

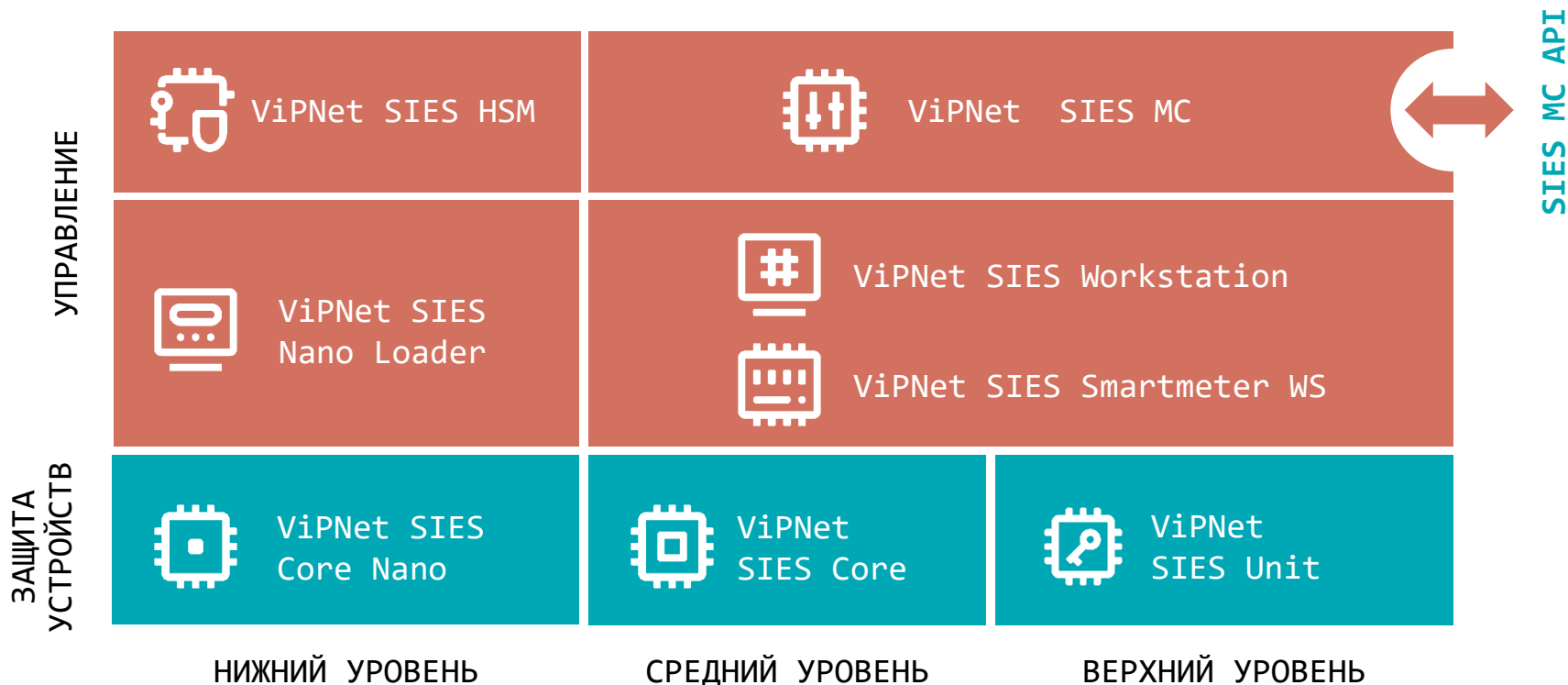
Как подружиться с крипточипом ViPNet SIES Core Nano



