НТЦ ИТ РОСА
Научно-технический центр
информационных технологий

ROSA Crypto Tool

Руководство пользователя

v1.0.0

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)

1. 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.

1.1 Панель инструментов

На панели инструментов располагаются пять кнопок.

Первые четыре кнопки предназначены для переключения режимов работы с СКЗИ, а именно:

- Подписать файл
- Проверить подпись
- Шифровать
- Расшифровать

На рисунке 2 представлена панель инструментов.

Рисунок 2 – Панель инструментов программы

Последняя кнопка называется «Параметры» и содержит в себе дополнительное подменю не относящееся напрямую к работе с СКЗИ.

1.2 Рабочая область

Рабочая область программы располагается под панелью инструментов.

При запуске программы, при условии того, что все остальные компоненты необходимые для полного её функционирования успешно установлены и работают, в рабочей области будет отображаться только приветствующий текст (рис 3).

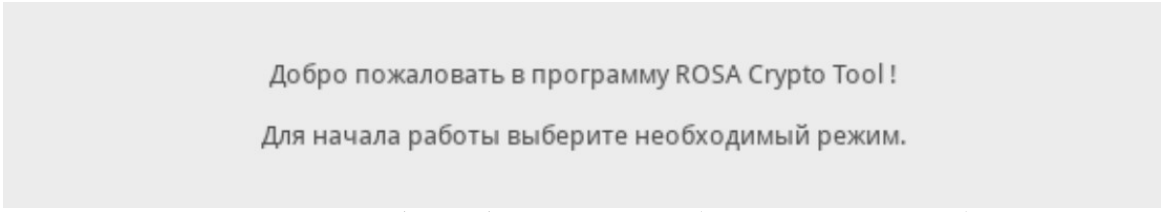

Рисунок 3 – Рабочая область программы (приветствующий текст)

В противном случае, под приветствующем текстом будет выведено соответствующее сообщение (рис 4).

Рисунок 4 – Рабочая область программы (приветствующий текст с заметкой)

При подключении или извлечении токена(ов) из компьютера, так же, под приветствующем текстом будет выведено соответствующее сообщение.

После выбора кого-либо из режимов, на панели инструментов, рабочая область обновляется на соответствующий набор графических элементов для работы с СКЗИ.

На рисунке 5 представлено статусное поле информирующее состояние токена(ов).

Рисунок 5 – Статусное поле

Это поле доступно во всех режимах.

2. Подпись файла

Для того, чтобы подписать файл, необходимо:

1. На панели инструментов выбрать режим «Подписать файл»
2. Выбрать файл с помощью кнопки «Выбрать»
3. В поле «Сертификат» из выпадающего списка выбрать необходимый контейнер.
4. Нажать на кнопку «Подписать файл»

На рисунке 6 представлен режим «Подписать файл».

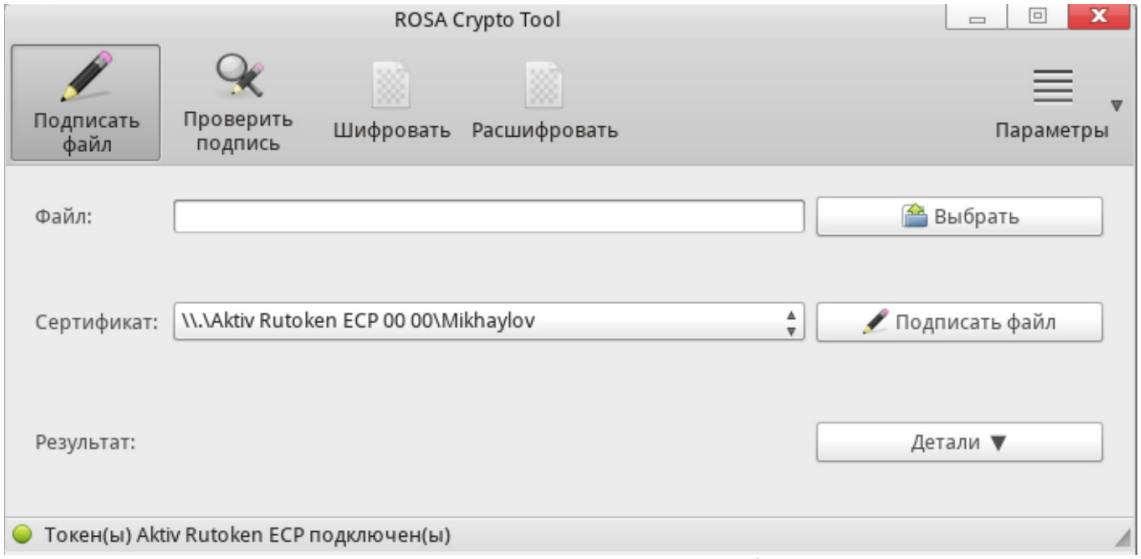

Рисунок 6 – Режим «Подписать файл»

После успешного выполнения операции, в поле «Результат» будет выведено соответствующее оповещение и в папке выбранного файла появится подписанный файл с расширением .sig.

Кнопка «Детали» раскрывает поле «Результат» для отображения более полной информации, доступной для выделения и копирования.

3. Проверка подписи

Для того, что бы проверить подпись файла, необходимо:

1. На панели инструментов выбрать режим «Проверить подпись».
2. Выбрать файл с помощью кнопки «Выбрать».
3. Если дополнительно необходимо установит сертификат из файла подписи и/или отделить исходный файл от файла подписи, то тогда выставляем галочки слева от имени соответствующей дополнительной опции.
4. Нажать на кнопку «Проверить подпись».

На рисунке 7 представлен режим «Проверка подписи»

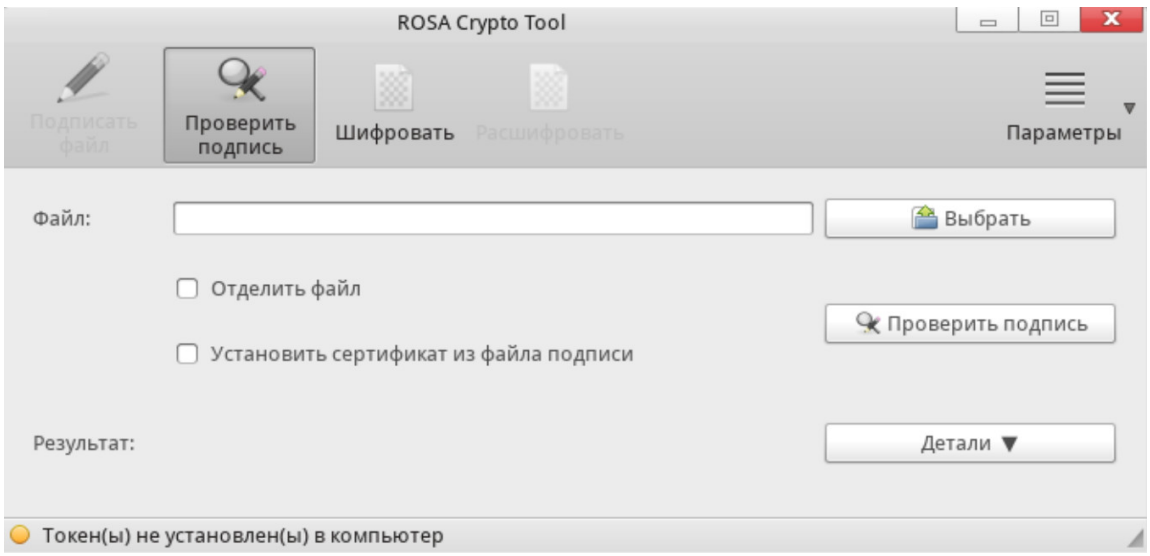

Рисунок 7 – Режим «Проверить подпись»

После выполнения операции, в поле «Результат» будет выведено соответствующее оповещение.

Кнопка «Детали» раскрывает поле «Результат» для отображения более полной информации доступной для выделения и копирования.

4. Шифрование

Для того, что бы выполнить шифрование файла, необходимо:

1. На панели инструментов выбрать режим «Шифровать».
2. Выбрать файл с помощью кнопки «Выбрать».
3. В поле «Сертификат» выбрать соответствующий сертификат с помощью которого необходимо зашифровать файл.
4. Нажать на кнопку «Шифровать».

На рисунке 8 представлен режим «Шифровать»

Рисунок 8 – Режим «Шифровать»

После успешного выполнения операции, в поле «Результат» будет выведено соответствующее оповещение и в директории выбранного файла появится файл подписи с расширением .enc.

Кнопка «Детали» раскрывает поле «Результат» для отображения более полной информации доступной для выделения и копирования.

