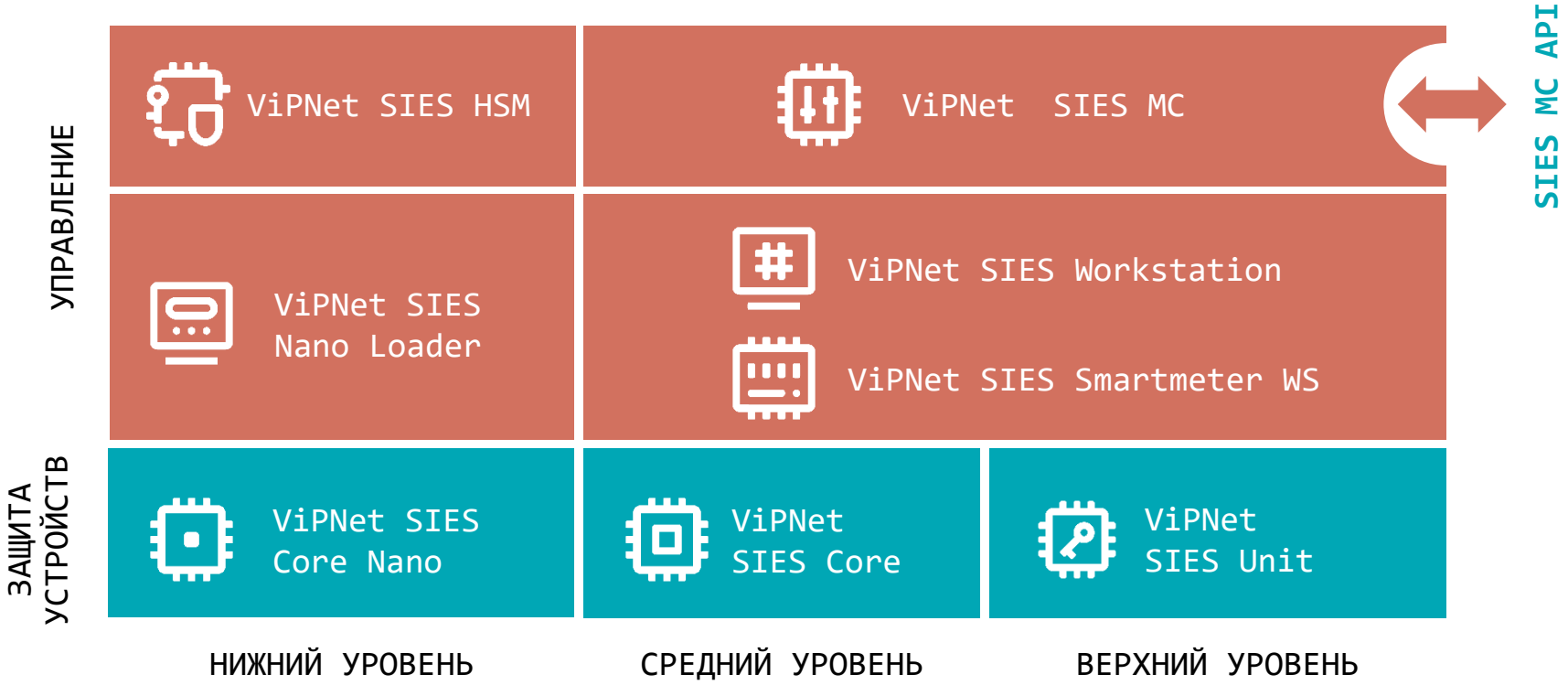
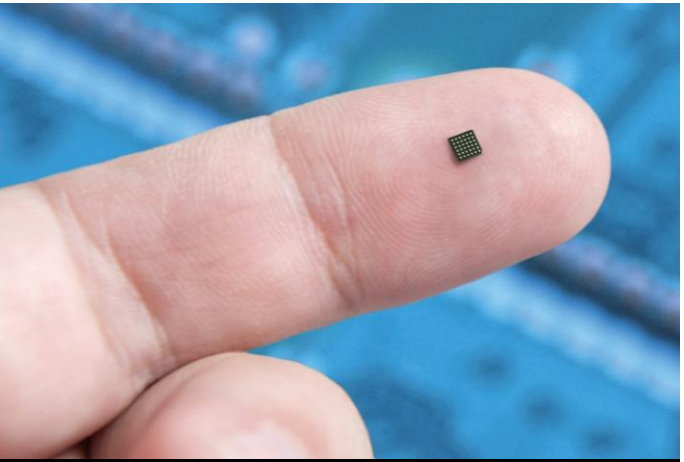
Как подружиться с крипточипом ViPNet SIES Core Nano

Алексей Власенко
ведущий менеджер продуктов

Состав решения ViPNet SIES



ПАК ViPNet SIES Core Nano



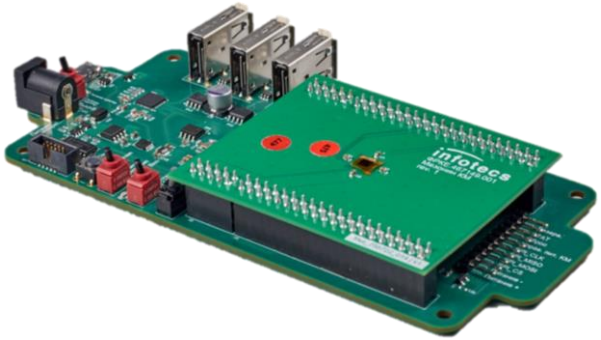
Встраивание:
- На аппаратном уровне – SPI
- На программном уровне – Core Nano API

Криптографический протокол CRISP:
- 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…+85^{0}C
- Форм-фактор – микросхема BGA36 3x3x0,4 мм

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

Комплект разработчика ViPNet SIES Core Nano DevKit



Предназначен для разработчиков защищаемых устройств, ведущих работы по встраиванию ViPNet SIES Core Nano

Состоит из:

- модуля SIES Core Nano Adapter;
- мезонинной платы с распаянным SIES Core Nano*

Комплект разработчика позволяет:

- ознакомиться с возможностями продукта ViPNet SIES Core Nano;
- разработать и отладить ПО защищаемого устройства для взаимодействия с ViPNet SIES Core Nano;
- реализовать сценарии защиты информации защищаемого устройства;
- подготовить стенд для проверки реализованных сценариев защиты информации;
- разработать конструкторскую, доработать пользовательскую и эксплуатационную документацию с учётом использования СКЗИ

* В ViPNet SIES Core Nano, установленный в комплекте разработчика, уже загружена вся ключевая информация из ViPNet SIES HSM ИнфоТеКС

ViPNet SIES Development kit варианты исполнения

Исполнение 1	Исполнение 2	Исполнение 3	Исполнение 4
ViPNet SIES Core (2 модуля)	ViPNet PKI Client с TLS Unit	ViPNet SIES Core (2 модуля)	ViPNet PKI Client с TLS Unit
ViPNet SIES Core SDK	ViPNet SIES Unit	ViPNet SIES Core SDK	ViPNet SIES Unit
ViPNet SIES Workstation	ViPNet SIES MC VA	ViPNet SIES Workstation	Подключение к ViPNet SIES MC ИнфоТеКС
ViPNet SIES Unit		ViPNet SIES Unit	
ViPNet PKI Client с TLS Unit		ViPNet PKI Client с TLS Unit	
ViPNet SIES MC VA		Подключение к ViPNet SIES MC ИнфоТеКС	** Может быть предоставлен при заказе комплекта разработчика ViPNet SIES Core Nano*