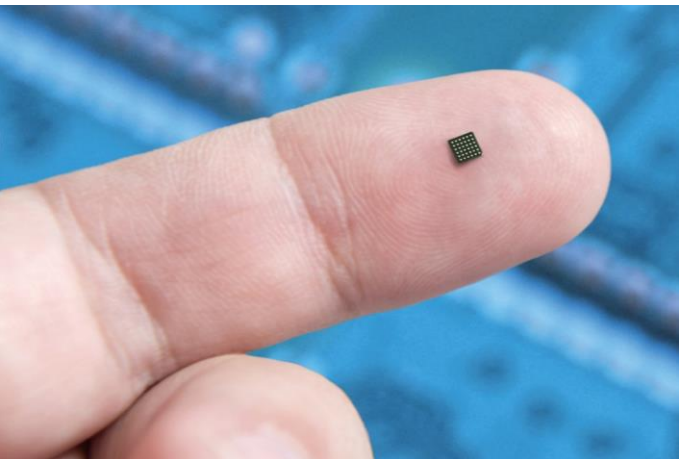
техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

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

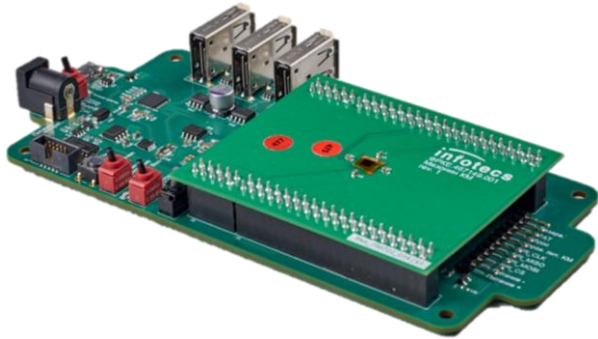
Функциональные особенности:

- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур $-40...+85^{\circ}\text{C}$
- Форм-фактор – микросхема BGA36 $3\times 3\times 0,4$ мм

Соответствие требованиям:

- СКЗИ класса КСЗ
- Защита от атак инженерного проникновения (СКЗИ-ИП)

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	<i>* Может быть предоставлен при заказе комплекта разработчика ViPNet SIES Core Nano</i>