5. Расшифрование

Для того, что бы выполнить расшифровывание файла, необходимо:

1. На панели инструментов выбрать режим «Расшифровать».
2. Выбрать файл с помощью кнопки «Выбрать».
3. В поле «Сертификат» из выпадающего списка выбрать необходимый контейнер.
4. Нажать на кнопку «Расшифровать».

На рисунке 9 представлен режим «Расшифровать»

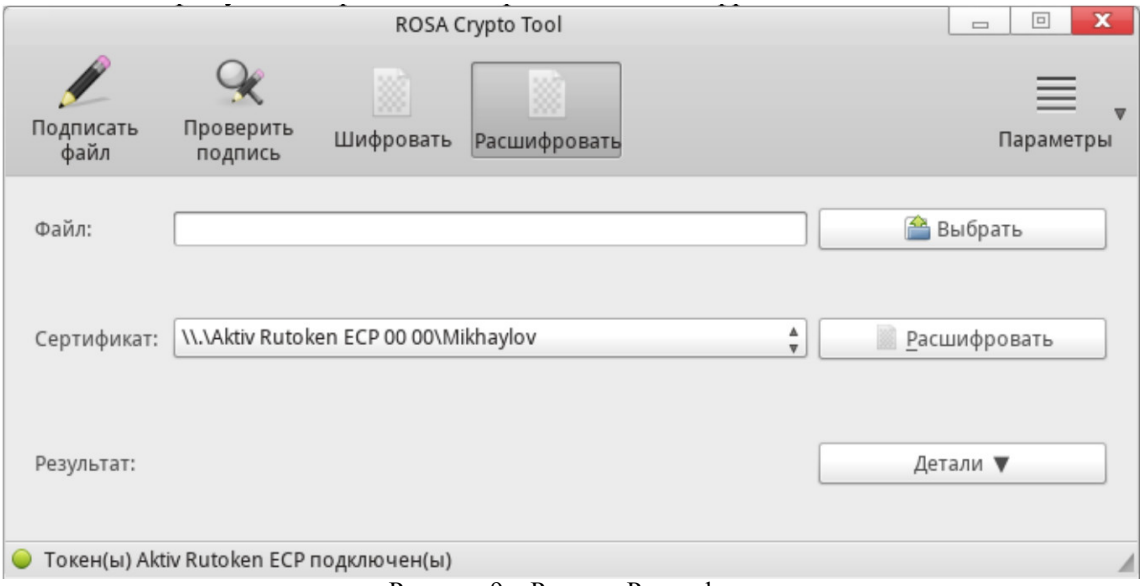

Рисунок 9 – Режим «Расшифровать»

После выполнения операции, в поле «Результат» будет выведено соответствующее оповещение.

Кнопка «Детали» раскрывает поле «Результат» для отображения более полной информации доступной для выделения и копирования.

6. Взаимодействие с файлом

6.1 Предпросмотр файла

В режиме «Подписать файл» или «Шифровать» доступна функция предпросмотра файла. Для её активации, необходимо:

1. Выбрать файл с помощью кнопки «Выбрать».

В поле «Файл» отобразится серый значок предпросмотра ввиде глаза (рисунок 10)

Рисунок 10 – Значок предпросмотра

2. Навести курсор на значок предпросмотра.

Значок предпросмотра поменяет свой цвет с серого на чёрный и справа от курсора мыши появится небольшое окно, в котором будет представлена часть выбранного файла.

