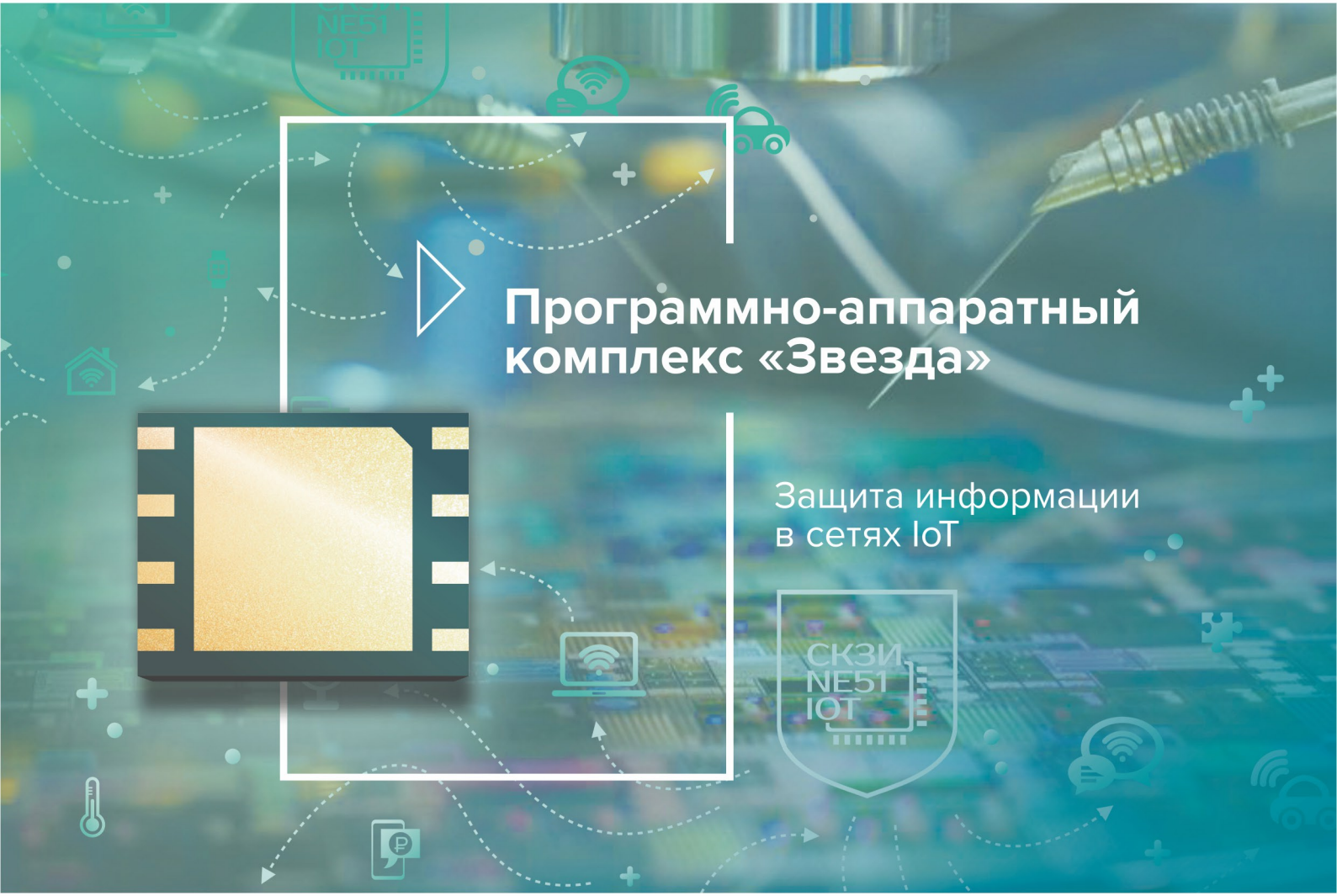
НИИМЭ
ЭЛЕМЕНТ



Программно-аппаратный комплекс «Звезда»

Защита информации
в сетях IoT

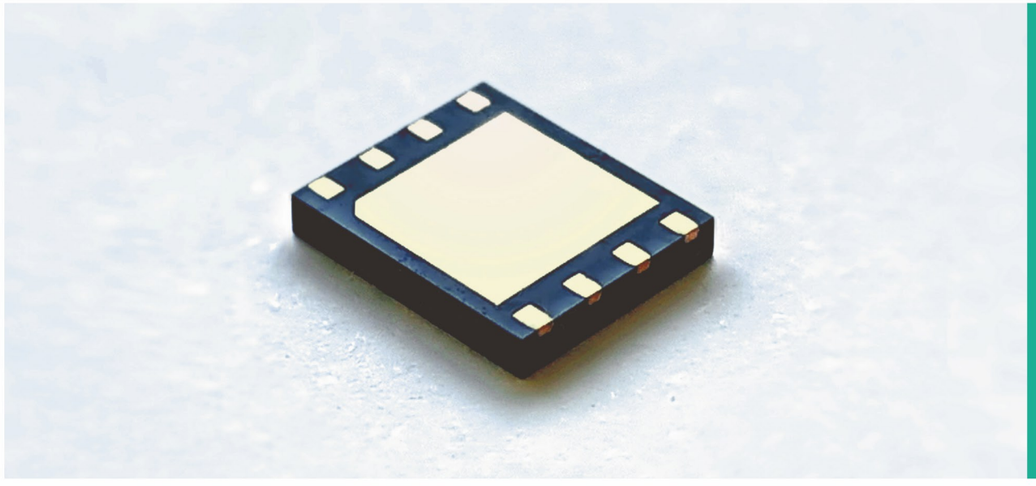
Содержание:

Программно-аппаратный комплекс «Звезда» 02
Ключевые особенности ПАК «Звезда» 04
Состав ПАК «Звезда» 05
Элемент безопасности 06
Модуль безопасности сервера 07
Криптосервис 09
АРМ администрирования криптосервиса 10
Протокол CRISP 11
Пример защиты данных при передаче информации 12

ПАК«Звезда»

Программно-аппаратный комплекс «Звезда» предназначен для обеспечения криптографической защиты информации в сетях интернета вещей (IoT). ПАК «Звезда» создает виртуальный защищенный канал передачи данных между конечными устройствами и управляющим сервером.

Ключевой элемент ПАК «Звезда» — разработанная АО «НИИМЭ» микросхема NE51IOT, сертифицированная ФСБ как встраиваемое СКЗИ по классу КС3, соответствует требованиям СКЗИ-НР (в части защиты от атак инженерного проникновения) и требованиям к средствам электронной подписи. Микросхема NE51IOT является элементом безопасности, обеспечивающим хранение криптографических ключей и выполнение криптографических алгоритмов на стороне конечного устройства и сервера.



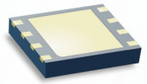
Сертифицированная микросхема NE51IOT может использоваться

- для защиты канала связи устройств IoT
- для производства аппаратных модулей безопасности (аппаратный корень доверия)
- для производства российских доверенных устройств
- для производства токенов электронной подписи (ЭП) с поддержкой российских криптоалгоритмов
- для построения HSM (Hardware Security Module) с российским чипом
- для встраивания в мобильные устройства
- для удаленного управления конфигурацией IoT устройств

Примеры защищаемых с помощью ПАК «Звезда» устройств

- **устройства промышленного интернета вещей (IIoT)**
- **приборы учета**
- **датчики системы безопасности**
- **умные светофоры**
- **системы управления доступом (СКУД)**
- **другие датчики и исполнительные устройства, в том числе устройства критической информационной инфраструктуры (КИИ)**

Ключевые особенности **ПАК «Звезда»:**



NE51IOT - микросхема первого уровня (разработана и производится в России)

Российские криптографические алгоритмы последнего поколения (ГОСТ Р34.12-2015 «Магма» для шифрования, ГОСТ Р34.10-2012 для расчета ЭП для передаваемых данных)

Микросхема NE51IOT имеет компактный размер, низкое энергопотребление, имеет возможность отключения питания при уходе устройства в режим сна (может использоваться в энергоэффективных устройствах)

Возможность подписания сообщений электронной подписью - позволяет конечному получателю проверять целостность и подлинность сообщений, в том числе архивных

