# Руководство оператора СКЗИ «MS\_KEY K» - «АНГАРА» Исп.8.х.х. с поддержкой технологии ISBC ESMART

Создание запросов и запись сертификатов ЭП для ЕГАИС с помощью ESMART PKI Client





V 1.2 ООО «НТЦ Альфа-Проект» 2018г.

Сайт: <u>www.angara.cards</u>

## Список терминов и сокращений

Термин	Описание					
MS_KEY ESMART AHFAPA	СКЗИ «MS_KEY К» - «АНГАРА» Исп.8.х.х с поддержкой					
	технологии ISBC ESMART					
ЕГАИС	Единая государственная автоматизированная					
	информационная система					
ЭП	Электронная подпись					
КЭП	Квалифицированная электронная подпись					
Электронный идентификатор, крипто-ключ,	СКЗИ «MS_KEY К» - «АНГАРА»					
программно-аппаратный криптопровайдер						
ПО	Программное обеспечение, ESMART PKI Client					
00	Операционная система					

# Введение

**MS\_KEY ESMART АНГАРА** объединил в себе СКЗИ «MS\_KEY K» - «АНГАРА» и технологию ISBC ESMART. Это устройство имеет широкую область применения, что позволяет использовать его в таких системах, как: ЕГАИС, КриптоПро и других системах защиты информации. Поддерживает интерфейсы APDU/PKCS#11. Более подробное описание смотрите в эксплуатационной документации.

В данной инструкции описывается процесс генерации с помощью приложения ESMART PKI Client ключевой пары ГОСТ 34.10-2001, создание запроса сертификата на основе этой ключевой пары и запись сертификата ЭП на ключевой носитель MS\_KEY ESMART АНГАРА.

# Этапы загрузки КЭП на программно-аппаратный криптопровайдер.

## 1. Установка ПО и авторизация на MS\_KEY ESMART АНГАРА

- Установите приложение ESMART PKI Client актуальной версии. После скачивания архива извлеките содержимое в папку. Выберите установочный файл: setup.exe (для 32-х разрядной (OC) или setup.x64.exe (для 64-х разрядной OC). Далее следуйте подсказкам программы-инсталлятора. Перезагрузите компьютер, если появится соответствующее сообщение.
- Запустите приложение ESMART PKI Client. Для этого в трее (область в правом углу панели задач (Рис.1) разверните окно программы, нажав один раз по иконке программы левой кнопкой мыши. Для удобства запуска можно создать ярлык и поместить его на Рабочий стол. Если свернуть окно приложения, приложение не выключается, а сворачивается в трей.





• **Подключите электронный идентификатор.** В главном окне программы появится информация об устройстве (Рис. 2).

Токен         Данные         Кинтейнеры         Ключи         Серпификаты         Утилиты         Журнал           ISBC ESMART Token 0	ESMART PKI Client 4.4.1	• PKI Client	0					-	×
ISBC ESMART Token 0         Ридер         Ридер           ID солог PKCS#11         5           Название         ISBC ESMART Token 0           Token         000117780000003A           Название         ESMART Token 0           Token         000117780000003A           Название         ESMART Token MS_KEY           Производитель         ISBC           Масель пар. системы         0.0           Версия пер. Пончальная длина РПКхода         4           Максимальная Дина РПКхода         8		Токен	Данные	Контейнеры	Ключи	Сертификаты	Утилиты	Журнал	\$ <u></u>
ISBC ESMART Token 0         Ридер           ID cnora PKCS#11         5           Название         ISBC ESMART Token 0           Токен         -           Серийный номер         0001177B0000003A           Название         ESMART Token MS_KEY           Производитель         ISBC           Версия опер. системы         0.0           Версия пор. системы         0.0           Объек памяли         72K           Максимальное количество сессий         10           Минимальная длина PINkoga         8		Авторизоваться	Инициализировать т	окен Сменить РІМ	I-код Разблокир	ровать PIN-код			
Версия разметки 2.1 Проемиљ Default 1.0 Число польток ввода PIN-кода 10 Число польток ввода SO PIN-кода 10	ISBC ESMART Token 0	Ридер ID слота РКС5#11 Название Токен Серийный номер Название Производитель Модель Версия опер. системы Версия опер. системы Версия опер. системы Версия процияки Объем памяти Макцимальнов количеств Минимальная длина PIN- Макцимальная длина PIN- Макцимальная длина PIN- Версия разметки Профиль Число полыток ввода SO	ю сессий кода Нкода РЮ-кода	5 ISBC ESMART T 0001177800000 ESMART Token ISBC ESMARTToken 0.0 0.0 72K 10 4 8 2.1 Default 1.0 10 10	oken 0 J3A MS_KEY ISKEY				