Паспорт, комплект пользовательской и эксплуатационной документации

Разработка сквозных сценариев с помощью КР ViPNet SIES Core Nano

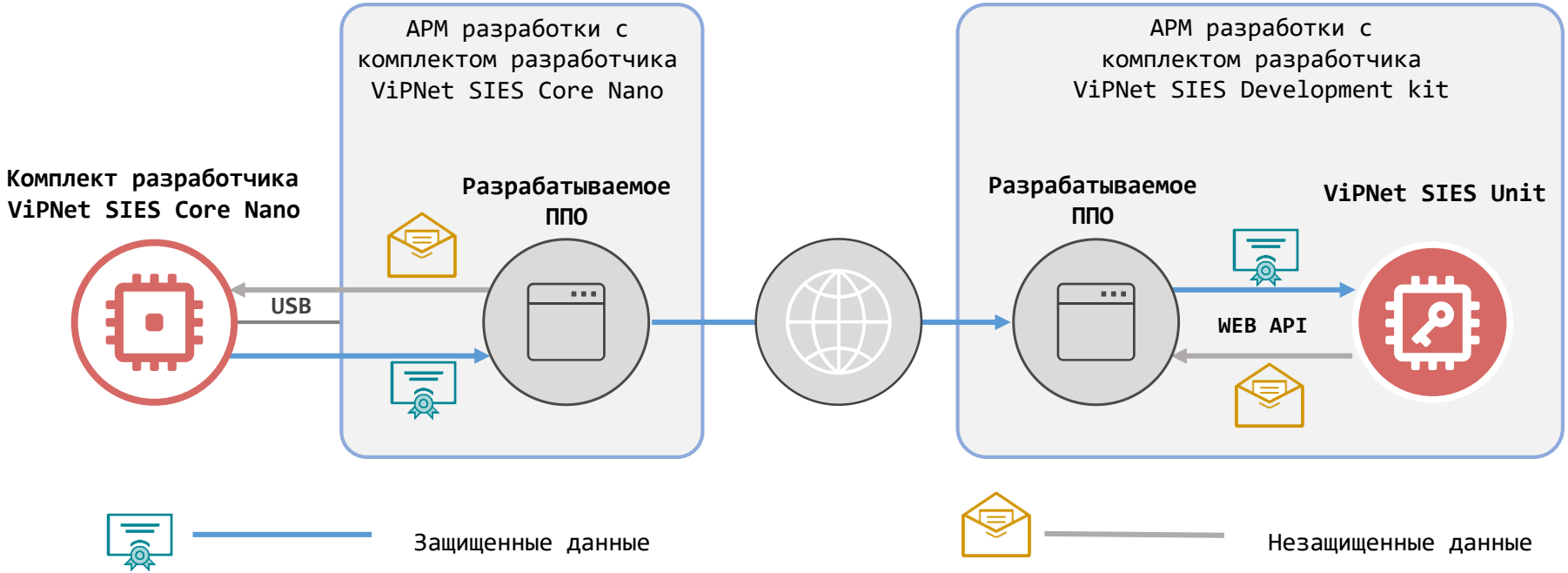
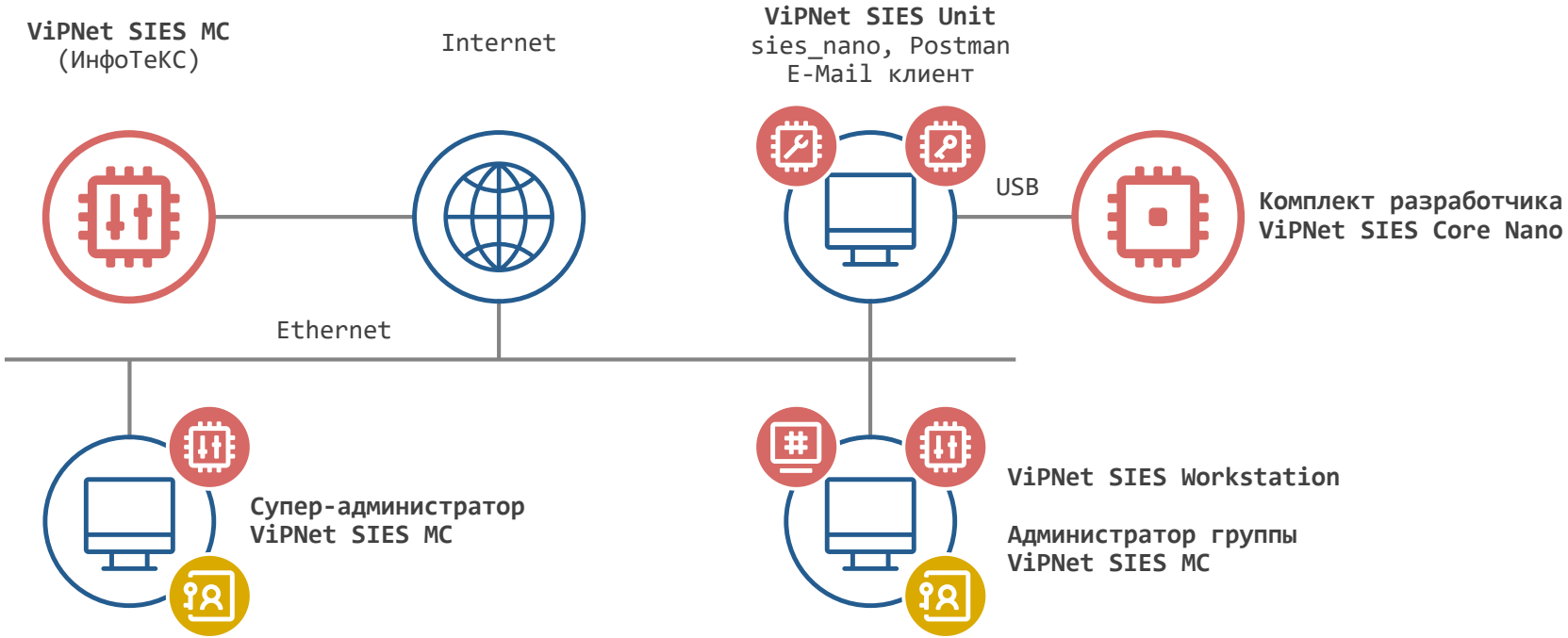