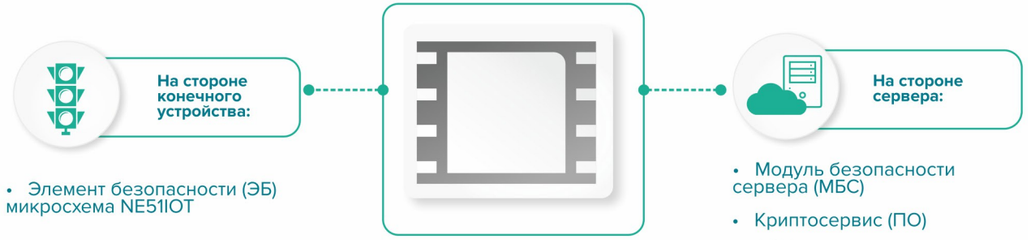
Удаленное управление криптографическими ключами – позволяет не останавливать работу устройства для регламентной замены ключей (для IoT устройств по согласованию с регулятором)

Защищённый канал передачи данных между устройством и сервером

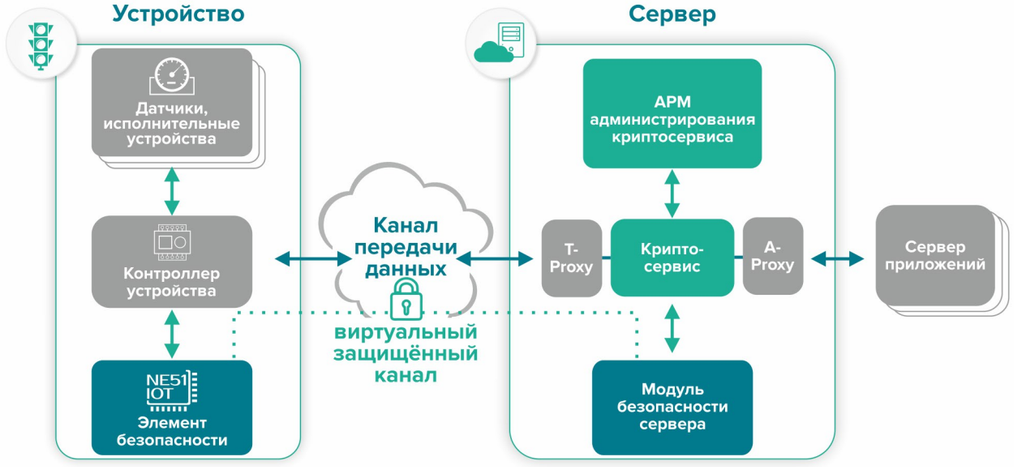
Совместимость с различными протоколами транспортного уровня (NBIoT, LoRa, NB-Fi, TCP и т.д.)

Протокол защищенной передачи данных CRISP, разработанный для Интернета вещей и стандартизованный в России

Состав ПАК «Звезда»



Пример встраивания ПАК «Звезда»



– программные компоненты ПАК «Звезда»

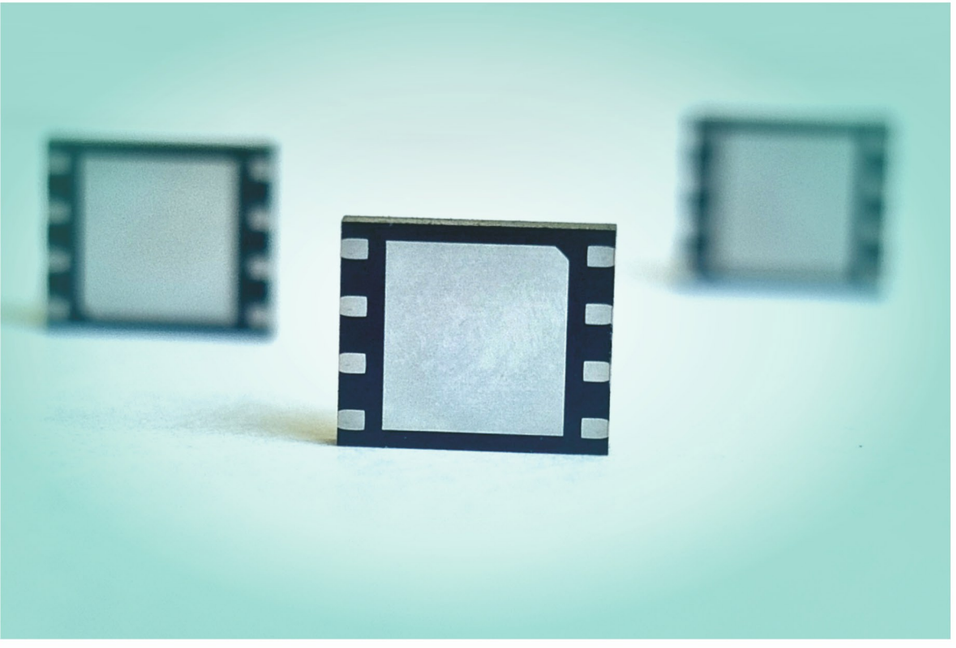
– аппаратные компоненты ПАК «Звезда»

