## Создание запроса на сертификат и формирование закрытого ключа

Для создания запроса на сертификат необходимо обновить VipNet CSP до актуальной версии:

**1.** В меню Пуск выберите пункт Все программы затем группу ViPNet в ней ViPNet CSP и щелкните значок Создание запроса на сертификат.



Рисунок: Вызов программы создания запроса на сертификат

2. На открывшейся странице выберите действие Запросить новый сертификат – для создания запроса на новый сертификат.

В разделе Параметры сертификата укажите следующие параметры:

В списке Криптопровайдер необходимо выбрать Infotecs GOST 2012/512, как показано на рисунке.

В Назначение выберите Подпись и шифрование, как показано на рисунке.

🔯 Служба сертификации	
infotecs	
VIPNet Victor Private Network	Создание запроса на сертификат Символом * отмечены поля, обязательные для заполнения
	<ul> <li>Запросить новый сертификат</li> <li>Запросить обновление действующего сертификата</li> </ul>
	Параметры сертификата Криптопровайдер: Infotecs GOST 2012/512 Cryptographic Service Provider Алгоритм хэширования: GOST 34.11-2012 256 Назначение: Подпись и шифоование
	Шаблон сертификата: Квалифицированный ChitaCA Параметры ключа: Ээкспортируемый Системный

В списке Шаблон сертификата выберите в зависимости от назначения сертификата: СМЭВ – для всех сотрудников без права формирования запросов в Росреестр;

СМЭВ ИОГВ РОСРЕЕСТР – для сотрудников ИОГВ и подведомственным им учреждений с правом формирования запросов в Росреестр;

**СМЭВ ОМСУ РОСРЕЕСТР** – для сотрудников ОМСУ и подведомственным им учреждений с правом формирования запросов в Росреестр;

СМЭВ АИС – для автоматизированных систем – формируется только по отдельному указанию.

Квалифицированный ChitaCA – квалифицированный сертификат для различных областей применения;

Квалифицированный ChitaCA ФЛ – квалифицированный сертификат различных областей применения для физического лица;

**ГИС ГМП** – для работы в государственной информационной системе о государственных и муниципальных платежах;

Квалифицированный ChitaCA ФНС – квалифицированный сертификат различных областей применения, в том числе для портала ФНС;

Квалифицированный ChitaCA Pocpeecrp – квалифицированный сертификат различных областей применения, в том числе для портала Росреестра.

**3.** В разделе Данные о владельце сертификата укажите необходимую информацию для формирования запроса на сертификат.

🐻 Служба сертификации	Number of Street or other Street Stre	and the second		- 0 <b>- X</b>
Шаблон сертификата:	Квалифицированный ChitaCA			*
Параметры ключа:	✓ Экспортируемый ☐ Системный			
Данные о владельце сертификата:				
ΦΝΟ	* Иванов Иван Иванович			
Фамилия	* Иванов	_		
Имя Отчество	* Иван Иванович			
Адрес электронной почты	pivanov@ivanov.ru			
Организация	Департамент по делам			
Подразделение				
Должность	Специалист			
Название улицы, номер дома	Амурская	_		
Населенный пункт	* Чита			
Область	* 75 Забайкальский край			
Страна	RU			
СНИЛС	12345678900			
ИНН	007512345678			
ОГРН	7512345678900			E
огрнип				
Сохранение запроса в файл				
Имя файла:	*C:\ProgramData\InfoTeCS\Requests\CertReq.p10	Обзор		
Кодировка:	DER O MIME (Base 64)			
	Сформировать запрос			
				12.42
			RU 🔺	13:42 22:11.2017

Рисунок: Заполнение данных для запроса на сертификат

Примечание: Если при выборе соответствующего шаблона не отображаются поля СНИЛС, ИНН и ОГРН, это означает, что необходимо обновить программное обеспечение ViPNet CSP до новой версии, указанной в инструкции.

При этом следует соблюдать следующие правила:

В связи с ограничением на длину полей запроса в 64 символа, следует использовать принятые в официальной деловой переписке сокращения наименований организаций, должностей сотрудников, подразделений, а также названий городов, районов и муниципальных образований с целью уложиться в ограничение длины 64 символа.

СНИЛС – указываются только 11 цифр, без разделяющих знаков.

Важно: Ответственность за полноту и достоверность сведений, указанных в запросе, несет лицо, формирующее запрос на сертификат.

## Указания по заполнению полей: 1. ФИО сотрудника.

ФИО должно быть указано полностью так, как оно указано в документе, удостоверяющем личность владельца (например, паспорт). Формат:

- а. первое слово Фамилия;
- б. 1 пробел;
- в. второе слово Имя;
- г. 1 пробел;
- д. третье слово Отчество (если имеется);

Если в фамилии, имени или отчестве в написании присутствует «дефис», то в сертификат так и вносится с дефисом без пробелов (например: Салтыков-Щедрин).

Если фамилия, имя или отчество состоит из нескольких слов разделенных пробелом, то в сертификат вносится одним словом, части которого соединены «подчеркиванием» без пробелов (например: фамилия «Ван чо» будет записана Ван\_чо).

Фамилия, имя и отчество (если имеется) должны разделяться 1 пробелом.

Не разрешается использовать пробел в начале и в конце текста.

## 2. Организация.

Каждое слово в тексте должно быть отделено 1 пробелом.

Не разрешается использовать пробел в начале и в конце текста.

Следующие символы разрешается использовать только в том случае, если они встречаются внутри официального названия организации:

3. Поля Подразделение и Название улицы, номер дома не являются обязательными к заполнению, но если в организации есть подразделения, то необходимо их указывать.

## 4. Населенный пункт.

Каждое слово в тексте должно быть отделено 1 пробелом.

Не разрешается использовать пробел в начале и в конце текста.

В название населенного пункта также входит название муниципального района (кроме названий областных, краевых и районных центров).

5. Поля Область и Страна остаются без изменений.

6. В поле СНИЛС указывается СНИЛС сотрудника без дефисов и пробелов – 11 цифр.

7. В поле **ИНН организации** указывается 10-значный ИНН организации с приписанными слева 00 – всего должно быть 12 цифр.

8. В поле ОГРН указывается ОГРН организации – 13 цифр.

**4.** Либо в разделе **Данные о владельце сертификата** укажите необходимую информацию об информационной системе, для которой формируется запрос на сертификат.

🚯 Служба сертификации	And Might Rep Loss Logo T.	And Charles and Antonia	100 mil 11	
<b>VIPNet</b> <sup>°</sup>	Создание запроса на сертификат Символом * отмечены поля, обязательные	для заполнения		•
	<ul> <li>Запросить новый сертификат</li> <li>Запросить обновление действ</li> </ul>	ующего сертификата		
	Параметры сертификата			
	Криптопровайдер:	Infotecs Cryptographic Service Provider	~	
	Алгоритм хэширования:	GOST R 34.11-94		
	Назначение:	Подпись и шифрование 🗸		
	Шаблон сертификата:	СМЭВ АИС		
	Параметры ключа:	✓Экспортируемый Системный		
	Данные о владельце сертификата:			E
	Отображаемое название АИС*	Сервер баз данных	]	
	Организация*	Департамент по делам	J	
	Подразделение		]	
	Название улицы, номер дома			
	Населенный пункт*	Чита		
	ИНН организации*	007512345678	-	
	огрн•	7512345678900	_	
	Область	75 Забайкальский край	-	
	Страна	RI		
		P. 10		
	Сохранение запроса в файл			
	Имя файла:*	C:\ProgramData\InfoTeCS\Requests\CertReq.p10	Обзор	
	Кодировка:	DER O MIME (Base 64)		+

Рисунок: Заполнение данных об информационной системе

При этом следует соблюдать правила заполнения полей, приведенные выше.

В разделе **Сохранение запроса в фай**л нажмите **Обзор** и укажите место на диске или съемном носителе, а также имя файла для сохранения файла запроса, имя файла следует выбирать так, чтобы можно было однозначно связать файл запроса и на кого этот запрос формировался.

		Имя файла:*	С:\Администра	ция MP Забайкальский, p10	Обзор
		Кодировка:	O DER	O MIME (Base 64)	
истить поля	Печать				

5. Присоедините сертифицированный носитель ключа электронной подписи. Нажмите кнопку Сформировать запрос. Эта кнопка появляется после того, как будут заполнены все поля, обязательные для заполнения (отмечены \*). Появится окно инициализации контейнера закрытого ключа, в качестве примера используется eToken, работа с Rutoken принципиально не отличается.

**Примечание:** до присоединения носителя, на компьютере должны быть установлены драйвера для Вашего типа носителя, которые можно скачать на сайте производителя. Введите PIN-код носителя.

Обычно заводские установки PIN-кодов: eToken – 1234567890 Rutoken - 12345678

ViPNet CSP - инициализация контейнера ключей
Укажите место хранения контейнера ключей.
Имя контейнера: rnd-3-F553-DF5E-37FB-BDF2-05DF-D7B4-7704
С Папка на диске: C:\Users\Firsov.R\AppData\Loca
● Выберите устройство: Rutoken S 64К (2b8f6cc0)     ▼
Введите ПИН-код:
🖂 Сохранить ПИН-код
ОК Отмена

Рисунок: Окно инициализации контейнера закрытого ключа

6. Следуйте указаниям, приведенным в окне Электронная рулетка.



**7.** В окне сообщения об успешном создании файла запроса на сертификат нажмите **ОК**, извлеките носитель из компьютера и храните его в надежном месте, исключающем доступ к нему посторонних лиц.

8. При необходимости создайте следующий запрос на сертификат.

9. После создания файла запроса страницу браузера Служба сертификации можно закрыть.

После создания запроса на сертификат, необходимо переслать файл запроса с расширением .p10 (и никаких других файлов) в Удостоверяющий центр на электронный адрес ucecp@e-zab.ru