Настройка защищенного соединения с сервисом службы меток доверенного времени удостоверяющего центра Банка России на примере использования СЗКИ «КриптоПро CSP» и «КриптоАРМ ГОСТ».

Для подключения к сервису службы меток доверенного времени удостоверяющего центра Банка России (далее – TSP) используется протокол TLS для организации защищенного соединения. Для создания защищенного соединения на рабочем месте пользователя необходимо настроить службу Stunnel.

Адреса для соединения с сервисом TSP:

- `tsp1.ca.cbr.ru:443`
- `tsp2.ca.cbr.ru:443`

Для подключения к сервису TSP используются:

1. СКЗИ «КриптоПро CSP»;
2. «КриптоАРМ ГОСТ»;
3. Утилита Stunnel для создания защищенного TLS-соединения.
4. Сертификат, для простановки электронной подписи. Сертификат должен быть установлен в хранилище «Личные» локального компьютера с привязкой к контейнеру ключа электронной подписи (см. рисунок 1).

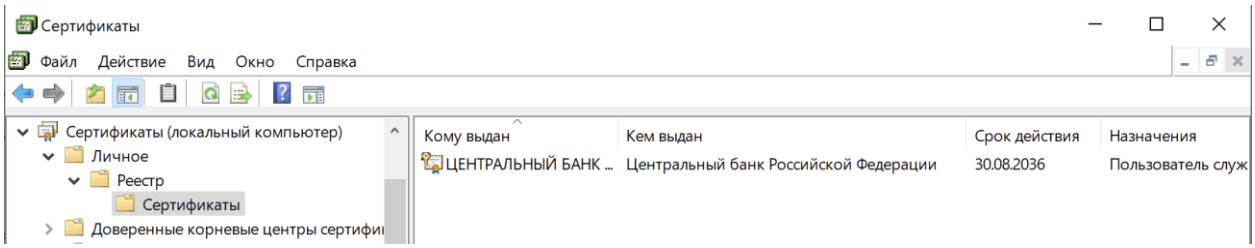

Рисунок 1. Сертификаты электронной подписи (локальный компьютер).

1. Установка Stunnel

Загрузить утилиту Stunnel можно в Центре загрузки на сайте ООО «КРИПТО-ПРО» (необходима авторизация).

После загрузки скопировать загруженный файл в каталог `C:\Stunnel` переименовав его в «`stunnel.exe`».

В командной строке от имени Администратора выполнить последовательно команды:

```
cd C:\Stunnel
stunnel.exe -install
```

2. Формирование файла конфигурации

В текстовом редакторе подготовить файл конфигурации со следующим текстом:

```
output = C:\Stunnel\stunnel_cli.log
service = Stunnel
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
debug = 7
[tls1-client-https-1]
client = yes
accept = 0.0.0.0:10001
connect = tsp1.ca.cbr.ru:443
[tls1-client-https-2]
client = yes
accept = 0.0.0.0:10002
connect = tsp2.ca.cbr.ru:443
```

где параметры `connect` содержат адрес TSP серверов удостоверяющего центра Банка России, `output` – путь до файла журналов, `service` – название службы Windows.
При необходимости полное описание опций можно найти на сайте ООО «Крипто-ПРО».

Указанный файл конфигурации сохранить в каталог `C:\Stunnel` с названием `stunnel.conf`

3. Запуск службы

Скопировать подготовленный файл конфигурации `stunnel.conf` в системный каталог `C:\Windows\System32.`

Запустить службу `Stunnel` через стандартную оснастку управления службами (`services.msc`) (см. рисунок 2).

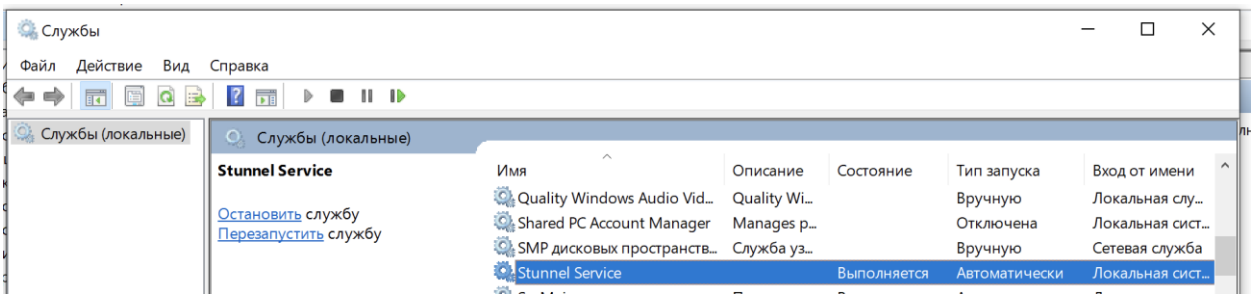

Рисунок 2. Запуск службы Stunnel

4. Установка метки доверенного времени

При подписании документа с использованием «КриптоАРМ ГОСТ» необходимо в качестве адреса службы меток доверенного времени указать:

http://localhost:10001/tsp (для доступа к серверу tsp1.ca.cbr.ru) либо http://localhost:10002/tsp (для доступа к серверу tsp2.ca.cbr.ru).

Пример параметров настройки подписи в «КриптоАРМ ГОСТ» приведен на рисунке 3. Результат выполнения операции подписания с установкой метки доверенного времени приведен на рисунке 4.

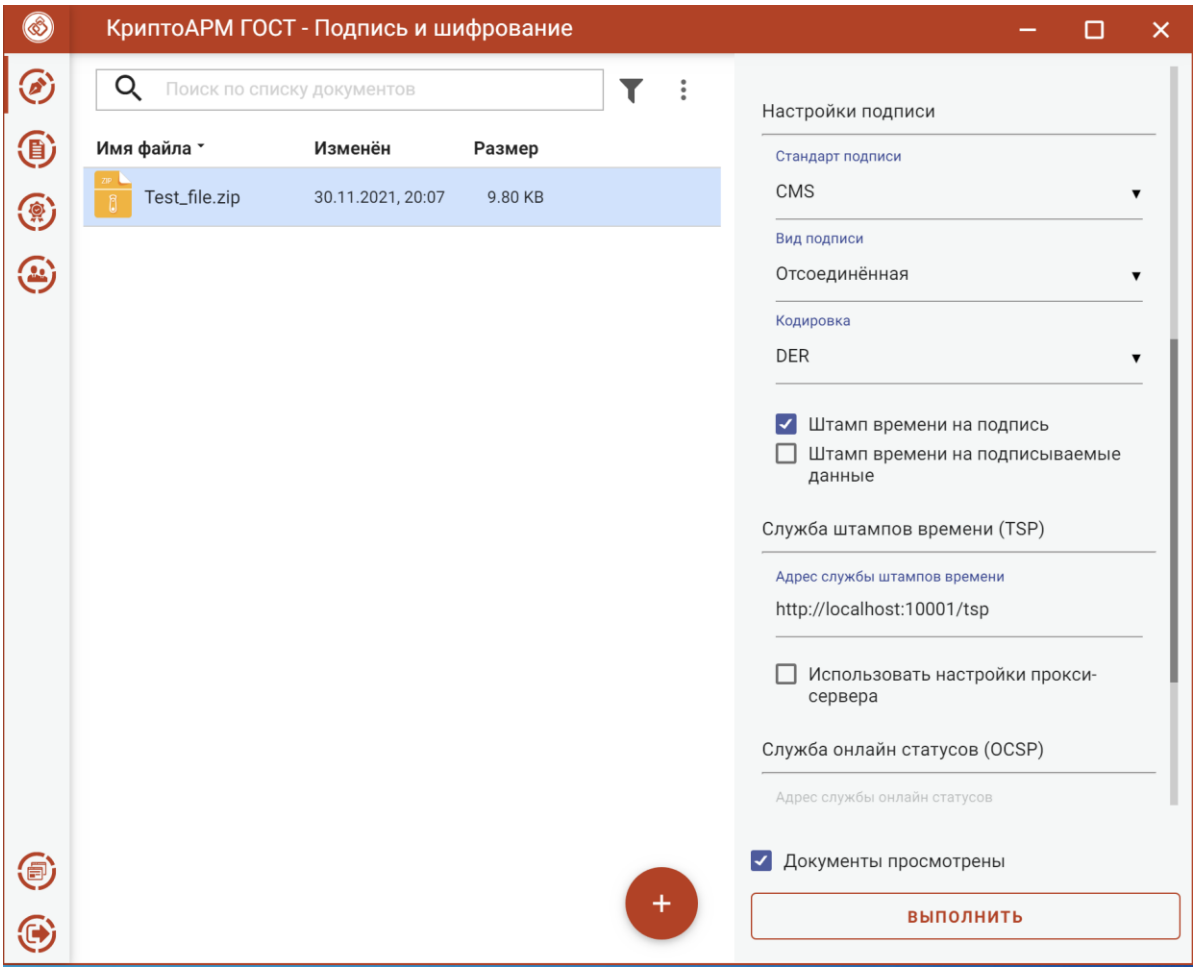

Рисунок 3. Параметры подписи.

