Установка ключа электронной подписи и сертификатов

Чтобы начать работу с электронной подписью, необходимо установить в операционную систему контейнер ключа подписи, сертификат пользователя, корневой сертификат Удостоверяющего центра и список отозванных сертификатов (далее - СОС).

Контейнер ключа подписи защищен для сертифицированных носителей ключей ЭП PIN-кодом, в других случаях – паролем, известным только пользователю (лицу, формировавшему запрос на сертификат).

Сертификат с открытым ключом (для проверки подлинности вашей подписи), сертификат уполномоченного лица Удостоверяющего центра и СОС выдаются Удостоверяющим центром при получении сертификата ключа подписи.

Установка ключа электронной подписи и личного сертификата пользователя.

- 1. Перенесите с флеш-носителя ключи электронной подписи на рабочий стол компьютера.
- 2. Запустите программу VipNet CSP.



3. В окне программы ViPNet CSP нажмите на Добавить контейнер. Выйдет окно инициализации контейнера ключей.

ViPNet CSP - инициализа	ция контейнера ключей	×
Укажите место х	ранения контейнера ключей.	
Имя контейнера:		\sim
. Папка на диске:	C:\Users\klimenko.a\AppData\Lo	<u>О</u> бзор
О Выберите устройство	не найдено	\sim
RU	ОК	Отмена

- 4. Выберите контейнер закрытого ключа электронной подписи, в зависимости, где он расположен. В данном примере, закрытый контейнер расположен на рабочем столе, в папке Тест Infotecs Containers.
- 5. После выбора закрытого контейнера в Имени контейнера будет отображен контейнер закрытого ключа электронной подписи. Нажимаем **Ок**.

VIPNet CSP ViPNet CSP Криптопровайдер VIP в операционной систе	— — X Net CSP предназначен для реализации криптографических функций еме Microsoft Windows.
Контейнеры ключей Подключаемые устройства Датчик случайных чисел Дополнительно	Ключ Укажите место хранения контейнера ключей. Ключ Укажите место хранения контейнера ключей. Имя Имя контейнера: mdF-8158-6284-6032-F68E-A044-EFF9-E13E Выберите устройство: не найдено ОК Отмена
	Установить сертификат Свойства Копировать в 前
© ОАО «ИнфоТеКС», 1991-2018 Версия 4.2 (8.51670). В составе продукт	ов ViPNet ОК Отмена Применить

6. После этого контейнер закрытого ключа отобразится в программе ViPNet CSP как показано на рисунке.

🔠 ViPNet CSP			- 🗆 X
ViPNet CSP Криптопровайдер ViP в операционной систе	Net CSP предназначен для реализации крипто ме Microsoft Windows.	эграфических функций	K
Контейнеры ключей Подключаемые устройства Датчик случайных чисел	Контейнеры ключей Ключи пользователя	× 0	Добавить контейнер
Дополнительно	Имя контейнера [md-f-815b-6284-6032-f68e-a044-eff9-e13e	Pacnoлoжение c:/users/klimenko.a/desktop/rect/infotecs/cd	a Konuposate s
© ОАО «ИнфоТеКС», 1991-2018 Версия 4.2 (8.51670). В составе продукт	os VIPNet	ОК Отме	ена Применить

- 7. Далее выбираем контейнер и нажимаем Установить сертификат. Выбираем сертификат открытого ключа, который находится в архивной папке cert, переданной удостоверяющим центром. Перед тем как установить сертификат, необходимо извлечь сертификат из архивной папки.
- 8. В открывшемся окне мастера установки сертификатов нажмите Далее.

Мастер установки сертификатов			
	Вас приветствует мастер установки сертификатов		
	Этот мастер поможет Вам установить сертификат в хранилище сертификатов операционной системы.		
	Для продолжения нажмите "Далее".		
	< <u>Н</u> азад <u>Далее ></u> Отмена <u>С</u> правка	3	

9. В открывшемся окне мастера установки сертификатов нажмите Далее.

Мастер установки сертификатов	Х
Выбор хранилища сертификатов Хранилища сертификатов - это области системы, в которых производится хранение сертификатов.	
Сертификат будет установлен в хранилище сертификатов:	
Текущего пользователя	
Компьютера (требуются права администратора)	
Установить сертификаты издателей	
Установить СОС	
< <u>Н</u> азад Далее > Отмена <u>С</u>	правка

10. В открывшемся окне мастера установки отметьте Указать контейнер с закрытым ключом, затем нажмите Далее.

Мастер установки сертифика	тов	\times
2	Готовность к установке сертификата.	
	Мастер готов к установке сертификата в системное хранилище.	
	Были указаны следующие параметры:	
	Выбрано хранилище сертификатов Текущего пользователя	
	Дополнительные параметры Не устанавливать сертификаты издателей. Не устанавливать списки отозванных сертификатов.	
	Вы можете указать контейнер с закрытым ключом. Информация о контейнере с закрытым ключом будет добавлена в хранилище сертификатов.	
	Указать контейнер с закрытым ключом 🗸 🗸	
1 1 1 1 1 1 1 1	Не привязывать к контейнеру	
	- Найти контейнер с закрытым ключом	
	< <u>Н</u> азад <u>Д</u> алее > Отмена <u>С</u> правка	

11. В открывшемся окне выбора контейнера выберете, Папка на диске, нажмите Обзор и выберете папку нахождения закрытого контейнера, затем нажмите кнопку ОК.

В данном примере, контейнер находится на рабочем столе, в папке Tect – Infotecs – Containers. Далее появится окно с запрашиваемым пин-кодом от закрытого контейнера, он находится в файле пароль, переданный Удостоверяющим центром.

12. Если появится запрос о сохранение сертификатов в контейнере, ответьте Да. Дождитесь завершения работы мастера, после чего программу VipNet CSP можно закрыть.



Установка корневого сертификата Удостоверяющего центра и СОС

Имена файлов сертификатов и СОС:

ChitaCA_20xx.crt – корневой сертификат Удостоверяющего центра. revokedCerts.crl - COC;

Эти файлы пользователь получает из Удостоверяющего центра в папках вида, где XX – год выпуска корневого сертификата и соответствующего ему списка отозванных сертификатов, поскольку срок действия ключа подписи составляет 1 год, то достаточно иметь папки за текущий и предыдущий год.

Установка сертификатов и СОС выполняется средствами операционной системы Windows.

Установка корневого сертификата Удостоверяющего центра:

- 1. Откройте папку с файлом сертификата и щелкните правой кнопкой мыши по значку сертификата.
- 2. В контекстном меню выберите пункт Установить сертификат.

Примечание: отсутствие вкладки **Установить сертификат** свидетельствует о том, что вы используете несертифицированную копию операционной системы Windows,

из которой вырезаны средства работы с сертификатами, в этом случае следует установить сертифицированную версию Windows.

Имя		Дата изменения	Тип		Размер
🔄 ChitaCA_2019.cer	OTKOLITI			кат безо	2 K
🔄 ChitaCA_2019_v2.ce	Улания	4		кат безо	2 K
guc_gost12.crl	Эстановить с	ертификат		тзыва се	2 K
🔄 guc_gost12.crt	/-Zip		~ ~	кат безо	2 K
revokedCerts.crl	CRC SHA		>	тзыва се	1 K
revokedCerts_v2.crl	🧉 Edit with Not	epad++		тзыва се	1 K
	🚷 Отправить п	исьмо адресату ViPNet			
	🔎 ViPNet Crypt	oFile	>		
	K Проверить н	а вирусы			
	K Проверить р	епутацию в KSN			
	🖻 Отправить				
	Открыть с по	мощью	>		
	Предоставит	ь доступ к	>		
	Восстановит	ь прежнюю версию			
	Отправить		>	L	
	Вырезать				
	Копировать				
	Создать ярль	ык		L	
	Удалить				
	Переименов	ать		L	

3. В окне приветствия мастера импорта сертификатов нажмите Далее.

🔶 🐉 Мастер импорта сертификатов	×
Мастер импорта сертификатов	
Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.	
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.	
Расположение хранилища (текущий пользователь) О <u>Л</u> окальный компьютер	
Для продолжения нажмите кнопку "Далее".	
Далее Отмен	а

4. На странице Хранилище сертификатов выберите Поместить все сертификаты следующее хранилище и нажмите Далее.

	×
 Завла сертификатов 	
Y	
Хранилище сертификатов Хранилища сертификатов - это системные области, в которых хранятся сертификаты.	
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.	
О Автоматически выбрать хранилище на основе типа сертификата	
Поместить все сертификаты в следующее хранилище	
Хранилище сертификатов:	
<u>О</u> бзор	
	_
Далее От	мена

5. На странице Выбора хранилища сертификатов выберите Доверенные корневые центры сертификации и нажмите **ОК**.

