Руководство к GUI-утилите

проверки электронной цифровой подписи на выбранном криптопровайдере

Автор: Максим Нестеров

Студент кафедры ИУ8-84

МГТУ им. Н. Э. Баумана

ЗАО «Актив-софт»

Москва

2016

Оглавление

[1. Описание программы 4](#_Toc458706101)

[2. Определения 5](#_Toc458706102)

[3. Элементы окон программы 8](#_Toc458706103)

[3.1 Главное окно 8](#_Toc458706104)

[3.2 Окно «Дополнительно» 13](#_Toc458706105)

[3.3 Окно «Ввод ключа» 14](#_Toc458706106)

[4. Выбор криптопровайдера 15](#_Toc458706107)

[5. Способы импорта открытого ключа (сертификата) 16](#_Toc458706108)

[5.1 Импорт сертификата через системное хранилище сертификатов 16](#_Toc458706109)

[5.2 Чтение файла сертификата 18](#_Toc458706110)

[5.3 Ввод открытого ключа 20](#_Toc458706111)

[6. Способы импорта подписи 21](#_Toc458706112)

[6.1 Чтение из файла 21](#_Toc458706113)

[6.2 Ввод подписи 21](#_Toc458706114)

[7. Способы импорта данных 22](#_Toc458706115)

[7.1 Чтение из файла 22](#_Toc458706116)

[7.2 Ввод данных 22](#_Toc458706117)

[8. Примеры 23](#_Toc458706118)

[9. Благодарности 24](#_Toc458706119)

[10. Контакты 24](#_Toc458706120)

# Описание программы

Актуальную версию программы и руководства см. по ссылке:

[*http://github.com/MaximillianMS/SignVerify*](http://github.com/MaximillianMS/SignVerify)

Данная программа предназначена для проверки электронной цифровой подписи. Для осуществления проверки необходимо выбрать нужный криптопровайдер (провайдер криптографических функций), который должен быть установлен и доступен на машине пользователя. В качестве примера в данном руководстве используется криптопровайдер от компании «КРИПТО-ПРО», позволяющий проверять электронную цифровую подпись (далее – просто *подпись*), изготовленную по стандарту ГОСТ Р 34.10-2001. На вход программа принимает данные в различных кодировках, из которых основные: Base64 и Hex. Наличие сертификата существенно упрощает прохождение проверки, так как не требуется знать дополнительные параметры подписи, такие как, например, тип выбранной эллиптической кривой. В программе имеется упрощенный анализатор формата данных, поэтому пользователю необходимо проверять правильно ли программа определила формат. Рекомендуется использовать именно выше перечисленные форматы и производить импорт данных с помощью файлов. Для ввода данных в окне приложения рекомендуется использовать «вставку» (т.е. сочетание клавиш «Ctrl-V» или «Правая кнопка мыши – вставить»). Как именно программа принимает данные можно посмотреть в соответствующем пункте (см. раздел 4, 5) в данном руководстве. Кроме того, поля, которые необходимо заполнить для успешного выполнения процедуры проверки подписи, программа выделяет красным и желтым цветом. Поля, выделенные желтым цветом, означают, что информацию можно предоставить различными способами, такими как ввод данных в текстовое окно приложения или импорт файла. После того, как будет осуществлен ввод информации через выбранный способ или выбран пункт списка, поле автоматически станет зеленым.

# Определения

В настоящем руководстве используются следующие термины с соответствующими определениями:

**Средства защиты информации** — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

**Электронная цифровая подпись (ЭЦП)** — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

**Средство криптографической защиты информации (СКЗИ)** – сертифицированные в порядке, установленном законодательством Российской Федерации, аппаратные и (или) программные средства, обеспечивающие шифрование, контроль целостности и применение ЭП при обмене электронными документами.

**Криптопровайдер** (**Провайдер криптографических функций**) — это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций CryptoAPI.

**CryptoAPI** — интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптопровайдером. Входит в состав операционных систем Microsoft. Большинство функций CryptoAPI поддерживается, начиная с Windows 2000.

**Цифровой сертификат** — цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа.

**Открытый ключ** — ключ, который может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего лица в виде отказа его от подписи документа. Открытый ключ подписи вычисляется, как значение некоторой функции от закрытого ключа, но знание открытого ключа не дает возможности определить закрытый ключ.

**Закрытый ключ** — ключ, известный только своему владельцу. Только сохранение пользователем в тайне своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего.

