



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 почта на адрес: quiksupport@argatech.com

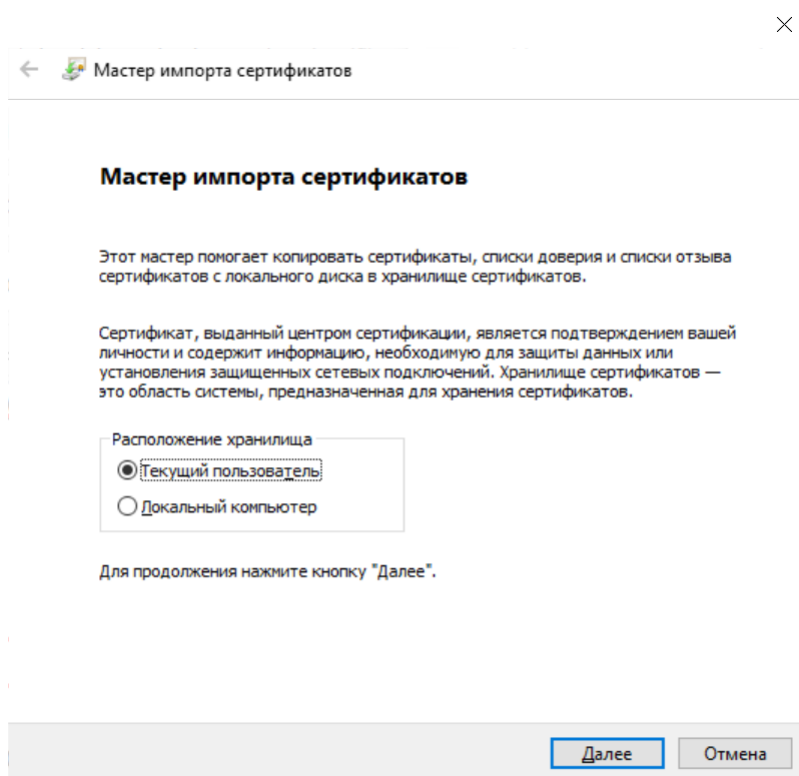


1. Импорт сертификата для корректной работы в QUIK Front 9.2 на Windows 7/8, Server 2012

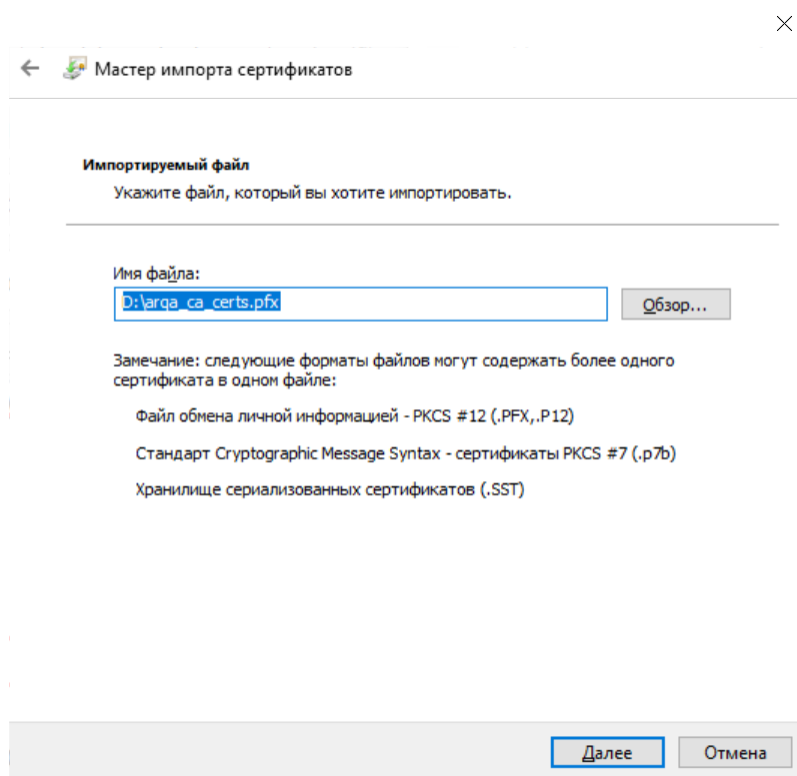
Если у вас на проблемном компьютере операционная система Windows 10, то сообщите нам об этом. Если используются Windows 7, Windows 8 или Windows Server 2012, то для устранения описанной в данном инциденте проблемы выполните следующие действия:

1. Скачайте архив по ссылке: https://arqatech.com/upload/faq/ARQA_ca_certs.zip.
2. Распакуйте архив.
3. Файл из архива ARQA_ca_certs.pfx запустите на исполнение (например, двойным кликом мыши) и последовательно выполните следующие шаги:

— В открывшемся окне нажмите на кнопку «Далее»:



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



← Мастер импорта сертификатов

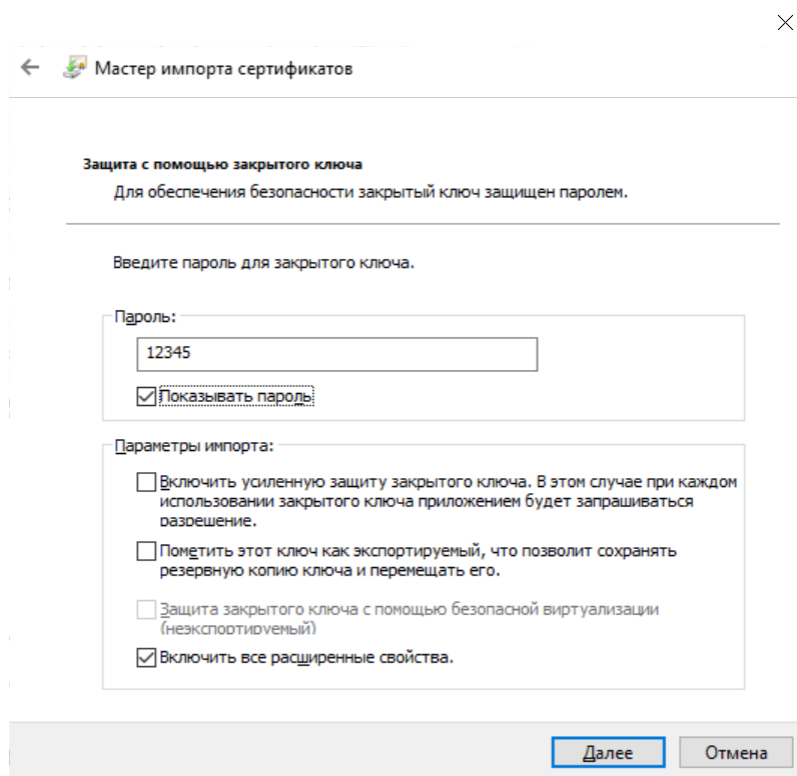
Импортируемый файл
Укажите файл, который вы хотите импортировать.

Имя файла:

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»:



← Мастер импорта сертификатов

Защита с помощью закрытого ключа
Для обеспечения безопасности закрытый ключ защищен паролем.

Введите пароль для закрытого ключа.

Пароль:

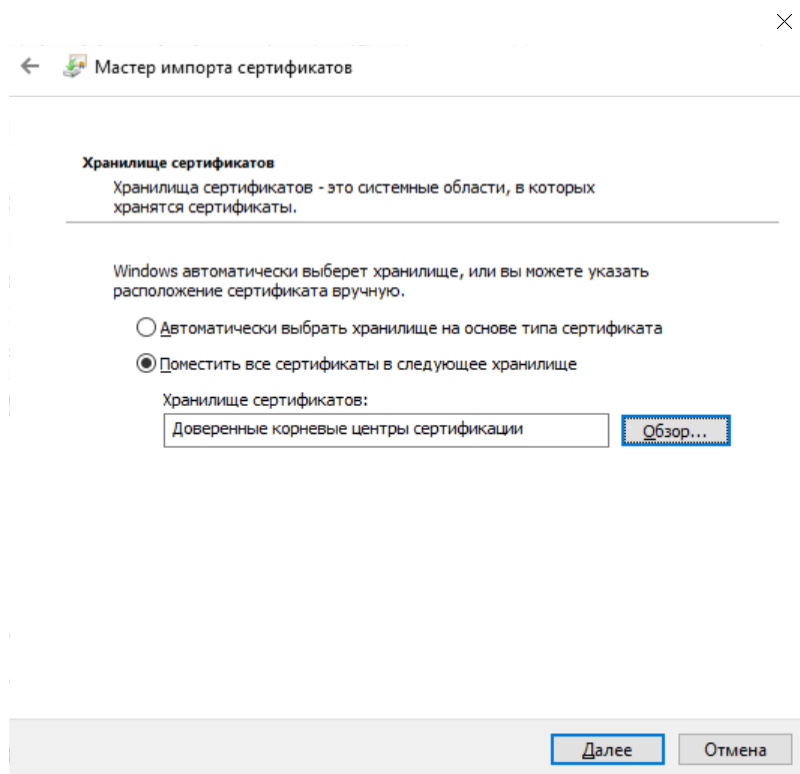
 Показывать пароль

Параметры импорта:

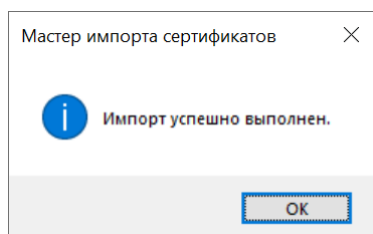
- Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании закрытого ключа приложением будет запрашиваться разрешение.
- Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.
- Защита закрытого ключа с помощью безопасной виртуализации (неэкспортируемый)
- Включить все расширенные свойства.



- 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»:



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



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





— Нажмите на кнопку «ОК», или «Yes» и запустите терминал версии 9.2.

