ROSA Crypto Tool

Руководство пользователя

v0.2.1

Оглавление

Введение

Программа ROSA Crypto Tool предназначена для работы с электронно-цифровыми подписями, хранящимися в контейнере формата .sig СКЗИ Крипто-Про.

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.

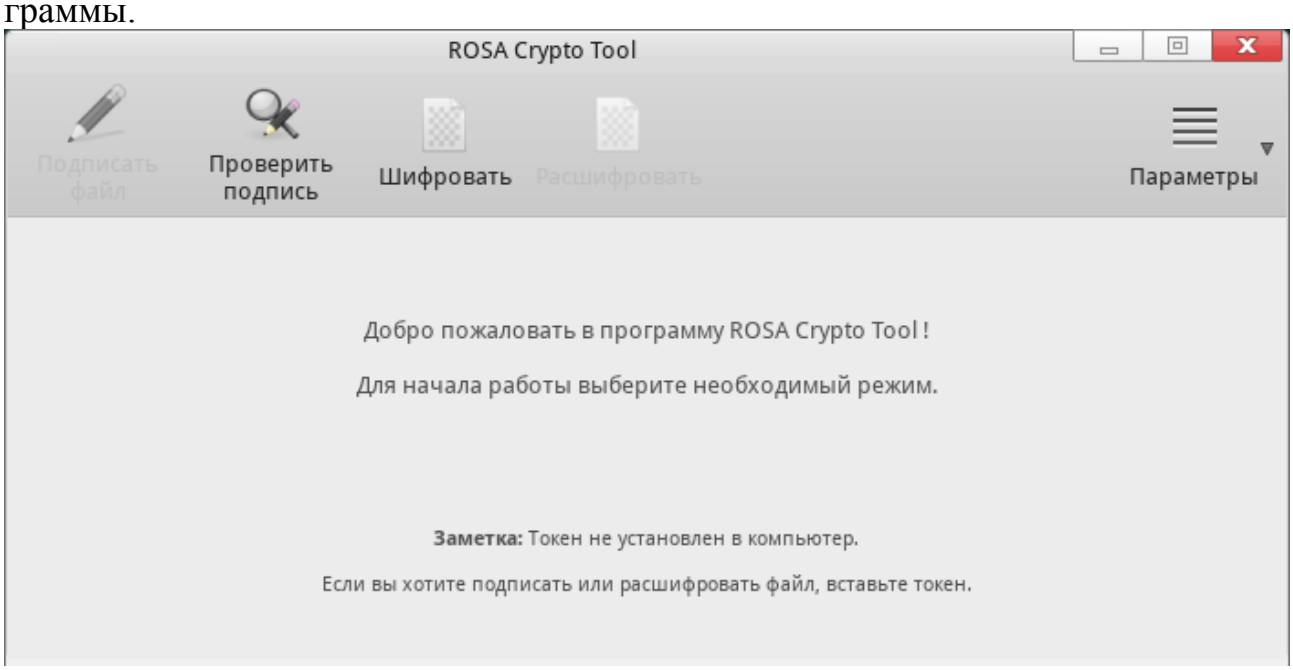

Рисунок 1 – Пользовательский интерфейс программы

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. Подписать файл

Для того, чтобы подписать файл, необходимо:

1. На панели инструментов выбрать режим «Подписать файл»
2. Выбрать файл с помощью кнопки «Выбрать»
3. Если в компьютере, к примеру, установлено несколько токенов, то в поле «Сертификат» из выпадающего списка выбрать необходимый.
4. Нажать на кнопку «Подписать файл»

На рисунке 6 представлен режим «Подписать файл»

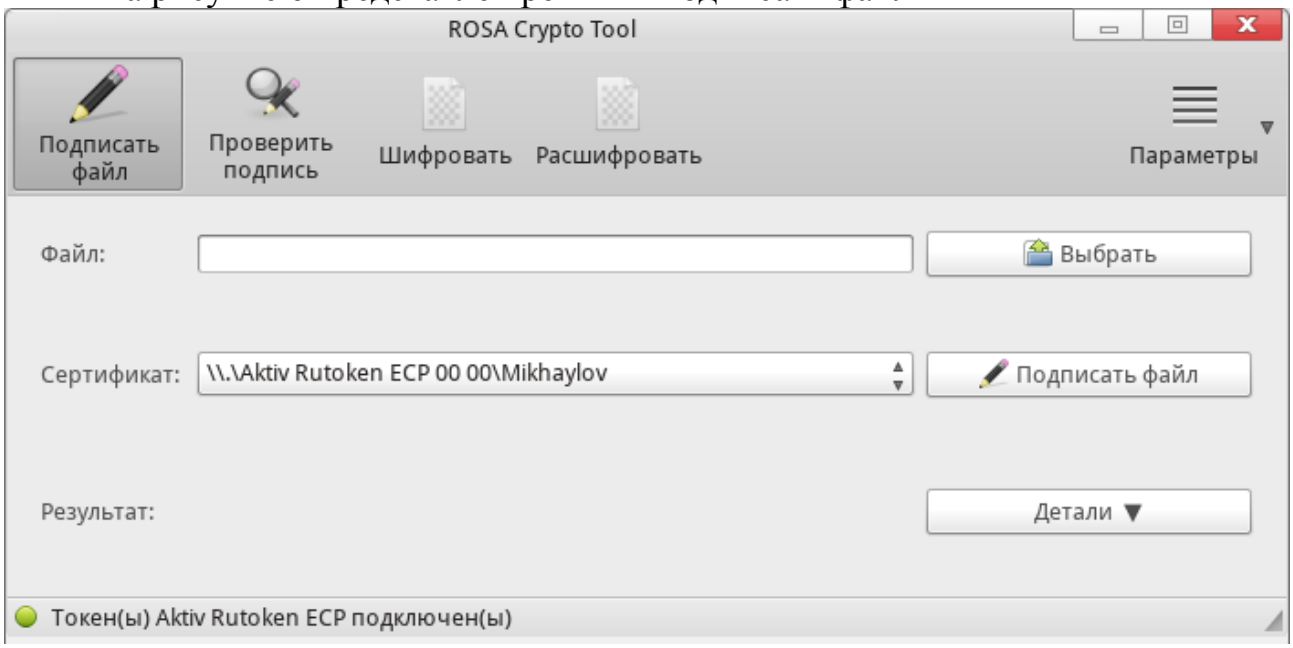

Рисунок 6 – Режим «Подписать файл»

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. Проверить подпись

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»

