

ContainerTool

Утилита предназначена для работы с ключевыми контейнерами криптопровайдеров ГОСТ и RSA.

Возможности утилиты:

- Поддержка отечественных криптопровайдеров КриптоПро CSP и ViP Net CSP
- Поддержка криптопровайдера RSA, встроенного в ОС Microsoft Windows
- Экспорт сертификатов и закрытых ключей поддерживаемых криптопровайдеров в формат OpenSSL
- Экспорт сертификатов и закрытых ключей поддерживаемых криптопровайдеров в формат PEM
- Модификация значения флага экспорта ключевых контейнеров

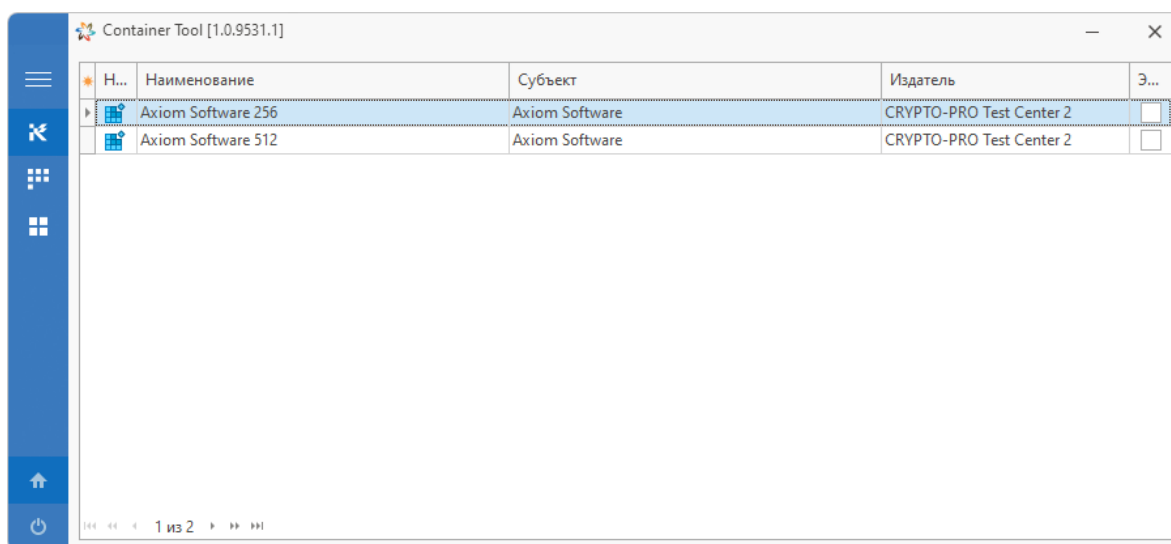
Требования:

- Операционная система Microsoft Windows (7 и выше)
- Для получения списка имеющихся ключевых контейнеров – наличие в системе соответствующих криптопровайдеров (криптопровайдер RSA от Microsoft встроен в систему)
- Для экспорта закрытых ключей и сертификатов – наличие OpenSSL с движком ГОСТ

При отсутствии в системе установленной и библиотеки OpenSSL с настроенным движком ГОСТ (отсутствии возможности открыть и использовать данный движок) экспорт объектов ключевых контейнеров будет невозможен.