Схема взаимодействия



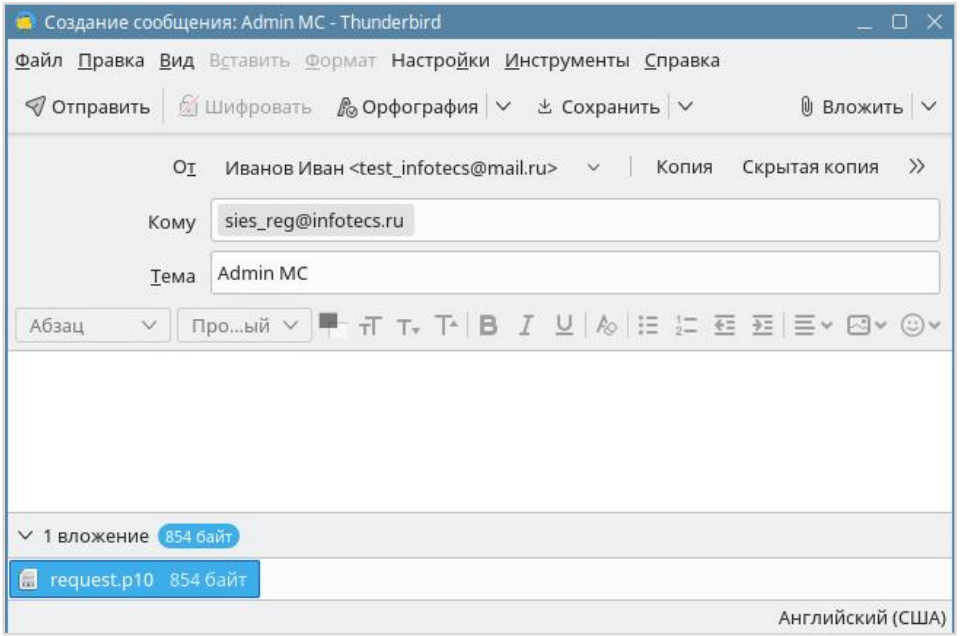
Работа с ViPNet SIES Core Nano без программирования

- Подключение к АРМ разработчика по USB
- Знакомство с VipNet SIES Core Nano
- Отладка и тестирование
- Не требует программирования или написания скриптов
- Работа из командной строки Linux
- Поддерживаются все прикладные функции

Запрос сертификатов для доступа к ViPNet SIES MC

Направьте запрос на сертификат по электронной почте на адрес sies_reg@infotecs.ru

В теме письма должно быть ключевое слово: «МС»