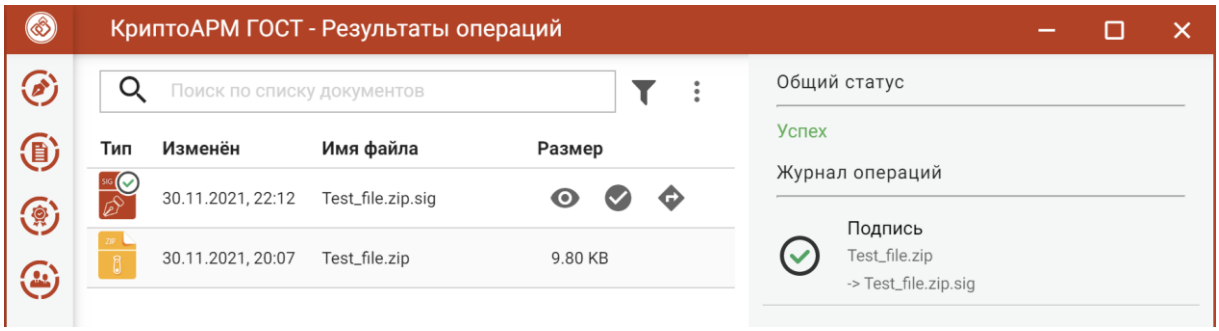

Рисунок 4. Результат выполнения операции подписания.

Настройка защищенного соединения с сервисом службы меток доверенного времени удостоверяющего центра Банка России на примере использования ПК «Сигнатура-клиент» версия 6

Для подключения к сервису службы меток доверенного времени удостоверяющего центра Банка России (далее – TSP) используется протокол TLS для организации защищенного соединения. Для создания защищенного соединения на рабочем месте пользователя необходимо настроить службу Stunnel.

Адреса для соединения с сервисом TSP:

- `tsp1.ca.cbr.ru:443`
- `tsp2.ca.cbr.ru:443`

Для подключения к сервису TSP используются:

1. ПК «Сигнатура-клиент» версия 6;
2. Утилита `spki1utl.exe;`
3. Утилита `stunnel.exe` для создания защищенного TLS-соединения;

Утилиты `spki1utl.exe` и `stunnel.exe` входят в состав ПК «Сигнатура-клиент» версия 6. Данные программы по умолчанию находятся в каталоге `C:/Program Files/MDPREI/spki .`

1. Формирование файла конфигурации

В текстовом редакторе открыть файл конфигурации `stunnel.conf`, расположенный по умолчанию в каталоге `C:/Program Files/MDPREI/spki` и заполнить его следующим текстом:

```
verify = 0
options = NO_SSLv2
options = NO_SSLv3
options = NO_TICKET
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1

[tls1-client-https-1]
client = yes
accept = 127.0.0.1:10001
connect = tsp1.ca.cbr.ru:443

[tls1-client-https-2]
client = yes
accept = 127.0.0.1:10002
connect = tsp2.ca.cbr.ru:443
```

Параметры `connect` содержат адреса TSP-серверов удостоверяющего центра Банка России.

2. Запуск stunnel.exe

Запустить `stunnel.exe`, находящийся по умолчанию в каталоге `C:/Program Files/MDPREI/spki`. При этом выводится окно выбора профиля ПО «Справочник сертификатов» (Рис 1) и окно выбора ключевого носителя.

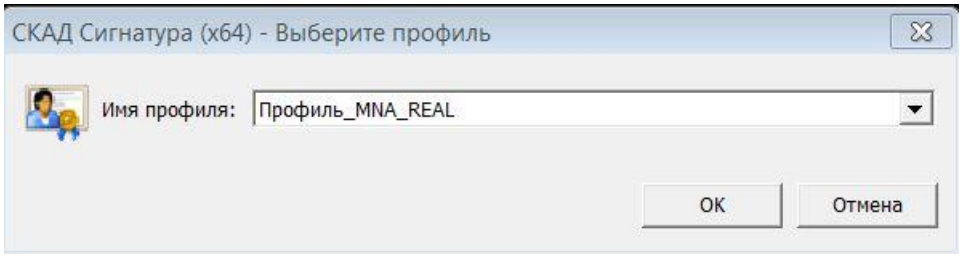

Рис. 1

После успешного выполнения команды выводится соответствующее сообщение. (Рис. 2)

Рис. 2

Обратите внимание, что для дальнейшей работы утилита `stunnel` должна оставаться в активном состоянии. Закрытие окна приведет к невозможности организации защищенного TLS-соединения.

3. Установка метки доверенного времени на подписанный электронной подписью файл.

