Инструкция

по изготовлению ключевой информации с использованием средства криптографической защиты информации «Модуль генерации ключей - 3» В настоящем документе описана процедура по изготовлению ключевой информации с использованием средства криптографической защиты информации «Модуль генерации ключей - 3».

Содержание

Об	означения и сокращения	.4
Tej	рмины и определения	.5
1.	Общие сведения	.6
2.	Установка СКЗИ «МГК-3»	.6
3	Настройка СКЗИ «МГК-3»	.8
4.	Изготовление ключевой информации	.10
5.	Распечатка запроса на выдачу сертификата	.14

Обозначения и сокращения

Сокращение	Расшифровка сокращения
МГК	Модуль генерации ключей
ОМНИ	Отчуждаемый машинный носитель информации
ПЭВМ	Персональная электронно-вычислительная машина
СКЗИ	Средство криптографической защиты информации
ТШ КБР	Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России
УЦ	Управляющий центр на базе СКЗИ «СКАД Сигнатура»

Термины и определения

Термин	Определение
Ключевая информация	Закрытые и открытые ключи, ключи шифрования, ключи ЭП, сертификаты ключей и другая вспомогательная технологическая информация, необходимая для обеспечения процессов изготовления, эксплуатации и управления криптографическими ключами

1. Общие сведения

В настоящем документе приведено описание генерации закрытого ключа и запроса на получение сертификата с использованием средства криптографической защиты информации «Модуль генерации ключей - 3». СКЗИ «МГК-3» распространяется Банком России совместно с СКЗИ «DiSec-W».

Клиент Банка России руководствуется нормативными документами Банка России и эксплуатационной документацией на СКЗИ при работе с ключевой информацией.

2. Установка СКЗИ «МГК-3»

Установка СКЗИ «Модуль генерации ключей «МГК-3»» выполняется на отдельную ПЭВМ, соответствующую требованиям документа «Правила пользования» из состава дистрибутивного комплекта СКЗИ «МГК-3».

Для инсталляции СКЗИ «МГК-3» пользователь должен обладать правами администратора OC Windows.

Установка СКЗИ «МГК-3» осуществляется путем запуска файла инсталляции ...\КС1-2\setup.exe, находящегося на установочном диске из состава дистрибутивного пакета.

В ходе установки инсталлятор потребует повышение прав, необходимо нажать «ОК».

Для продолжения установки нажать «Далее».



Путь установки, не изменять. Для продолжения установки нажать «Далее».



Для продолжения установки необходимо нажать «Далее».



Для продолжения установки нажать «Установить».

Всё готово к установке Программа установки готова начать установку Модуль генера на ваш компьютер.	ации ключей	
Нажмите «Установить», чтобы продолжить, или «Назад», есл просмотреть или изменить опции установки.	и вы хотите	
Папка установки: C:\Program Files (x86)\Factor-TS\Request3		*
Папка в меню «Пуск»: FACTOR Applications\Модуль генерации ключей 3.0		
4	4	Ŧ

Для продолжения установки нажать «Завершить».

👸 Установка — Модуль гене	рации ключей
	Завершение Мастера установки Модуль генерации ключей
	Программа Модуль генерации ключей установлена на ваш компьютер. Приложение можно запустить с помощью соответствующего значка.
ФАКТОР	Нажмите «Завершить», чтобы выйти из программы установки.
	I Запустить checkwin.exe
	Завершить

Если программа установилась корректно, в окне «Проверка целостности по списку» будет выдано уведомление «Контрольные суммы проверены успешно».

Установка СКЗИ «МГК-3» выполнена. Для завершения необходимо закрыть окно нажав красный крест в верхнем правом углу.



Если будет обнаружено несовпадение, то программа укажет файл, для которого имеет место ошибка контрольной суммы. В этом случае требуется обязательная замена программного обеспечения.

3 Настройка СКЗИ «МГК-3»

Первый запуск СКЗИ «МГК-3» должен выполняться от имени администратора.

Нажать правой кнопкой мыши по ярлыку и выбрать «Запуск от имени администратора».

Моду генера ключе	Открыть Расположение файла	
	🟫 TortoiseSVN	>
	😌 Запуск от имени администратора	

После запуска программы на экран будет выведено главное окно «Модуль генерации ключей» с формой, содержащей поля, необходимые для заполнения при формировании ключей и запросов на сертификаты.