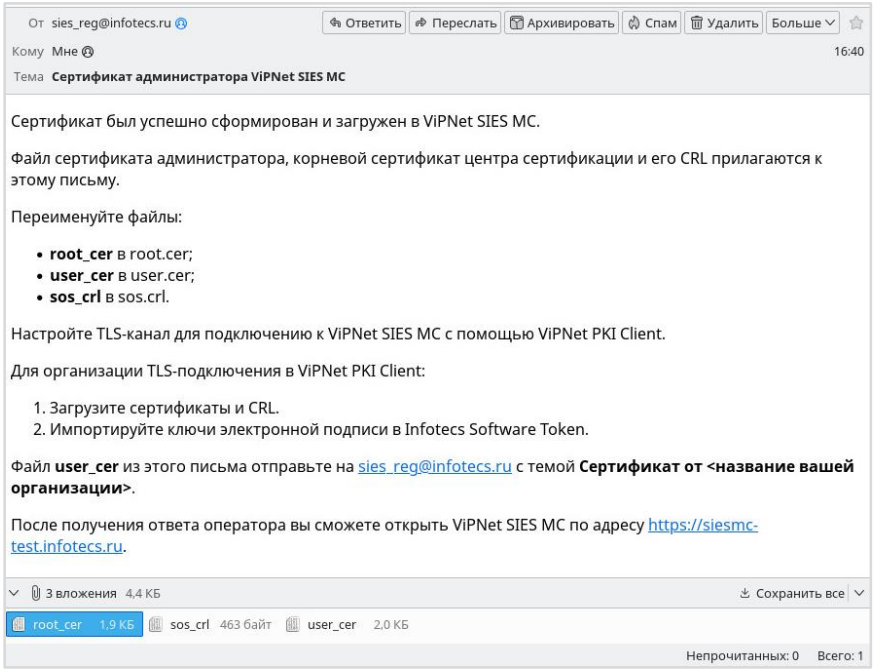


Запрос сертификатов для доступа к ViPNet SIES MC

Получите письмо, содержащее:

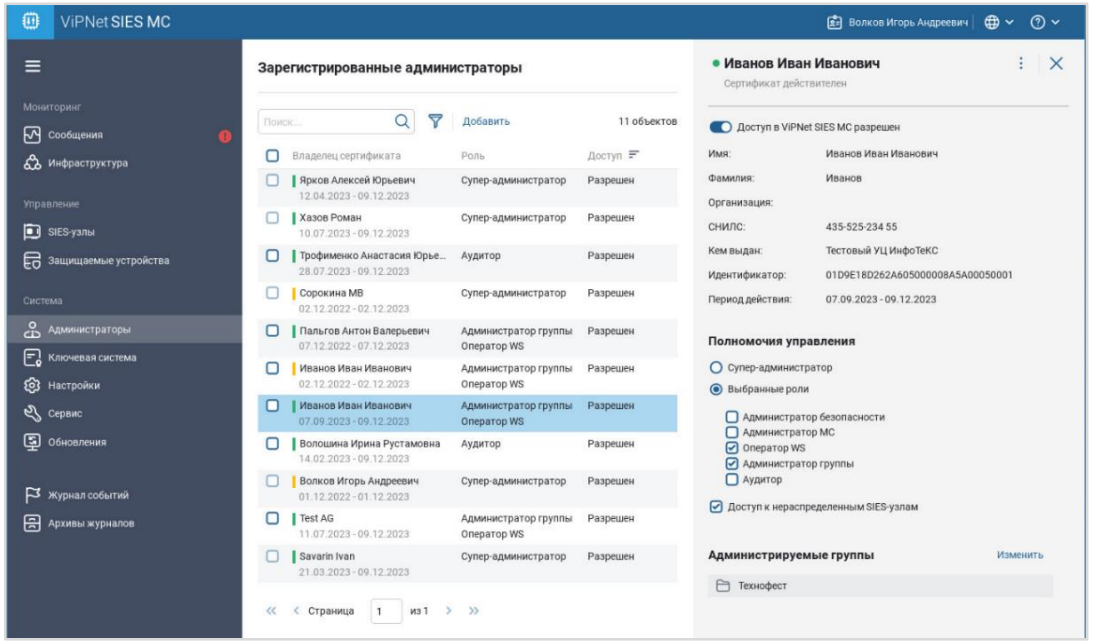
- Сертификат администратора ViPNet SIES MC
- Корневой сертификат
- Список отзыва сертификатов