**Хэш-функция (collision-resistant hash-function)** – функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим

свойствам:

1) по данному значению функции сложно вычислить исходные данные,

отображаемые в это значение;

2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции;

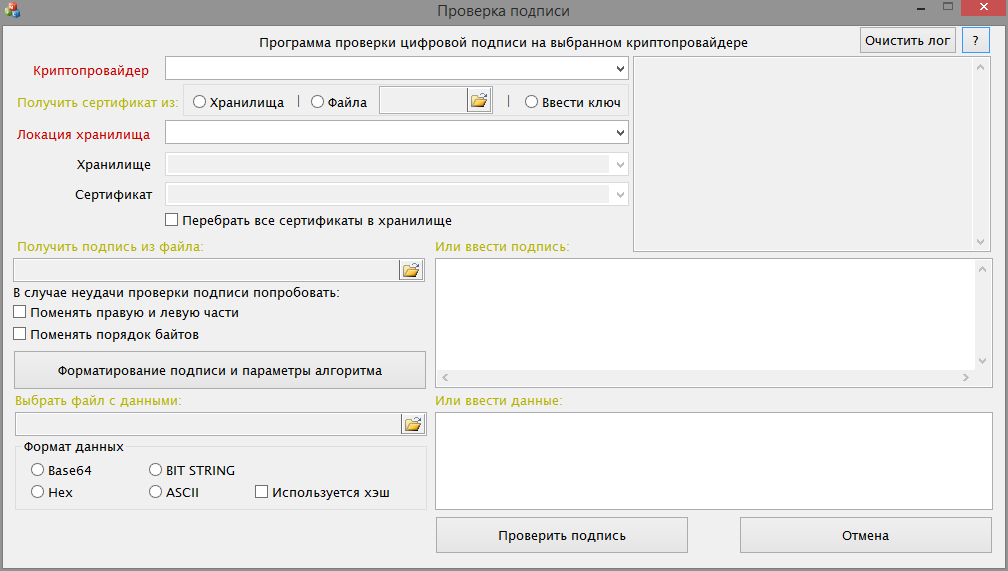
3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

**Хэш-код (hash-code)** – строка бит, являющаяся выходным результатом хэш-функции.

**Отсоединенная электронная цифровая подпись** – это подпись, создаваемая отдельно от подписываемого файла, а сам подписываемый файл никак не изменяется.

# Элементы окон программы

## Главное окно



**21**

**20**

**19**

**18**

**17**

**16**

**13**

**15**

**14**

**12**

**11**

**10**

**9**

**8**

**5**

**7**

**6**

**3**

**2**

**1**

**4**

Рисунок 1 – Главное окно программы

На Рисунке 1 показаны элементы главного окна программы:

1. Список криптопровайдеров

Метка «Криптопровайдер» и соответствующий комбо-бокс. Выбор криптопровайдера из списка приводит к установлению поля в зеленый цвет.

1. Радиокнопка «Хранилища»

Выбирает режим импорта сертификата их хранилища сертификатов.

1. Радиокнопка «Файла» и поле с названием файла сертификата и кнопкой открытия диалога выбора файла сертификата

Радиокнопка выбирает режим импорта сертификата их хранилища сертификатов. Файл выбирается с помощью нажатия на иконку папки. Также радиокнопка автоматически выбирается при нажатии на иконку папки сразу.

1. Радиокнопка «Ввести ключ»

Открывает диалог ввода открытого ключа (см. Рисунок 2).

1. Текстовое поле «Лог программы»

Данное текстовое поле предназначено для вывода информации о работе программы.

1. Кнопка «Очистить лог»

Нажатие на кнопку выполняет очистку текстового поля «Лог программы» (элемент 5).

1. Кнопка «О программе»

Открывает окно с информацией о программе.

1. Список локаций

Метка «Локация хранилища» и соответствующий комбо-бокс. Выбор локации из списка приводит к установлению поля в зеленый цвет. Доступно только при выборе режима «Хранилища» (элемент 2).

1. Список хранилищ

Метка «Хранилища» и соответствующий комбо-бокс. Список хранилищ обновляется после выбора локации. Выбор хранилища из списка приводит к установлению поля в зеленый цвет. Доступно только при выборе режима «Хранилища» (элемент 2).

1. Список сертификатов

Метка «Сертификат» и соответствующий комбо-бокс. Список сертификатов обновляется после выбора хранилища (элемент 9). Выбор сертификата из списка приводит к установлению поля в зеленый цвет. Доступно только при выборе режима «Хранилища» (элемент 2).

