



ОПИСАНИЕ ПО
«МОДУЛЬ ДЛЯ РАБОТЫ С ЭЦП».
Функциональные характеристики и
техническая инфраструктура

Версия: 2.12.0

4 августа 2025

Оглавление

1 Введение	3
2 Назначение ПО	3
3 Основные функции	4
4 Краткое описание ПО	4

1 Введение

Настоящий документ описывает функциональные характеристики и техническую инфраструктуру ПО «Модуль для работы с ЭЦП» (далее – «GostSignProxy») в рамках интеграции организации-партнёра (далее – «Партнёр») с Сервисами «ЗОЛОТАЯ КОРОНА»¹ и предназначен для сетевых специалистов и сотрудников информационной безопасности Партнёра.

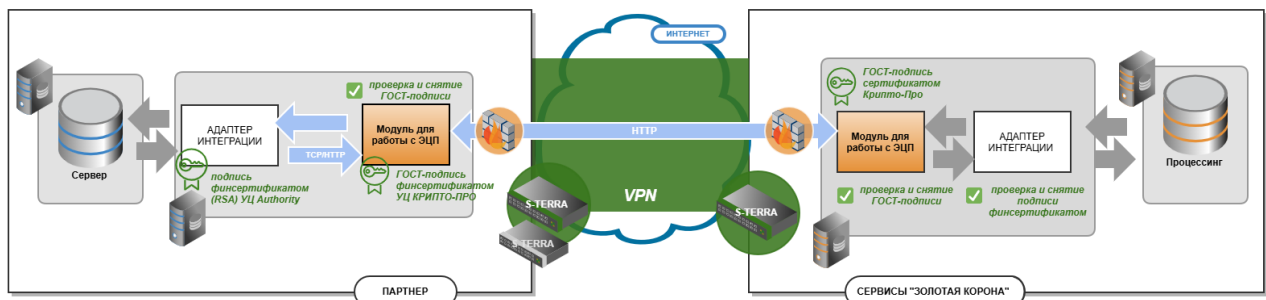
2 Назначение ПО

GostSignProxy предназначен для аутентифицированного обмена с проверкой электронной подписи входящих запросов или формированием электронной подписи исходящих запросов при организации информационного взаимодействия с Партнёрами в соответствии с ГОСТ Р 34.10-2012. GostSignProxy позволяет обеспечить информационное взаимодействие с несколькими Партнёрами одновременно.

GostSignProxy работает с сертификатом и средством криптографической защиты информации «КриптоПро JCP» версии v2.0.41940-A.

GostSignProxy актуальной версии работает только с «КриптоПро JCP» v2.0.41940-A (для JAVA 11).

Сетевая схема взаимодействия программно-аппаратного комплекса Партнёра с Сервисами «ЗОЛОТАЯ КОРОНА» показана на рисунке ниже.



- 1) Адаптер интеграции на стороне Партнёра снабжает запрос электронной подписью (ЭП), формируемой с использованием сертификата, который Партнёр получил в удостоверяющем центре (УЦ) Authority (<https://info.authority.ru/>), и передает его GostSignProxy.
- 2) GostSignProxy снабжает полученный от адаптера запрос ГОСТ-подписью, формируемой с использованием сертификата, который Партнёр получил в УЦ ООО «КРИПТО-ПРО».

¹ Под Сервисами «ЗОЛОТАЯ КОРОНА» в контексте настоящего документа понимаются различные сервисные функции Программно-аппаратных комплексов, посредством которых ЗАО «ЗОЛОТАЯ КОРОНА» оказывает услуги Партнёрам. Например, Сервисы «Платформы банковского самообслуживания» (СБП, обслуживание эквайринговой инфраструктуры банка и пр.), Сервисы «Золотая Корона-Денежные Переводы» и другие.

- 3) GostSignProxy передает запрос в адрес процессинга Сервисов по HTTP (HTTPS) через VPN-канал.

3 Основные функции

Основными функциями GostSignProxy являются:

- Взаимодействие со средством криптографической защиты информации «КриптоПро JCP».
- Формирование электронных подписей исходящих запросов с использованием криптопровайдера «КриптоПро JCP».
- Проверка электронных подписей входящих запросов.
- Обеспечение шифрованного соединения с использованием TLS-протокола.

4 Краткое описание ПО

GostSignProxy представляет собой архив с дистрибутивом, в котором содержатся следующие папки:

- **bin** – файлы запуска GostSignProxy,
- **conf** – конфигурационные файлы,

Описание настройки конфигурационных файлов изложено в документе «Руководство по установке, настройке и эксплуатации ПО «Модуль для работы с ЭЦП».

- **jar** – скомпилированная программа.

Описание установки GostSignProxy изложено в документе «Руководство по установке, настройке и эксплуатации ПО «Модуль для работы с ЭЦП».

Настройки Модуля задаются в файле gostSignProxy_config.xml.

Пример конфигурационного файла:

Значения в примере ниже, выделенные красным цветом, нужно заменить соответствующими значениями, необходимыми для вашего экземпляра GostSignProxy.

Входящие сообщения по HTTP:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<config>
  <listen>
    <http url="http://host_in:port_in">
      <routeHttp url="http://host_out:port_out">
        <sign alias="gost_key_name" storage="key_storage_name">
          algorithm="GOST3411_2012_256withGOST3410_2012_256" attr="cryptopro"/>
        <verify alias="zk_pub_cert" storage="path_to_storage">
          password.enc="password_enc" algorithm="GOST3411_2012_256withGOST3410_2012_256"
            attr="cryptopro"/>
      </routeHttp>
    </http>
  </listen>
</config>
```

ОПИСАНИЕ ПО «МОДУЛЬ ДЛЯ РАБОТЫ С ЭЦП»

```
<const name="routemsg" value="bank_id"/>
</httpHeaders>
</routeHttp>
</http>
</listen>
</config>
```

host_in:port_in – адрес для входящих сообщений от адаптера, задается на стороне Партнёра.

host_out:port_out – адрес для исходящих сообщений, предоставляется сотрудниками Сервиса, с которым Партнёр организует интеграцию.

bank_id – идентификатор Партнёра для маршрутизации, задается на стороне Сервиса, с которым Партнёр организует интеграцию.

Описание параметров **gost_key_name**, **key_storage_name**, **zk_pub_cert**, **path_to_storage**, **password (password_enc)** – изложено в документе «Руководство по установке, настройке и эксплуатации ПО «Модуль для работы с ЭЦП».

Минимальные требования для окружения ПО GostSignProху:

GostSignProху устанавливается на любую платформу, на которой установлены следующие продукты:

- ОС Linux (Ubuntu или Astra Linux)
- OpenJDK v 11
- «КриптоПро JCP» версии v2.0.41940-A

Подробное описание установки и настройки «CryptoPro JCP» см. в официальной документации криптопровайдера.

Для эксплуатации ПО GostSignProху потребуются следующие ключи для формирования ГОСТ-подписи:

- header.key
- masks.key
- masks2.key
- name.key
- primary.key
- primary2.key

Описание по подготовке ключей изложено в документе «Руководство по установке, настройке и эксплуатации ПО «Модуль для работы с ЭЦП».