Рис. 2

Пройдите авторизацию. Чтобы зарегистрироваться на электронном идентификаторе, нажмите «Авторизоваться» на верхней панели (Рис.З а). В открывшемся окне введите восьмизначный PIN-код пользователя (Рис. 3 б).

По умолчанию ПИН-код пользователя: 12345678. Для интеллектуальных карт и USB-ключей MS\_KEY ESMART АНГАРА также могут использоваться алфавитные и служебные символы. Оптимально, надежный пароль должен содержать символы минимум 3 типов, например, заглавные и строчные буквы и цифры, или буквы, цифры и служебные символы. Благодаря аппаратной защите PIN-код может быть проще, т.к. электронный идентификатор защищен от подбора пароля методом перебора. После того как несколько раз был введен неверный пароль, носитель блокируется. Получить доступ к хранящимся на заблокированном носителе ключам, данным и сертификатам невозможно. Разблокировать криптопровайдер может администратор, который предъявляет SO PIN.

После авторизации на карте откроется доступ к защищенным объектам, появится возможность создавать, импортировать и удалять объекты.



Авторизация			×
Введите PI	N	••	]
	ОК	Отмена	]
Рис. 3 б			_





## 2. Генерация ключевой пары

• Сгенерируйте ключевую пару. Для этого перейдите во вкладку «Ключи», выберите пункт «Сгенерировать ключевую пару». В открывшемся окне выберите тип ключевой пары ГОСТ 34.10-2001. Нажмите кнопку «ОК» (Рис. 4).

Токен	Данные	Контейнер	ы	Ключи	Сертификаты
🔒 Выйти Обн	ювить <mark>С</mark> охранить	ключ Сгенери	ровать ключ	Сгенерирова	ать ключевую пар
	Генер	ация ключевой п	ары	×	
	Тип	ключевой пары	FOCT 34.10	~	
	Pas	мер ключа (бит)	512	~	
		Параметры ГОСТ			
			ОК	Отмена	

Рис. 4

• На основе созданной ключевой пары сформируйте запрос сертификата и сохранить его. Выберите нажатием левой клавиши мыши ключевую пару ГОСТ 34.10-2001. В окне появятся дополнительные функции. Нажмите на пункт: «Запрос сертификата» (Рис. 5 а).

Токен		Данные	Контейнеры	Ключи	Сертификаты
Выйти Запрос сер	Обновить гификата	Сохранить к	люч Сгенерир	овать ключ Сген	ерировать ключевую пару
📴 🗞 Ki	ючевая пара Г	OCT 34.10 ∉10f	a989-7e98-409a-a6c	le-0e7f675d086e)	

Рис. 5 а

При нажатии на символ «+» (Рис. 5 а), Вы можете просмотреть дополнительную информацию о ключевой паре (Рис. 5 б).



Рис. 5 б



### 3. Формирование запроса на сертификат ЭП

- Создайте запрос сертификата и сохраните его в файле. Заполните форму (Рис. 6 а):
  - укажите актуальные данные;
  - в пункте «Расширения» выберите опцию «ЕГАИС»;
  - укажите применение ключа: «Электронная подпись», «Шифрование ключей», «Шифрование данных», «Неотрекаемость»;
  - выберите параметр «Юридическое лицо» или «Физическое лицо», на которое будет выдан сертификат<sup>1</sup>;
  - Формат запроса рекомендуется выбрать «PEM».

Данные         Данные           Ф Уклическое лица         Кридическое лица           ФИО         Иванов Иван Иванович           ФИО         Иванов Иван Иванович           Фамлиия         Иванов           Филанческое лица         Физическое лица           Филанческое лица         Физическое лица           Фамлия         Иванов           Фамлия         Иванов           Мия Отчество         Иван Иванович           Email         email@email.ru           Должность         Должность           Отдел         Наименование отдела           Организация         ООО "Ромашка"           Арес         ул. Пенина, д. 1, стр. 1           Город         Москва           Регион         77 Москва           Страна         Россия (Российская Федерация) (*           ИНН         123456789012           ОГРН         ОГРНИП           12345678901230         ОГРНИП           12345678901230         ОГРНИП           123456789012345         ОГРНИП           Снилс         123456789012           ОГРНИП         123456789012           ОГРНИП         12345678910           Неструкт. има         ГА/С	Данные Физическое лицо ФИО И Фамилия И Имя Отчество И Е-mail е Должность Отдел Н Организация И	<ul> <li>Юридическое лицо</li> <li>Иванов Иван Иванович</li> <li>Иванов</li> <li>Иванов</li> <li>Иванович</li> <li>иташееташ.ru</li> <li>Наименование отдела</li> <li>Иванов И.И.</li> </ul>	Данные Физическое и Наименование Фамилия Имя Отчество Е-mail Должность Отдел	лицо  Кридическое лицо ООО "Ромашка" Иванов Иван Иванович email@email.ru Генеральный директор Наименование отдела
ФИО         Иванов Иван Иванович         Наименование         ООО "Ромашка"           ФИО         Иванов Иван Иванович         Наименование         Шванов           Филикия         Иванов         Иванов         Иванов           Филикия         Иванов         Иванов         Иванов           Симк Отчество         Иванович         Еттаl         Ertal@email.ru           Должность         Отдел         Наименование отдела         Оогаринация         Пожность           Отдел         Наименование отдела         Оогаринация         Пожность         Отдел         Наименование отдела           Организация         ИП Иванов И.И.         Должность         Пенеральный директор         Отдел           Организация         ИП Иванов И.И.         Адрес         ул. Пенина, д.1, стр.1         Город           Город         Москва         Раския         Ооганизация         ООС "Ромашка"           ИНН         123456789012         ОГР         Посква         Регион         77 Москва           Страна         Россия (Российская Федерация) (         ИНН         123456789012         ОГРН         123456789012           ОГРН         123456789012345         ОГРНИП         12345678910         Неструкт. имя         КРР-123456789 <td< td=""><td>ФИО И Фамилия И Имя Отчество И Е-mail е Должность Отдел Н Организация И</td><td>Иванов Иван Иванович Иванов Иван Иванович аmail@email.ru Наименование отдела ПП Иванов И.И.</td><td>Наименование Фамилия Имя Отчество Е-mail Должность Отдел</td><td>ООО "Ромашка" Иванов Иван Иванович еmail@email.ru Генеральный директор Наименование отдела</td></td<>	ФИО И Фамилия И Имя Отчество И Е-mail е Должность Отдел Н Организация И	Иванов Иван Иванович Иванов Иван Иванович аmail@email.ru Наименование отдела ПП Иванов И.И.	Наименование Фамилия Имя Отчество Е-mail Должность Отдел	ООО "Ромашка" Иванов Иван Иванович еmail@email.ru Генеральный директор Наименование отдела
Фамилия         Иванов         Фамилия         Иванов           Иня Отчество         Иван Иванович         Вания         Ван	Фамилия И Имя Отчество И Е-mail е Должность Отдел Н Организация И	1ванов 1ван Иванович mail@email.ru łаименование отдела 1П Иванов И.И.	Фамилия Имя Отчество Е-mail Должность Отдел	Иванов Иван Иванович email@email.ru Генеральный директор Наименование отдела