Установите полученные сертификаты и список отзыва



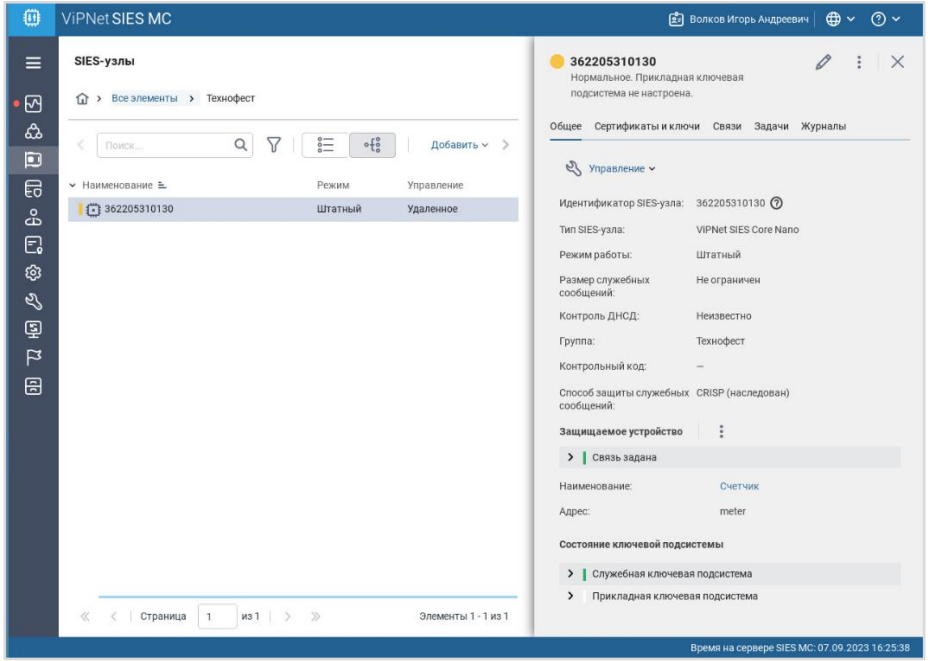
Предоставление прав для управления группой

Супер-администратор ViPNet SIES MC ИнфоТеКС настраивает права для управления вашей группой защищаемых устройств и SIES-узлов



Добавление ViPNet SIES Core Nano

Добавляем ViPNet SIES Core Nano из комплекта разработчика в ViPNet SIES MC, используя его серийный номер



Ввод в эксплуатацию ViPNet SIES Unit

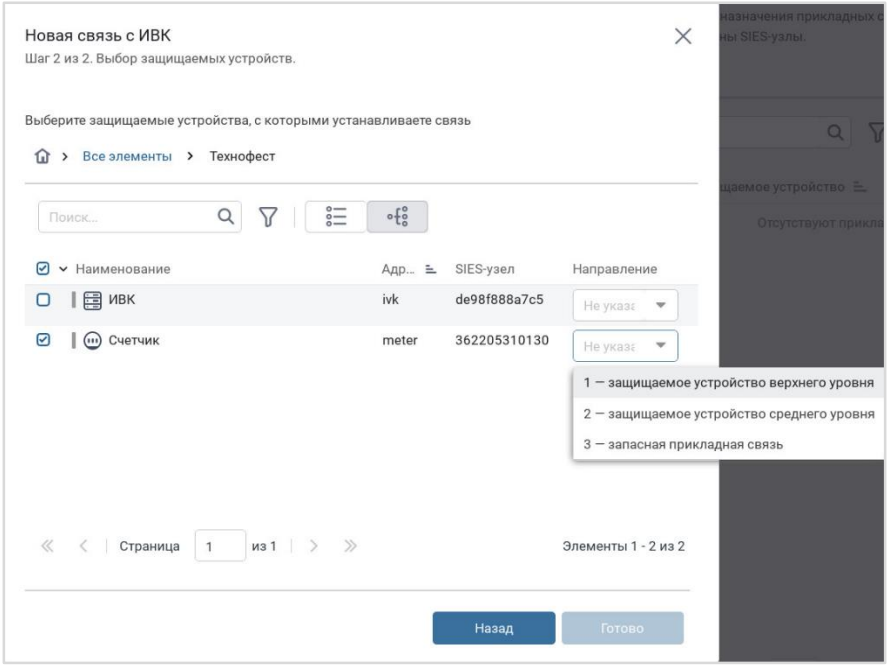
Устанавливаем
и настраиваем
ViPNet SIES Unit

```
ID: 000000000000
Type: 5
Version: 2.5.0.440
Mode: Initialization

0. ViPNet SIES Unit details
1. Reset to factory settings
2. Verify integrity
3. Generate service key pair
4. Complete ViPNet SIES Unit initialization
5. Settings
6. Exit
```