Хранилище с Хранилиц хранятся	ертификатов ца сертификатов - это системные области, в которых сертификаты.	
Windows pacrono AB To Xp	Выбор хранилища сертификата × выберите хранилище сертификатов, которое вы хотите использовать.	ать иката <u>О</u> бзор

6. В окне Мастер импорта сертификатов нажмите Далее.

		\times
←	뒏 Мастер импорта сертификатов	
	Хранилише сертификатов	
	Хранилища сертификатов - это системные области, в которых	
	хранятся сертификаты.	
	Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.	
	Автоматически выбрать хранилище на основе типа сертификата	
	Опроместить все сертификаты в следующее хранилище	
	Хранилище сертификатов:	
	Доверенные корневые центры сертификации Обзор	
	Далее Отмен	a

- 7. На следующей странице нажмите Готово.
- 8. В окне Мастер импорта сертификатов появится сообщение об успешном импорте сертификата. Нажмите Ок, установка завершена.
- 9. Для каждого сертификата безопасности указанных на рисунке, сделайте тоже самое.

Имя	Дата изменения	Тип	Размер
🔄 ChitaCA_2019.cer	09.01.2019 9:59	Сертификат безопасности	2 КБ
🔄 ChitaCA_2019_v2.cer	18.01.2019 8:47	Сертификат безопасности	2 КБ
guc_gost12.crl	09.01.2019 10:07	Список отзыва сертификатов	2 КБ
🔄 guc_gost12.crt	15.01.2019 9:51	Сертификат безопасности	2 КБ
revokedCerts.crl	09.01.2019 9:59	Список отзыва сертификатов	1 КБ
revokedCerts_v2.crl	18.01.2019 9:19	Список отзыва сертификатов	1 KE

Установка списка отозванных сертификатов (СОС)

- 1. Откройте папку с файлом СОС и щелкните правой кнопкой мыши по значку списка.
- 2. В контекстном меню выберите пункт Установить список отзыва (CRL).

Примечание: отсутствие вкладки Установить список отзыва (CRL) свидетельствует о том, что вы используете несертифицированную копию операционной системы Windows, из которой вырезаны средства работы

Имя	^	Дата изменения	Тип	Размер
ChitaCA_2019.c	er	09.01.2019 9:59	Сертификат безопасности	2 КБ
🔄 ChitaCA_2019_v	/2.cer	18.01.2019 8:47	Сертификат безопасности	2 КБ
E ChitaCA_2019_v ChitaCA_2019_v guc_gost12.cr guc_gost12.cr revokedCerts.	2.cer 18.01.2019 8:47 Открыть Установить список отзыва (CRL) 7-Zip CRC SHA ど Édit with Notepad++ Ornpaвить письмо адресату ViPNet ViPNet CryptoFile Проверить на вирусы Гроверить репутацию в KSN Отправить с помощью		Сертификат безопасности Сертификат безопасности гок отзыва сертификатов кок отзыва сертификатов сок отзыва сертификатов	2 KB 2 KG 2 KG 1 KG 1 KG
	Предоставить дост Восстановить през Отправить Вырезать Копировать Создать ярлык Удалить	уп к кнюю версию		
AMAS DE	Свойства			

- 3. Дальше на все предложения мастера установки нажимайте кнопку Далее, в конце работы нажмите кнопку Готово, дождитесь окончания работы мастера и сообщения об успешном завершении работы.
- 4. Для каждого списка отозванного сертификата, указанных на рисунке, сделайте тоже самое.

Лмя	Дата изменения	Тип	Размер
🔄 ChitaCA_2019.cer	09.01.2019 9:59	Сертификат безопасности	2 КБ
🔄 ChitaCA_2019_v2.cer	18.01.2019 8:47	Сертификат безопасности	2 КБ
🖲 guc_gost12.crl	09.01.2019 10:07	Список отзыва сертификатов	2 КБ
🔄 guc_gost12.crt	15.01.2019 9:51	Сертификат безопасности	2 КБ
E revokedCerts.crl	09.01.2019 9:59	Список отзыва сертификатов	1 KE
revokedCerts_v2.crl	18.01.2019 9:19	Список отзыва сертификатов	1 KE