ROSA Crypto Tool

Руководство

Оглавление

Введение

Программа ROSA Crypto Tool предназначена для работы с электронно-цифровыми подписями хранящимися в контейнере формата .sig СКЗИ КриптоПро.
В программе предусмотрена реализация подписи и проверки подписи файлов в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 (см. Приложение А)

Внешний вид программы

На рисунке 1 приведено изображение пользовательского интерфейса программы.

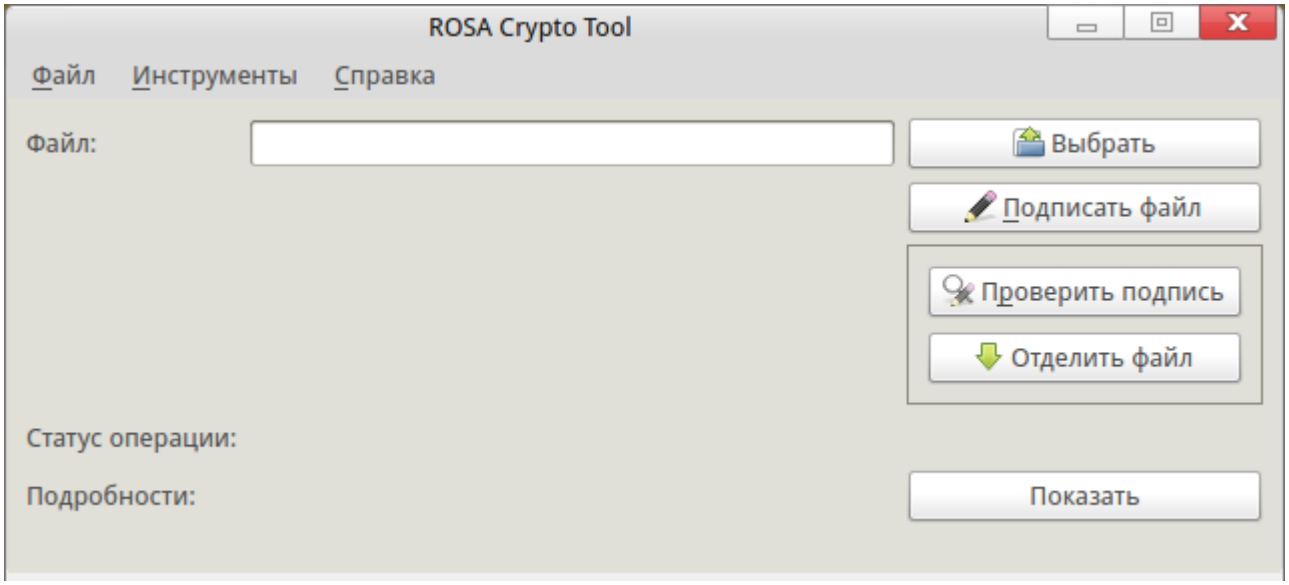

Рисунок 1 – Пользовательский интерфейс программы

Ниже будут описаны основные компоненты рабочего окна пользовательского интерфейса программы

Панель меню

Панель меню имеет всего три раздела:
- Файл
- Инструменты
- Справка

На рисунке 2 изображена панель меню.

Рисунок 2 – Панель меню программы

В разделе «Файл» находятся опции выбора файла и выхода из программы. В инструментах располагаются все необходимые опции для работы (подписи, проверки и т.д.). О самой программе и её справочную информацию можно найти в разделе «Справка».

Рабочая область

Рабочая область программы состоит из:

- поля «Файл» в котором будет отображаться имя выбранного файла
- поля «Статус операции». Здесь отображается общая информация о проделанном действии
- поля «Подробности» содержит в себе детальную информация о проделанной операции. По-умолчанию эта область скрыта.

На рисунке 3 изображена основная рабочая область программы

Рисунок 3 – Рабочая область программы

На рабочей области так же представлены кнопки:

- Выбрать
- Подписать файл
- Проверить подпись
- Отделить файл
- Показать

Подробнее о функциях каждой кнопки можно узнать из разделов представленных ниже.