Иня Отчество         Иван Иванович         Иня Отчество         Иван Иванович           Етпаil         етпаil@email.ru         Должность         Етпаil         етпаil@email.ru           Должность         Отдел         Наименование отдела         Отдел         Наименование отдела           Организация         ИП Иванов И.И.         Должность         Генеральный директор           Организация         ИП Иванов И.И.         Организация         ОО0 "Ромашка"           Адрес         ул. Ленина, д. 1, стр. 1         Адрес         Ул. Ленина, д. 1, стр. 1           Город         Москва         Регион         77 Москва           Регион         77 Москва         Регион         77 Москва           Страна         Россия (Российская Федерация) ( ∨         Страна         Россия (Российская Федерация)           ИНН         123456789012         ОГРН         123456789012           ОГРН         12345678910         Неструкт. имя         КРР=1234567891           Неструкт. имя         ГСТ Р 34.10-2001         СНИПС         1234567891           Пополнательное имя субъекта         Етпаl	Имя Отчество и Е-mail е Должность и Отдел И Организация и	1ван Иванович mail@email.ru Наименование отдела 1П Иванов И.И.	Имя Отчество E-mail Должность Отдел	Иван Иванович email@email.ru Генеральный директор Наименование отдела
Email         email@email.ru         Должность           Отдел         Наименование отдела         Отдел         Должность         Генеральный директор           Организация         ИП Иванов И.И.         Адрес         Ул. Пенина, д.1, стр.1         Адрес         Ул. Пенина, д.1, стр.1           Город         Москва         Организация         ООО "Ромашка"           Адрес         Ул. Пенина, д.1, стр.1         Город         Москва           Регион         77 Москва         Регион         77 Москва           Страна         Россия (Российская Федерация) ( ∨         Страна         Россия (Российская Федерация)           ИНН         123456789012         ИНН         123456789012         ОГРН ИП           ОГРНИП         123456789103         ОГРН ИП         12345678910           Неструкт. имя         ЕГАИС         Раширения         ЕГАИС           Тип Ключа         ГОСТ Р 34.10-2001         Тип Ключа         ГОСТ Р 34.10-2001           ИРN          Полькность         Неотрекаемость           Шифрование ключа         Опольки ключа         Польк ошифрование           Электронная подпись         Неотрекаемость         У Злектронная подпись         Неотрекаемость           Ишфрование данных         Только расшифрование <td< td=""><td>Е-mail е Должность Е Отдел Е Организация V</td><td>mail@email.ru Наименование отдела 1П Иванов И.И.</td><td>E-mail Должность Отдел</td><td>email@email.ru Генеральный директор Наименование отдела</td></td<>	Е-mail е Должность Е Отдел Е Организация V	mail@email.ru Наименование отдела 1П Иванов И.И.	E-mail Должность Отдел	email@email.ru Генеральный директор Наименование отдела
Должность         Должность         Генеральный директор           Отдел         Наименование отдела         Отдел         Наименование отдела           Организация         ИП Иванов И.И.         Организация         ООС "Ромашка"           Адрес         ул. Ленина, д. 1, стр. 1         Адрес         Ул. Ленина, д. 1, стр. 1           Город         Москва         Город         Москва           Регион         77 Москва         Город         Москва           Страна         Россия (Российская Федерация) ( ∨         ИНН         123456789012           ИП И         123456789012         ОГРН         123456789012           ОГРНи         1234567890123         ОГРНиП         1234567890123           ОГРНиП         12345678910         Неструкт. имя         КРР=12345678910           Неструкт. имя         ГРАИС         Тим Ключа         ГОСТ Р 34.10-2001           Дополнительное имя субъекта         Егаис         Егаи         Егаи           Применение ключа         Голько шифрование         Полько расшифрование         Полько расшифрование           Применение ключа         Только расшифрование         Только расшифрование         Полько расшифрование	Должность Отдел (Н Организация //	Наименование отдела ПП Иванов И.И.	Должность Отдел	Генеральный директор Наименование отдела
Отдел         Наименование отдела         Отдел         Наименование отдела           Организация         ИП Иванов И.И.         Организация         ООО "Ромашка"           Адрес         ул. Ленина, д.1, стр.1         Адрес         ул. Ленина, д.1, стр.1           Город         Москва         Город         Москва           Регион         77 Москва         Город         Москва           Страна         Россия (Российская Федерация) ( ∨         ИНН         123456789012           ОГРН         123456789012         ОГРН         123456789012           ОГРНиП         12345678910         ОГРНИП         12345678910           Неструкт. имя         ЕГАИС         ОГОТ Р 34.10-2001         Гим Ключа           Полотичтельное имя субъекта         Еглай         Еглай         Еглай           ПРV4	Отдел	Наименование отдела 1П Иванов И.И.	Отдел	Наименование отдела
