Решение ViPNet SIES глазами разработчика

Марина Сорокина

Решение ViPNet SIES

ВСТРАИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ УСТРОЙСТВ АВТОМАТИЗАЦИИ И УСТРОЙСТВ IIOT

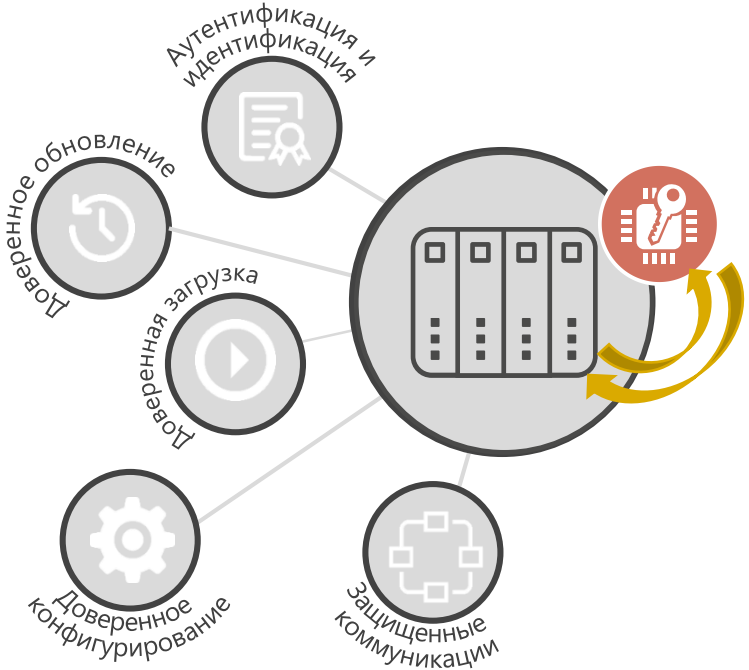
ЗАЩИТА КОММУНИКАЦИЙ • ЗАЩИТА КОНЕЧНЫХ УЗЛОВ • ЗАЩИТА ДАННЫХ • АУТЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

План вебинара

1. Обзор решения ViPNet SIES
2. Решение ViPNet SIES. Обзор нового
3. С чего начать встраивание ViPNet SIES?
4. Встраивание ViPNet SIES Core
5. Установка ViPNet SIES Unit
6. Интеграция центра управления ViPNet SIES MC

Обзор решения ViPNet SIES

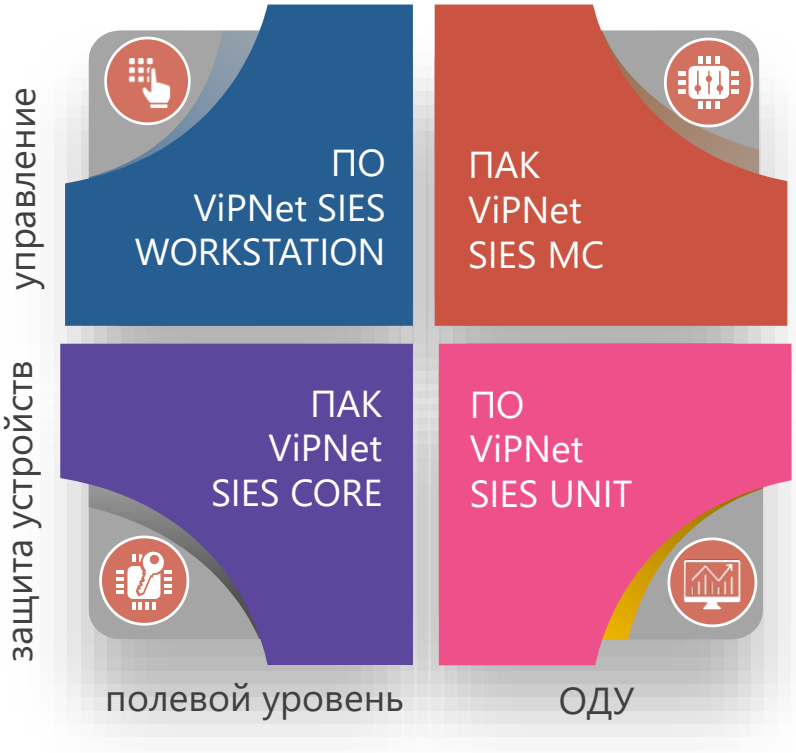
Меры безопасности, реализуемые в системе с помощью решения ViPNet SIES



Сценарии защиты информации:

- Обеспечение конфиденциальности передаваемых данных
- Обеспечение аутентичности и целостности передаваемых данных
- Доверенное локальное и удаленное обновление ПО устройства
- Доверенное локальное и удаленное конфигурирование устройства
- Доверенная загрузка устройства
- Двухфакторная аутентификация на устройстве

Состав решения ViPNet SIES



- Законченные СКЗИ класса КС1 и КС3, не требуют оценки влияния
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств

Криптографические операции, доступные защищаемым устройствам

ГОСТ Р 34.11-2012
ГОСТ 34.11-2018

ГОСТ 28147-89

ГОСТ Р 34.12-2015
ГОСТ Р 34.13-2015
ГОСТ 34.12-2018
ГОСТ 34.13-2018

ГОСТ Р 34.10-2012
ГОСТ 34.10-2018

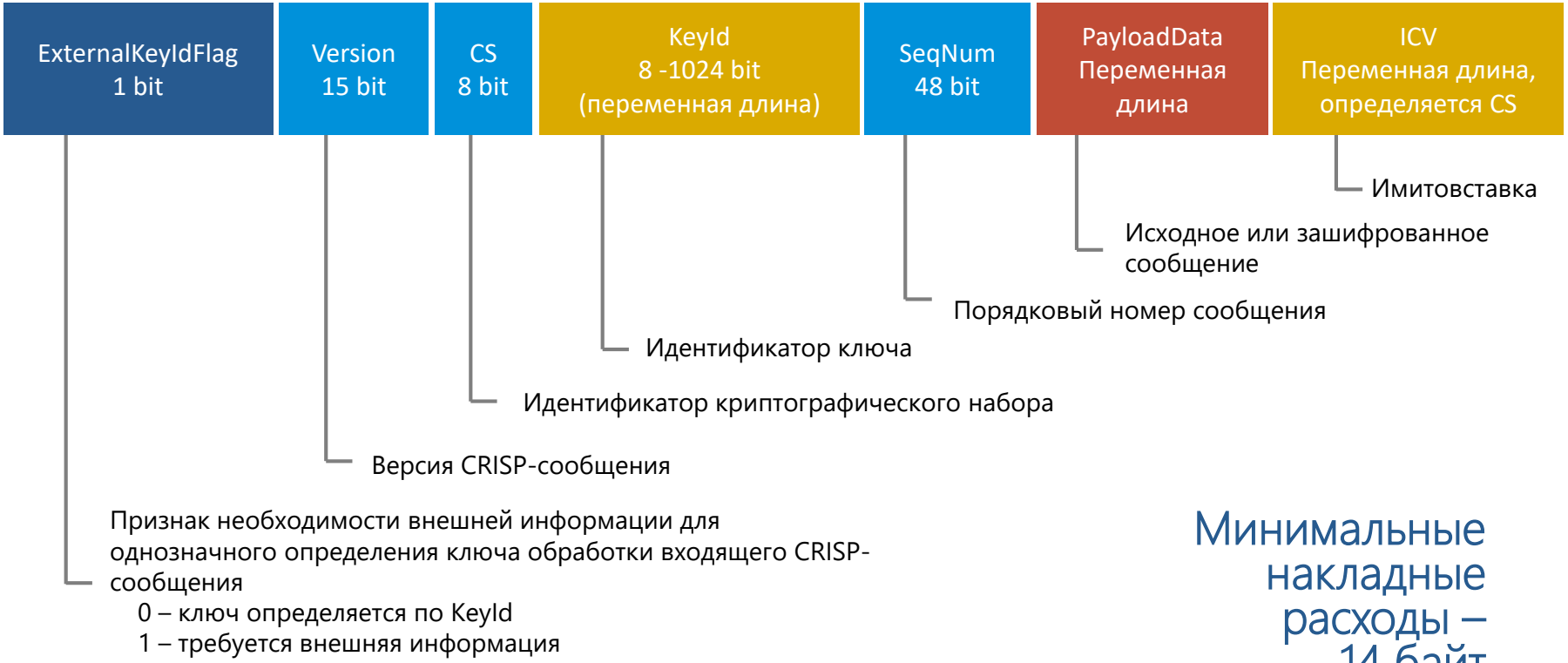
Криптографический протокол CRISP

Cryptographic Industrial Security Protocol
- неинтерактивный протокол защищенной передачи данных для индустриальных систем, M2M и IIoT коммуникаций

- Обеспечение целостности
- Обеспечение конфиденциальности (опционально)
- Защита от навязывания повторных сообщений
- Окно принятых сообщений

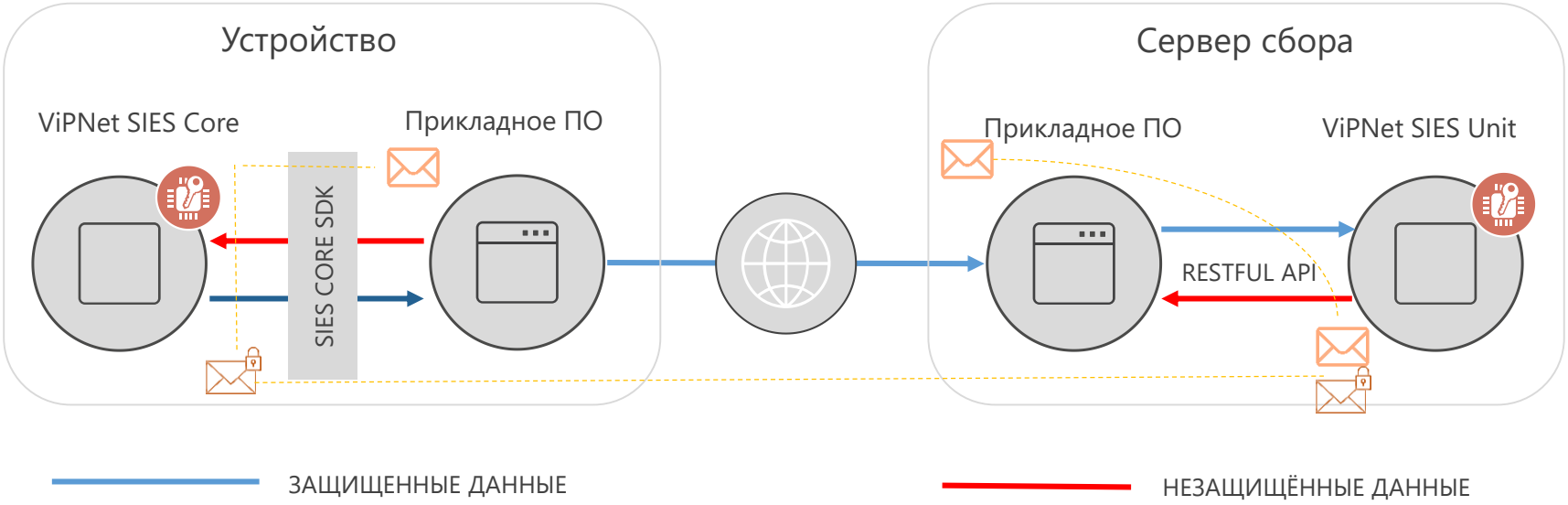
- Общий секретный ключ
- Защита данных – блочный шифр, имитовставка
- Поддержка адресных (один-к-одному) сообщений
- Поддержка многоадресных (один-ко-многим, подписочная модель) сообщений
- Явная и неявная адресация абонентов