Проверка подписи файла

Для того, что бы проверить подпись файла, необходимо:
1. Выбрать файл с помощью кнопки «Выбрать» или
   Верхнее меню - Файл - Выбрать файл (горячая комбинация клавиш Ctrl+O)
2. Нажать на кнопку «Проверить подпись» или
   Верхнее меню - Инструменты - Проверить подпись

После этого, в поле «Статус операции» будет выведено соответствующее оповещение.

Чтение файла

Для того что бы прочитать файл, необходимо:
1. Выбрать файл с помощью кнопки «Выбрать» или
   Верхнее меню - Файл - Выбрать файл (горячая комбинация клавиш Ctrl+O)
2. Нажать на кнопку «Отделить файл» или
   Верхнее меню - Инструменты - Отделить файл

После этого, в директории файла подписи над которым проводилась данная операция, появится новый файл, доступный для прочтения соответствующими программами, а в поле «Статус операции» будет выведено соответствующее оповещение.

Подпись файла

Перед первым использованием токена для осуществления подписи файлов в дальнейшем, необходимо, единожды произвести установку сертификата на компьютер. Для этого выберите Верхнее меню - Инструменты - Установить сертификат. В поле «Статус операции» будет выведено соответствующее оповещение.

Для того, что бы выполнить подписание файла, необходимо:
1. Выбрать файл с помощью кнопки «Выбрать» или
   Верхнее меню - Файл - Открыть файл (горячая комбинация клавиш Ctrl+O)
2. Нажать на кнопку «Подписать файл» или
   Верхнее меню - Инструменты - Подписать файл

После этого, в поле «Статус операции» будет выведено соответствующее оповещение.

Поле Подробности

Для отображения подробной информации о совершённой операции необходимо нажать на кнопку «Показать». После этого, кнопка «Показать» поменяется на кнопку «Скрыть» и раскроется большое поле в котором будет выведена соответствующая информация доступная для копирования.
Что бы свернуть область подробной информации необходимо нажать на кнопку «Скрыть».

Заметка к Альфа версии

Данная программа находится на стадии альфа. Поэтому в программе отсутствует возможность:

- выбора сертификата при наличии их более одного на токене (будет использоваться первый входящий)
- шифрование и расшифрование файлов методами СКЗИ КриптоПро

Приложение А

Порядок перехода к использованию национального стандарта
ГОСТ Р 34.10-2012 в средствах электронной подписи для информации,
не содержащей сведений, составляющих государственную тайну,
в случаях, подлежащих регулированию со стороны ФСБ России
в соответствии с действующей нормативной правовой базой

(выписка из документа ФСБ России № 149/7/1/3-58 от 31.01.2014
"О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования")

Для средств ЭП, техническое задание на разработку которых утверждено после 31 декабря 2012 года, должна быть предусмотрена реализация функций средства в соответствии с ГОСТ Р 34.10-2012 хотя бы по одному из определяемых стандартом вариантов требований к параметрам (использование варианта, соответствующего длине секретного ключа порядка 256 бит, является предпочтительным, поскольку обеспечивает достаточный уровень криптографической стойкости и лучшие эксплуатационные характеристики, в том числе при совместной реализации со схемой ГОСТ Р 34.10-2001). После 31 декабря 2013 года не осуществлять подтверждение соответствия средств ЭП Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27.12.2011 г. № 796, если в этих средствах не предусмотрена реализация функций средства в соответствии с ГОСТ Р 34.10-2012 хотя бы по одному из определяемых стандартом вариантов требований к параметрам. Исключение может быть сделано

для средств ЭП, удовлетворяющих одновременно следующим условиям:
техническое задание на разработку средства утверждено до 31 декабря 2012 года;
в соответствии с техническим заданием разработка средства завершена после 31 декабря 2011 года;
подтверждение соответствия средства указанным Требованиям ранее не осуществлялось.
Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается.