Метаморфоз крипточипа: инициализация и ввод в эксплуатацию ViPNet SIES Core Nano

Алексей Власенко

Ведущий менеджер продуктов

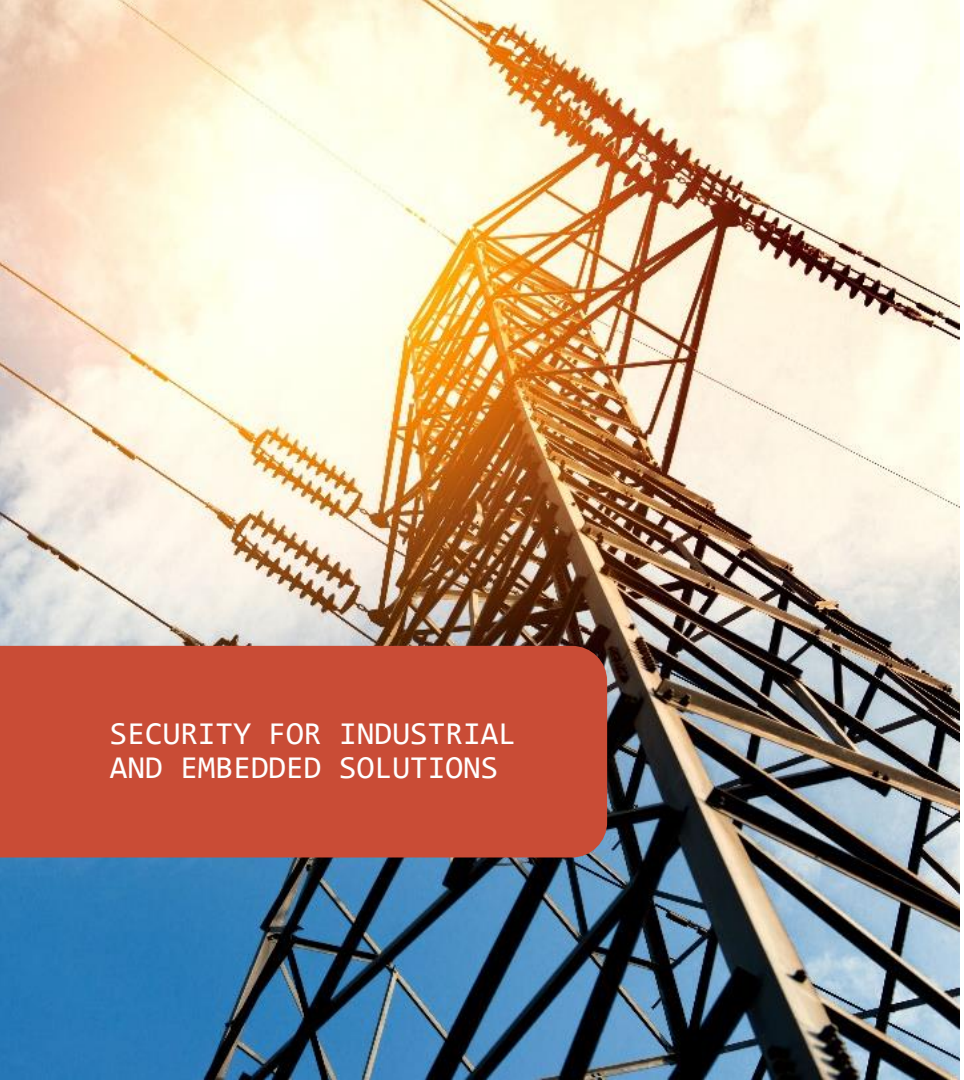
инфотекс ТЕХНОФЕСТ

Красный поток

Решение ViPNet SIES

Немного теории

инфотекс

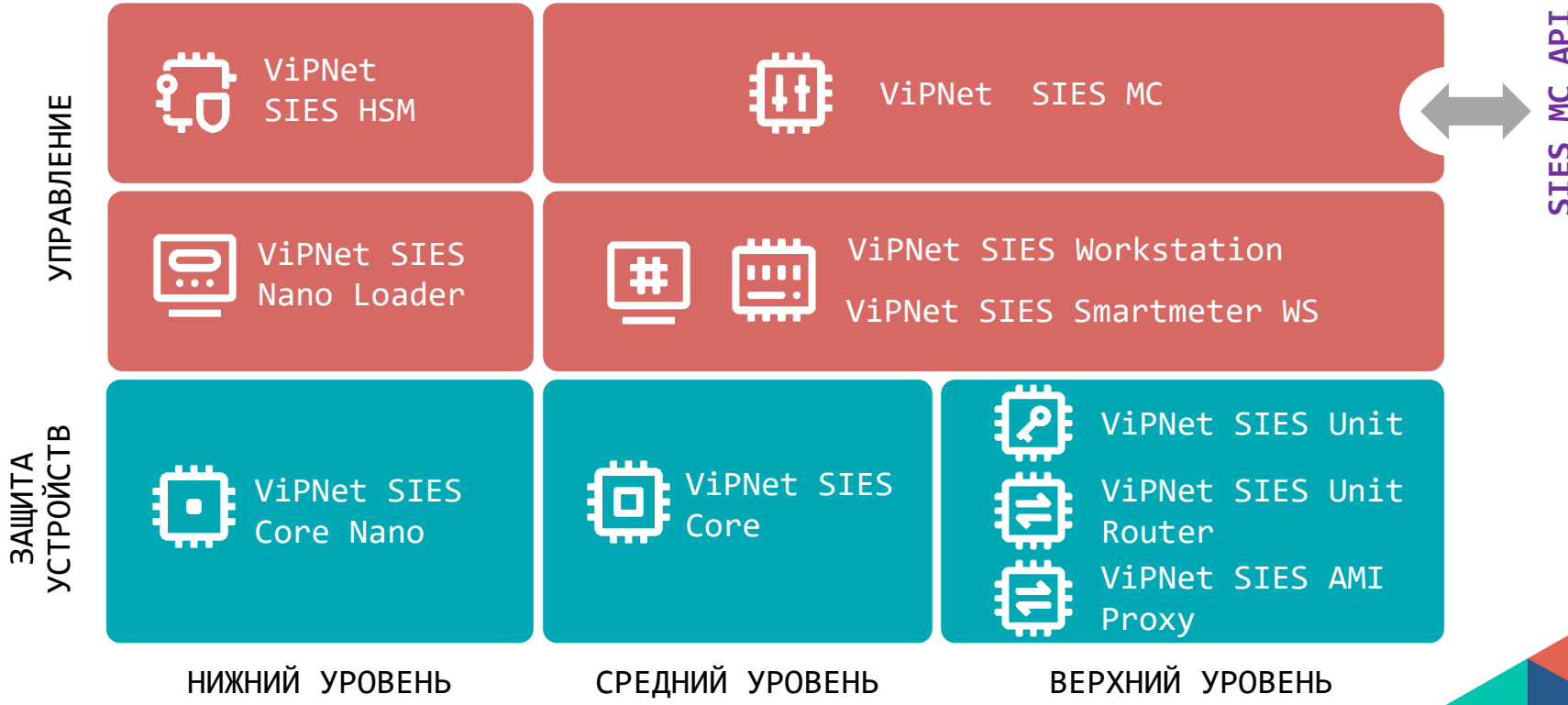


Решение ViPNet SIES

Встраиваемые криптографические средства защиты информации:

- для устройств автоматизации на всех уровнях АСУ
- для M2M-устройств
- для АСКУЭ/ИСУЭ
- для IIoT-устройств

Состав решения ViPNet SIES



Центр управления ViPNet SIES MC

ПАК ViPNet SIES MC 10000
- До 1 млн устройств
- СКЗИ класса КС3

ПАК ViPNet SIES MC 3000
- До 3000 устройств
- СКЗИ класса КС3

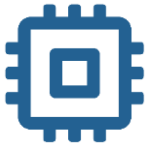
ПАК ViPNet SIES MC IoT
- До 2 млн устройств
- СКЗИ класса КС3

ViPNet SIES MC VA
- До 5000 устройств
- СКЗИ класса КС1

- Ключевой и Удостоверяющий центры
- Управление связями в системе
- Дистанционная смена ключевой информации
- Управление активами
- Доступ к интерфейсу по WebUI
- API для подключения и управления сторонними СКЗИ
- Сертификат СКЗИ класса КС3 и КС1

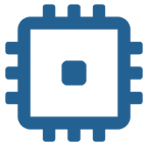
SIES-узлы

СКЗИ, выполняющие прикладные криптографические операции с данными защищаемых устройств