Элемент безопасности

ЭБ – микросхема NE51IOT, которая обеспечивает защиту информации на стороне устройства

ОБЕСПЕЧИВАЕТ

- организацию защищенного канала связи
- формирование электронной подписи сообщения
- выполнение криптографических операций для решения особых задач потребителя, например, проверка ЭП обновления ПО устройства, управление ключами и паролями устройства и т.п.
- хранение криптографических ключей
- поддержку удаленного управления криптографическими ключами для IoT устройств (по согласованию с регулятором)



Варианты корпусировки ЭБ:

- **смарт-карта (ID1)**
- **mini-SIM (2FF)**
- **micro-SIM (3FF)**
- **nano-SIM (4FF)**
- **eSIM (MFF2)**

Основные характеристики :

- объем энергонезависимой памяти **16 Кбайт**
- допустимое число перезаписей в энергонезависимую память **не менее 500 000**
- длительность хранения информации **не менее 16 лет**
- ориентировочное время обработки пакета данных **100 мс/сообщение (192 байта)**
- максимальный размер пакета данных без использования режима цепочки **480 байт**
- последовательный интерфейс передачи данных **ISO 7816**
- срок действия криптографических ключей для микросхемы NE51IOT - **до 3х лет**
- срок действия криптографических ключей в составе IoT устройств - **до 16 лет** (по согласованию с регулятором)

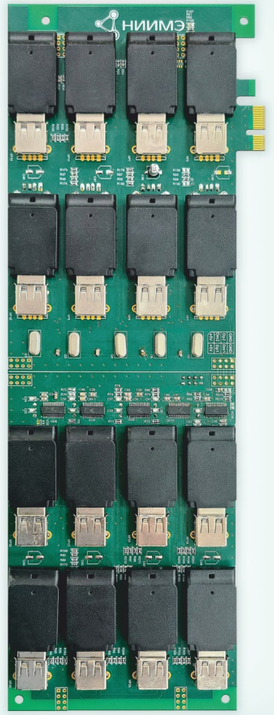
Модуль безопасности сервера

Модуль безопасности сервера используется на стороне сервера, обеспечивает хранение ключей и выполнение криптографических операций, необходимых для обмена с устройствами, управления ключами, а также отвечает за авторизацию привилегированных пользователей

Для обеспечения отказоустойчивости и повышения производительности сервера МБС изготавливается в виде кластера из нескольких микросхем NE51IOT.

Варианты исполнения:

- **плата PCI-Express**
- **смарт-карта (ID1)**
- **mini-SIM (2FF)**
- **micro-SIM (3FF)**
- **nano-SIM (4FF)**
- **eSIM (MFF2)**



Криптосервис

Криптосервис – программное обеспечение, реализующее основные функции ПАК «Звезда» на серверной стороне:

- формирование исходящих сообщений для защищенной передачи данных
- обработка входящих сообщений: проверка целостности, расшифровка и извлечение данных
- управление криптографическими ключами модуля безопасности сервера
- удаленное управление криптографическими ключами элементов безопасности IoT устройств (по согласованию с регулятором)
- интеграция конечных устройств в PKI (генерация/выгрузка запросов на сертификат/сертификатов ключей устройств и сервера, загрузка сертификатов ключей устройств и сервера, подписанных внешним УЦ и т.д.)
- мониторинг нагрузки