На рисунке 11 представлен предпросмотр файла

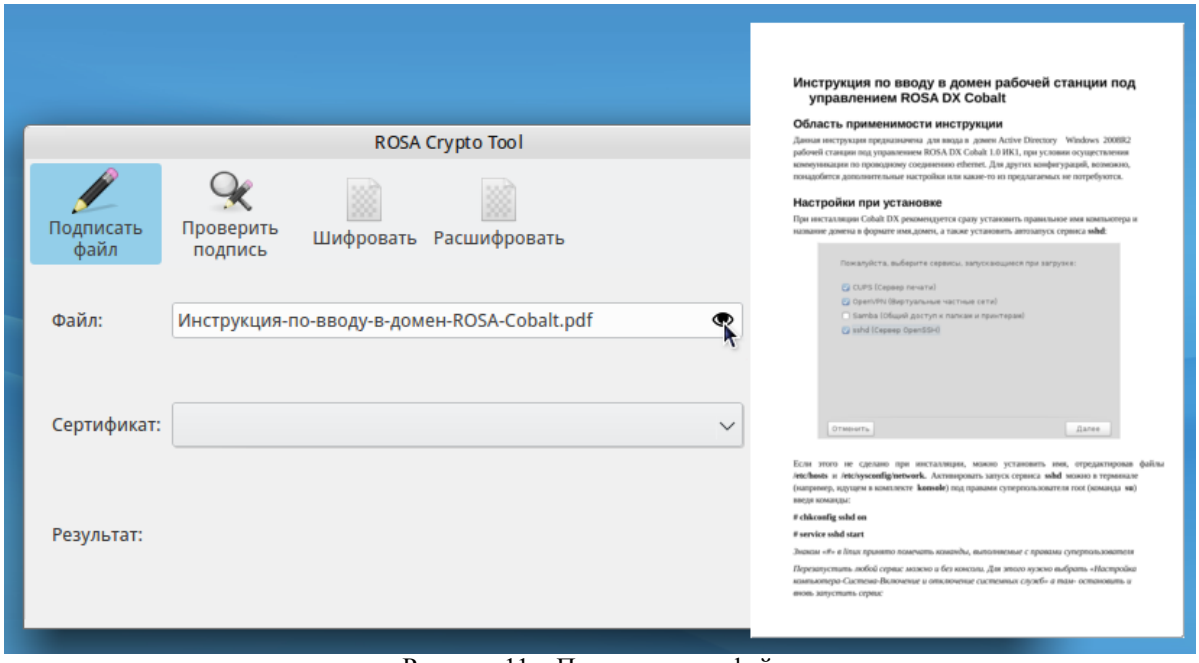

Рисунок 11 – Предпросмотр файла

С полным перечнем поддерживаемых форматов файла, доступного для предпросмотра, можно ознакомиться в Приложение Б.

6.2 Расположение файла

Что бы узнать расположение файла в системе (абсолютный путь) необходимо навести курсор мыши на поле «Файл» и подождать некоторое время.

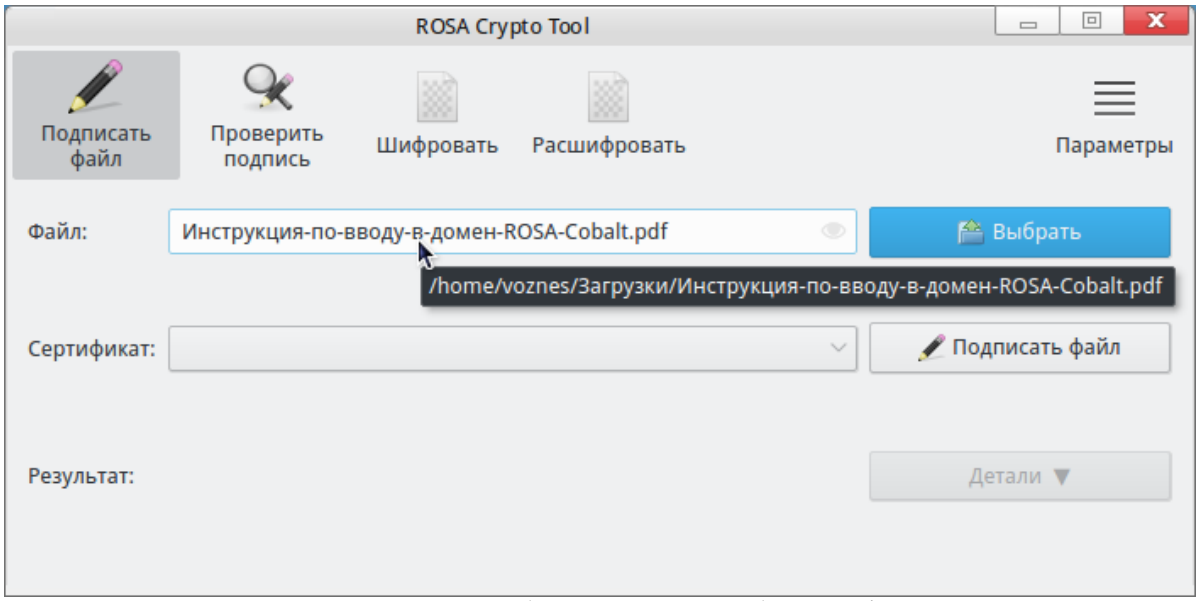

Рисунок 12 – Вывод абсолютного пути выбранного файла

Появится всплывающая подсказка содержащая абсолютный путь выбранного файла (рисунок 12)

6.3 Открытие файла внешней программой

Для открытия выбранного файла внешней программой необходимо:
1. Навести курсор мыши на значок предпросмотра (рисунок 13)

