Инструкция по пользованию центром сертификации



- **1.** Нужно связаться с нашими менеджерами и запросить регистрационные данные в системе «КИТ».
- 2. После получения регистрационных данных Вам нужно зайти на сайт <u>www.kitps.ru</u> в раздел «Центр сертификации», далее скачать и установить корневой сертификат (расширение .cer). Сделать это нужно в течении 24 часов с момента регистрации Ваших данных в системе!

Процесс установки:

1. После скачивания и открытия сертификата, Вы увидите такое окно:

цие Состав	Путь сертификации
Нет доверия центра серт установите доверенных сертификаци	ания о сертификате а к этому корневому сертификату ификации. Чтобы включить доверие, этот сертификат в хранилище к корневых сертификатов центров ии.
Кому выд	дан: kitps.ru
Кем выда	an: kitps.ru
Лейстрите	лен с 24.02.2011 по 21.02.2021
деяствите	

Рис. 1.

2. Нужно нажать кнопку «Установить сертификат...», откроется мастер установки. Нажмите «Далее» и увидите окно (рис. 2), в котором необходимо выбрать пункт «Поместить все сертификаты в следующее хранилище».

Мастер импорта сертификатов
Хранилище сертификатов
Хранилища сертификатов - это области системы в которых производится хранение сертификатов.
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную. Одвтоматически выбрать хранилище на основе типа сертификата
Поместить все сертификаты в следующее хранилище
Хранилище сертификатов:
< <u>Н</u> азад Далее > Отмена

Рис. 2.

3. Нажмите кнопку «Обзор» и выберите хранилище под названием «Доверенные корневые центры сертификации». Нажмите «ОК».

Выбор хранилища сертификата 🛛 ? 🔀				
Выберите хранилище сертификатов.				
— — Личные 📃				
🚽 🔤 Доверенные корневые центры сертификаци				
Доверительные отношения в предпри				
— 🧰 Промежуточные центры сертификаци				
🔄 🦳 Доверенные издатели 👝				
Сертификаты к которым нет доверик				
Показать физические хранилища				
ОК Отмена				
Рис. 3.				

4. Нажмите «Далее» и Вы увидите следующее окно (рис. 4). Нажмите «Готово».



Рис. 4.

5. Если у Вас появилось окно, показанное на рисунке ниже, нажимайте «Да». На этом установка сертификата будет окончена.

Предупр	еждение системы безопасности	×			
1	Готовится установка сертификата от центра сертификации (ЦС) в этом домене: kitps.ru				
	Не удается проверить, что сертификат принадлежит "kitps.ru". Обратитесь к "kitps.ru" и подтвердите его происхождение. Следующие числа будут полезны для данного процесса:				
	Отпечаток (sha1) : C6C9ACCE 3CA40ACE 5B1E88ED EFB5BF5B AB563C1D				
	Предупреждение: Если установить данный корневой сертификат, то Windows автоматически будет доверять любому сертификату, выданному ЦС. Установка сертификата без отпечатка может привести к риску безопасности. "Да" указывает, что риск принимается.				
	Установить данный сертификат?				
	Да []				

Рис. 5.

6. Вот так будет выглядеть начальное окно, если всё было сделано правильно и у Вас нет никаких ограничений на компьютере.

	став Путь сертификации
Этот с •В •В	сведения о сертификате ертификат предназначается для: се политики выдачи се политики применения
Ком	у выдан: kitps.ru
Кем	выдан: kitps.ru
Дей	ствителен с 24.02.2011 по 21.02.2021

Рис. 6.

3. Вам снова нужно зайти на сайт <u>www.kitps.ru</u> в раздел «Центр сертификации», только уже сделать «Запрос получения сертификата для входа в мониторинг». Откроется страница с таким содержанием:

Запрос сертификата

Логин:			
Пароль:			
Введите изображенные символы:	ZOVS		
	Получить сертификат		
Рис. 7.			

- **4.** Полученные от менеджера логин и пароль нужно ввести в соответствующие поля. При правильном вводе на экране появится ссылка на скачивание сертификата для входа в мониторинг.
- **5.** Скачивание и установка сертификата (расширение .*pfx*).

Процесс установки:

1. После скачивания и открытия сертификата, откроется мастер установки, нажмите «Далее», откроется следующее окно:

Мастер импорта сертификатов 🛛 🔀
Импортируемый файл
Укажите импортируемый файл.
Имя фа <u>й</u> ла:
Путь к сертификату на вашем компьютере
Замечание: нижеуказанные форматы файлов могут содержать в одном файле более одного сертификата: Файл обмена личной информацией - PKCS #12 (.PFX,.P12) Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b) Хранилище сериализованных сертификатов (.sst)
< <u>Н</u> азад Далее > Отмена

Рис. 8.

2. Указав путь к файлу, и нажав «Далее», Вам предложат ввести пароль (рис. 9). Это тот же пароль, которые Вы вводили при запросе на получение сертификата. Галочки ставятся по Вашему усмотрению.

Пароль Для обеспечения безопасности закрытый ключ защищен паролем.
Вредите пароль для закрытого ключа
Пароль:
Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании приложением закрытого ключа будет выдаваться запрос.
Пометить этот ключ как экспортируемый, что позволит вам сохранять архивную копию ключа и перемещать его.
————————————————————————————————————

Рис. 9.

3. Нажмите «Далее» и в появившемся окне (рис. 10) выберите первый пункт: «Автоматически выбрать хранилище на основе типа сертификата».

Мастер импорта сертификатов	R
Хранилище сертификатов	
Хранилища сертификатов - это области системы в которых производится хранение сертификатов.	
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.	
Автоматически выбрать хранилище на основе типа сертификата	
О Поместить все сертификаты в следующее хранилище	
Хранилище сертификатов:	
<u>Q</u> 630p	
< <u>Н</u> азад Далее > Отмена]

Рис. 10.

4. «Далее» -> «Готово». Установка сертификата завершена.

Поздравляем! Теперь для доступа к мониторингу нужно нажать «Вход для агентов» на главной странице сайта <u>www.kitps.ru</u>.

Внимание! Обязательно проверьте системное время на Вашем компьютере! Оно должно соответствовать реальному, иначе вход в мониторинг будет невозможен.