Структура CRISP-сообщения

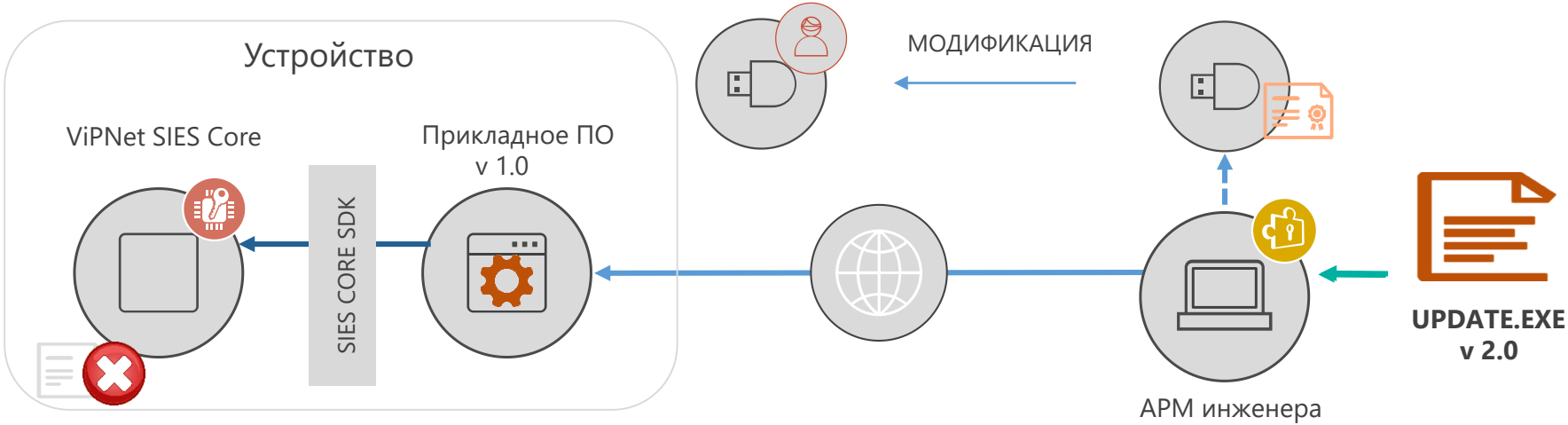


Минимальные накладные расходы – 14 байт

Защита коммуникаций с помощью ViPNet SIES



Доверенное обновление контроллера с помощью ViPNet SIES



Ключевая система ViPNet SIES

ViPNet SIES – платформа безопасности для

- Защиты устройств в разрезе концепции «Secure-by-design»
- Защиты устройств автоматизации, включая защиту передачи данных по промышленным сетям Industrial Ethernet и Fieldbus
- Защиты IIoT- устройств, включая включая защиту передачи данных по LPWAN- сетям

Решения ViPNet SIES
Обзор нового

ViPNet SIES Unit 2.0

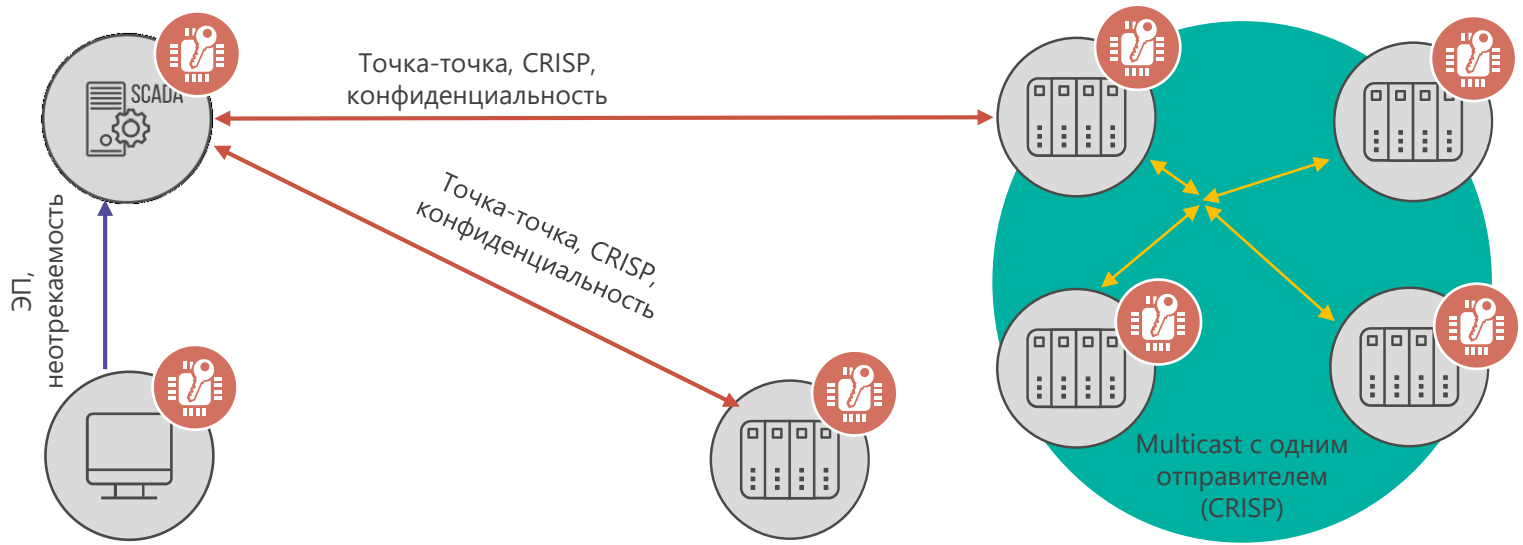
- Поддержка Linux и Windows
- Лицензирование из ViPNet SIES MC (не нужна standalone-лицензия)

- Выпуск релиза: февраль ’20
- Технический релиз: доступен по запросу

ViPNet SIES Core 2.2

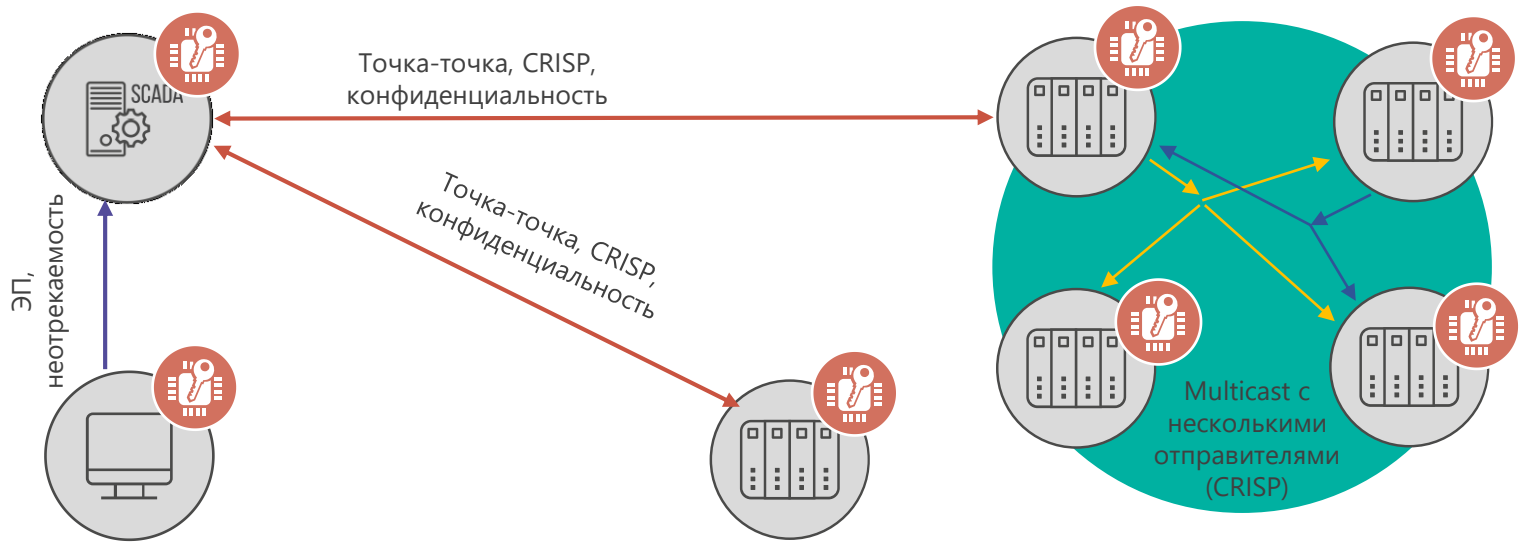
- SIES Core API для интерфейса SPI
- Возможность загрузки энтропии без рассинхронизации прикладных связей

Защита многоадресных сообщений: Multicast с одним отправителем



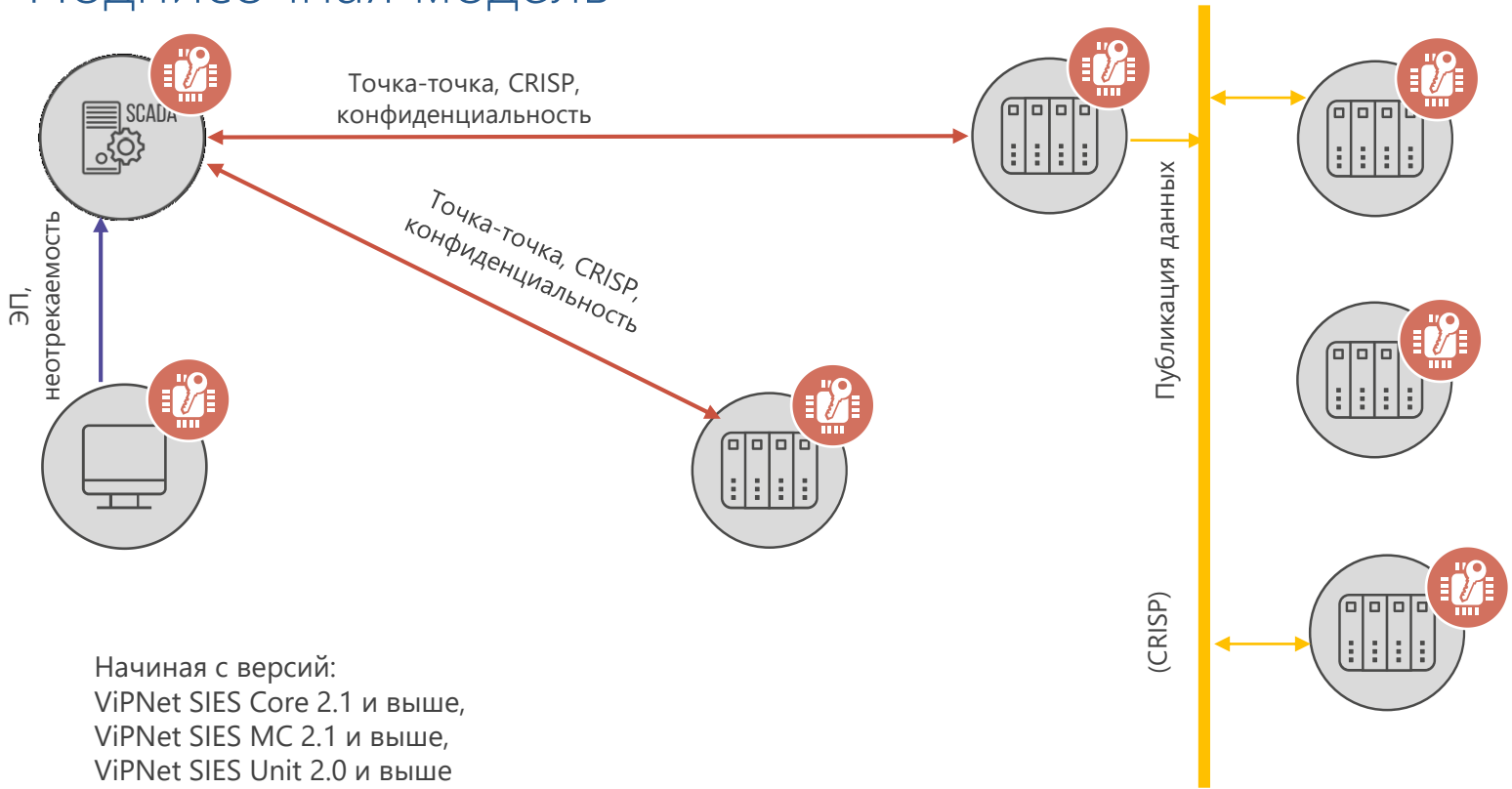
Начиная с версий:
ViPNet SIES Core 2.1 и выше,
ViPNet SIES MC 2.1 и выше,
ViPNet SIES Unit 2.0 и выше