Паспорт, комплект пользовательской и эксплуатационной документации

Разработка сквозных сценариев с помощью КР ViPNet SIES Core Nano

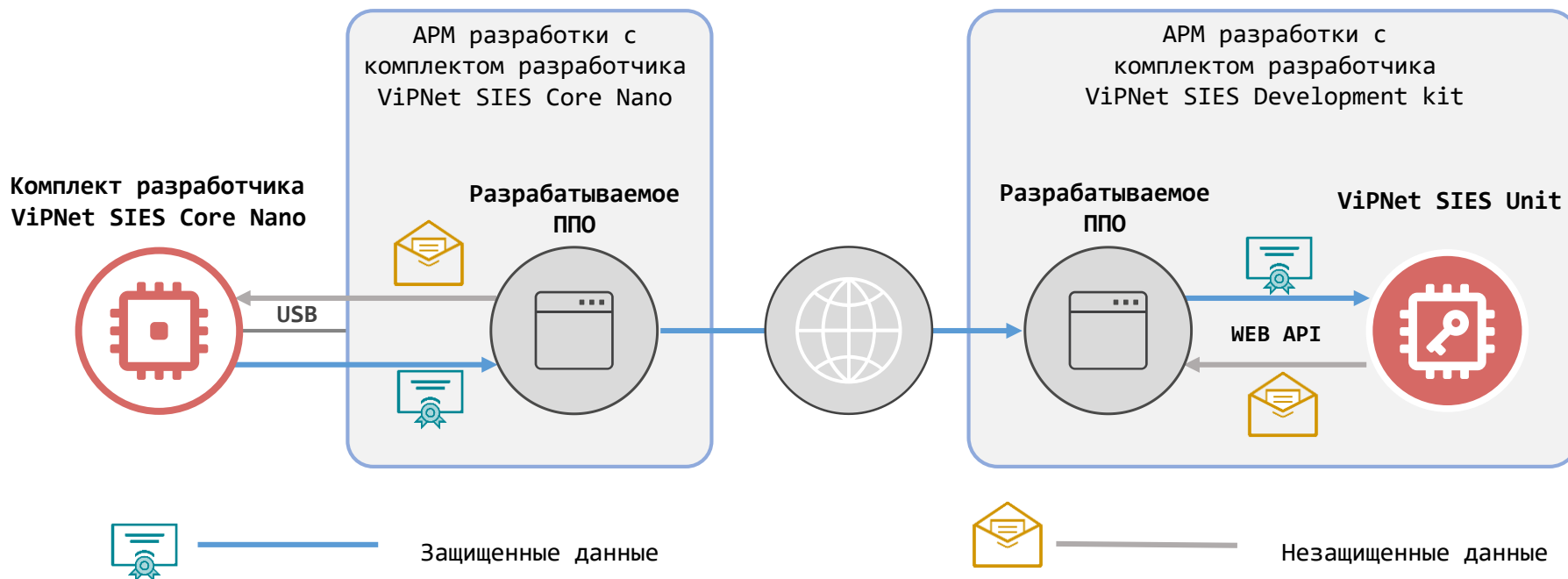
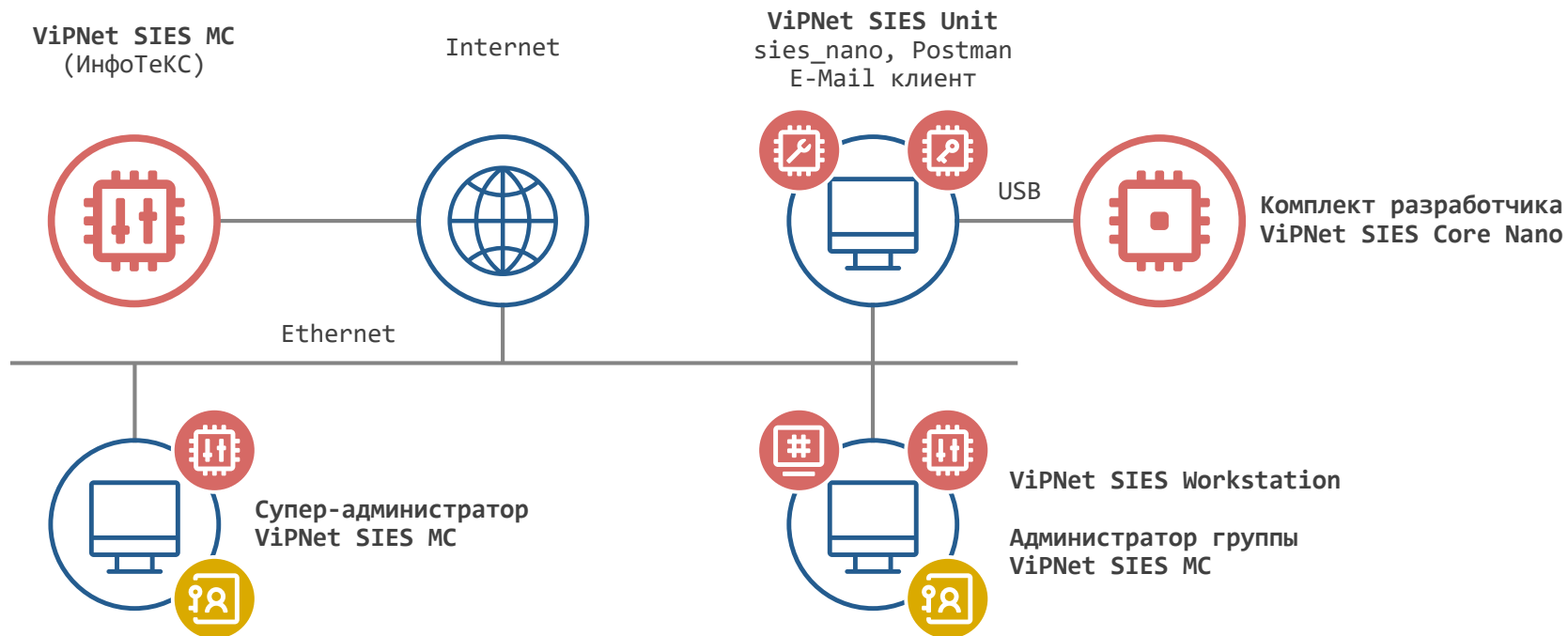