Информация о владельце:	(Ch)	
Общее имя (CN):	Фамилия (SN):	Имя и отчество (GN):
Наименование населённого пункта (L):	Наименование организации (0):	Наименование субъекта РФ (S):
Подразделение организации (OU):	I Накиченование страны (С): RU	Должность(Т):
Адрес электронной почты (Е):	Agpec (ST):	1 2 1
Формирование запроса на квалифи инн:	цированный сертификат ЭП ОГРН:	снилс:
Формарование запроса на квалинии	шрованный сертификат 3П ОГРН: Параметры квалифицированного сертификата	
Перанитри Инно- Паранитри Использование лочис С Палко аП С 31 и шифореание	шорованный сертноника 30 ОГРН: Паранитры казаничицированного сертнониката	сияло
Прочетры ИНИ. Парачетры Исплазование клона Спольз 30 г. С 31 г. шинрование Парачетры клона Р ПОС Г > 310 2012 (256) (ние файо загрос)	исроевный сертиника ЭП ОГРН: Паранитры казаничированног сертиника а	сийлас Илучшотный клох С гост Р 3410/2012 (512

Нажать на кнопку «Улучшенный ключ». После этого откроется дополнительное окно.

ібщее имя (CN)): bridtfeneder	Фамилия	a (SN):	Имя и от	чество (GN):	
аименование	населённого пункта (L):	Наимено	вание организации (О):	Наимено	вание субъекта	PΦ (S):
одразделение	организации (ОU):	Hаимено RU	вание страны (С):	Должнос	ть(Т):	_
дрес электр	Выбор параметров	Same 2		-	×	
[Иня					
валифициро	Электронная почта		1.3.6.1.5.5.7.3.4			
	IPSec		1.3.6.1.5.5.8.2.2		=	
Формиров	Цифровые права		1.3.6.1.4.1.311.10.5.1			
HHS	ІКЕ-посредник IP-без	пасности	1.3.6.1.5.5.8.2.2			
	Агент восстановлени	я ключеи	1.3.6.1.4.1.311.21.6			
	Агент запроса сертис	MKata	136141311215			
	Аудит TLS трафика	101040	1.2.643.2.2.34.1			NY.
1	Бессрочная подписка		1.3.6.1.4.1.311.10.3.13		*	~
араметры: - спользован	Добавить Уда	лить		ок	Cancel	
Только ЭП	С ЭП и шифрование	-	_	< -	Элучшенный к	люч
араметры клю ГОСТ Р.3410	ича I-2012 (256)	5			C FOCT P.	3410-2012 (512)
мы файла запр	ioca.					

Нажать кнопку «Добавить».

Общее имя (CN)		Фамилия (SN):	Имя и отчеств	o (GN):	
 Наименование н	населённого пункта (L):	 Наименование организации (0):	Наименование	субъекта РФ (S)	
Подразделение	организации (OU):	 Наименование страны (С): RU	Должность(Т):		
Адрес электр	выбор параметров	Same (P)		23	
Квалифициро Формиров ИНН: Параметры –	Иня ОЛО Электронная ПРЗес Цифровые пр. Ист-посредновые пр. Ист-по	Remue OID:		E	X
Использован С Только ЭП (Параметры клю С ГОСТ Р.3410 Имя файла запр	С ЭП и шифрование ча -2012 (256) оса:	200	9ny C	шенный ключ ГОСТ Р.3410-20	12(
0			- Ch- 111	1	

Заполнить поля OID следующими значениями:

Название (Имя)	Значение OID
Базовый идентификатор расширенной области	1.3.6.1.4.1.10244.7.1.1.32
применения ключа	
Авторизация Клиентов	1.3.6.1.4.1.10244.7.1.1.32.3
Авторизация АРМ КПКИ	1.3.6.1.4.1.10244.7.1.1.32.5
для Информационно-аналитических и статистических	1.3.6.1.4.1.3670.4.20.7
систем Банка России	
ІКЕ-посредник IР-безопасности	1.3.6.1.5.5.8.2.2