ПАК ViPNet SIES Core

ПО ViPNet SIES Unit



ПАК ViPNet SIES Core Nano

СКЗИ Пользова-теля АСУ

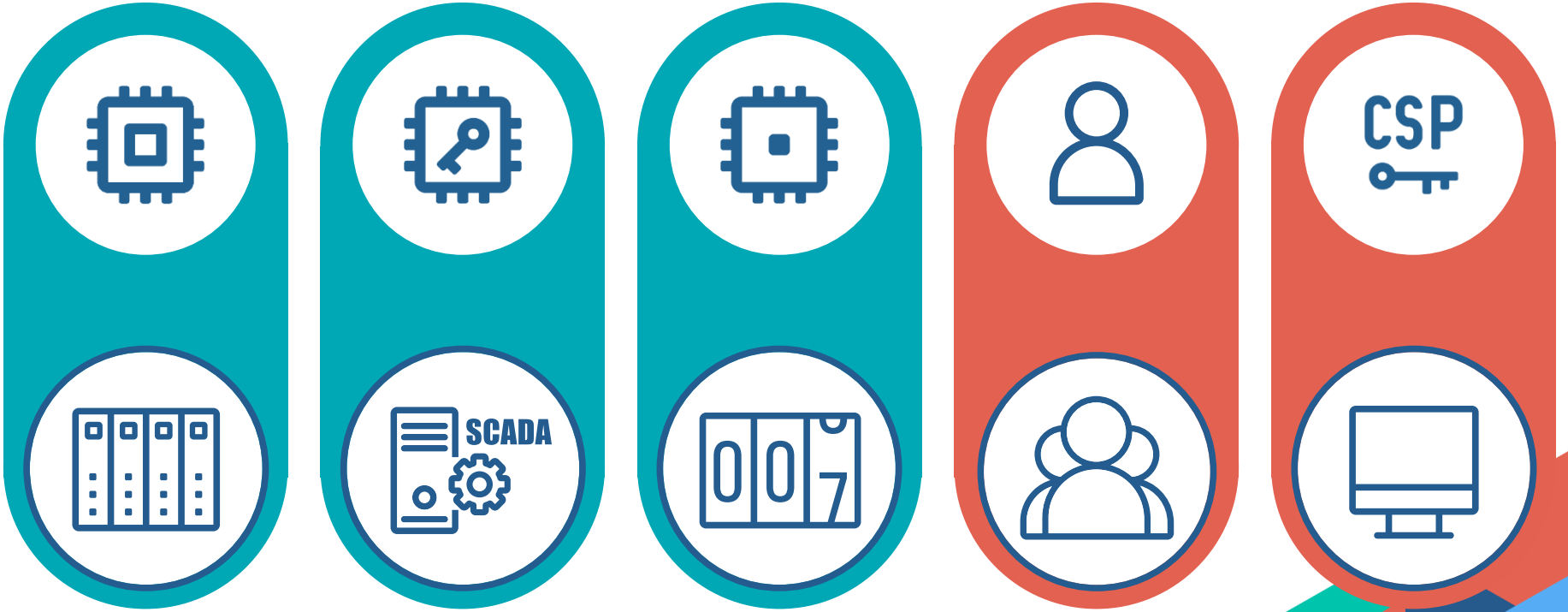
Токены/смарт-карты сервисного инженера, инженера КИП и др.

Другой SIES-узел

Криптопровайдеры, прочие PKI-продукты, библиотеки, сторонние СКЗИ с реализацией CRISP

Защищаемые устройства

Средства обработки информации, интегрированные с SIES-узлами



ViPNet SIES Unit

Встраивание

- ПО устанавливается и работает как сервис ОС
- Интеграция на программном уровне – RESTfull API (HTTP/1.1), gRPC API (HTTP/2) или SDK

Криптографические функции

- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Зашифрование/расшифрование (CMS)
- Вычисление/проверка ЭП (CMS)
- Вычисление/проверка хэш-кода