Схема взаимодействия



Работа с VipNet SIES Core Nano без программирования

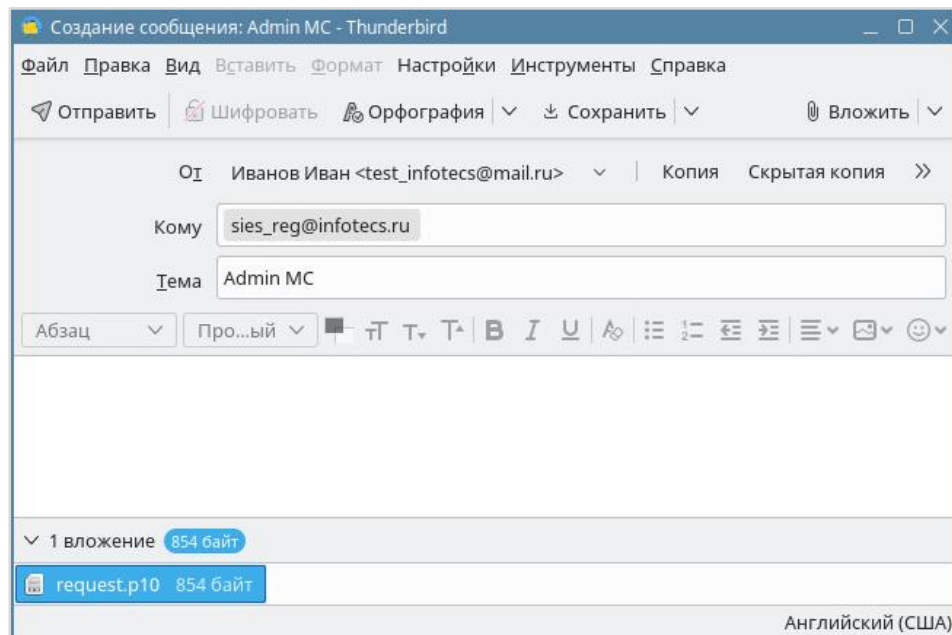


- Подключение к АРМ разработчика по USB
- Знакомство с VipNet SIES Core Nano
- Отладка и тестирование
- Не требует программирования или написания скриптов
- Работа из командной строки Linux
- Поддерживаются все прикладные функции

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: «MC»

