SubstIdentifier
Используемый алгоритм:	Хэш - ГОСТ Р SubstHash, ЭП - ГОСТ Р SubstGost
Используемое средство электронной подписи:	Бикрипт 5.0
Прошу предоставить копию сертификата ключа проверки электронной подписи в бумажной форме	

Реквизиты документа удостоверяющего личность:	Вид документа:	
	Серия:	Номер:
	Дата выдачи:	
	Наименование органа выдавшего документ:	Код подразделения:
Реквизиты документа о полномочиях:	Название документа:	
	Номер:	Дата:
Прошу зарегистрировать заявителя в ЕСИА (в соответствии с 33-ФЗ от 12.03.2014г.) Способ доставки пароля (один из):		
На адрес электронной почты:		
На номер мобильного телефона:		

Настоящим подтверждаю, что приведенные в настоящем Заявлении сведения являются достоверными, указаны правильно, мною также представлены документы подтверждающие сведения указанные в заявлении или их надлежащим образом заверенные копии.

Настоящим \_\_\_\_\_

(ФИО заявителя/уполномоченного представителя юридического лица данные, которого вносятся в сертификат)

**Заявитель (уполномоченный представитель):**

\_\_\_\_\_  
Подпись

\_\_\_\_\_  
ФИО

**Подпись и полномочия уполномоченного представителя удостоверяю**

\_\_\_\_\_  
Подпись Руководителя

\_\_\_\_\_  
ФИО Руководителя

МП

\* В заявлении используются понятия определенные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»