1. Чек-бокс «Перебрать все сертификаты в хранилище»

Установка данного чек-бокса приводит, при проверке подписи, к перебору всех сертификатов, лежащих в данном хранилище. Используется только в том случае, если подпись представлена в сыром виде (то есть импортирована не в формате «PEM» -отсоединенной подписи). Доступно только при выборе режима «Хранилища» (элемент 2).

1. Поле с названием файла подписи и кнопкой открытия диалога выбора файла подписи

Используется для импорта непосредственно подписи, представленной в форматах Base64, Hex в случае, если используются «сырые» данные, а также в формате «PEM», закодированном в тех же форматах. Файл выбирается с помощью нажатия на иконку папки. После выбора файла подписи автоматически будет определен ее формат. Выбрать формат вручную можно с помощью кнопки «Формат подписи и параметры алгоритма» (элемент 16). После выбора файла метка «Получить подпись из файла» будет автоматически установлена в зеленый цвет.

1. Текстовое поле для ввода подписи «Или ввести подпись»

Предназначено для ввода подписи, представленной в различных форматах. Выбрать формат вручную можно с помощью кнопки «Формат подписи и параметры алгоритма» (элемент 16).

1. Чек-бокс «Поменять правую и левую части»

В том случае, если подпись представлена не в формате «PEM», установка данного чек-бокса приводит к изменению подписи следующим образом: так как подпись в некоторых случаях представляет собой точку на эллиптической кривой, то возможно, что при получении подписи ее координаты были перепутаны, поэтому программа также опробует в случае неудачи переставить координаты, каждая из которых представлена ровно половиной подписи.

1. Чек-бокс «Поменять порядок байтов»

В том случае, если подпись представлена не в формате «PEM», установка данного чек-бокса приводит к изменению подписи следующим образом: так как в некоторых случаях при получении подписи имеет место изменение порядка следования байтов в подписи, то программа также опробует в случае неудачи переставить байты в обратном порядке.

1. Кнопка «Формат подписи и параметры алгоритма»

Нажатие на кнопку приведет к открытию диалогового окна «Дополнительно» (см. «Окно “Дополнительно”»).

1. Поле с названием файла данных и кнопкой открытия диалога выбора файла данных

Используется для импорта непосредственно файла, для которого была получена подпись, файл будет считан в побайтовом режиме. После выбора файла метка «Выбрать файл с данными» будет автоматически установлена в зеленый цвет.

1. Текстовое поле для ввода данных «Или ввести данные»

Предназначено для ввода данных, для которых была создана подпись, представленных в различных форматах. Выбрать формат нужно с помощью группы радиокнопок «Формат данных». Также, если используется хэш-значение, вместо самих данных, необходимо поставить галочку в чек-боксе «Используется хэш», который находится в той же группе радиокнопок (элемент 19).

1. Группа радиокнопок «Формат данных» и чек-бокс «Используется хэш»

Выбор той или иной радиокнопки в данной группе определит формат данных, для которых была создана подпись, если данные вводятся непосредственно в текстовое поле. Чек-бокс «Используется хэш» предназначен для того случая, когда в программу передаются не сами данные, а их хэш-значение. В этом случае необходимо также выбрать хэш-функцию в окне «Дополнительно» (см. «Окно “Дополнительно”»).

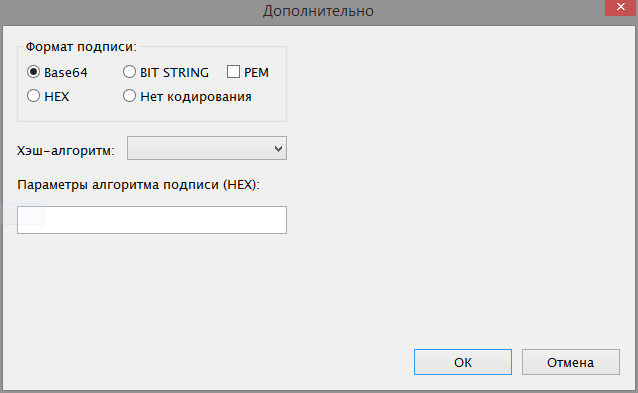
1. Кнопка «Проверить подпись»

Нажатие на данную кнопку запускает алгоритм проверки подписи. Информация об результатах проверки и ошибках выводится в «Лог программы» (элемент 5).

1. Кнопка «Отмена»

Нажатие на данную кнопку равносильно нажатию на «крестик» в правом верхнем углу диалогового окна – освобождает ресурсы, занятые программой, и закрывает ее.