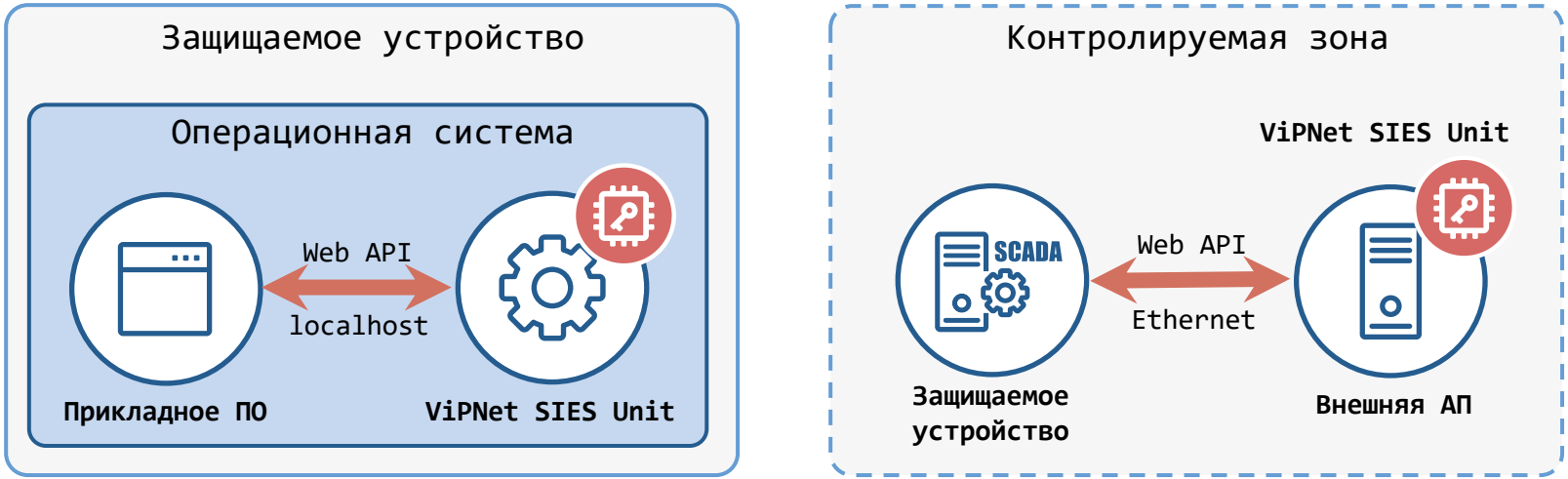
Функциональные особенности

- Поддерживаемые архитектуры: x86-32, x86-64, ARM
- Поддерживаемые ОС: Windows, Linux, Astra Linux, Альт СП
- Установка на защищаемое устройство или выделенную платформу

Соответствие требованиям

- СКЗИ класса КС1 и КС3

Интеграция ViPNet SIES Unit



ViPNet SIES Unit Router

Функции

- Повышение производительности ViPNet SIES Unit
- Распределение запросов на выполнение криптографических операций между несколькими ViPNet SIES Unit
- Обеспечивает единую точку входа для подключения множества защищаемых устройств к нескольким ViPNet SIES Unit
- Автоматическая генерация таблицы маршрутизации запросов
- Резервирование ViPNet SIES Unit

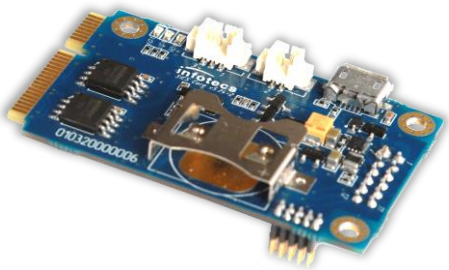
Функциональные особенности

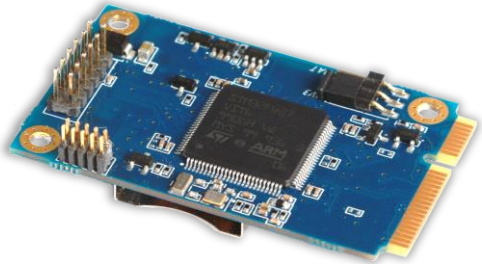
- Программный комплекс работает как служба ОС
- Поддержка резервирования (кластер ViPNet SIES Unit Router)
- Поддерживаемые архитектуры: x86-64
- Поддерживаемые ОС: Astra Linux, Альт СП

Соответствие требованиям

- Не является СКЗИ и не подлежит обязательной сертификации

ViPNet SIES Core





Встраивание

- На аппаратном уровне – UART, USB, SPI, I2C
- Подключение – разъем PLD2, USB-micro, Mini PCI-E
- На программном уровне – SIES Core API, SDK для Linux (ARM, x86), Windows, RTOS

Криптографические функции

- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Зашифрование/расшифрование (CMS)
- Вычисление/проверка ЭП (CMS)
- Вычисление/проверка хэш-кода

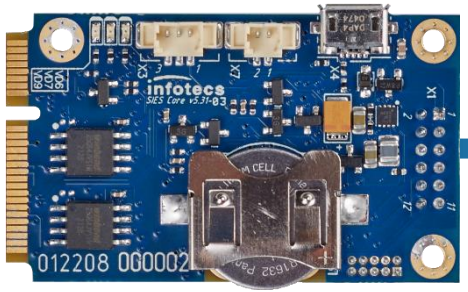
Функциональные особенности

- Форм-фактор – плата PCI Express® Full-Mini Card
- Поддержка ДНСД для эксплуатации вне контролируемой зоны
- Рабочий диапазон температур -40…+70^{0}C

