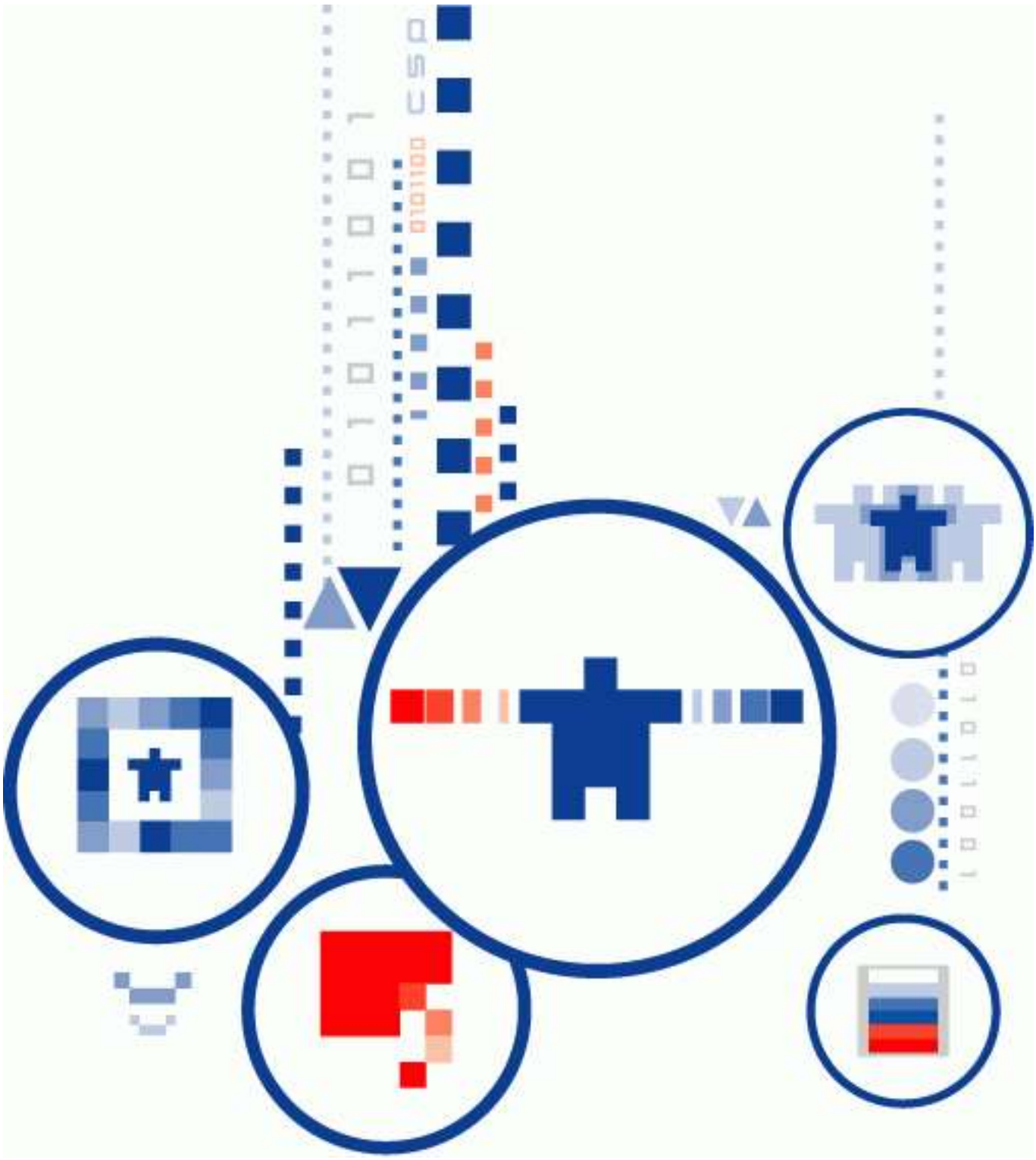
УТВЕРЖДЁН
ЖТЯИ.00113-01 90 01-ЛУ

ЖТЯИ.00113-01 90 01



КриптоПро HLF

Инструкция по использованию

АННОТАЦИЯ

Настоящий документ содержит описание модуля КриптоПро HLF, предназначенного для использования российских криптографических алгоритмов, предоставляемых КриптоПро CSP 5.0 в системах распределённого реестра, построенных с помощью Hyperledger Fabric v1.4.

Документ предназначен для пользователей и администраторов программных продуктов, построенных на платформе Hyperledger Fabric v1.4, как ознакомительный материал перед установкой и эксплуатацией модуля «КриптоПро HLF».

