



Импорт сертификата в QUIK Front 9.2 на Windows 7/8, Server 2012



Содержание

 1. Импорт сертификата для корректной работы в QUIK Front 9.2 на Windows 7/8, Server 2012

 3

Ваши пожелания и комментарии к данному документу направляйте по электронной почтена adpec: <u>quiksupport@arqatech.com</u>



Импорт сертификата для корректной работы в QUIK Front 9.2 на Windows 7/8, Server 2012

Если у вас на проблемном компьютере операционная система Windows 10, то сообщите нам об этом. Если используются Windows 7, Windows 8 или Windows Server 2012, то для устранения описанной в данном инциденте проблемы выполните следующие действия:

- 1. Скачайте архив по ссылке: <u>https://arqatech.com/upload/faq/ARQA ca certs.zip</u>.
- 2. Распакуйте архив.
- **3.** Файл из архива ARQA_ca_certs.pfx запустите на исполнение (например, двойным кликом мыши) и последовательно выполнить следующие шаги:

 \times

_ В открывшемся окне нажмите на кнопку «Далее»:

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 нажните кнопку "Далее".

_ В данном окне также нажмите на кнопку «Далее»:

 Мастер импорта сертификатов	
Импортируемый файл	
Укажите файл, который вы хотите импортировать.	
Иня файла:	
D:\arqa_ca_certs.pfx Q630p	
Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:	
Файл обмена личной информацией - PKCS #12 (.PFX,.P12)	
Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)	
Хранилище сериализованных сертификатов (.SST)	

___ Введите пароль «12345» и нажмите на кнопку «Далее»:

Защи	та с помощью закрытого ключа
Д	ля обеспечения безопасности закрытый ключ защищен паролем.
в	ведите пароль для закрытого ключа.
	ароль:
	12345
	Локазывать пароды
	араметры импорта:
	Включить усиленную защиту закрытого ключа. В этом случае при каждо использовании закрытого ключа приложением будет запрашиваться разрешение.
	Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.
	Защита закрытого ключа с помощью безопасной виртуализации (неэкспортируемый)
	Включить все расширенные свойства.

 (\mathbf{O})

В открывшейся форме установите переключатель «Поместить все сертификаты в следующее хранилище», а в качестве хранилища выберите «Доверенные корневые центры сертификации» после чего нажмите на кнопку «Далее»:

Хран	лище сертификатов		
>	ранилища сертификатов - это системные обл ранятся сертификаты.	асти, в которых	
V F	indows автоматически выберет хранилище, и асположение сертификата вручную.	или вы можете ук	азать
	О Автоматически выбрать хранилище на о	снове типа серти	фиката
	Поместить все сертификаты в следующи	ее хранилище	
	Хранилище сертификатов:		
	Доверенные корневые центры сертиф	икации	<u>О</u> бзор

В открывшемся окне нажмите на кнопку «Готово», после чего отобразится сообщение:



В зависимости от настроек безопасности ПК, также может появиться сообщения следующего вида:



	Security Warning	x
<u>^</u>	You are about to install a certificate from a certification authority (CA) claiming to represent: DigiCert Trusted Root G4	
	Trusted Root G4". You should confirm its origin by contacting "DigiCert Trusted Root G4". The following number will assist you in this process:	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.	
	Vo you want to install this certificate? Yes No	

____ Нажмите на кнопку «OK», или «Yes» и запустите терминал версии 9.2.