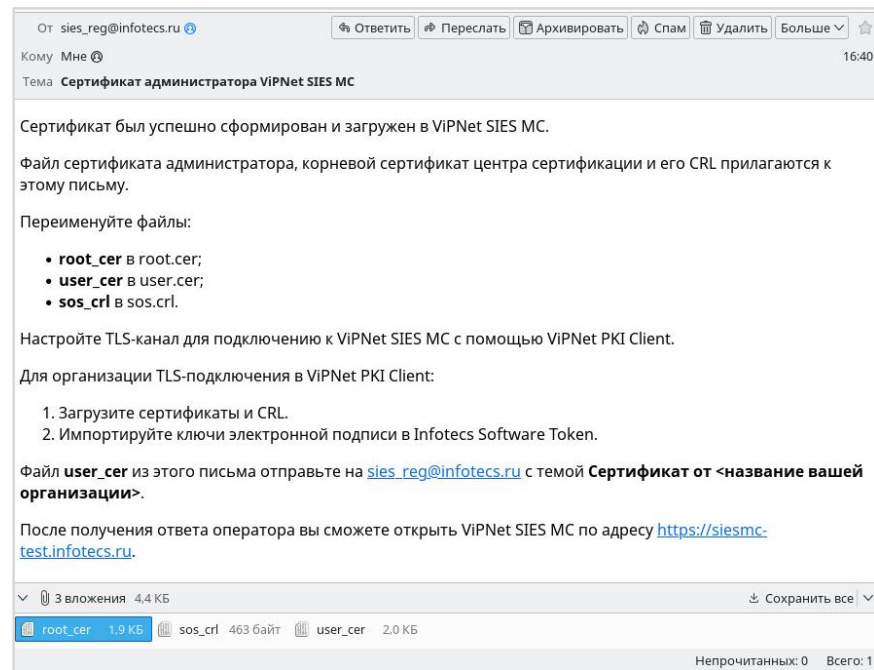


Запрос сертификатов для доступа к VIPNet SIES MC

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

Зарегистрированные администраторы

Владелец сертификата	Роль	Доступ
Ярков Алексей Юрьевич 12.04.2023 - 09.12.2023	Супер-администратор	Разрешен
Хазов Роман 10.07.2023 - 09.12.2023	Супер-администратор	Разрешен
Трофименко Анастасия Юрье... 28.07.2023 - 09.12.2023	Аудитор	Разрешен
Сорокина МВ 02.12.2022 - 02.12.2023	Супер-администратор	Разрешен
Пальгов Антон Валерьевич 07.12.2022 - 07.12.2023	Администратор группы Оператор WS	Разрешен
Иванов Иван Иванович 02.12.2022 - 02.12.2023	Администратор группы Оператор WS	Разрешен
Иванов Иван Иванович 07.09.2023 - 09.12.2023	Администратор группы Оператор WS	Разрешен
Волощина Ирина Рустановна 14.02.2023 - 09.12.2023	Аудитор	Разрешен
Волков Игорь Андреевич 01.12.2022 - 01.12.2023	Супер-администратор	Разрешен
Test AG 11.07.2023 - 09.12.2023	Администратор группы Оператор WS	Разрешен
Savarin Ivan 21.03.2023 - 09.12.2023	Супер-администратор	Разрешен

Иванов Иван Иванович
Сертификат действителен

Доступ в ViPNet SIES MC разрешен

Имя: Иванов Иван Иванович
Фамилия: Иванов
Организация:
СНИЛС: 435-525-234 55
Кем выдан: Тестовый УЦ ИнфоТеКС
Идентификатор: 01D9E18D262A60500008A5A00050001
Период действия: 07.09.2023 - 09.12.2023

Полномочия управления

Супер-администратор
 Выбранные роли

- Администратор безопасности
- Администратор MC
- Оператор WS
- Администратор группы
- Аудитор

Доступ к нераспределенным SIES-узлам

Администрируемые группы Изменить

Технофест

Добавление ViPNet SIES Core Nano

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

The screenshot displays the ViPNet SIES MC management console. The main window is titled "SIES-узлы" and shows a list of nodes. A table lists the node with ID 362205310130, which is currently in "Штатный" (Standard) mode and "Удаленное" (Remote) management state.

Наименование	Режим	Управление
362205310130	Штатный	Удаленное

The right-hand pane shows the configuration details for the selected node (362205310130). The status is "Нормальное. Прикладная ключевая подсистема не настроена." The configuration includes:

- Идентификатор SIES-узла: 362205310130
- Тип SIES-узла: ViPNet SIES Core Nano
- Режим работы: Штатный
- Размер служебных сообщений: Не ограничен
- Контроль ДНСД: Неизвестно
- Группа: Технофест
- Контрольный код: -
- Способ защиты служебных сообщений: CRISP (наследован)
- Защищаемое устройство: Связь задана
- Наименование: Счетчик
- Адрес: meter

At the bottom, the status of the key subsystem is shown as "Служебная ключевая подсистема" and "Прикладная ключевая подсистема". The footer indicates the server time: "Время на сервере SIES MC: 07.09.2023 16:25:36".

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

Новая связь с ИВК

Шаг 2 из 2. Выбор защищаемых устройств.

Выберите защищаемые устройства, с которыми устанавливаете связь

🏠 > Все элементы > Технофест

Поиск...

<input checked="" type="checkbox"/>	Наименование	Адр...	SIES-узел	Направление
<input type="checkbox"/>	ИВК	ivk	de98f888a7c5	Не указ...
<input checked="" type="checkbox"/>	Счетчик	meter	362205310130	Не указ...