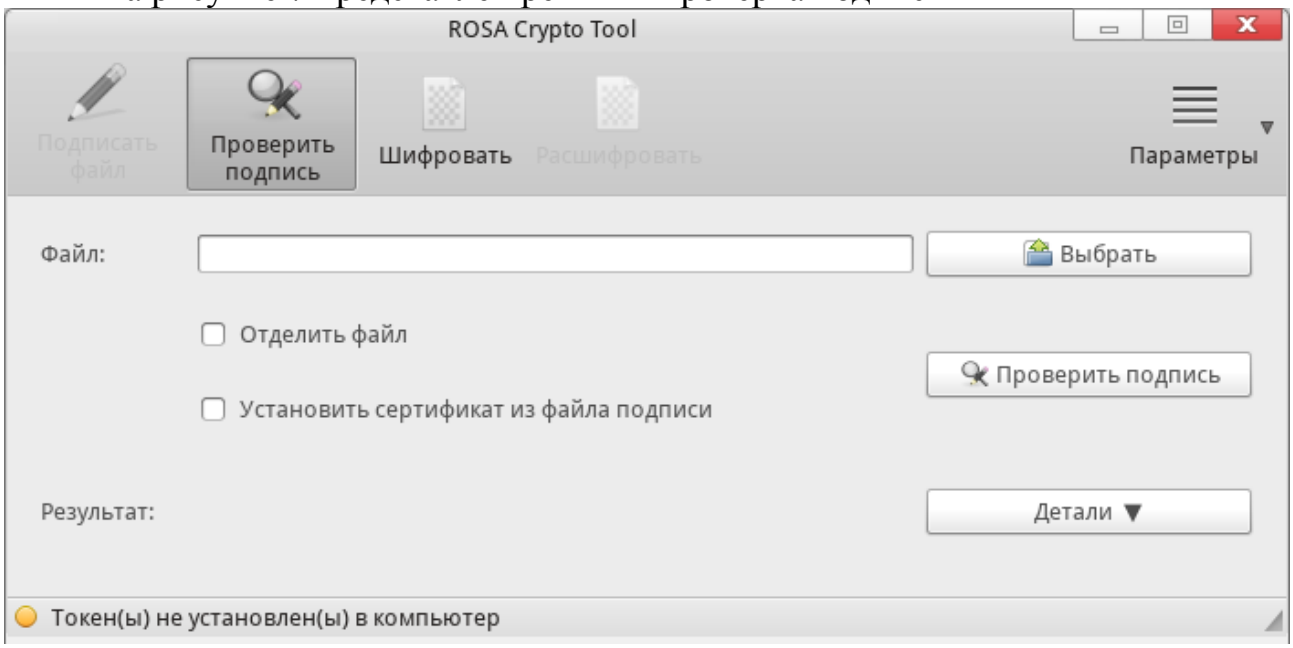

Рисунок 7 – Режим «Проверить подпись»

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. Шифровать

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»

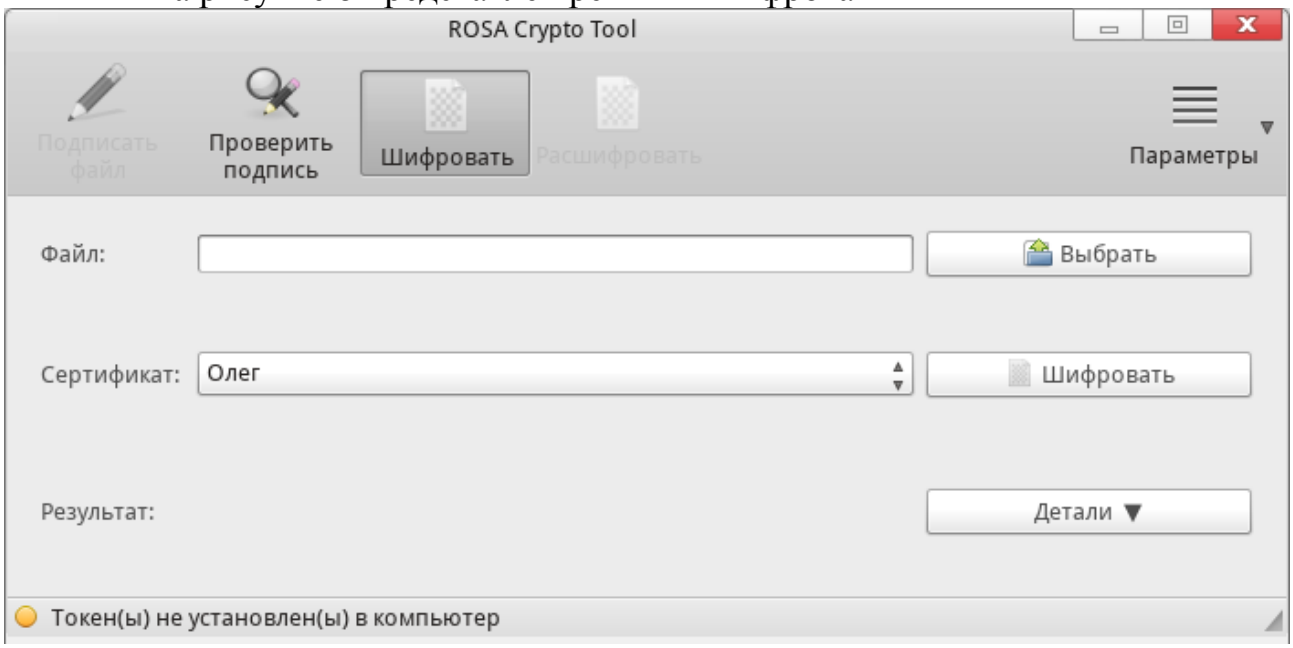

Рисунок 8 – Режим «Шифровать»