Эбщее имя (CN):	nate note	Фамилия (SN):	Имя и отч	ество (GN):	
Чаименование н	аселённого пункта (L):	наименование организации (0):	Наименов	ание субъекта РФ	P (S):
Тодразделение (организации (OU):	 Наименование страны (С): RU	Должност	ь(Т):	
Адрес электрон	Выбор параметров			×	1
Квалифицирова Формирова ИНН: Параметры: —	Иня ОІD Подписывание Подписькорнея Подпись корнея Подпись ответа Полтовая релли Проверка подли Проверка серея Установка шта Добавить Уда	зание: атор расширенной области применения нение OID: 6.6.1.4.1.10244.7.1.1.32 ОК Cancel		Cancel	A N
1спользование О Только ЭП (Опоча. О ЭП и шифрование			Улучшенный клю	4
Тараметры ключ • ГОСТ Р.3410- 1мя файла запро	Ha 2012 (256) Soca:	201		C FOCT P.341	0-2012 (51:
0	Crouppurper		D. 1102		

По окончании добавления всех OID необходимо убедиться, что добавление OID выполнено успешно.

Имя	OID		_ ^
Пользователь IP-без	1.3.6.1.5.5.7.3.7		
Почтовая репликаци	1.3.6.1.4.1.311.21.19		
Проверка подлиннос	1.3.6.1.5.5.7.3.2		
Проверка подлиннос	1.3.6.1.5.5.7.3.1		
Проверка сервера л	1.3.6.1.4.1.311.10.6.2		
Установка штампа в	1.3.6.1.5.5.7.3.8		
Базовый идентифик	1.3.6.1.4.1.10244.7.1.1.32		
Авторизация Клиентов	1.3.6.1.4.1.10244.7.1.1.32.3		
для Информационно	1.3.6.1.4.1.3670.4.20.7		~

Дополнительные OID добавлены. Нажать кнопку «Cancel».

4. Изготовление ключевой информации

i.

В качестве ключевого носителя для хранения закрытого ключа допускается применять любой носитель, разрешенный к использованию в соответствии с эксплуатационной документацией на СКЗИ «МГК-3».

Для генерации закрытого ключа и запроса на получение сертификата, требуется заполнить поля согласно данным, полученным из Банка России. Пример заполнения полей приведен ниже.

10

Общее имя (CN):	Фамилия (SN):	Имя и отчество (GN):
CLN-4452512300001		
Наименование населённого пункта (L):	Наименование организации (0):	Наименование субъекта РФ (S):
KSTSHKBR	CLIENT-TEST	
Подразделение организации (ОU): 4525123000	Наименование страны (С):	Должность(T):
Адрес электронной почты (Е):	Appec (ST):	1 1 1
4525123000@kpki.cbrgate.ru	45	
Квалифицированный сертификат ЭЦ Формирование запроса на квалифи ИНИ:	цированный сертификат ЭП ОГРЯ:	снилс:
Чеалифицированный сертификат ЭШ Формирование запроса на квалифи ИНИ:	сированый сертификат ЭП ОГРН: Параметры квалифицированного сертификата	снилс:
Свалифицированный сертификат 311 Формирование запроса на квалифи ини: Параметры: Спользование ключа: Только 31 € 311 и диеоорание	цированый сертификат ЭП ОГРН: Параметры квалифицированного сертификата	Улучшенный ключ
Челифицирование запроса на квалифи Формирование запроса на квалифи ини Параметры: Колољзование клоча: С только ЭП € ЭП и шифрование Параметры клоча © ГОСТ Р.3410-2012 (256) Мия файла запроса: Вараметры с	цированный сертификат ЭП ОГРЯ: Параметры квалифицированного сертификата	СНИЛС: Улучшенный ключ С гост Р.3410-2012 [51.
Квалифицирование запроса на квалифи Формирование запроса на квалифи инн Параметры: Коловъзование клоча: Только ЭП (© ЭП и шифрование Параметры клоча © ГОСТ Р. 3410-2012 (256) Мия файла запроса: C:VCLN-4452512300001.req	цированный сертификат ЭП ОГРЯ: Параметры квалифицированного сертификата	СНИЛС: Улучшенный ключ С гост Р.3410-2012 (51:

В поле «Использование ключа» выбрать «ЭП и Шифрование».

Нажать _____ и указать место сохранения расположение файла запрос.