Для того чтобы установить метку доверенного времени на ранее подписанный электронной подписью файл в командной строке необходимо ввести соответствующую команду (Рис. 3)

Пример:

```
C:\Program Files\MDPREI\spki\spki1utl.exe" -tssign -in
C:\Users\Администратор\Desktop\Тест\4567890.p7s -out
C:\Users\Администратор\Desktop\Тест\4567890.p7s.ts -url
http://127.0.0.1:10001/tsp/
```

```
C:\Users\Администратор>"C:\Program Files\MDPREI\spki\spki1utl.exe" -tssign -in C
:\Users\Администратор\Desktop\Тест\4567890.p7s -out C:\Users\Администратор\Deskt
op\Тест\4567890.p7s.ts -url http://127.0.0.1:10001/tsp/
```

Рис. 3

Утилита `spki1utl.exe` запускается со следующими параметрами:

`-tssign` – вызов функции подписания с установкой метки доверенного времени;

`-in` – путь до файла, на который необходимо установить метку доверенного времени;

`-out` – путь до файла с установленной меткой доверенного времени с расширением «`.ts`»

`-url` – указывается **http://localhost:10001/tsp** (для доступа к серверу tsp1.ca.cbr.ru) либо **http://localhost:10002/tsp** (для доступа к серверу tsp2.ca.cbr.ru).

При запуске команды запрашивается окно выбора профиля ПО «Справочник сертификатов» (Рис. 4) и окно выбора ключевого носителя.

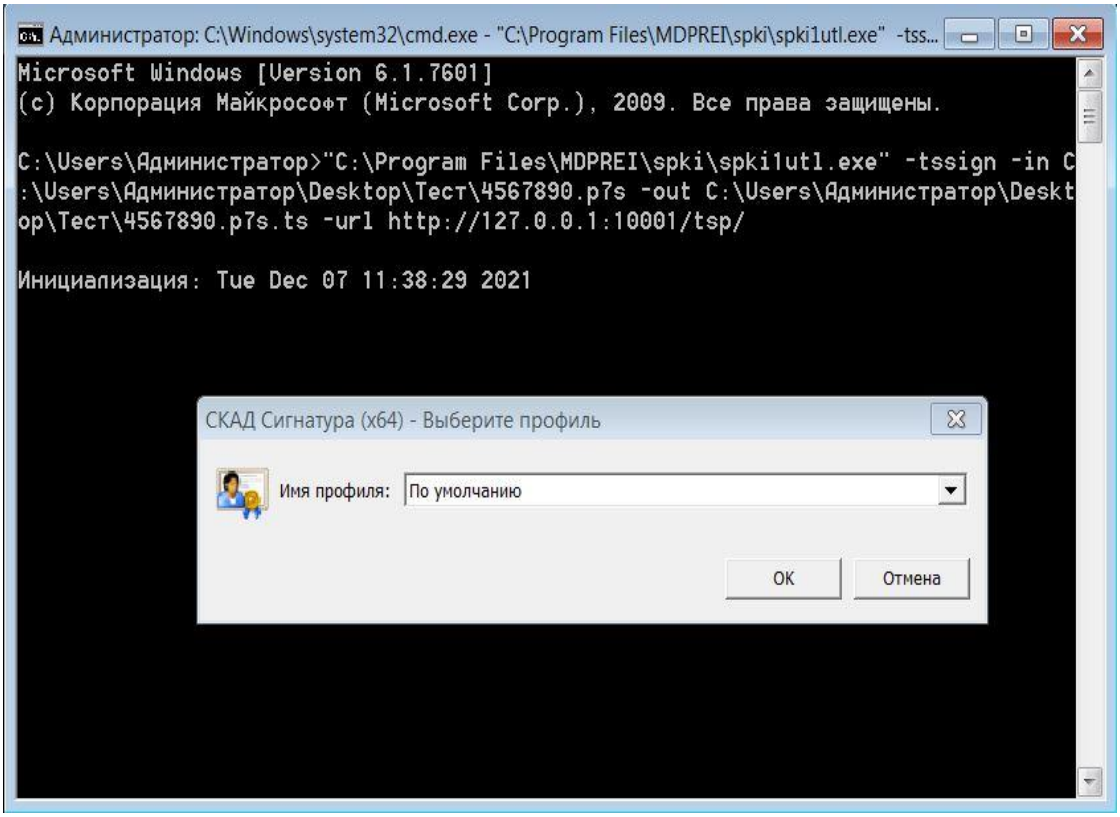

Рис. 4

При успешном выполнении команды будет создан файл, содержащий метку доверенного времени (с расширением «.ts») и будет выведено сообщение результате работы команды (Рис. 5)

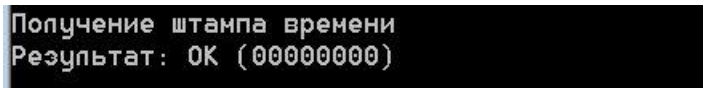

Рис. 5