Организация         ИП Иванов И.И.         Организация         ООО "Ромашка"           Адрес         ул. Пенина, д.1, стр.1         Арес         ул. Пенина, д.1, стр.1           Город         Москва         Город         Москва           Регион         77 Москва         Город         Москва           Страна         Россия (Российская Федерация) (          Страна         Россия (Российская Федерация) (            ИНН         123456789012         ИНН         123456789012           ОГРНИП         123456789012345         ОГРНИП         12345678910           СНИЛС         12345678910         СНИЛС         12345678910           Неструкт. имя         ЕГАИС          СНИЛС         12345678910           Тип Ключа         ГОСТ Р 34.10-2001          Неструкт. имя         КРР=123456789           Расширения         ЕГАИС          Тип Ключа         ГОСТ Р 34.10-2001           Дополнительное имя субъекта         Еглай           Дополнительное имя субъекта           Еглай          Пололи и субъекта           Пололи с с бъекта           Еглай           Пололи и с с бъекта             Применение ключа	Организация 🛛	П Иванов И.И.	000000000000000000000000000000000000000	
Адрес       ул. Ленина, д.1, стр.1         Город       Москва         Регион       77 Москва         Страна       Россия (Российская Федерация) ( ∨         ИНН       123456789012         ОГРНИП       123456789012         ОГРНИП       123456789012345         ОГРНИП       12345678910         Неструкт. имя       Страна         Расширения       ЕГАИС         Тип Ключа       ГОСТ Р 34.10-2001         ИР       ОГР         Пуч4       Полько шифрование         Электронная подпись       Неотрекаемость         Шифрование ключай       Только шифрование         Шифрование ключай       Только расшифрека         ОКен ключами       Только расшифрование			орі апизация	000 "Ромашка"
Город Москва Регион 77 Москва Регион 77 Москва Регион 77 Москва Страна Россия (Российская Федерация) ( ✓ ИНН 123456789012 ОГРН ОГРН 1234567890122 ОГРН 123456789012345 ОГРНИП 123456789012345 ОГРНИП 12345678910 Неструкт. имя Расширения ЕГАИС ГОСТ Р 34.10-2001 ✓ Попланительное имя субъекта Еглай ГРЧ ОГР 34.10-2001 ✓ Полменение ключа Электронная подпись У Неотрекаемость Шифрование ключаи Электронная подпись У Неотрекаемость Шифрование ключаи Обмен ключами	Адрес у	л. Ленина, д.1, стр.1	Адрес	ул. Ленина, д.1, стр.1
Регион         77 Москва           Страна         Россия (Российская Федерация) ( ∨           ИНН         123456789012           ОГРН         123456789012345           ОГРНИП         123456789012345           ОГРНИП         123456789012345           ОГРНИП         123456789012345           ОГРНИП         123456789012345           ОГРНИП         123456789012345           СНИЛС         12345678910           Неструкт. имя         СНИЛС           Расширения         ЕГАИС           Тип Ключа         ГОСТ Р 34.10-2001           Пруч4         Попличительное имя субъекта           Еглай         Дополнчительное имя субъекта           Вокторенкия подпись         Неотрекаемость           У Электронная подпись         Неотрекаемость           Шифрование ключай         Только расшифрование           Шифрование ключай         Только расшифрование           Шифрование ключай         Только расшифрование	Город	Лосква	Город	Москва
Страна         Россия (Российская Федерация) ( ~         Страна         Россия (Российская Федерация) ( ~           ИНН         123456789012         ИНН         123456789012         ИНН         123456789012           ОГРН         0ГРНИП         123456789012345         ОГРНИП         12345678910         ОГРНИП           Снилс         12345678910         ОГРНИП         12345678910         СНИЛС         12345678910           Неструкт. имя	Регион 7	77 Москва	Регион	77 Москва
ИНН 123456789012 ОГРН 1234567890123 ОГРНИП 123456789012345 СНИЛС 12345678910 Неструкт. имя Расширения ЕГАИС	Страна Г	Россия (Российская Федерация) ( 🗸	Страна	Россия (Российская Федерация) (
ОГРН	инн П	23456789012	инн	123456789012
ОГРНИП       123456789012345         СНИЛС       12345678910         Неструкт. имя	ОГРН		ОГРН	1234567890123
СНИЛС 12345678910 Неструкт. имя Расширения ЕГАИС Тип Ключа ГОСТ Р 34.10-2001 Дополнительное имя субъекта Еглай ПРV4 DNS UPN Применение ключа Электронная подлись Иеотрекаемость Шифрование ключей Только расшифровка Обмен ключами	огрнип Г	23456789012345	огрнип	
Спилс       12343070310         Неструкт. имя       Пеструкт. имя         КРР=123456789       Расширения         ЕГАИС       Расширения         ГОСТ Р 34.10-2001       Пил Ключа         Пополнительное имя субъекта       ГОСТ Р 34.10-2001         Дополнительное имя субъекта       Дополнительное имя субъекта         Е-mail       При4         IPv4       IPv4         DNS       DNS         UPN       DNS         Злектронная подпись       Неотрекаемость         Шифрование ключай       Только расшифровка         Обмен ключами       Обмен ключами	снилс [	22/6670010	снивс	12345678910
Неструкт. имя КРР = 123436763 Расширения ЕГАИС Тип Ключа ГОСТ Р 34.10-2001 Дополнительное имя субъекта Е-mail IPv4 DNS UPN Применение ключа Флотолнительное имя субъекта Е-mail IPv4 DNS UPN Применение ключа Флотонительное имя субъекта Е-mail IPv4 DNS UPN Применение ключа Флотонии е-main подпись Обмен ключами Обмен ключами		2343076310	Ulassina	12343070310
Расширения ЕГАИС Тип Ключа ГОСТ Р 34.10-2001 Дополнительное имя субъекта Е-mail IPv4 DNS UPN Применение ключа Фоложительное имя субъекта Е-mail IPv4 DNS UPN Применение ключа Фложание ключа Применение ключа Филожание ключа Фложание ключа Применение ключа Филожание ключа Филожан	неструкт. имя		неструкт. имя	KFF=123436783
Тип Ключа         ГОСТ Р 34.10-2001         Тип Ключа         ГОСТ Р 34.10-2001           Дополнительное имя субъекта	Расширения	ЕГАИС ~	Расширения	ЕГАИС
Дополнительное имя субъекта       Дополнительное имя субъекта         E-mail       E-mail         IPv4       IPv4         DNS       DNS         UPN       DNS         Фрименение ключа       Применение ключа         Применение ключа       Применение ключа         Фифрование ключей       Только шифрование         Шифрование ключами       Только расшифровка         Обмен ключами       Обмен ключами	Тип Ключа	TOCT P 34.10-2001 V	Тип Ключа	FOCT P 34.10-2001
Е-mail       Е-mail         IPv4       IPv4         DNS       DNS         UPN       DNS         Фрименение ключа       UPN         Применение ключа       Применение ключа         Электронная подлись       Неотрекаемость         Шифрование ключей       Только шифрование         Шифрование данных       Только расшифровка         Обмен ключами       Обмен ключами	Дополнительное имя	субъекта	Дополнительное	имя субъекта
IPv4       IPv4         DNS       DNS         UPN       UPN         Применение ключа       UPN         Применение ключа       Применение ключа         Электронная подлись       Неотрекаемость         Шифрование ключей       Только шифрование         Шифрование данных       Только расшифровка         Обмен ключами       Обмен ключами	E-mail		E-mail	
DNS       DNS         UPN       DNS         Применение ключа       UPN         Ф Электронная подпись       Неотрекаемость         Шифрование ключей       Только шифрование         Шифрование данных       Только расшифровка         Обмен ключами       Обмен ключами	IPv4		IPv4	
UPN       UPN         Применение ключа       Применение ключа         Электронная подлись       Неотрекаемость         Шифрование ключей       Только шифрование         Шифрование данных       Только расшифровка         Обмен ключами       Обмен ключами	DNS		DNS	
Применение ключа	UPN		UPN	
<ul> <li>У Электронная подпись</li> <li>✓ Неотрекаемость</li> <li>✓ Электронная подпись</li> <li>✓ Неотрекаемость</li> <li>✓ Шифрование ключей</li> <li>Только шифрование</li> <li>✓ Шифрование данных</li> <li>Только расшифровка</li> <li>Обмен ключами</li> <li>✓ Обмен ключами</li> </ul>	Применение ключа		Применение клю	4a
Шифрование ключей         Только шифрование         Шифрование ключей         Только шифрование           Шифрование данных         Только расшифровка         Шифрование данных         Только расшифровка           Обмен ключами         Обмен ключами         Обмен ключами	🗹 Электронная подг	пись 🗹 Неотрекаемость	Электронная	подпись 🗹 Неотрекаемость
Шифрование данных         Только расшифровка         Шифрование данных         Только расшифровка           Обмен ключами         Обмен ключами         Обмен ключами	🗹 Шифрование ключ	чей 🗌 Только шифрование	Иифрование	ключей 🗌 Только шифрование
Обмен ключами	🗹 Шифрование данн	ных 🔲 Только расшифровка	🗹 Шифрование	данных 🔲 Только расшифровка
	🗌 Обмен ключами		Обмен ключа	ми
Формат Формат	Формат		Формат	