Нажать на кнопку «Улучшенный ключ» и с помощью зажатой кнопки «CTRL» и левой кнопки мыши выбрать следующие пять OID и нажать «OK»:

Название (Имя)	Значение OID
Базовый идентификатор расширенной области	1.3.6.1.4.1.10244.7.1.1.32
применения ключа	
Авторизация Клиентов	1.3.6.1.4.1.10244.7.1.1.32.3
Авторизация АРМ КПКИ	1.3.6.1.4.1.10244.7.1.1.32.5
для Информационно-аналитических и статистических	1.3.6.1.4.1.3670.4.20.7
систем Банка России	
ІКЕ-посредник IР-безопасности	1.3.6.1.5.5.8.2.2

Выбор параметров			×
Имя		OID	^
Электронная почта		1.3.6.1.5.5.7.3.4	
IPSec		1.3.6.1.5.5.8.2.2	
Цифровые права		1.3.6.1.4.1.311.10.5.1	
ІКЕ-посредник IP-безопа	асности	1.3.6.1.5.5.8.2.2	
Агент восстановления к	лючей	1.3.6.1.4.1.311.21.6	
Агент запроса сертифик	ката	1.3.6.1.4.1.311.20.2.1	
Архивация закрытого к	люча	1.3.6.1.4.1.311.21.5	
Аудит TLS трафика		1.2.643.2.2.34.1	×
<			>
Добавить Удали	ить	ОК	Cancel

11

Имя	OID		^
Пользователь ІР-без	1.3.6.1.5.5.7.3.7		
Почтовая репликаци	1.3.6.1.4.1.311.21.19		
Проверка подлиннос	1.3.6.1.5.5.7.3.2		
Проверка подлиннос	1.3.6.1.5.5.7.3.1		
Проверка сервера л	1.3.6.1.4.1.311.10.6.2		
Установка штампа в	1.3.6.1.5.5.7.3.8		
Базовый идентифик	1.3.6.1.4.1.10244.7.1.1.32		
Авторизация Клиентов	1.3.6.1.4.1.10244.7.1.1.32.3		
для Информационно	1.3.6.1.4.1.3670.4.20.7		¥

Нажать кнопку «Сгенерировать запрос». После нажатия появится генератор датчика случайных чисел (ДСЧ), где следует с максимальной амплитудой водить мышкой от края до края монитора для его заполнения.

Процедура инициализации ДСЧ
Для прохождения процедуры инициализации подвигайте мышкой с максимальной амплитудой.
Выполнено: 0%

Сообщение	
1	Инициализация выполнена!
	ОК

Следует указать ОМНИ, на который будет выполнена загрузка закрытого ключа.

При использовании в качестве ключевого носителя USB-flash выбрать носитель для сохранения закрытого ключа, нажать кнопку «Выбрать».

Выберите носитель	-	X
Выберите съемный носител	ь для генерации закрытого) ключа:
Носитель	Метка тома	Серийный номер
D:V	Нет метки	18de1179
1		
Выбрать Повтор		Отмена

Будет предложено вести пароль для закрытого ключа.

ВНИМАНИЕ! Поле «Пароль» необходимо оставить пустым и нажать кнопку «ОК».

я ключевого носителя

При использовании в качестве ключевого носителя Rutoken (полный перечень разрешенных ключевых носителей приведён в документации на СКЗИ «DiSec-W») выбрать носитель для сохранения закрытого ключа, нажать кнопку «Выбрать».

Носитель	Метка тома	Серийный	номер
D:N	Нет метки	18de1179	-
Aktiv Rutoken ECP 0	Rutoken ECP <n< th=""><th>o label></th><th>3cde8127</th></n<>	o label>	3cde8127

После этого будет предложено вести пароль для Rutoken. После ввода пароля следует нажать кнопку «Ок».



По окончании будет выдано сообщение об успешном завершении.

Вниман	/e	×
0	Запрос успешно сформиров С:\CLN-4452512300001.req	ан и сохранен в файле:
		ОК

По окончании на съемном носителе будут лежать 3 файла, где:

- Файл с расширением *.nam — это отпечаток работы программы МГК;

- Файл с расширением *. p15 это закрытый ключ;
- Файл с расширением *.req это запрос на выдачу сертификата.

О Компьютер Компьютер Съемный,	ииск (D:)		▼ 49	Поиск: Съемнь	ій д 🔎
Упорядочить 🔻 Общий доступ 🔻	Новая папка			!≡ ▼ [1 🕡
🔺 🔆 Избранное	Имя	Дата изм	енения	Тип	Разме
〕 Загрузки	1b364f1f.nam	08.10.202	21 0:26	Файл "NAM"	
🕮 Недавние места	1b364f1f.p15	08.10.202	1 0:26	Файл "Р15"	
📃 Рабочий стол	Cln-45222222200.req	08.10.202	21 0:26	Файл "REQ"	
🔏 OneDrive					
и 词 Библиотеки					
PowerShell Scripts					
Видео					
Документы					
🔚 Изображения					
🛛 👌 Музыка					
🛯 🖳 Компьютер					
Мальный диск (С:)					
Съемный диск (D:)					

Далее файл с расширением *.req необходимо отправить в регистрационный центр Банка

России.