Защита многоадресных сообщений: Multicast с несколькими отправителями



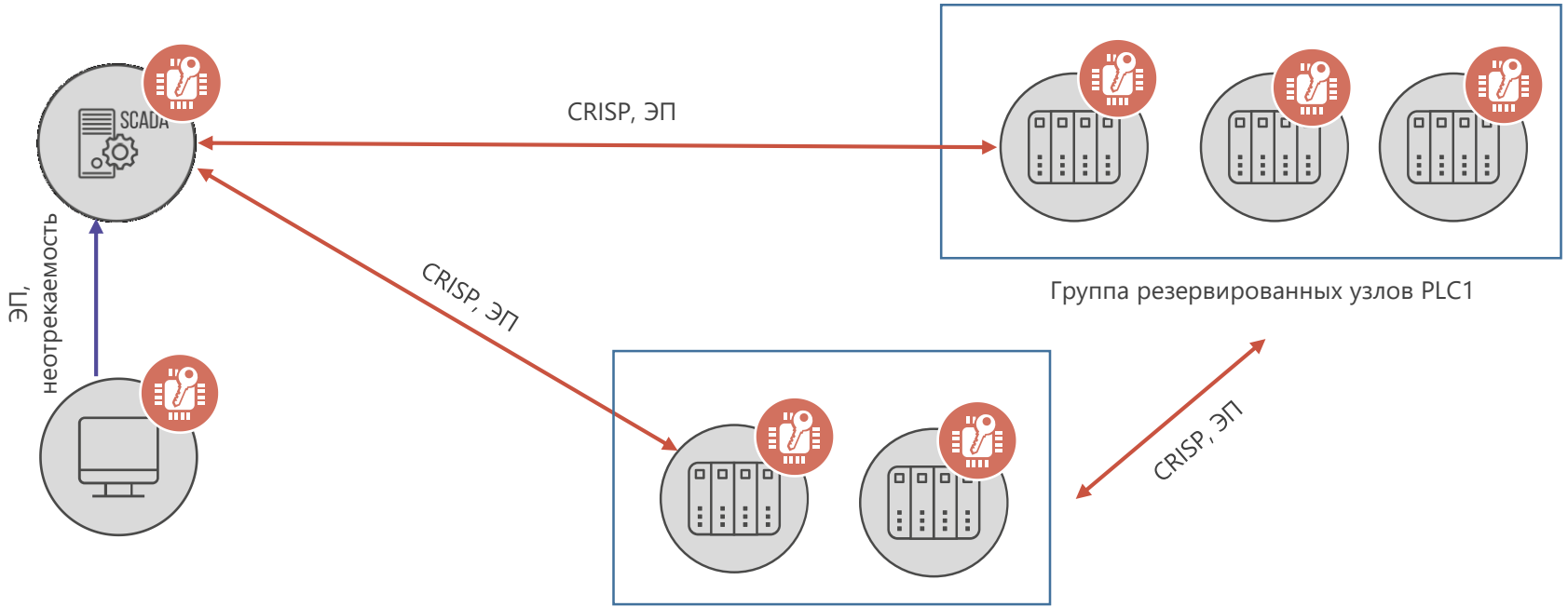
Начиная с версий:
ViPNet SIES Core 2.1 и выше,
ViPNet SIES MC 2.1 и выше,
ViPNet SIES Unit 2.0 и выше

Защита многоадресных сообщений: Подписочная модель



Начиная с версий:
ViPNet SIES Core 2.1 и выше,
ViPNet SIES MC 2.1 и выше,
ViPNet SIES Unit 2.0 и выше

Поддержка схем резервирования



Начиная с версий:
ViPNet SIES Core 2.1 и выше,
ViPNet SIES MC 2.1 и выше,
ViPNet SIES Unit 2.0 и выше

Пересмотрены принципы управления компонентами решения ViPNet SIES

ПАК ViPNet SIES Core

ПО ViPNet SIES Unit

Пользователь

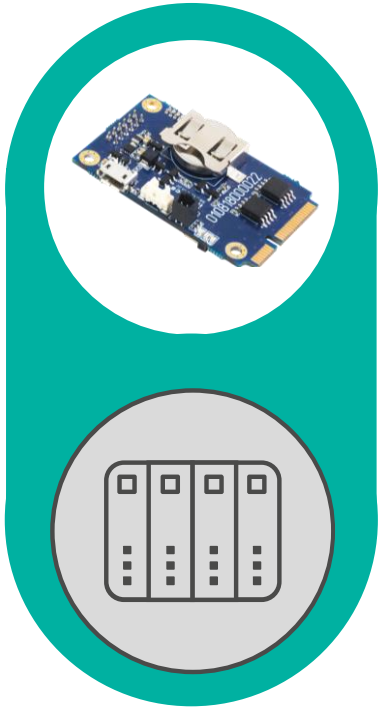
Сервисный инженер, Инженер КИП с собственным Token/Smart-картой

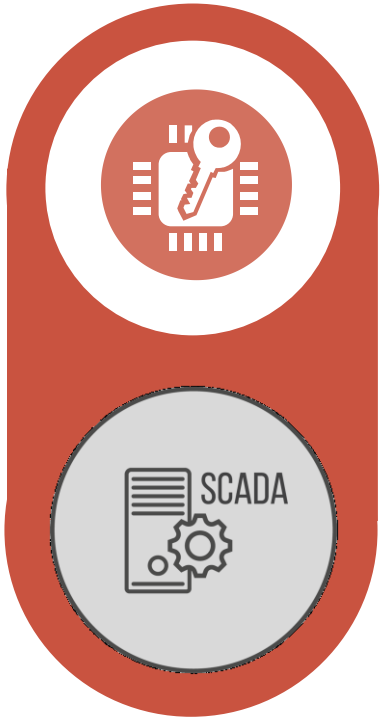
Другой SIES-узел

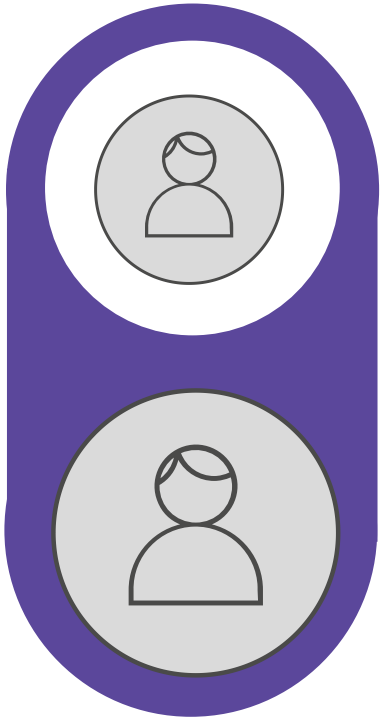
Криптопровайдеры и прочие PKI-продукты

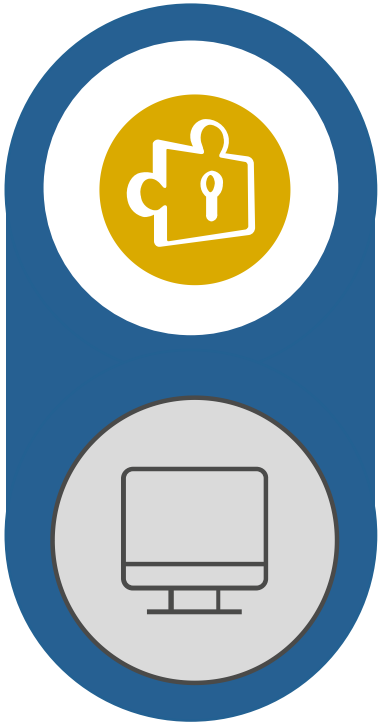
Начиная с версий: ViPNet SIES MC 2.1 и выше

Выделение объектов управления на уровне АСУ



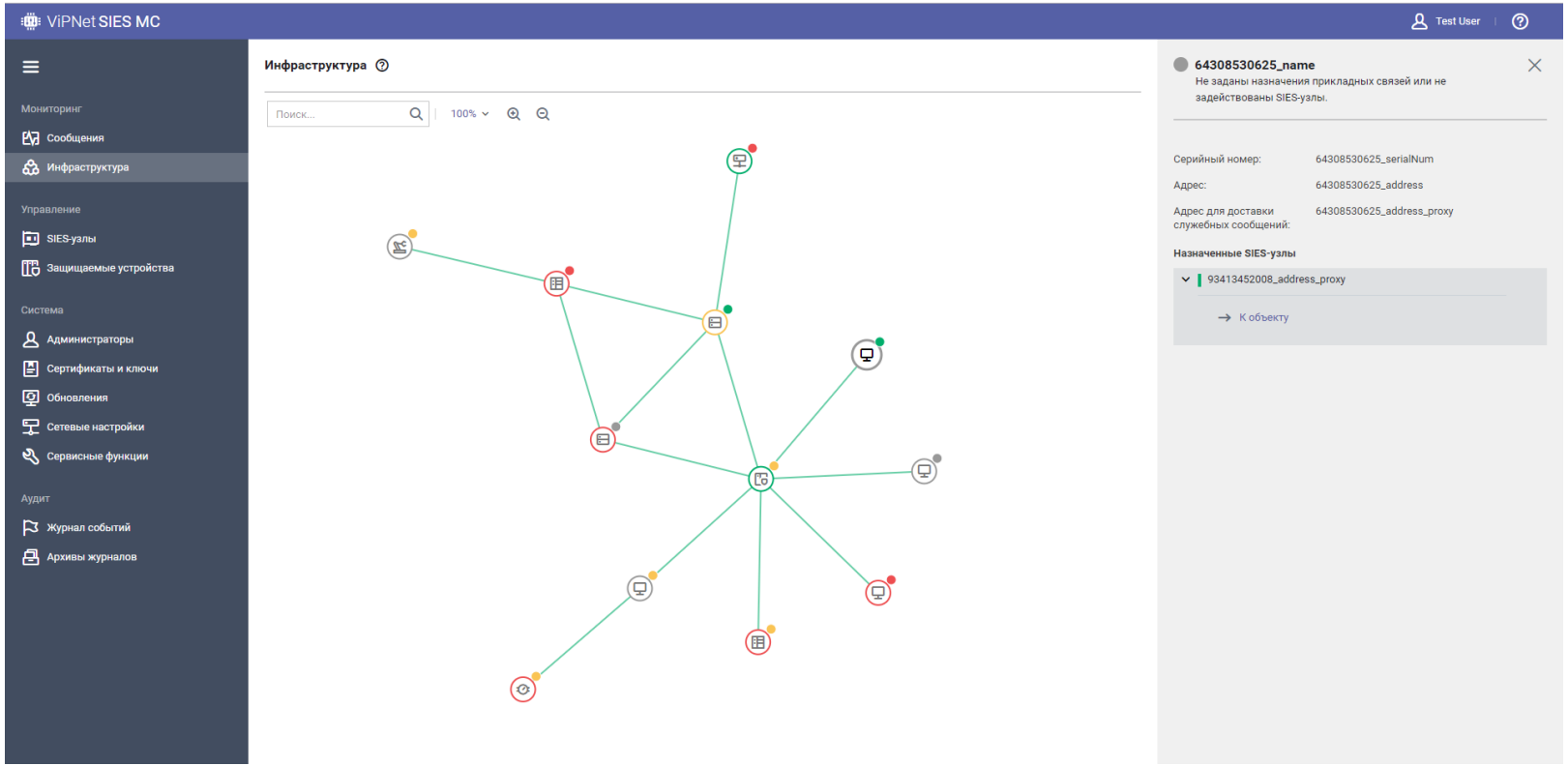






Начиная с версий: ViPNet SIES MC 2.1 и выше

Отображение объектов инфраструктуры



Начиная с версий: ViPNet SIES MC 2.2 и выше

С чего начать встраивание ViPNet SIES

Постановка задачи

Входные данные:

- Сценарии защиты информации
- Архитектура конечного решения
- Нефункциональные характеристики
- Аппаратная составляющая

Проект по встраиванию решения ViPNet SIES

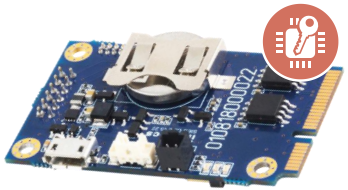
ViPNet SIES Development kit

Project

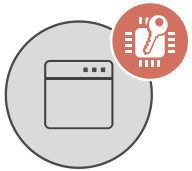
1. Знакомство с документацией на решение VIPNet SIES
2. Развертывание инфраструктуры VIPNet SIES
3. Знакомство с решением VIPNet SIES на практике
4. Доработка ПО изделия
5. Доработка аппаратной части изделия
6. Разработка тестов и тестового окружения
7. Тестирование
8. Доработка документации (КД, ПД, пользовательской документации)
9. Доработка технологической документации

ViPNet SIES Development kit

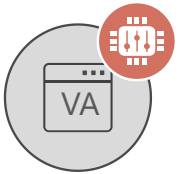
Продукты решения ViPNet SIES



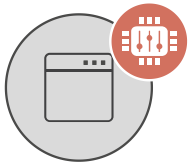
2 x ПАК ViPNet SIES Core



1 x ПО ViPNet SIES Unit (на 50 связей)



1 x ПО ViPNet SIES MC VA (1 администратор)



1 x ПО ViPNet SIES Workstation (Windows)

Средства инфраструктуры

1 x ПО ViPNet PKI Client с TLS Unit (Win – версия) для ViPNet SIES Workstation
1 x ПО ViPNet PKI Client с TLS Unit для рабочего места администратора

Средства разработки

ViPNet SIES Core SDK

Утилита SIES Core

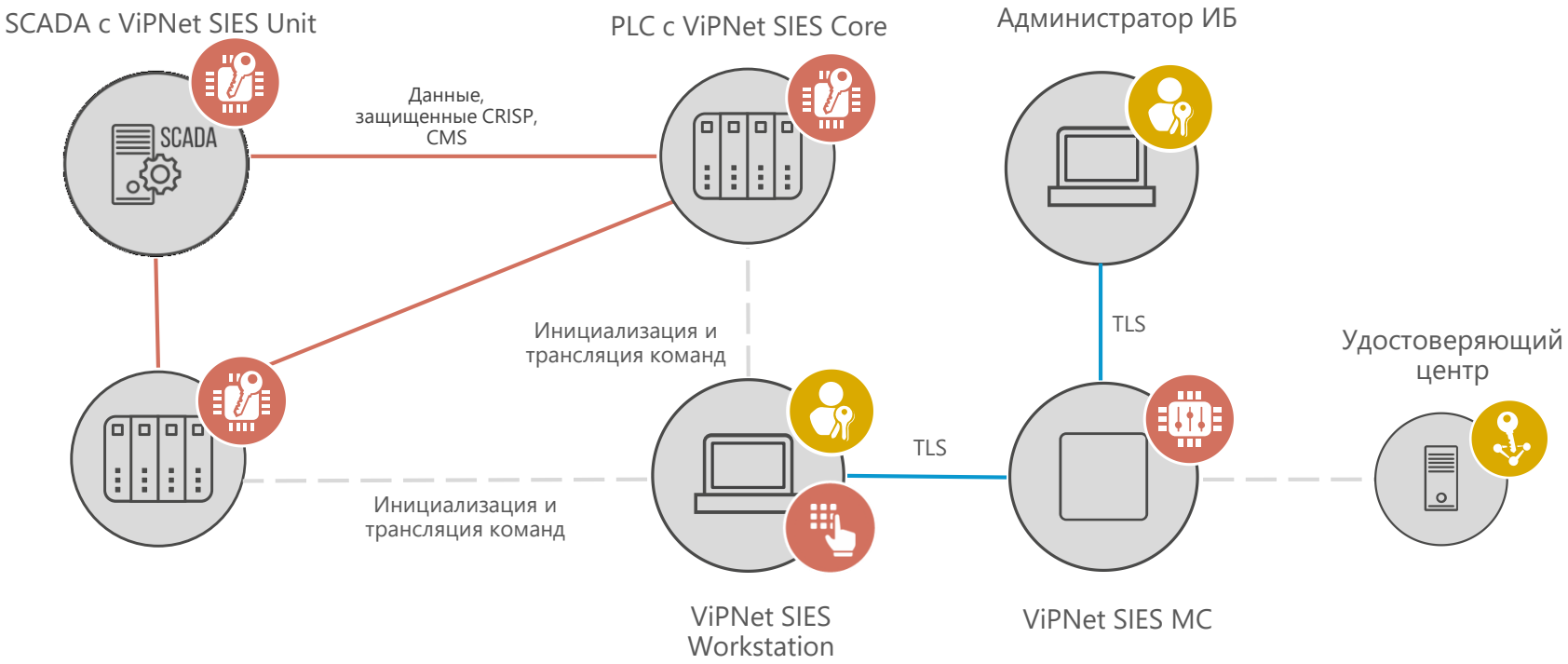
Документация

Описание протоколов

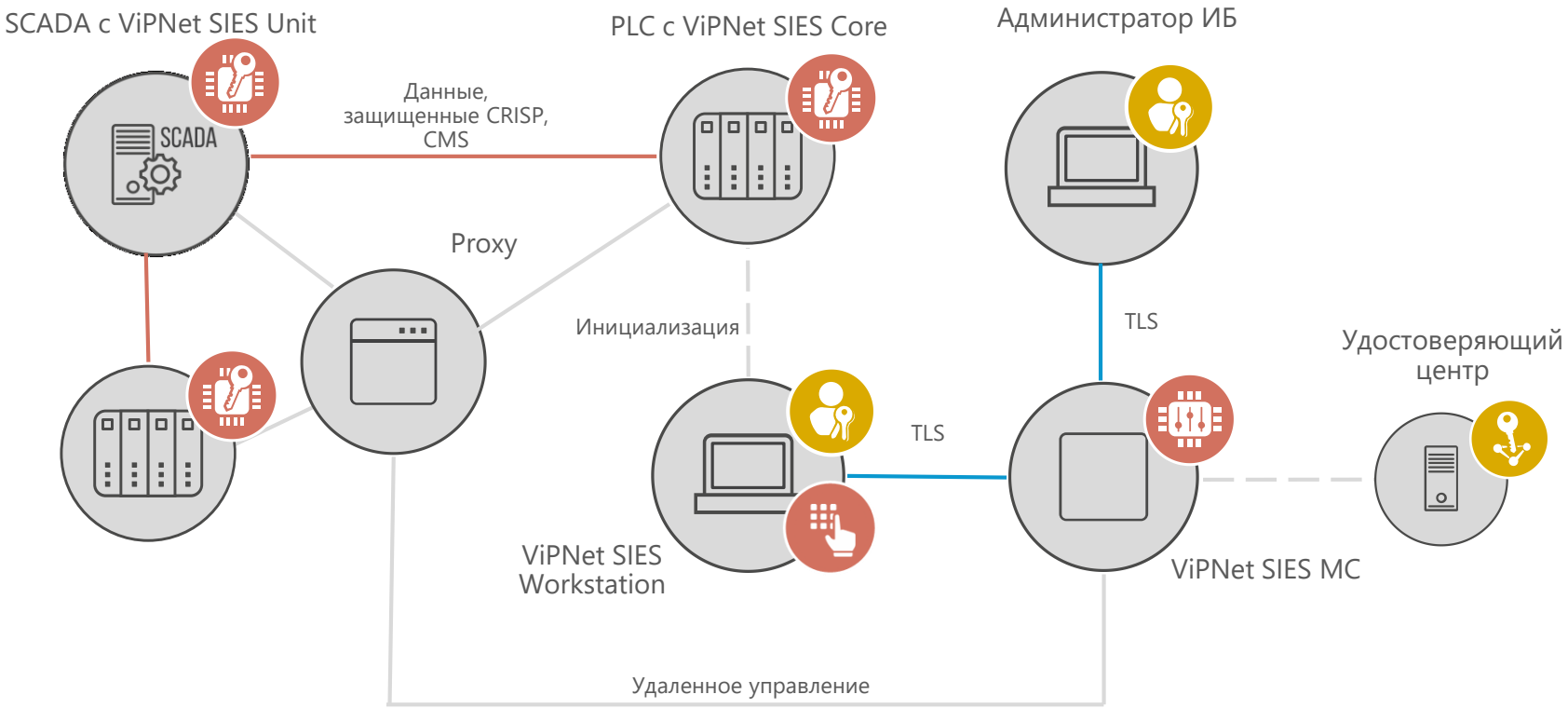
Пользовательская документация на продукты