Использование ContainerTool

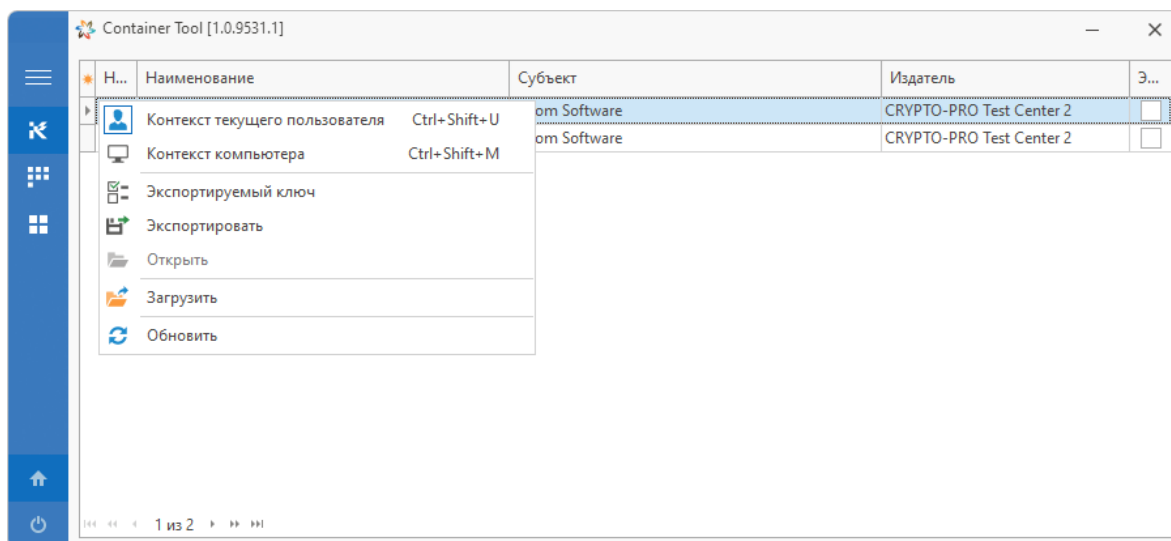
Утилита отображает список ключевых контейнеров активного контекста (пользователя или компьютера) выбранного криптопровайдера:



Для криптопровайдера RSA от Microsoft отображаются не все имеющиеся ключевые контейнеры, а только те из них, для которых был найден соответствующий сертификат.

Переключение криптопровайдера осуществляется на панели навигации. По умолчанию выбран криптопровайдер КриптоПро CSP.

Переключение контекста криптопровайдера осуществляется через контекстное меню списка ключевых контейнеров (либо через соответствующие комбинации горячих клавиш):



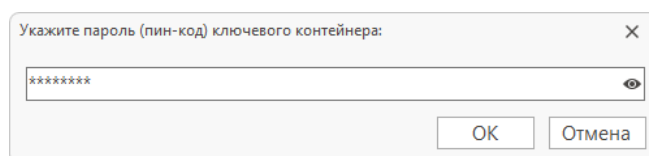
Также контекстное меню списка ключевых контейнеров позволяет:

- Модифицировать значение флага экспорта выбранного ключевого контейнера. Сам контейнер должен располагаться в реестре, в директории на диске или на аппаратном ключе (usb-токене) одного из поддерживаемых видов
- Экспортировать сертификат и закрытый ключ из ключевого контейнера в файлы формата OpenSSL (каждый экспортируемый объект помещается в отдельный файл) и PEM (все объекты помещаются в один файл)
- Загружать с диска ключевые контейнеры, расположенные вне зоны видимости соответствующего криптопровайдера – директорий для криптопровайдера КриптоПро CSP и файлов для криптопровайдера ViP Net CSP

Модификация значения флага экспорта

Пункт "Экспортируемый ключ" контекстного меню выбранного ключевого контейнера отображает текущее значение его флага экспорта и позволяет переключать это значение.

В том случае, когда для модификации ключевого контейнера требуется знание соответствующего пароля, утилита предложит пользователю указать его:



Как правило, знание пароля требуется для ключевых контейнеров, хранящихся на аппаратных ключах, а также для ключевых контейнеров криптопровайдера ViP Net CSP.

Экспорт объектов ключевого контейнера

Для того чтобы использовать тот или иной сертификат (с соответствующим ему закрытым ключом) в ПО, способном работать с сертификатами подписи через OpenSSL, этот сертификат должен быть выгружен в файл(ы) соответствующего формата. Утилита позволяет осуществлять такую выгрузку (экспорт) в одном из двух вариантах:

- Формат OpenSSL. Каждый объект ключевого контейнера (закрытый ключ, открытый ключ, сертификат) может быть выгружен отдельно от остальных объектов в соответствующий файл. Закрытый ключ может быть защищен паролем
- Формат PEM. Закрытый ключ и сертификат выгружаются в один файл. Закрытый ключ может быть защищен паролем:

Экспорт ключевого контейнера

Axiom Software 256

Формат экспорта ключевого контейнера
PEM

Файл данных
D:\AxiomSoftware256.pem

Шифрование закрытого ключа
AES-256 CBC

Пароль закрытого ключа

OK Отмена