После генерации запроса на выдачу сертификата с помощью СКЗИ «МГК-3» файл *.req

будет иметь следующее:

Subject:
E=cln-45222222200@kpki.cbrgate.ru
OU=4522222222
O=CLIENT-TEST
STREET=45
L=KSTSHKBR
C=RU
CN=CLN-45222222200
Enhanced Key Usage
IP security IKE intermediate (1.3.6.1.5.5.8.2.2)
Unknown Key Usage (1.3.6.1.4.1.3670.4.20.7)
Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32)
Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32.1)

ВНИМАНИЕ! Поле ST в СКЗИ «МГК-3» в файле *.req будет иметь поле STREET.

5. Распечатка запроса на выдачу сертификата

Для распечатки запроса необходимо выполнить следующее:

- 1) Открыть командную строчку с помощью команды cmd;
- 2) Набрать команду C:\>certutil.exe <имя запроса>.req >>

 %USERPROFILE%\Desktop\<имя запроса>.txt

Для примера команда может выглядеть следующим образом:

 $C:\certutil.exe CLN-4452512300001.req >> %USERPROFILE%\Desktop\ CLN-4452512300001.txt.$

После выполнения команды на рабочем столе будет создан файл CLN-4452512300001.txt.

 Содержимое файла CLN-4452512300001.txt использовать для оформления распечатки запроса на выдачу сертификата. Пример запроса на выпуск сертификата ключа проверки электронной подписи

PKCS10 Certificate Request: Version: 1 Subject: E=cln-4525555000@kpki.cbrgate.ru OU=4525555000 O=CLIENT-TEST STREET=45 L=KSTSHKBR C=RU CN=CLN-452555500002 Name Hash(sha1): 9e8ecf78626ae864f52802c43c785d89bf698b76 Name Hash(md5): 91d38b6b9b7bbb556d94e07a36f50b84 Public Key Algorithm: Algorithm ObjectId: 1.2.643.7.1.1.1.1 Algorithm Parameters: 0000 30 13 06 07 2a 85 03 02 02 23 01 06 08 2a 85 03 0010 07 01 01 02 02 1.2.643.2.2.35.1 1.2.643.7.1.1.2.2 Public Key Length: 0 bits Public Key: UnusedBits = 00000 04 40 38 b9 81 d1 7a 23 30 61 f0 a8 3c 21 dc 4c 0010 ba 90 31 62 d2 16 d4 ff 87 58 3d d2 b1 51 4c 88 0020 ff 11 2c c5 2d 86 72 54 12 7c e9 55 a1 ee 13 bf 0030 44 99 14 71 34 bb a5 c6 9b 9f 78 bd 5a f7 51 bb 0040 6f da Request Attributes: 1 1 attributes: Attribute[0]: 1.3.6.1.4.1.311.2.1.14 (Certificate Extensions) Value[0][0], Length = 41Certificate Extensions: 2 2.5.29.15: Flags = 1(Critical), Length = 4 Key Usage Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0) 2.5.29.37: Flags = 0, Length = 26 Enhanced Key Usage IP security IKE intermediate (1.3.6.1.5.5.8.2.2) Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32) Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32.3) Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32.5) Unknown Key Usage (1.3.6.1.4.1.3670.4.20.7) Signature Algorithm: Algorithm ObjectId: 1.2.643.7.1.1.3.2 Algorithm Parameters: 05 00 Signature: UnusedBits=0 0000 cc d5 f2 b6 bd b0 2d 9d d4 d1 8c bc fd 6d 33 f1 0010 03 3f 44 da 44 98 2d e6 29 54 5f 58 79 73 14 75 0020 8f da 73 fa ab 5e b7 80 72 59 fe bc 02 8a 48 e6 0030 65 ff 33 8e 17 26 08 d3 1d 1c cb 50 f0 2d c7 f9 Signature does not match Public key: 80070032

Ответственный за ключ:		/	_ /
Руководитель организации/центра _	/	/	/
или его заместитель			
М.П.			