Соответствие требованиям

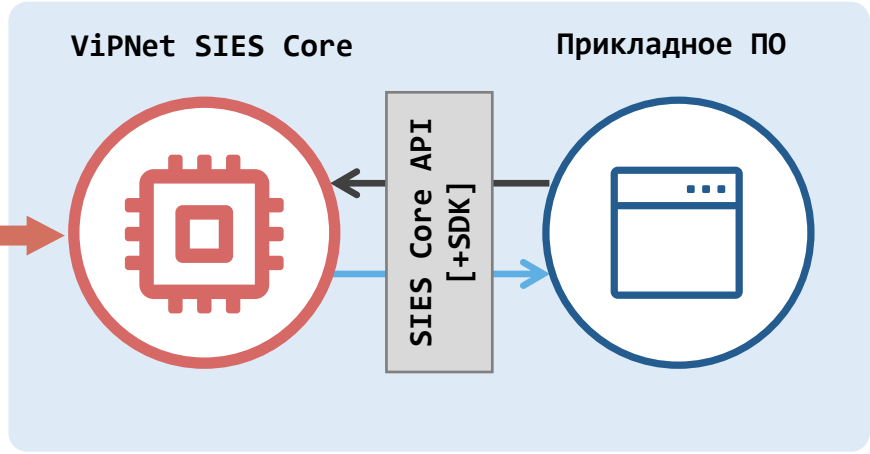
- СКЗИ класса КС3

Интеграция ViPNet SIES Core



ViPNet SIES Core

UART/USB/SPI/I2C

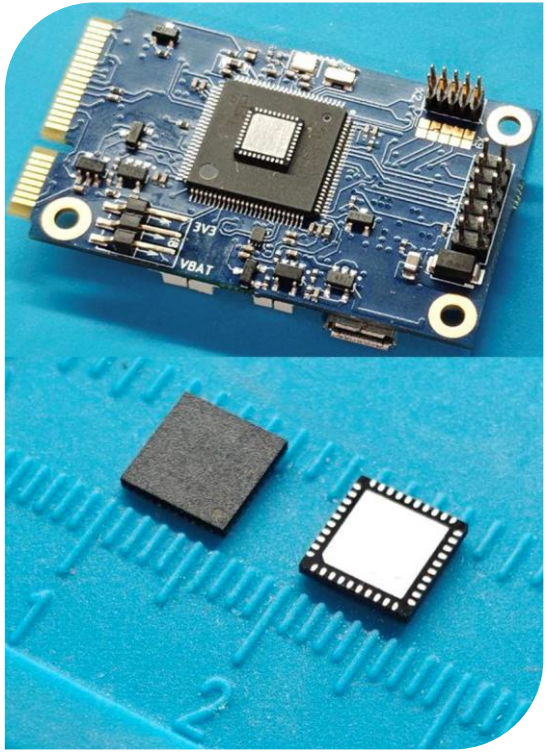


Защищаемое устройство
(ПЛК, УСПД, УСО, шлюз и т.п.)

Данные

Защищенные данные

ViPNet SIES Core Nano



Встраивание

- На аппаратном уровне – SPI
- На программном уровне – SIES Core Nano API

Криптографические функции

- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Вычисление/проверка хэш-кода

Функциональные особенности

- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур -40^0C…$+85^0$C
- Форм-фактор – микросхема **QFN40**
- Эксплуатация вне контролируемой зоны

Соответствие требованиям

- СКЗИ класса КС3
- Защита от атак инженерного проникновения(СКЗИ-НР)

ViPNet SIES Core Nano:

несменные долговременные ключи сроком действия до 16 лет

Ключи загружаются на заводе, изготавливающем устройство, с помощью ViPNet SIES Nano Loader

Средство генерации ключей – ViPNet SIES HSM

- К 1: симметричный ключ для обмена данными с устройством верхнего уровня (парная связь)
- К 2: симметричный ключ для обмена данными с устройством среднего уровня (парная связь)
- К 3: симметричный ключ для обмена данными с устройством (парная связь)
- К 4: симметричный ключ для собственных нужд ViPNet SIES Core Nano (парная связь)
- К 5: симметричный ключ для резервированной связи с верхним уровнем
- Служебный симметричный ключ для обмена данными с **центром управления ViPNet SIES MC**

Резервный набор ключей

ViPNet SIES Core Nano:

временные и групповые ключи

Генерация и смена ключей во время эксплуатации

Загрузка через ViPNet SIES MC

Временные симметричные ключи для обмена данными между устройствами со сроком действия до 1 года (до 20 ключей)

Средство генерации ключей – ViPNet SIES MC

Групповой (мультивещательный) ключ со сроком действия до 16 лет

Средство генерации ключей – ViPNet SIES HSM

Защита данных с помощью протокола CRISP

- Целостность
- Конфиденциальность (опционально)
- Защита от навязывания повторных сообщений
- Аутентификация источника сообщений

* *Протокол CRISP (ГОСТ Р 71252-2024) входит в перечень рекомендованных Минцифры России протоколов для ИСУЭ и IIoT*

- Защита адресных и групповых сообщений
- Бессесионный криптографический протокол
- Минимальные накладные расходы (overhead)и минимальная нагрузка на сеть
- Универсальный стандартизированный протокол защиты любых протоколов ИСУЭ

ViPNet SIES Nano Loader

автоматизированное рабочее место подготовки к эксплуатации ViPNet SIES Core Nano

Функции

- Проверка целостности ПО
- Загрузка ПО в ViPNet SIES Core Nano
- Контроль серийного номера ViPNet SIES Core Nano
- Запрос ключевой информации из ViPNet SIES HSM
- Загрузка ключевой информации в ViPNet SIES Core Nano
- Экспорт данных о подготовленных ViPNet SIES Core Nano