## Окно «Дополнительно»



**24**

**23**

**22**

Рисунок 2 – Окно «Дополнительно»

На Рисунке 2 показаны элементы окна «Дополнительно»:

1. Группа радиокнопок «Формат подписи» и чек-бокс «PEM»

Выбор той или иной радиокнопки в данной группе определит формат подписи, при ее импорте из файла или вводе в текстовое поле. Чек-бокс «PEM» предназначен для того случая, когда подпись импортируется в формате «PEM».

1. Хэш-функция

Метка «Хэш-функция» и соответствующий комбо-бокс. Список алгоритмов обновляется при каждом выборе криптопровайдера. Выбор хэш-функции из списка приводит к использованию данного хэш-функции при проверке подписи. Необходимо только при проверке подписи без сертификата (см. раздел 4.3).

1. Параметры подписи алгоритма

Данное текстовое поле предназначено для ввода параметров алгоритма проверки подписи в формате HEX. Необходимо заполнять только при проверке подписи без сертификата (см. раздел 4.3).

## Окно «Ввод ключа»

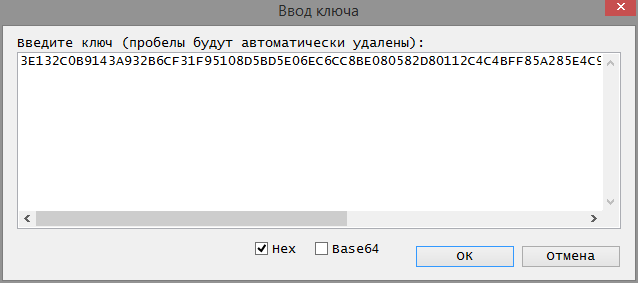


Рисунок 3 – Окно «Ввод ключа»

На Рисунке 3 показано окно «Ввод ключа». Ключ может быть введен в форматах «HEX» или «Base64». Программа автоматически определит формат ключа.

# Выбор криптопровайдера

Для проверки подписи необходимо выбрать криптопровайдер. При запуске программы приложение определяет список установленных криптопровайдеров в системе пользователя (элемент 1):

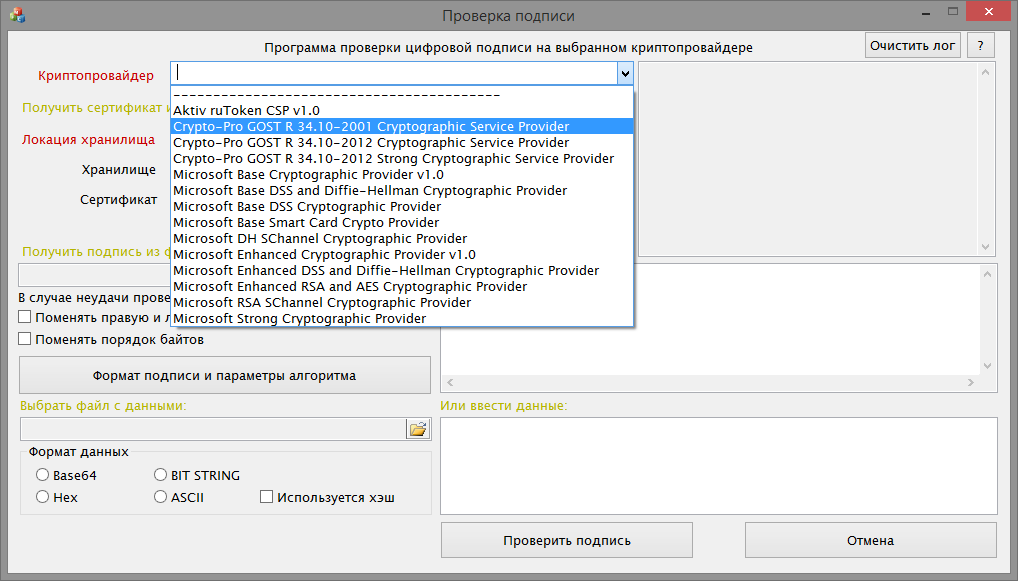


Рисунок 4 – Выбор криптопровайдера

После того как криптопровайдер будет выбран, программа получит список хэш-функций и обновит их список (элемент 23).

# Способы импорта открытого ключа (сертификата)

В программе существует три способа импорта открытого ключа: два – с помощью сертификатов и один – непосредственный ввод ключа.

## Импорт сертификата через системное хранилище сертификатов

Если требуемый сертификат присутствует в системном хранилище, то есть его можно найти через стандартный менеджер просмотра установленных сертификатов «certmgr.msc» (см. Рисунок 5), то необходимо выбрать этот режим импорта.