Инструкция по разворачиванию решения

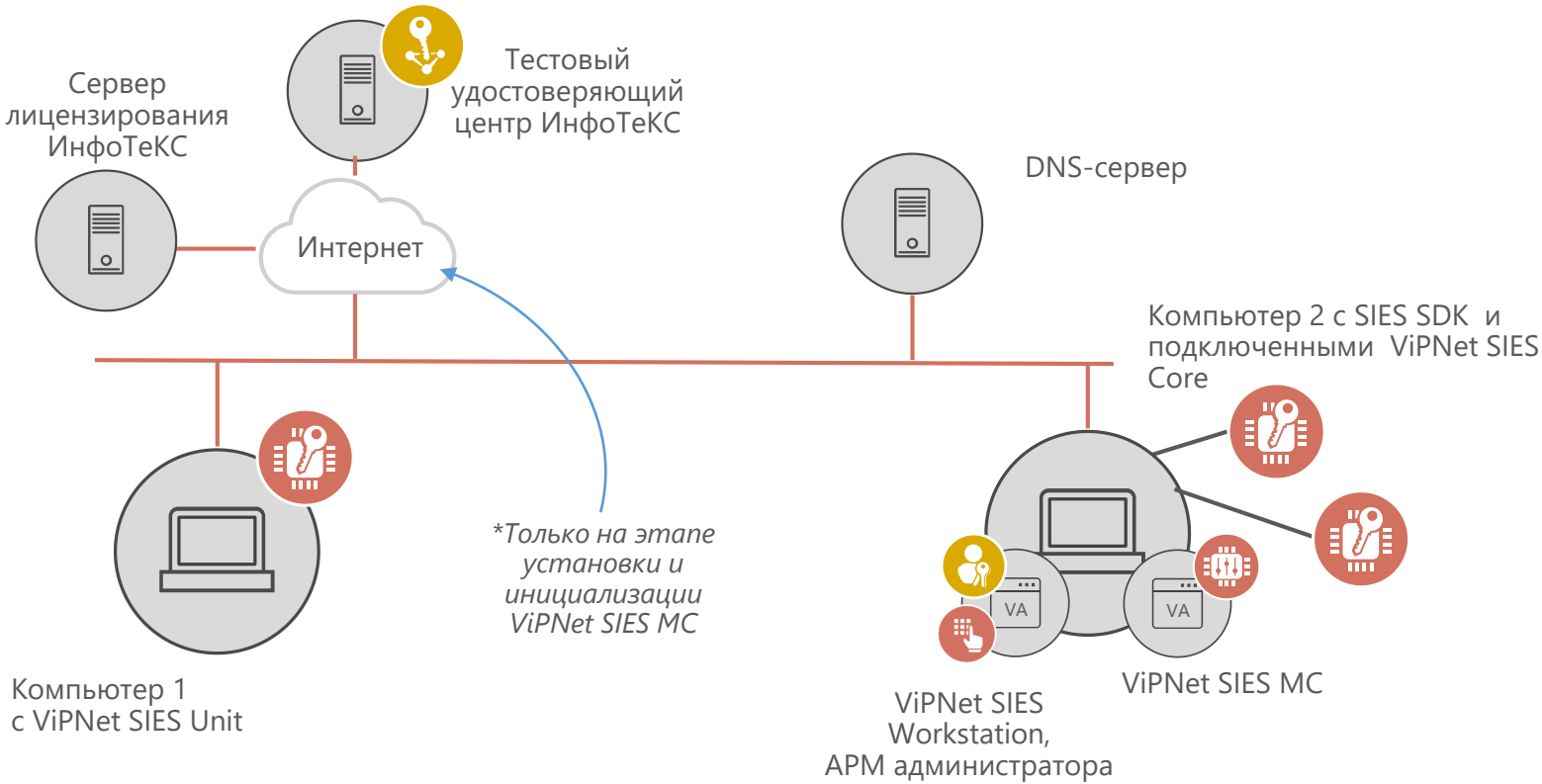
Разворачивание инфраструктуры: типовой проект (min)



Разворачивание инфраструктуры: типовой проект (max)

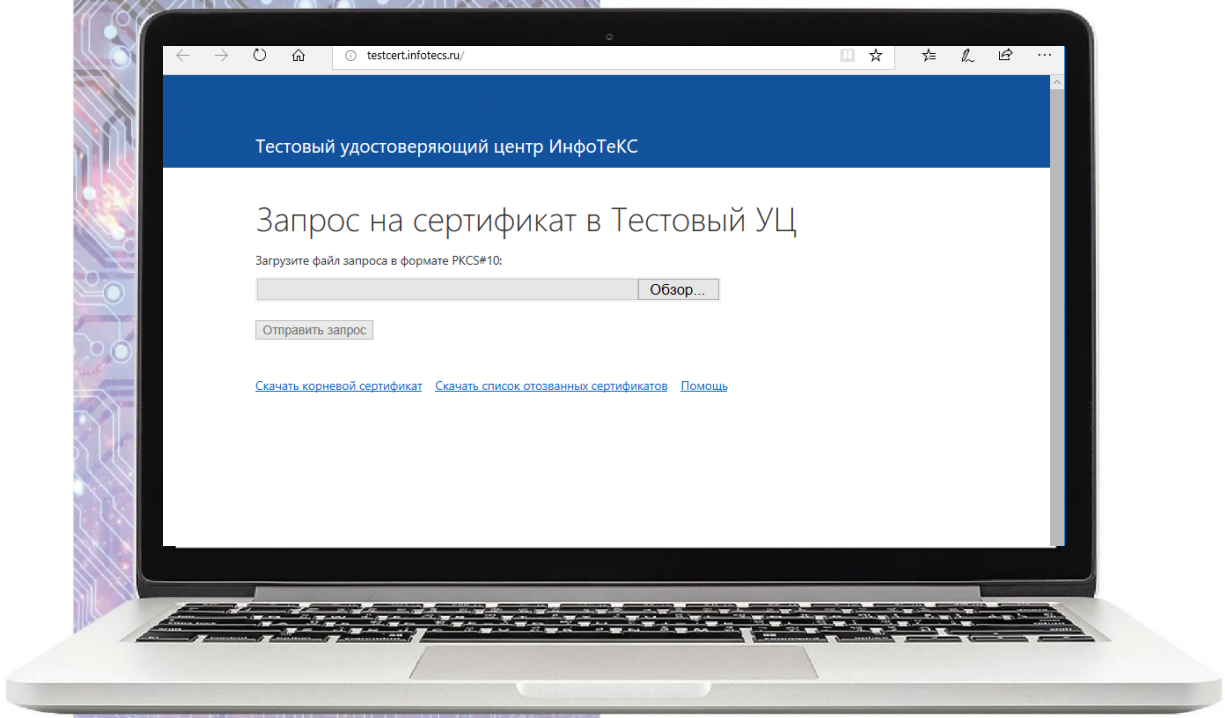


Разворачивание инфраструктуры: установка ViPNet Development kit



Разворачивание инфраструктуры

- Настройка рабочего места администратора ИБ
- Выпуск сертификата администратора
- Установка и инициализация ПАК ViPNet SIES MC
- Установка ПО ViPNet SIES Workstation



Тестовый удостоверяющий центр

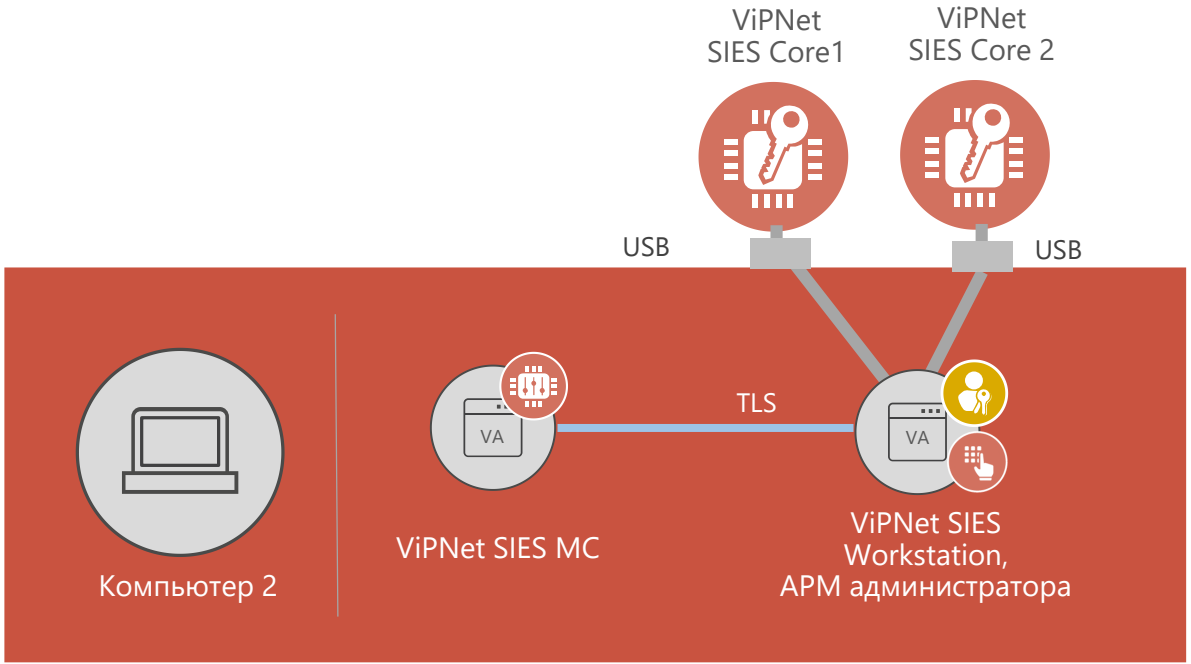
Для выдачи сертификатов администратора и ViPNet SIES MC можно использовать тестовый УЦ:

http://testcert.infotecs.ru/

Пользовательская ключевая подсистема

Пользовательская ключевая подсистема

Инициализация ПАК ViPNet SIES Core



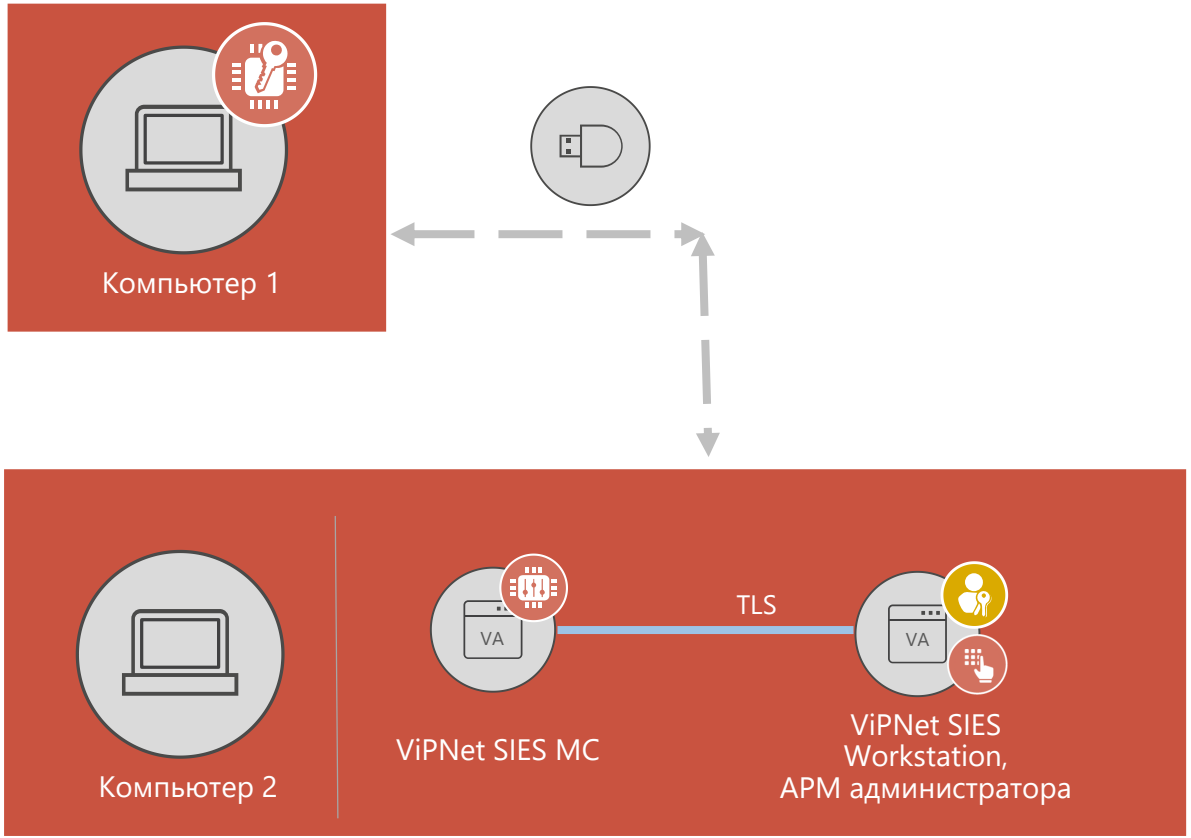
ViPNet SIES Workstation

- Инициализация ViPNet SIES Core 1
- Инициализация ViPNet SIES Core 2

ViPNet SIES MC

- Выставление для ViPNet SIES Core локального режима управления
- Создание защищаемых узлов
- Связывание защищаемых узлов и ViPNet SIES Core