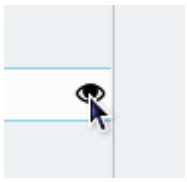

Рисунок 13 – Курсор мыши на значке предпросмотра

2. Совершить один «клик» по значку предпросмотра

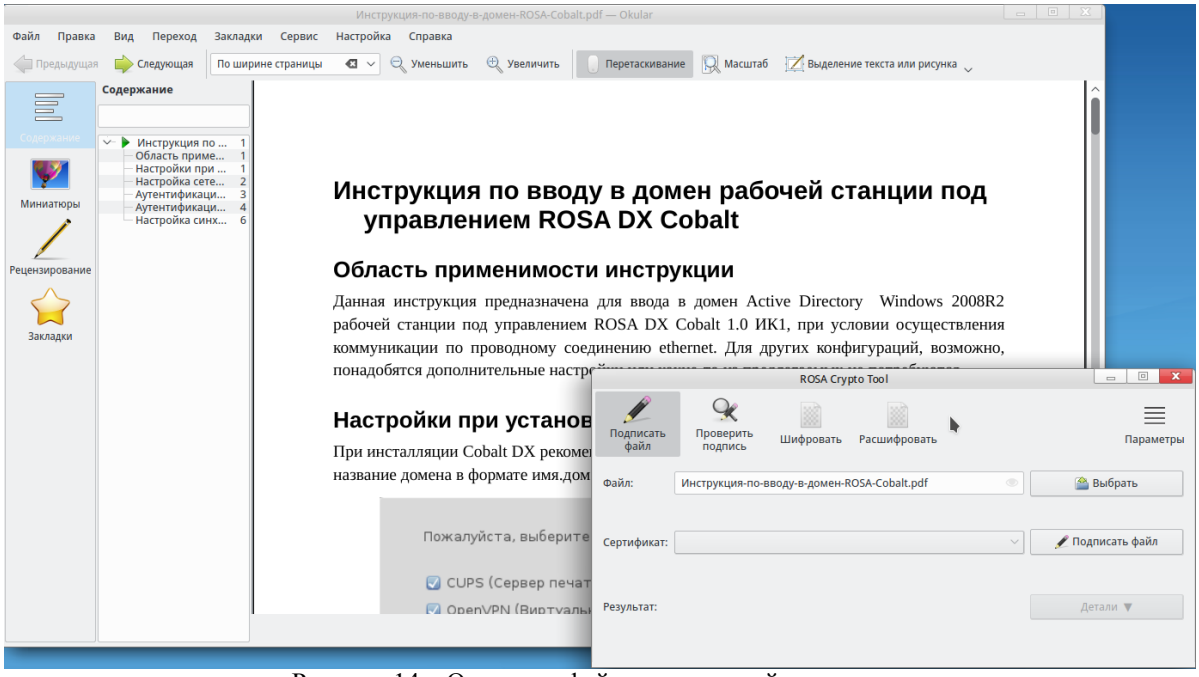

Рисунок 14 – Открытие файла в сторонней программе

На рисунке 14 представлено открытие файла типа pdf в сторонней программе запущенной путём одинарного клика на значок предпросмотра.

7. Параметры

Кнопка «Параметры» содержит в себе дополнительное подменю, включающее в себя такие опции как:

1. Проверка компонентов программы – проверяет наличие необходимых компонентов для успешной работы программы и соответствующее оповещение пользователя.
2. О программе ROSA Crypto Tool – выводит краткую информацию о программе.
3. Справка – открывает руководство пользователя.
4. Выход – осуществляет выход из программы.

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 No 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. No 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.

ВНИМАНИЕ

Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается.

Приложение Б

Тип файла	Расширение файла
Текстовый документ	doc, doc6, doc95, docx, docx7, docbook, ooxml, xml, xhtml, latex, ltx, bib, txt, odt, fodt, ott, pdf, rtf, stw, sxw, text, uot
Веб-документ	etext, html10, html, mediawiki, text10
Таблица	csv, dbf, dif, fods, ods, ots, slk, stc, sxc, uos, xls, xls5, xls95, xlt, xlt5, xlt95, xlsx
Изображение	bmp, emf, eps, fodg, gif, jpg, met, odd, otg, pbm, pct, pgm, png', ppm, ras, std, svg, svm, swf, sxd, tiff, wmf, xpm
Презентация	odg, odp, otp, pct, potm, pot, ppm, pptx, pps, ppt, pwp, sda, sti, sxi, uop