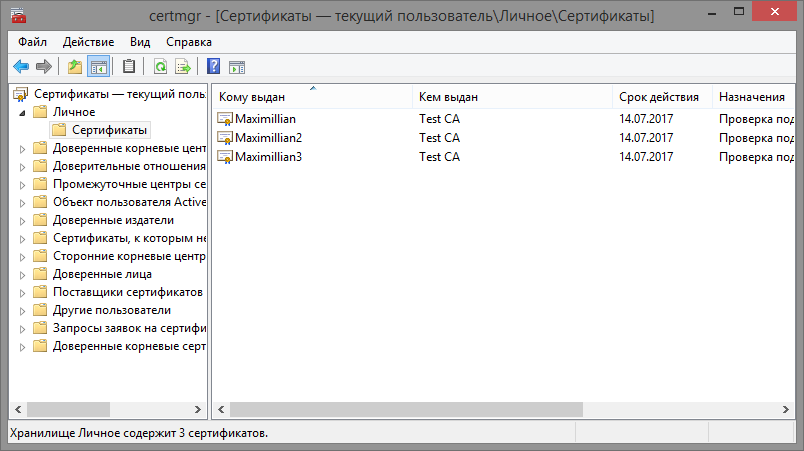


Рисунок 5 – Менеджер сертификатов ОС Windows

Пусть требуемый сертификат имеет название «Maximillian». В данном списке он самый первый. Выберем этот сертификат в нашей программе.

Для этого выберем локацию хранилища сертификатов. В данном руководстве и данной программе «локацией» называется место, в котором находятся хранилища на компьютере пользователя. Так как сертификат находится в каталоге «Личное» (англ. «My») текущего пользователя (анг. «CurrentUser»), то необходимо в поле «Локация хранилища» (элемент 8) выбрать «CurrentUser», в поле «Хранилище» (элемент 9) выбрать «My», а в поле «Сертификат» (элемент 10) выбрать требуемый сертификат, то есть в нашем случае «Maximillian».

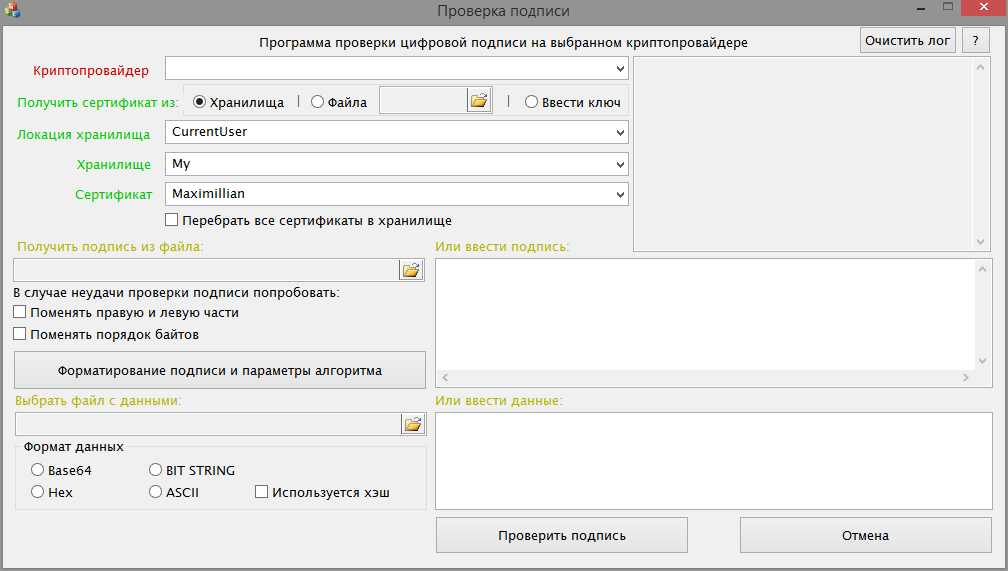


Рисунок 6 – Импорт сертификата из локального хранилища

Если пользователь не уверен, какой из сертификатов, лежащих в хранилище, ему требуется, то программа может перебрать все сертификаты. Для этого необходимо установить галочку в чек-бокс «Перебрать все сертификаты в хранилище» (элемент 11). И если на каком-то из этих сертификатов подпись пройдет проверку, то программа остановит поиск и выведет название этого сертификата в лог.

## Чтение файла сертификата

Если требуемый сертификат представлен в виде файла, лежащего в файловой системе пользователя, то необходимо выбрать этот файл с сертификатом с помощью второго режима импорта сертификата (см. Рисунок 7).