Рис. 6 а

<sup>&</sup>lt;sup>1</sup> Неструктурированное имя: UN (1.2.840.113549.1.9.2) – обязательно к заполнению. Должен быть записан один из вариантов: - для ЮЛ должны присутствовать 4 символа КПП= или КРР= и далее 9 цифр КПП организации, сотрудником которого является владелец СКПЭП.

<sup>-</sup> для ИП должны присутствовать только 4 символа КПП= или КРР=.

ОГРНИП: OGRNIP (1.2.643.100.5) (только для ИП). Текст длиной 15 цифр. Не разрешается использовать пробел в начале и в конце текста. Заполните это поле, если требуется.

Далее нажмите кнопку «Сгенерировать», и после формирования запроса сохраните его, нажав соответствующую клавишу. После успешного сохранения файла закройте окно запроса сертификата с помощью клавиши «Закрыть» (Рис. 6 б).



• На основе сохранённого запроса сформируйте сертификат КЭП. Квалифицированный сертификат открытого ключа производится удостоверяющим центром (УЦ) с применением средств КЭП.

#### 4. Записать сертификат на электронный идентификатор

 Запишите полученный сертификат на MS\_KEY ESMART АНГАРА. Для этого перейдите во вкладку «Сертификаты» и нажмите кнопку «Добавить» (Рис. 7). Обратите внимание, что на момент записи сертификата вы должны быть авторизованы на устройстве.

Токен	Д	анные	Контейнеры	Ключи	Сертификаты
🔒 Выйти 🛛	Обновить	Добавить			
			Рис 7		

В открывшемся окне выберите сертификат, который был сгенерирован по Вашему запросу и нажмите кнопку «Открыть» (Рис. 8).

Для ЕГАИС.cer		
Имя файла: Для ЕГАИС.cer	<ul> <li>(*.cer;*.crt)</li> </ul>	

Рис. 8

Нажмите на клавишу «ОК» в окне с уведомлением о завершении записи сертификата на электронный носитель (Рис. 9).



Рис. 9



• *Контейнер сформирован.* После завершения установки Вашего сертификата, информацию о нем можно посмотреть во вкладке «Контейнеры» (Рис. 10 а).

Токен	Данные	Контейнеры	Ключи	Сертификаты
🔒 Выйти Обн	овить Добавить			
	"МультиСофт Системз"	', SN=Иванов, G=Иван Ив	ванович, Till=2017-04	-26. Co

Рис. 10 а

При нажатии на значок «+» (Рис. 10 а) сформированного контейнера откроется его содержимое: ключевая пара и сертификат (Рис.10 б).

Токен		Данные	Контейнеры	Ключи	Сертификаты	
🔒 Выйти	Обновить	Добавить	Просмотр Переиме	новать Удалить		
	I=000 "Мульт	иСофт Систем:	з", SN=Иванов, G=Иван Ив	занович, Till=2017-04-	-26, Cp	
	Ключевая і	пара ГОСТ 34.1 ытый ключ ГОС	10 (f10fa989-7e98-409a-a6de ^T 34 10	e-0e7f675d086e)		
	Oткр	ытый ключ ГОС	CT 34.10			
5	Сертифика	т CN="000 ""I	МультиСофт Системз'''''', S	N=Иванов, G=Иван I	Иванович, E=multisoft@mult	isoft.ru,

Рис. 10 б.