Инициализация ПО ViPNet SIES Unit



Компьютер 1

- Установка ViPNet SIES Unit
- Инициализация ViPNet SIES Unit

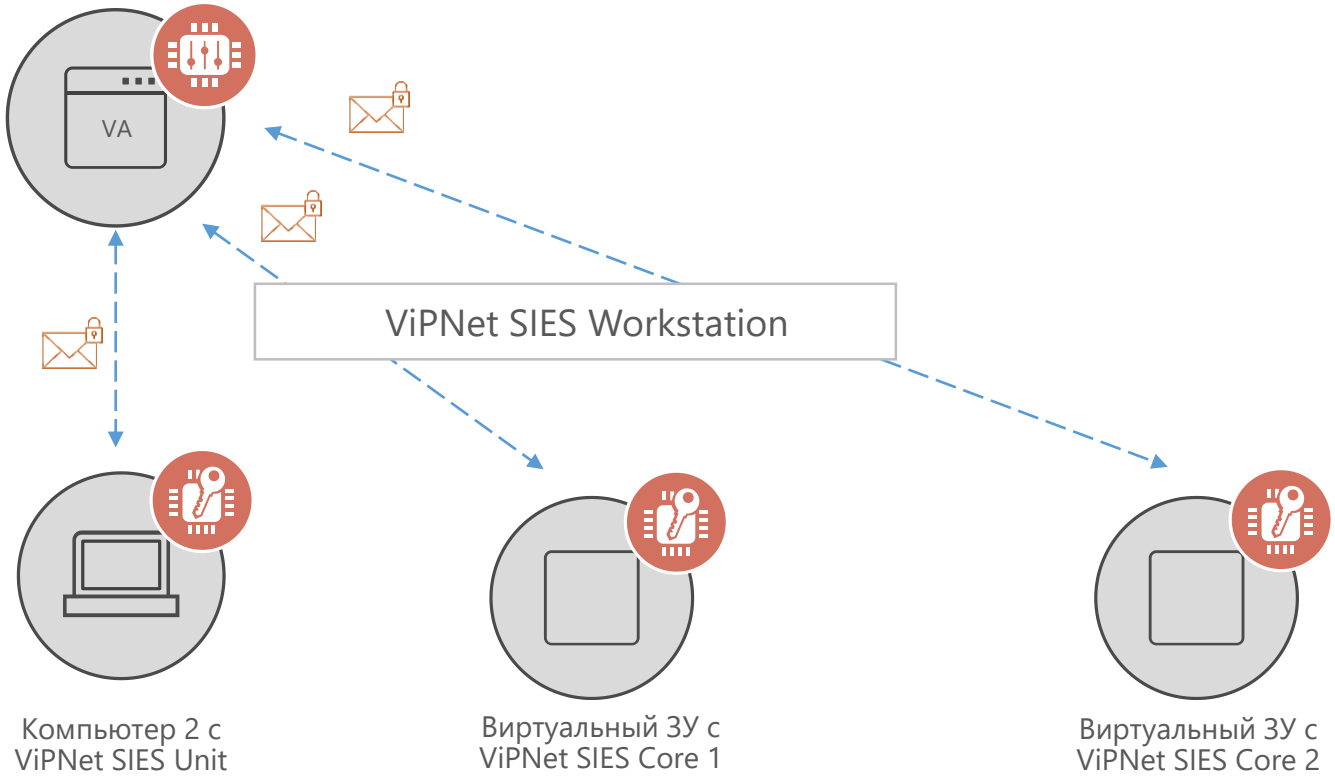
ViPNet SIES MC

- Создание защищаемого узла
- Связывание защищаемого узла и ViPNet SIES Unit

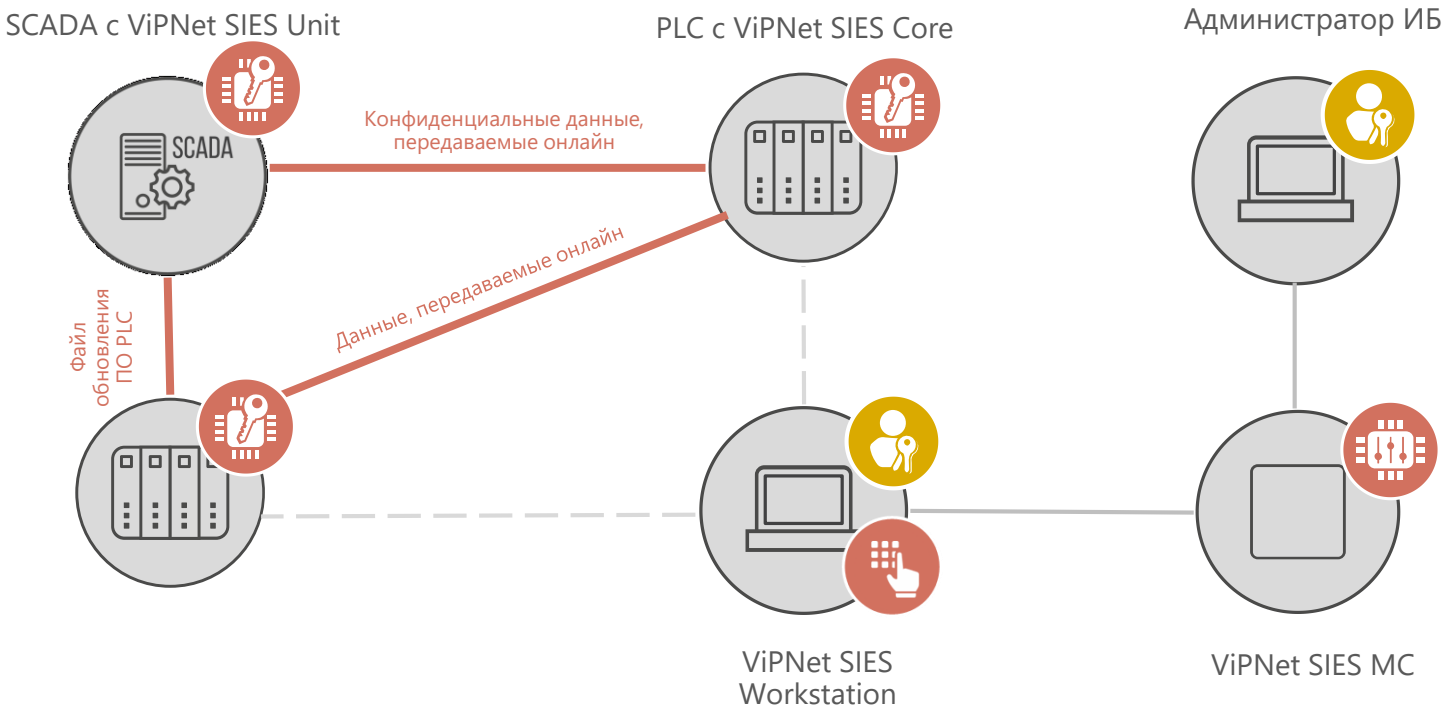
Служебная ключевая подсистема

Служебная ключевая подсистема

Служебная ключевая подсистема



Настройка прикладных связей для сценариев безопасности



Настройка прикладных связей для сценариев безопасности

Задание связей между устройствами

Синхронизация связей

Загрузка ключей на ViPNet SIES Core через ViPNet SIES Workstation

Загрузка ключей на ViPNet SIES Unit через ручную выгрузку команд (только для версии 1.3) или через ViPNet SIES Workstation (2.0)

Пользовательская документация: Сценарии работы ViPNet SIES

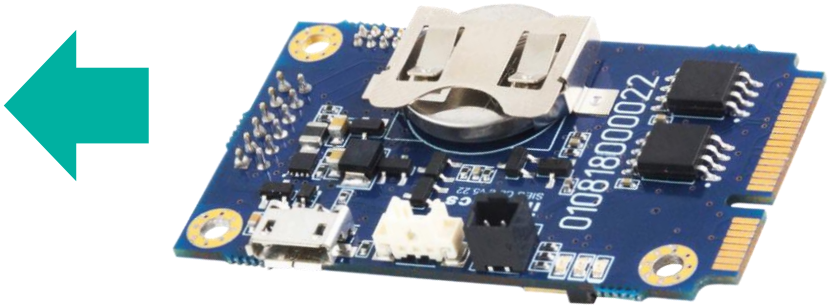
Бизнес сценарии:

- Обеспечение целостности информации
- Обеспечение конфиденциальности информации
- Обеспечение целостности с помощью хэш-кода
- Обеспечение неотказуемости от авторства данных
- Доверенное обновление ПО защищаемого устройства
- Доверенное обновление файла конфигурации
- Защищенная выгрузка журнала
- Криптографическое преобразование пароля для его хранения
- Локальная аутентификация на устройстве
- Аутентификация на удалённом АРМ
- Защита мультивещательных сообщений
- Защита сообщений, передаваемых в рамках подписочной модели

Служебные сценарии:

- Обмен служебными конвертами с центром управления ViPNet SIES MC

Встраивание ViPNet SIES Core

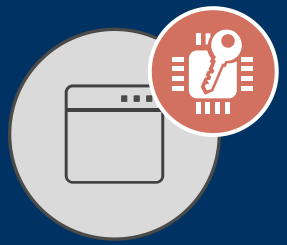


Интеграция ПАК SIES Core

На аппаратном уровне – USB, UART, SPI

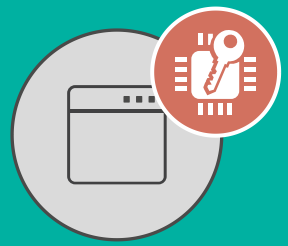
На программном уровне – SIES Core API (RATP+прикладной протокол)

ViPNet SIES Core SDK



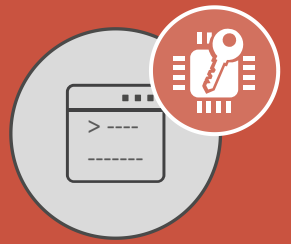
ДИСТРИБУТИВ С НАБОРОМ ГОТОВЫХ БИБЛИОТЕК ПОД ОС LINUX :

- DEBIAN 7 (ARMEL, ARMHF, X86/64)
- UBUNTU 12 (X86/64)



ДИСТРИБУТИВ С НАБОРОМ ГОТОВЫХ БИБЛИОТЕК ПОД ОС WINDOWS:

- WINDOWS 7 (X86/64)
- WINDOWS 8 (X86/64)
- WINDOWS 8.1 (X86/64)
- WINDOWS 10 (X86/64)
- WINDOWS EMBEDDED STANDARD 7 (SP1) (X86/64)
- WINDOWS EMBEDDED 8 STANDARD (X86/64)
- WINDOWS EMBEDDED 8.1 STANDARD (X86/64)
- WINDOWS 10 IOT ENTERPRISE (X86/64)
- WINDOWS XP EMBEDDED (X86/64)



БИБЛИОТЕКИ В ИСХОДНЫХ КОДАХ ДЛЯ ВСТРАИВАЕМЫХ СИСТЕМ НА ЯЗЫКЕ «СИ» :

ТРЕБОВАНИЯ К РЕСУРСАМ:

- ОБЪЕМ ПЗИ – 20 КБ
- ОБЪЕМ ОЗУ – 10 КБ
- ОБЪЕМ СТЕКА – 10 КБ

ViPNet SIES Core SDK

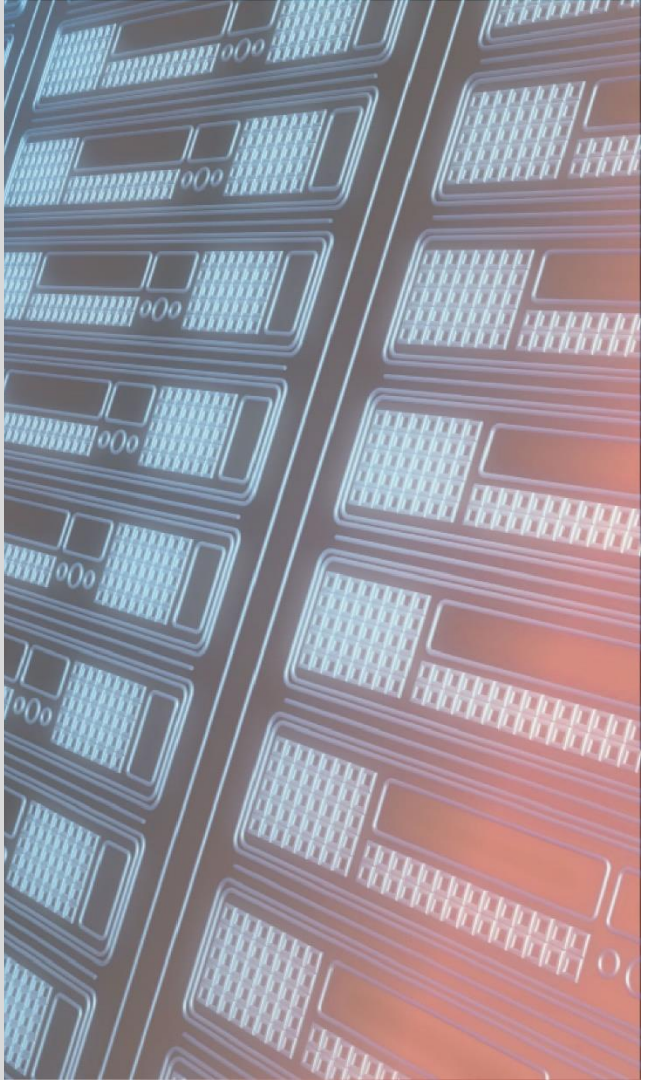
Реализация функционала:

Вызов прикладных функций ViPNet SIES Core через API

Передача защищенных конвертом к ViPNet SIES Core от ViPNet SIES MC и обратно через защищённое устройство

Утилита ViPNet SIES Core

Предоставление доступа к функциям ViPNet SIES Core через интерфейс командной строки



Утилита ViPNet SIES Core позволяет ознакомиться с функциональными возможностями ViPNet SIES SDK без программирования

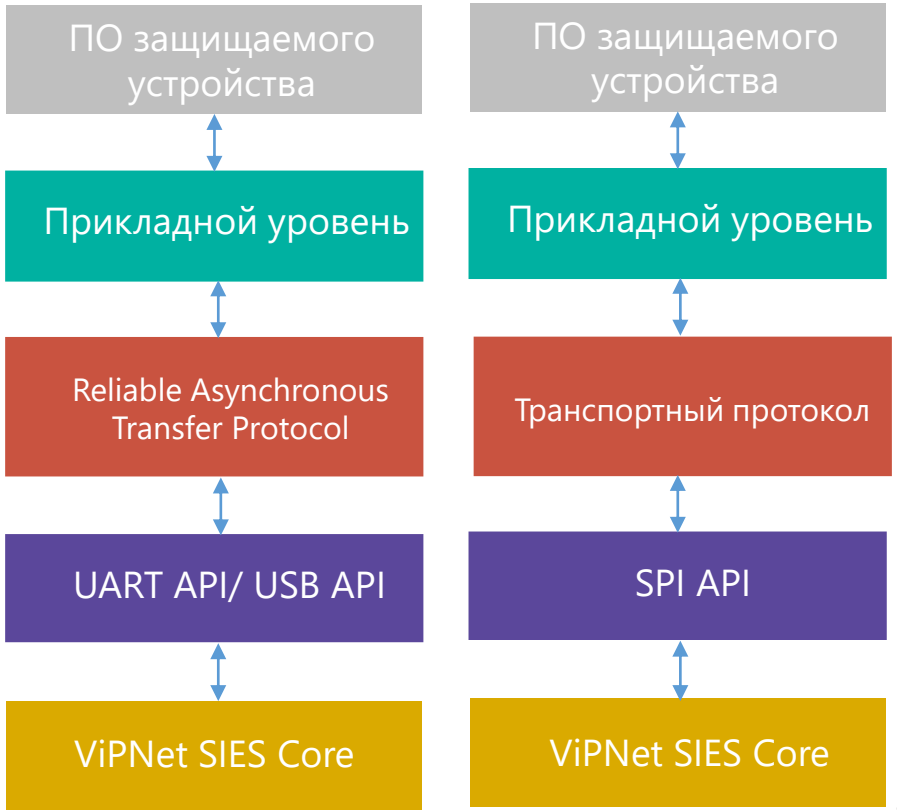
Что делать, если нет SDK под устройство?

Описание протокола ViPNet SIES Core

Документация:

- Описание прикладного протокола
- Описание команд

RATP: RFC 916
https://tools.ietf.org/html/rfc916



Установка ViPNet SIES Unit

Интеграция ПО ViPNet SIES Unit

Поддерживаемые ОС:

SIES Unit в составе ViPNet PKI Client 1.3:

- Windows 7/8/8.1/10 (x86/64)
- Windows Server 2008 R2/2012/2012 R2/ 2016

ViPNet SIES Unit 2.0:

- Windows 7/8/8.1/10 (x86/64)
- Windows Server 2008/R2/2012/2012 R2/ 2016
- Debian 9, Ubuntu 16, Ubuntu 18 и др ОС Linux:
  - gcc v.6 и выше,
  - systemd система инициализации,
  - x86/64 архитектура процессора
  - менеджер пакетов deb/rpm формата
- Astra Linux Special Edition (Смоленск) 1.6 (x86/64)

ViPNet SIES Unit API

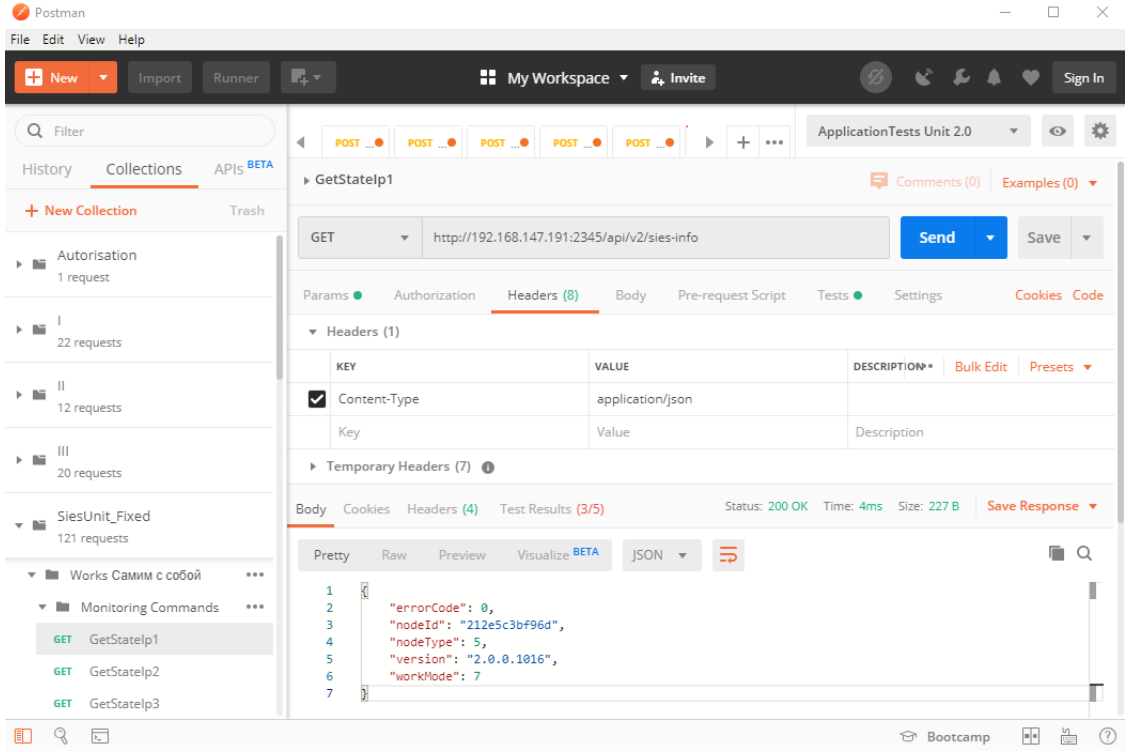
В ViPNet SIES Unit реализован **криптографический** RESTAPI Web-интерфейс:

- Версия HTTP 1.1
- Кодировка Base64

Можно использовать готовые библиотеки, которых большое количество на разных языках программирования

Можно использовать готовые утилиты для работы

ViPNet SIES Unit API



Отладка стандартными средствами:

- Postman
- Wireshark
- Использование систем журналирования ОС:
  - в Windows Event Viewer
  - в Linux journalctl