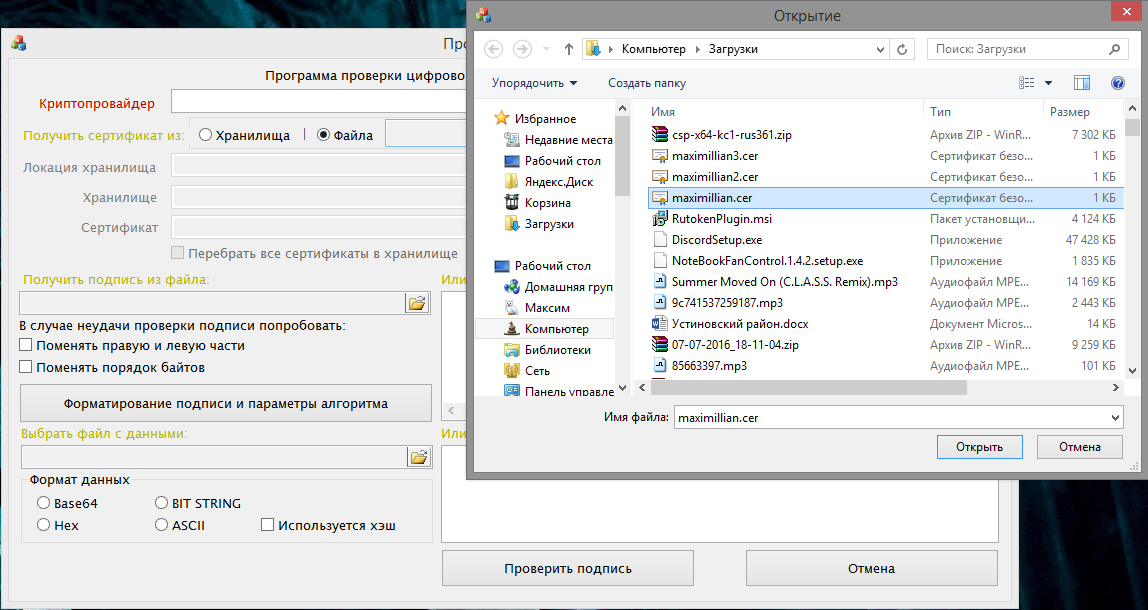


Рисунок 7 – Импорт сертификата из файла

Файл сертификата должен быть в ASCII кодировке.

Файл сертификата должен быть обрамлен хедерами и содержать сертификат в кодировке Base64.

Пример файла сертификата:

-----BEGIN CERTIFICATE-----



-----END CERTIFICATE-----

## Ввод открытого ключа

В том случае, если файл сертификата отсутствует, пользователь может ввести открытый ключ в «сыром виде». Для этого необходимо выбрать режим «Ввести ключ» (элемент 4). Откроется окно ввода ключа (см. Рисунок 3). При вводе ключа программа сама попытается определить кодировку. Предпочтительно, чтобы ключ был закодирован в формате либо «HEX», либо «Base64».

После ввода ключа следует выбрать хэш-функцию, которая использовалась при создании подписи. Для этого необходимо выбрать криптопровайдер и затем нажать на кнопку «Формат подписи и параметры алгоритма» (элемент 16). Откроется окно «Дополнительно» (см. Рисунок 2). Далее пользователю нужно выбрать хэш-функцию (элемент 23) и ввести параметры алгоритма в формате «HEX».

Параметры алгоритма представляют собой информацию, используемую криптопровайдером для выполнения процедуры проверки подписи. Она может включать, например, тип эллиптической кривой и др. Для криптопровайдера «Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider» используется по умолчанию значение: «301206072A85030202230106072A850302021E01», которое содержит идентификатор «1.2.643.2.2.35.1», что указывает криптопровайдеру использовать эллиптическую кривую «А» от CryptoPro. Если ваш криптопровайдер поддерживает в качестве параметров по умолчанию передачу пустой строки, оставьте это поле пустым.

# Способы импорта подписи

## Чтение из файла

Если у пользователя полученная подпись представлена в виде файла, то этот файл можно открыть c помощью элемента 12. Программа попытается автоматически определить формат подписи и выведет его в лог. Если формат подписи отличается от того, который выбрала программа, пользователь может его изменить в окне «Дополнительно» (см. Рисунок 2 и группа элементов 22). Если подпись является отсоединенной подписью в формате «PEM», следует убедиться, что чек-бокс «PEM» в группе элементов 22 отмечен галочкой. Если используется сырая подпись и в том случае, если пользователь не уверен в правильном порядке байтов, в программе можно выставить специальные чек-боксы (элементы 14 и 15), позволяющие провести проверку подписи с различными вариантами расположения байтов.

## Ввод подписи

Пользователь может ввести подпись в окне программы (элемент 13). Программа попытается автоматически определить формат подписи и выведет его в лог. Если формат подписи отличается от того, который выбрала программа, пользователь может его изменить в окне «Дополнительно» (см. Рисунок 2 и группа элементов 22). Если подпись является отсоединенной подписью в формате «PEM», следует убедиться, что чек-бокс «PEM» в группе элементов 22 отмечен галочкой. Если используется сырая подпись и в том случае, если пользователь не уверен в правильном порядке байтов, в программе можно выставить специальные чек-боксы (элементы 14 и 15), позволяющие провести проверку подписи с различными вариантами расположения байтов. Так как при каждом изменении вводимых данных программа выводит информацию об формате подписи, используйте кнопку «Очистить лог» (элемент 6) для удаления лишней информации в логе программы.

# Способы импорта данных

Для проверки подписи программе требуются данные, для которых эта подпись была создана. Также вместо данных программа принимает их хэш-значение.

## Чтение из файла

Если у пользователя имеется файл данных, для которого была создана подпись, то он может просто выбрать файл (элемент 17). При нажатии на кнопку, откроется стандартное диалоговое окно проводника. После выбора файла метка «Выбрать файл с данными» станет зеленого цвета.

## Ввод данных

Если требуется ввод данных или вместо файла у пользователя есть хэш-значение, то данные можно ввести в окне программы (элемент 18). Формат данных пользователю следует выставить самостоятельно (элемент 19).

# Примеры

Данные содержатся в файле «Data.txt» (директорию см. в Контактах) и представляют собой строку:

«ABRACADABRAAVADAKEDAVRA»

Имеются сертификаты «Maximillian», «Maximillian2», «Maximillian3».

Пусть отсоединенная подпись была создана по алгоритму ГОСТ 34.10-2001 с помощью закрытого ключа, для которого открытый содержится в сертификате «Maximillian» и файле «PublicKey.txt», и содержится в файле «PEMSign.txt». Соответственно «сырая» подпись содержится в файле «SimpleSign.txt».

Соответственно «сырая» подпись и открытый ключ представлены в формате «HEX». Отсоединенная подпись представлена в формате «PEM» и закодирована в «Base64».

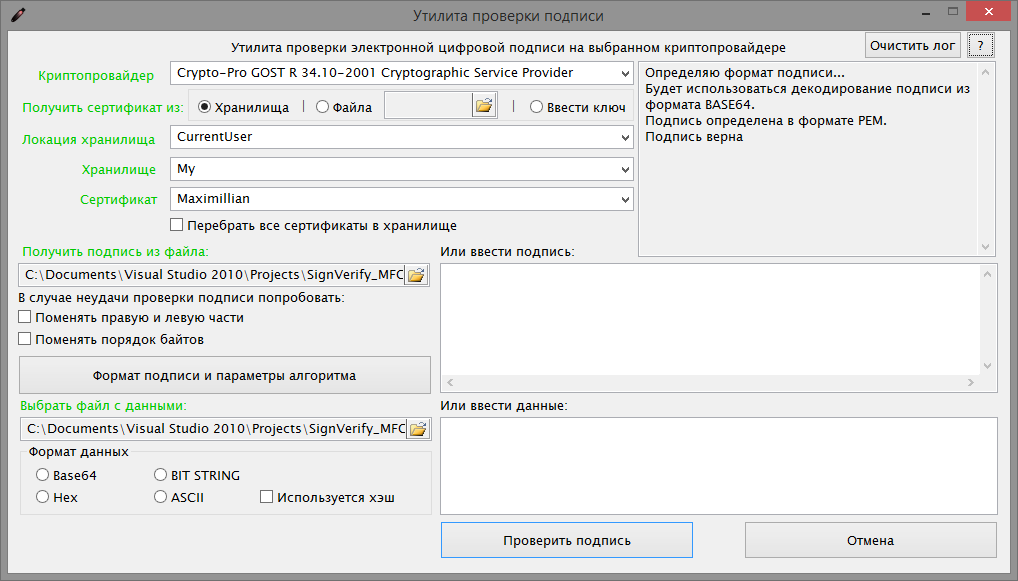


Рисунок 8 – Проверка подписи в формате «PEM»