Информация о разработчике модуля «КриптоПро HLF»:

ООО "КРИПТО-ПРО"

105037, г. Москва, Измайловский проезд, дом 10, корпус 2, этаж 1, помещение IV

Телефон: (495) 995 4820

https://cryptopro.ru

email: info@cryptopro.ru

СОДЕРЖАНИЕ

1. Общие положения

Модуль КриптоПро HLF, разработанный на базе сертифицированного СКЗИ КриптоПро CSP, обеспечивает возможность использования российских криптографических алгоритмов для реализации функций создания и проверки электронной подписи, шифрования/расшифрования данных в распределённых реестрах на основе Hyperledger Fabric v1.4.

При сертификации решений на основе Hyperledger Fabric v1.4 с встроенным модулем КриптоПро HLF требуемые исследования будут ограничиваться проверками корректности использования в решении функций модуля КриптоПро HLF для реализации целевого функционала, а также проверками выполнения требований и рекомендаций по обеспечению информационной безопасности и защиты от несанкционированного доступа.

При этом проверки корректности реализации самих криптографических алгоритмов и работы с криптографическими ключами в процессе выполнения решением целевых функций в данном случае не требуются.

2. Основные функции

Модуль КриптоПро HLF обеспечивает:

- Реализацию интерфейса BCCSP
- Поддержку российских и межгосударственных стандартов в области криптографической защиты информации:
  - ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (ГОСТ 34.10-2018)
  - ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (ГОСТ 34.11-2018)
  - ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Взаимодействие с сертифицированным ФСБ России СКЗИ КриптоПро CSP 5.0.

3. Состав КриптоПро HLF

Модуль КриптоПро HLF содержит следующие компоненты:

- Плагин Golang, реализованный в виде библиотеки cpro.so, предоставляющий интерфейс `bccsp.BCCSP`
- СКЗИ КриптоПро CSP 5.0, реализующее российские криптографические алгоритмы в соответствии с интерфейсом CryptoAPI и обеспечивающее управление ключевыми элементами системы
- Модули, модифицирующие исходные коды Hyperledger Fabric v1.4, позволяющие добавить идентификаторы алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ 28147-89.

4. Установка КриптоПро HLF

Для возможности использования поддерживаемых российских и межгосударственных стандартов к репозиторию Hyperledger Fabric v1.4 необходимо применить патч, добавляющий идентификаторы соответствующих алгоритмов из репозитория `https://github.com/deemru/fabric/tree/v1.4.1-gost`

После установки модифицированной версии Hyperledger Fabric v1.4 необходимо установить BCCSP плагин из состава дистрибутива в (`/usr/lib/cpro.so`) и установить СКЗИ КриптоПро CSP 5.0 согласно документации.

Для использования КриптоПро HLF пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Для просмотра информации о лицензии выполните:

```
# cpconfig -license -view
```

Для ввода лицензии выполните:

```
# cpconfig -license -set <серийный_номер>
```

Серийный номер следует вводить с соблюдением регистра символов.

В файлах `orderer.yaml` и `core.yaml` необходимо подключить плагин в секции BCCSP:

```
Default: PLUGIN
PLUGIN:
    Library: /usr/lib/cpro.so
    Config:
    Hash: SHA2
    Security: 256
    FileKeyStore:
    KeyStore: /etc/hyperledger/fabric/msp/keystore
```

Сборка Hyperledger Fabric v1.4 для использования с плагином BCCSP:

```
GOPATH=/go GO_TAGS=pluginsenabled make peer orderer
```

5. Использование интерфейса BCCSP

Плагин, входящий в состав КриптоПро HLF, предоставляет интерфейс bccsp.BCCSP, позволяющий использовать российские криптографические алгоритмы, реализованные в СКЗИ КриптоПро CSP.

Модуль КриптоПро HLF обеспечивает только реализацию программного интерфейса и должен работать совместно с СКЗИ «КриптоПро CSP», средствами которого реализуются криптографические алгоритмы и работа с ключевой информацией. Поэтому для корректной работы модуля КриптоПро HLF прежде всего необходимо установить и настроить СКЗИ «КриптоПро CSP 5.0» в соответствии с эксплуатационной документацией на него, сгенерировать или экспортировать ключевую информацию.

Работа с КриптоПро HLF полностью определяется прикладным кодом бизнес-логики блокчейн-приложения. Ниже приведены команды для создания и экспорта сертификата для импорта в Hyperledger Fabric v1.4.

Получение тестового сертификата:

```
/opt/cprocsp/bin/amd64/cryptcp -creatcert -provtype 80 -rdn
  "CN=fab1,OU=COP" -cont "\\\\.\\HDIMAGE\\fab1" -ku -du -ex -ca
  http://cryptopro.ru/certsrv
```

Экспорт сертификата:

```
/opt/cprocsp/bin/amd64/certmgr -export -dest fab1.pem -base64
```

Сертификаты располагаются в `admincerts` и `signcerts`.