Функциональные особенности

- Форм-фактор: ViPNet SIES Nano Loader (настольный ПК) + ViPNet SIES Nano Array Adapter (оснастка для подключения ViPNet SIES Core Nano)
- Одновременная подготовка до 10 ViPNet SIES Core Nano

Соответствие требованиям

- СКЗИ класса КС3

ViPNet SIES Nano Loader

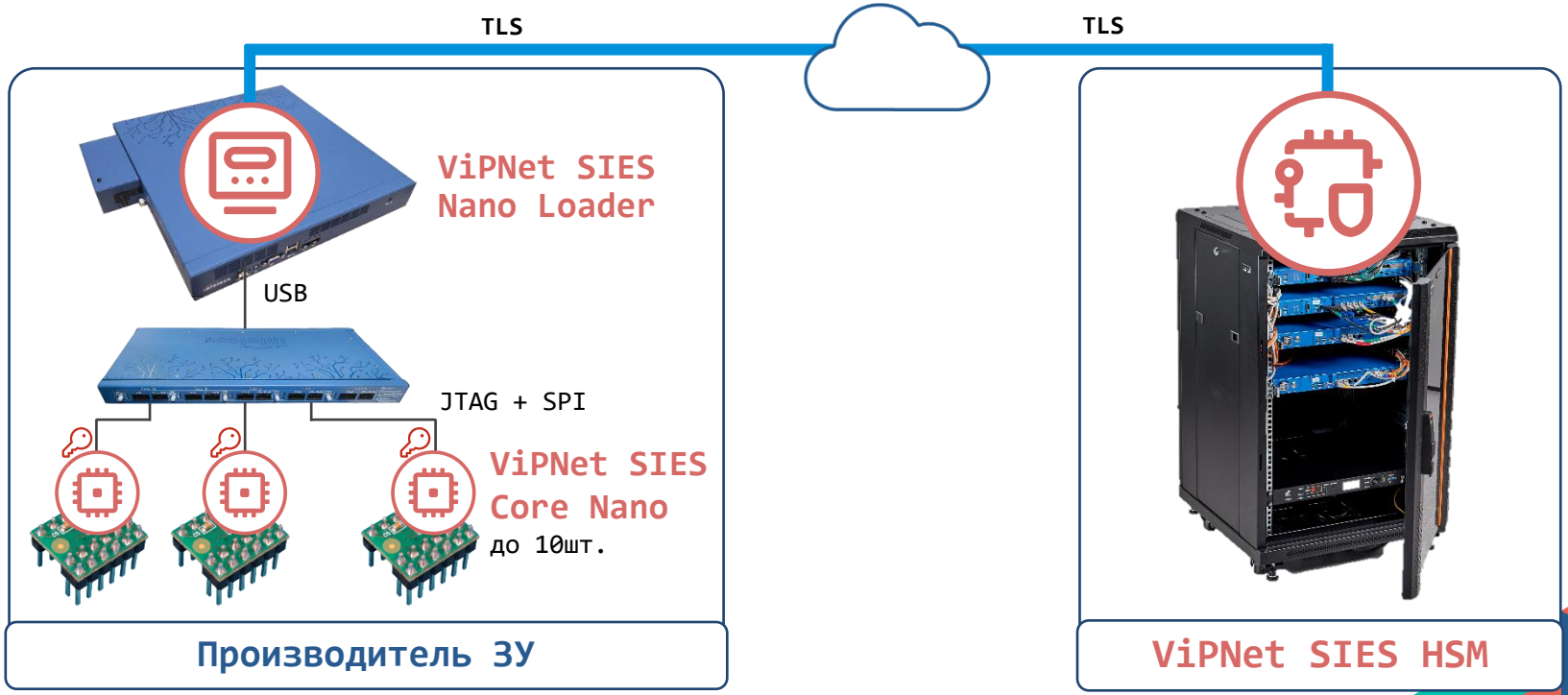
ViPNet SIES Nano Loader
АРМ инициализации SIES Core Nano

ViPNet SIES Nano Array Adapter
оснастка для подключения

Комплекс ViPNet SIES HSM

- Долговременное защищенное хранение ключевой информации ViPNet SIES Core Nano
- Регистрация производителей устройств и их АРМ ViPNet SIES Nano Loader
- Генерация и предоставление ключевой информации по запросу ViPNet SIES Nano Loader
- Предоставление ключевой информации по запросу ViPNet SIES MC
- Хранение БД соответствия серийного номера устройства, СКЗИ и загруженных ключей