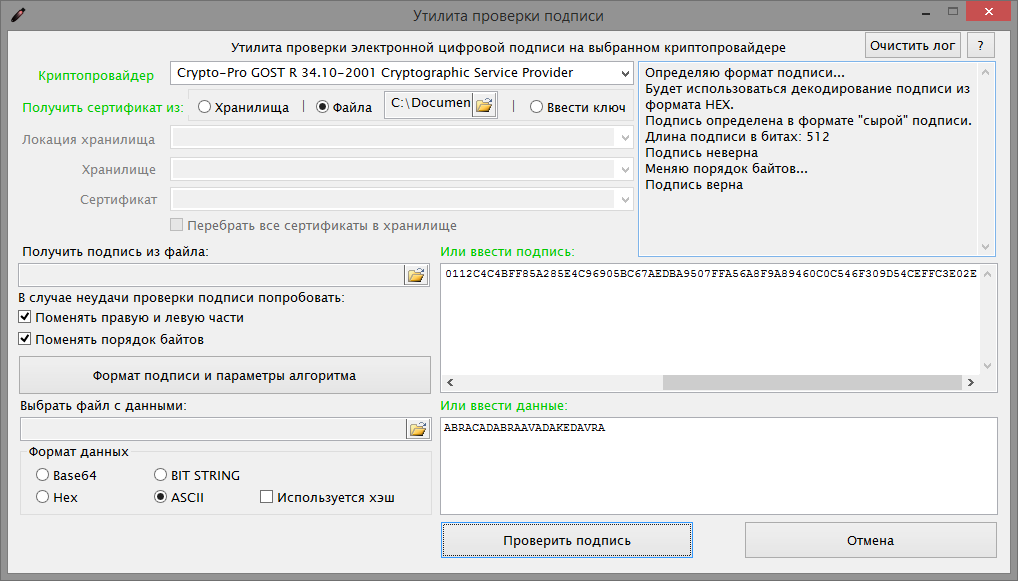


Рисунок 9 – Проверка подписи с использованием сырых данных

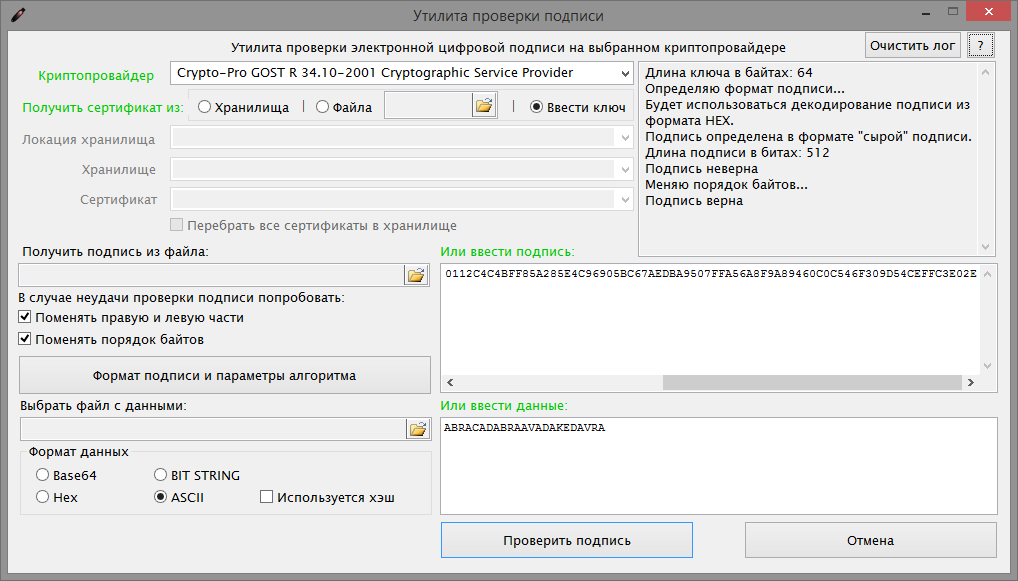


Рисунок 10 – Проверка подписи с вводом ключа

# Благодарности

Благодарю за предоставленную информацию, поддержку и наставления:

* Руководителя отдела тестирования: Алексея Лазарева
* Заместителя руководителя отдела тестирования: Евгения Аникушина
* Сотрудников отделов веб-разработки, программирования и тестирования
* Компанию ЗАО «Актив-софт» за возможность прохождения практики

# Контакты

E-mail: [maxim00795@mail.ru](mailto:maxim00795@mail.ru)

Вконтакте: <http://vk.com/robertmiles>

Skype: maxim12252

Актуальная версия программы и руководства доступна по ссылке: <http://github.com/MaximillianMS/SignVerify>