1 – защищаемое устройство верхнего уровня
2 – защищаемое устройство среднего уровня
3 – запасная прикладная связь

« < | Страница 1 из 1 | > »

Элементы 1 - 2 из 2

Назад Готово

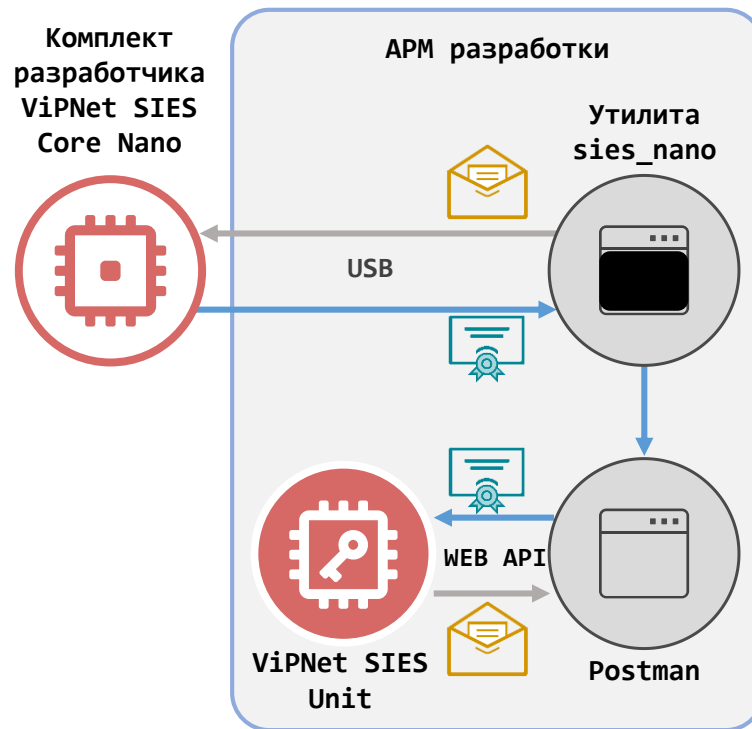
Проверка прикладного сценария

- Зашифруем в ViPNet SIES Core Nano строку с помощью 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



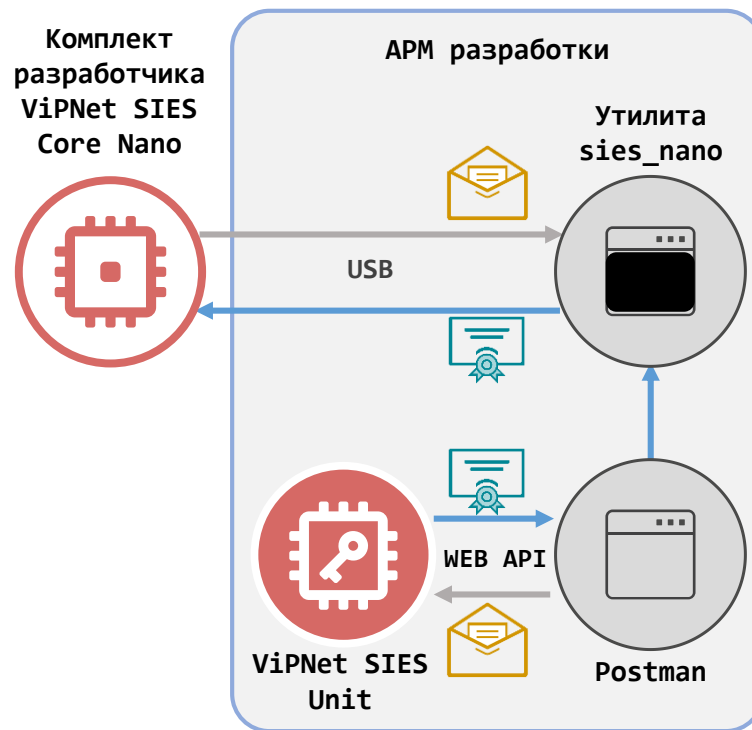
Проверка прикладного сценария

- Зашифруем в ViPNet SIES Core Nano строку с помощью 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 infotecs
2023 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363