Производство устройств с ПАК ViPNet SIES Core Nano

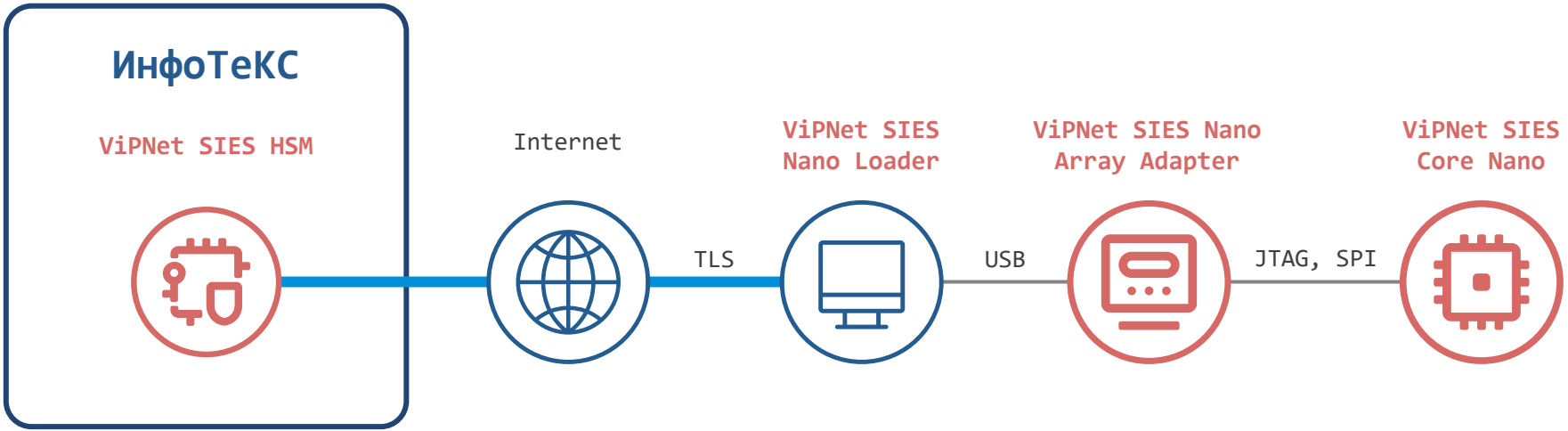


Инициализация ViPNet SIES Core Nano

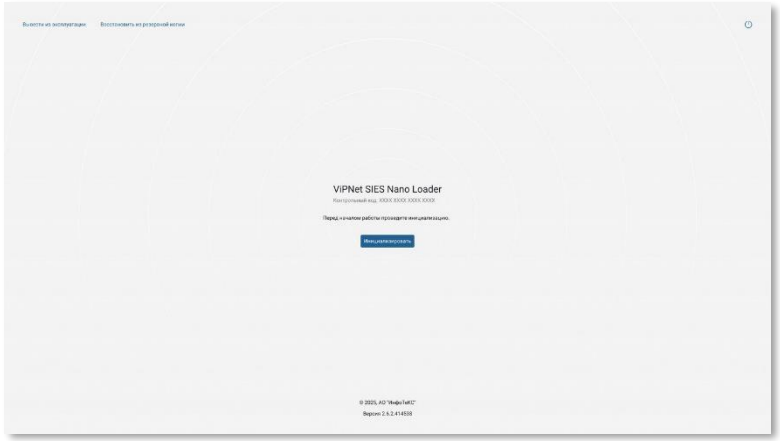
От теории к практике

инфотекс

Схема взаимодействия



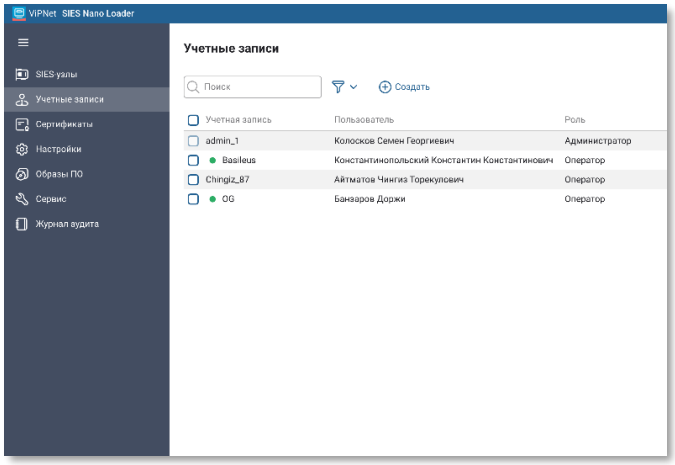
ViPNet SIES Nano Loader подготовка к эксплуатации



Инициализация

- Регистрация администратора ViPNet SIES Nano Loader
- Регистрация ViPNet SIES Nano Loader в ViPNet SIES HSM
- Формирование запросов на сертификаты:
  - ViPNet SIES Nano Loader для TLS
  - ViPNet SIES Nano Loader для защиты ключей
- Загрузка сертификатов:
  - Корневой сертификат ViPNet SIES HSM
  - Список отозванных сертификатов
  - ViPNet SIES Nano Loader для TLS
  - ViPNet SIES Nano Loader для защиты ключей

Пользователи ViPNet SIES Nano Loader



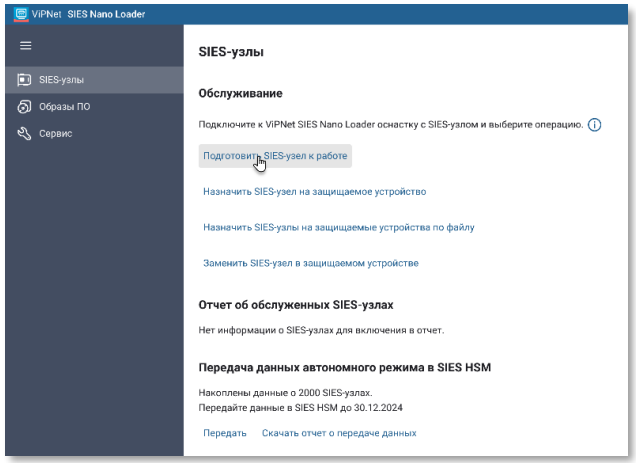
Администратор

- Управление ключевой информацией
- Управление журналами
- Управление настройками
- Управление пользователями
- Резервное копирование и восстановление
- Загрузка образов ПО ViPNet SIES Core Nano

Оператор

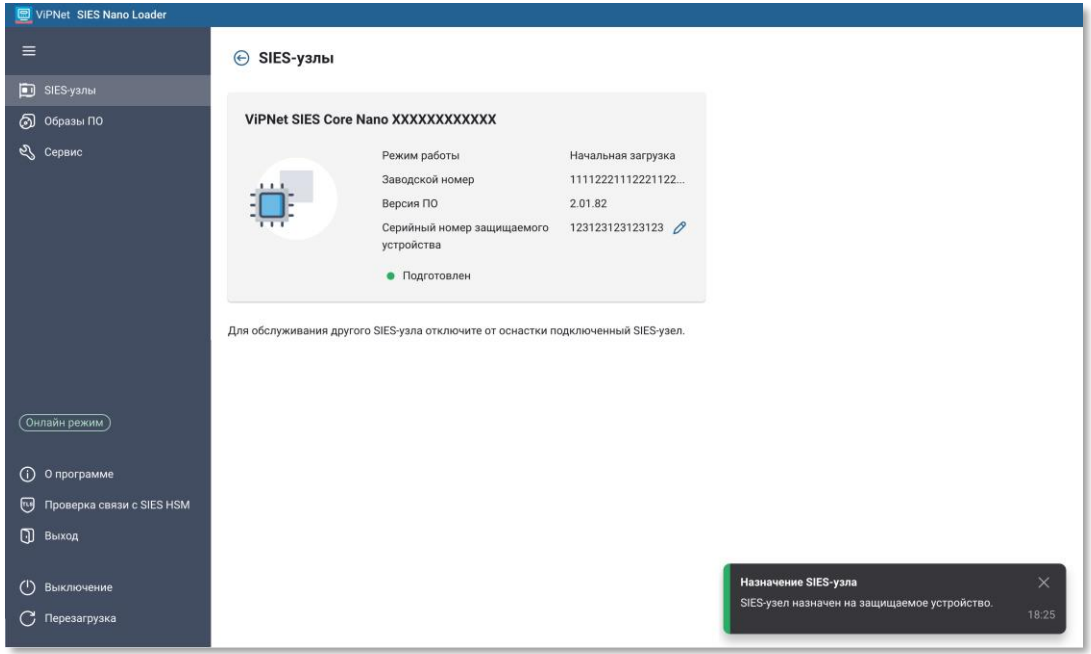
- Подготовка ViPNet SIES Core Nano к эксплуатации
- Загрузка ключей для подготовки ViPNet SIES Core Nano
- Отправка данных в ViPNet SIES HSM
- Выгрузка ведомости и отчетов о подготовленных ViPNet SIES Core Nano

Подготовка ViPNet SIES Core Nano



- Выбор образа ПО ViPNet SIES Core Nano
- Загрузка ПО в ViPNet SIES Core Nano
- Запрос ключей в ViPNet SIES HSM
- Загрузка ключей в ViPNet SIES Core Nano
- Назначение ViPNet SIES Core Nano на защищаемое устройство
- Отправка информации о подготовленных ViPNet SIES Core Nano и защищаемых устройствах в ViPNet SIES HSM
- Выгрузка ведомости о подготовленных ViPNet SIES Core Nano

Завершение подготовки ViPNet SIES Core Nano



САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН · Актив · TS Solution · AXOFT

Подписывайтесь на наши соцсети