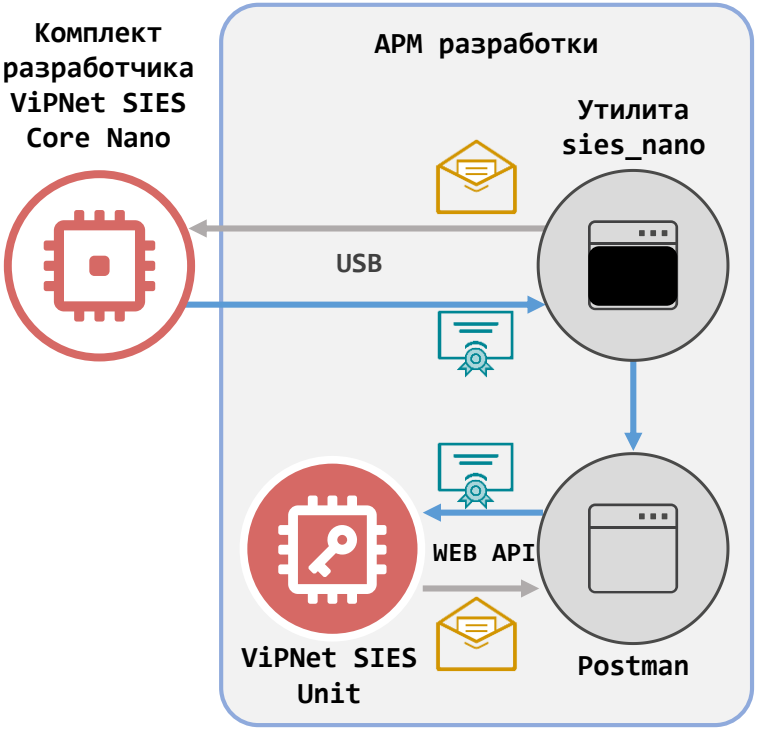
Создание прикладных связей

- Создаем прикладные связи между защищаемыми устройствами
- Синхронизируем созданные связи для отправки ключевой информации в SIES-узлы



Проверка прикладного сценария

- Зашифруем в ViPNet SIES Core Nano строку с помщью утилиты sies_nano
- Расшифруем полученный текст в ViPNet SIES Unit с помощью Postman

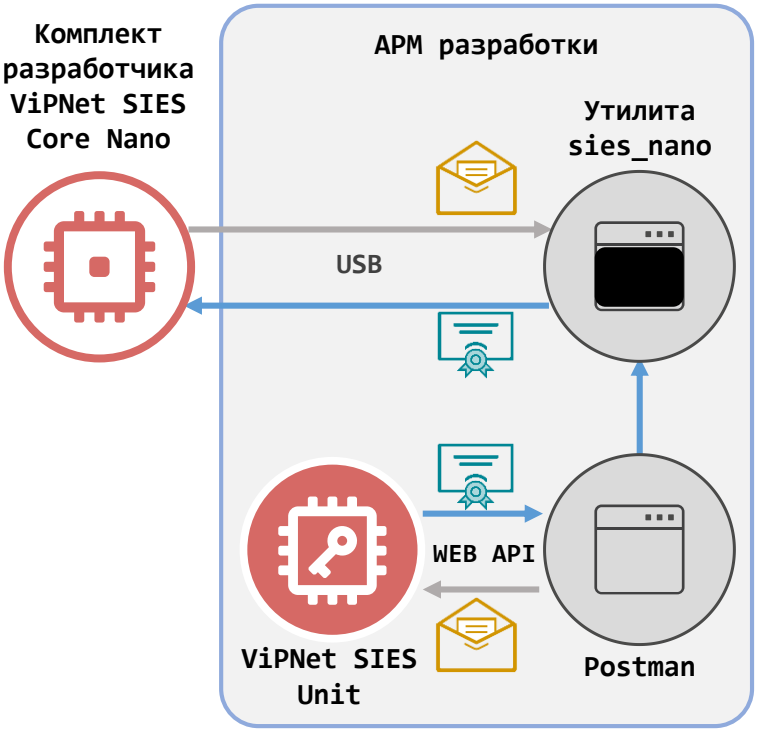


Не забывайте о преобразовании формата данных:

- ViPNet SIES Unit – base64
- ViPNet SIES Core Nano - бинарный

Проверка прикладного сценария

- Зашифруем в ViPNet SIES Core Nano строку с помщью утилиты sies_nano
- Расшифруем полученный текст в ViPNet SIES Unit с помощью Postman



Не забывайте о преобразовании формата данных:

- ViPNet SIES Unit – base64
- ViPNet SIES Core Nano - бинарный

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363