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. Расшифровать

Для того, что бы выполнить расшифровывание файла, необходимо:

1. На панели инструментов выбрать режим «Расшифровать»
2. Выбрать файл с помощью кнопки «Выбрать»
3. Если в компьютере, к примеру, установлено несколько токенов, то в поле «Сертификат» из выпадающего списка выбрать необходимый.
4. Нажать на кнопку «Расшифровать»

На рисунке 9 представлен режим «Расшифровать»

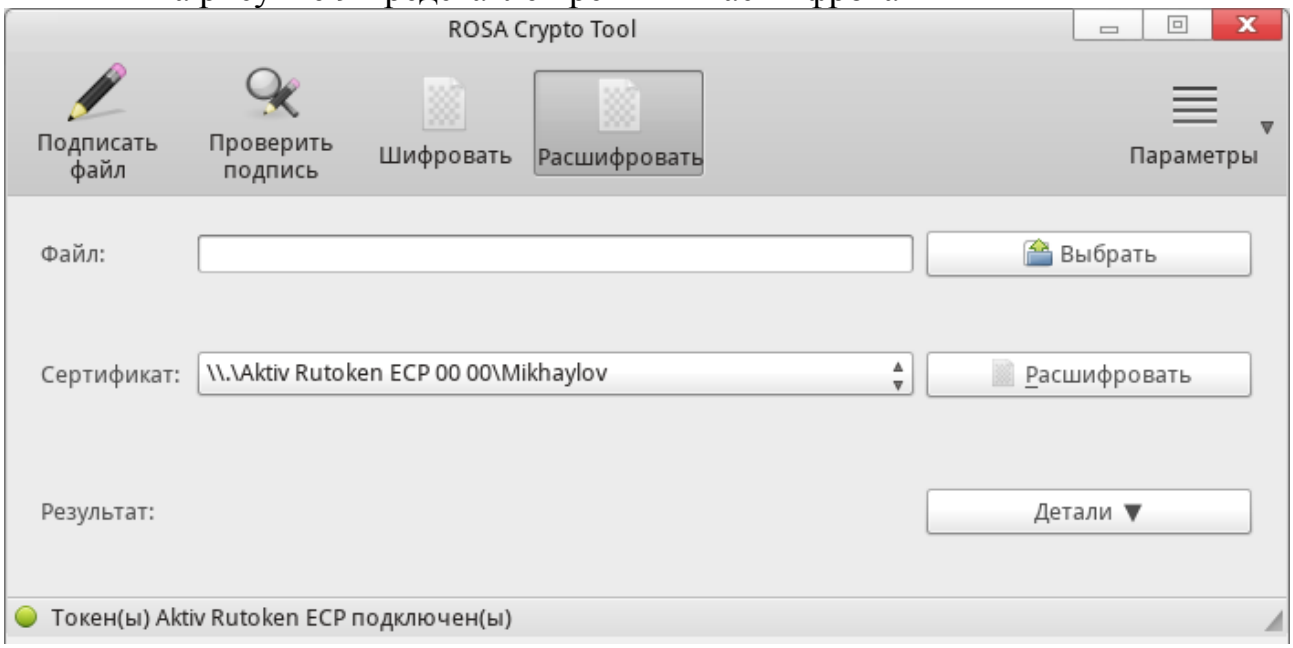

Рисунок 9 – Режим «Расшифровать»

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. Параметры

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

- *Проверка компонентов программы* – проверяет наличие необходимых компонентов для успешной работы программы и соответствующее оповещение пользователя.
- *О программе ROSA Crypto Tool* – выводит краткую информацию о программе
- *Справка* – открывает руководство пользователя
- *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 № 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.