ViPNet SIES Unit API – отладка стандартными средствами

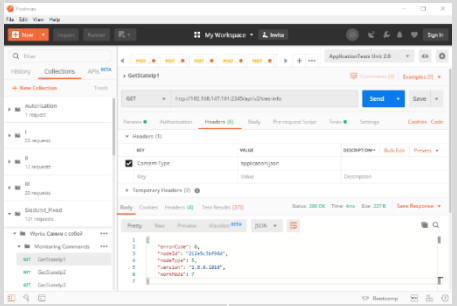
Защищаемое устройство

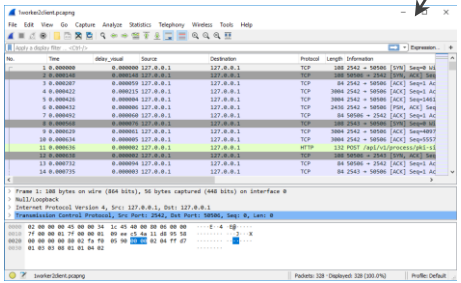
ППО

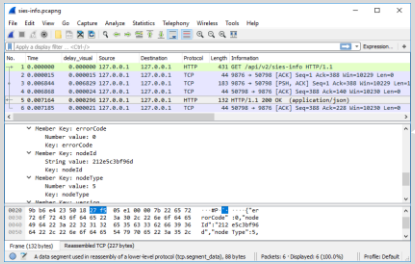
ViPNet SIES Unit/
ViPNet SIES Core

Защищаемое устройство

ППО





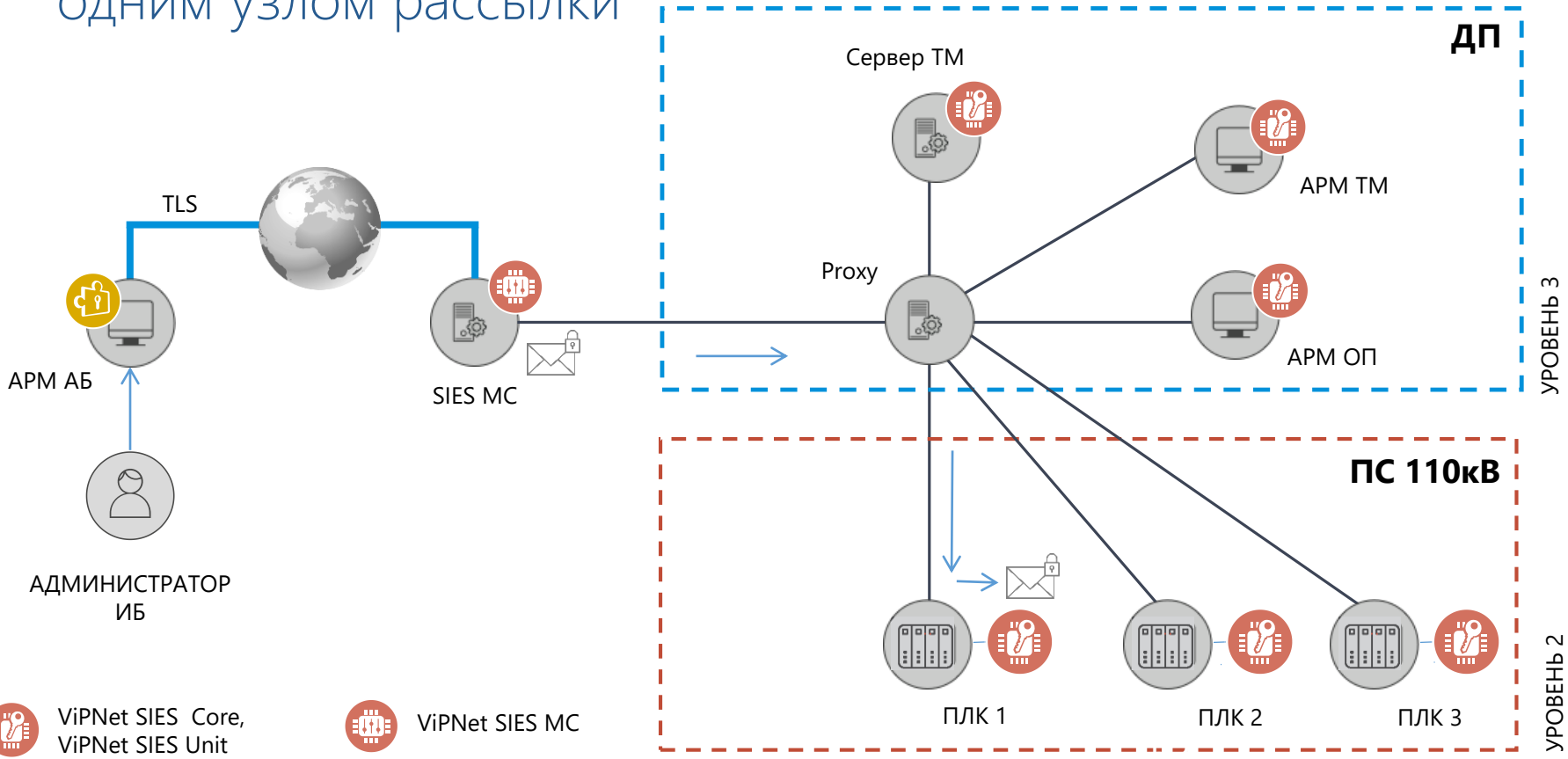


127.0.0.1

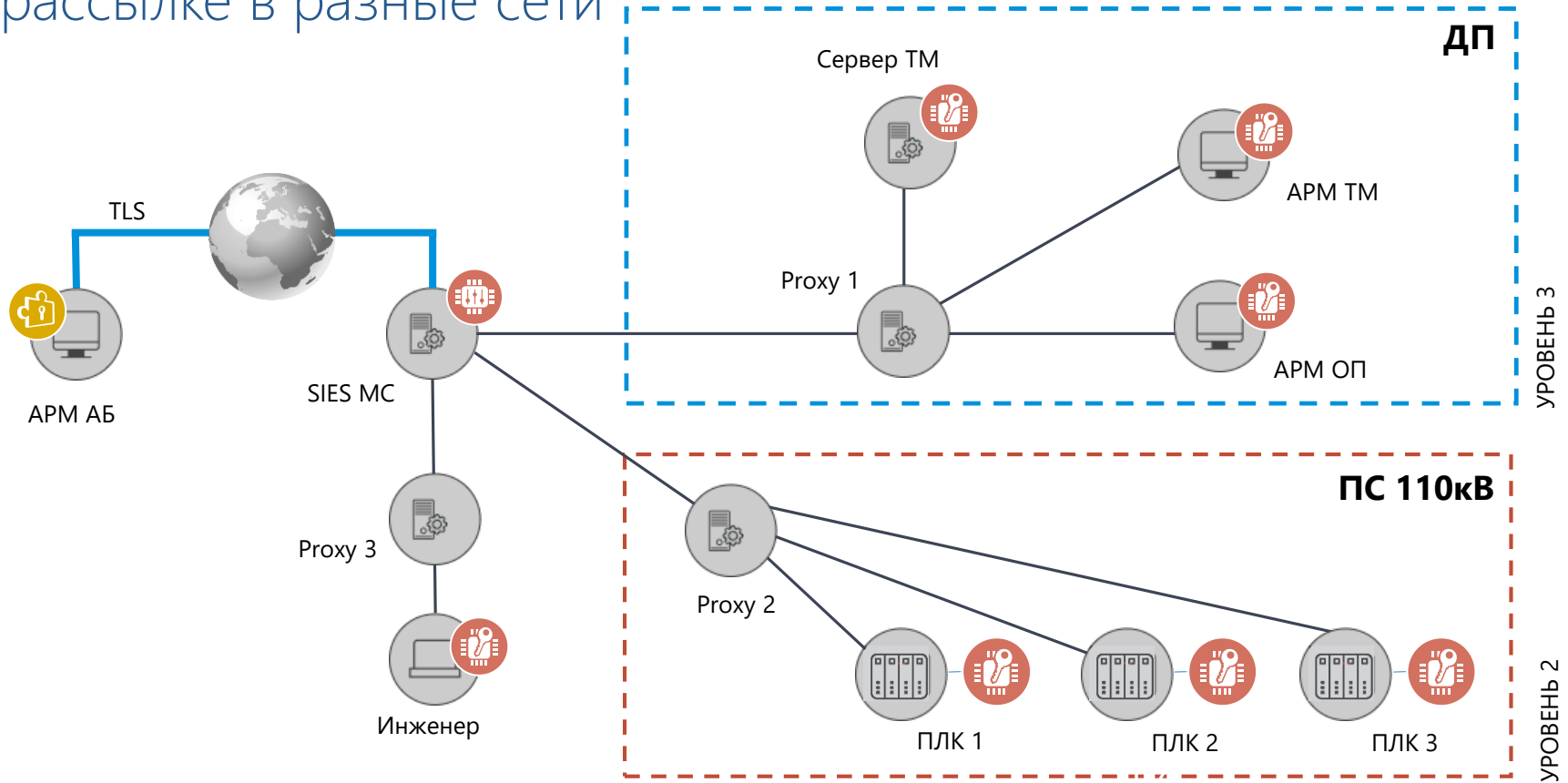
ViPNet SIES Unit

Интеграция ViPNet SIES MC в систему для удаленного управления SIES-узлами

Удаленное управление из ViPNet SIES MC с одним узлом рассылки



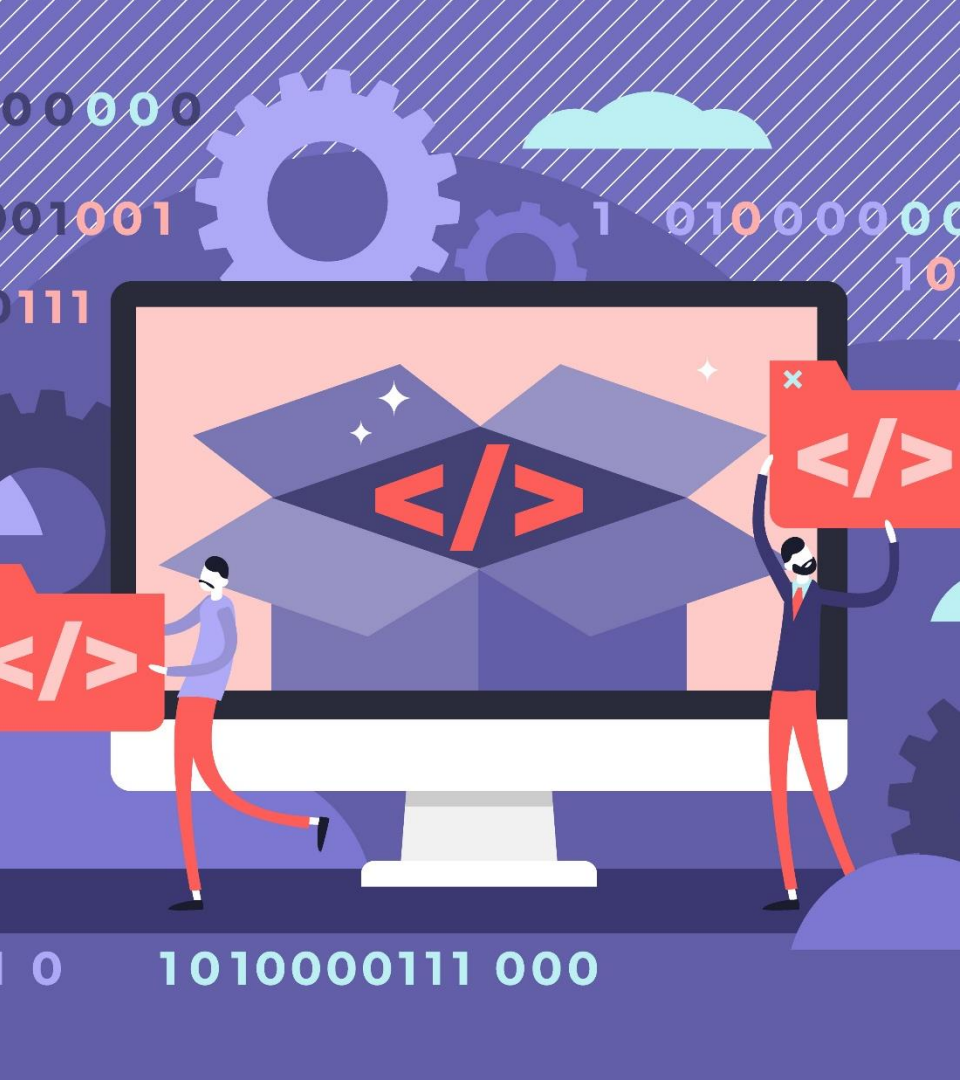
Удаленное управление из ViPNet SIES MC при рассылке в разные сети



ViPNet SIES MC RESTful API

- Обработка запросов на получение из защищенных конвертов ViPNet SIES MC в адрес SIES-узлов;
- Обработка запросов на передачу в ViPNet SIES MC конвертов от SIES-узлов (ответы)

  - HTTP-протокол версии 1.1
  - Кодировка BASE64



Разработка PROXY

Описание в комплекте документации ViPNet SIES MC - ViPNet SIES MC. Руководство разработчика:

Запрос конвертов в адрес SIES-узлов

Возврат конвертов с ответами SIES-узлов

Разработка рекомендаций по процессу установки, разворачивания и эксплуатации защищенных устройств с продуктами ViPNet SIES Core/ ViPNet SIES Unit

- Требования к распространению СКЗИ
- Требования к размещению СКЗИ
- Требования к обслуживанию СКЗИ
- Требования к персоналу

infotecs

Спасибо
за внимание!