АРМ администрирования криптосервиса

АРМ администрирования криптосервиса – программное обеспечение на стороне сервера для управления работой криптосервиса и удаленного управления ЭБ на подключенных устройствах

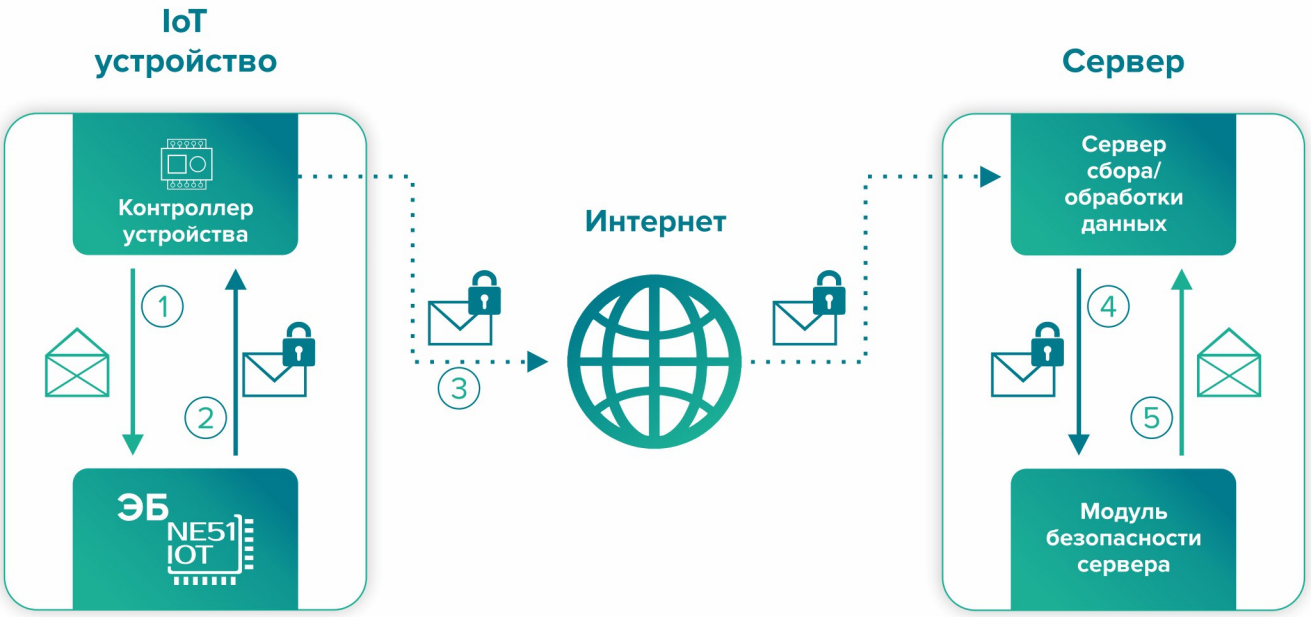
Протокол CRISP

Для защищенного обмена данными между элементом безопасности конечного устройства и криптосервисом используется модифицированный индустриальный протокол CRISP

Ключевые особенности протокола CRISP

- не требует предварительной установки сессии
- небольшая длина заголовка – важно при передаче небольших объемов данных в сетях IoT
- обеспечение целостности передаваемых данных – каждое сообщение снабжается имитовставкой
- использование уникальных счетчиков обеспечивает защиту от повторной передачи
- возможность подтверждения доставки сообщений в обе стороны в синхронном режиме работы
- поддерживается механизм цепочечной передачи данных для отправки сообщений более 480 байт
- возможность передачи ЭП устройства вместе с данными
- возможность шифрования передаваемых данных
- каждое устройство имеет уникальные ключи
- для каждого сообщения генерируются уникальные сессионные ключи

Пример защиты данных при передаче информации от IoT-устройства серверу



– данные в незашифрованном виде

– данные в зашифрованном виде

① ② ③ ④ ⑤ – последовательность прохождения данных от устройства к серверу

124460, Россия, Москва, Зеленоград,
ул. Академика Валиева, д. 6/1
+7 495 229 72 99 +7 495 229 70 00
niime@niime.ru