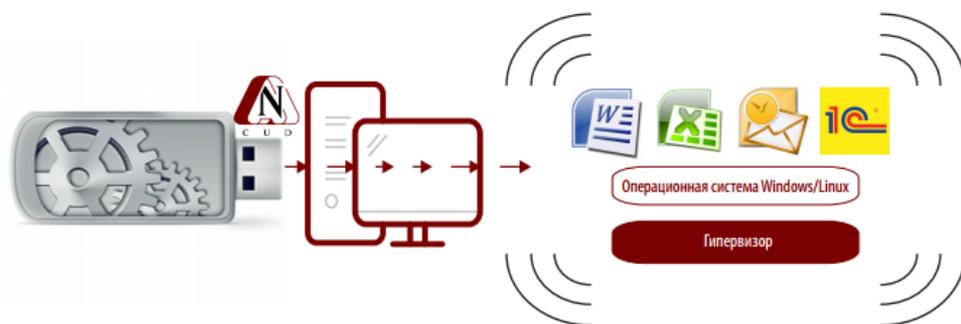




ANCTD
• ANGSTREM CUSTOM DESIGN •

Доверенные носители информации



Дударев Дмитрий
Александрович
Исполнительный директор

Краткое содержание презентации

**Микроконтроллер
MIK51SC72D**

Многофункциональный и защищенный от внешних воздействий микроконтроллер с аппаратно реализованными криптоалгоритмами

АНКАДЕР

Мобильное защищенное рабочее место с замкнутой программной средой для безопасной обработки пользовательской информации

Доверенные носители «Озон»

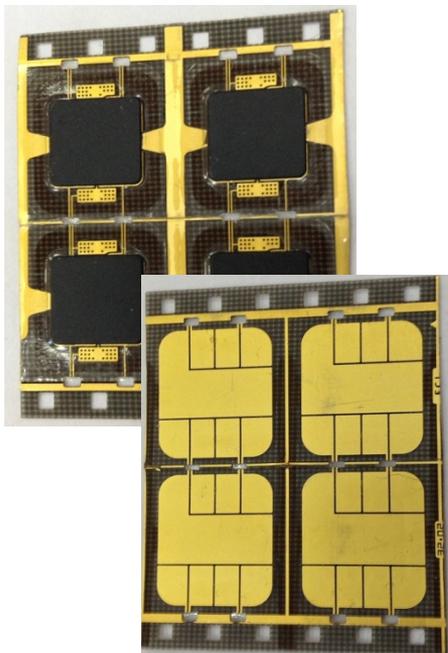
Доверенные носители информации с мощным процессором в пылезащищенном и противоударном корпусе с улучшенными специальными свойствами

**Мониторинг доверенных
носителей**

Определение местонахождения контролируемых носителей в режиме реального времени

Защищенный микроконтроллер MIK51SC72D

Разработка ОАО «НИИМЭ и Микрон» при участии ООО Фирма «АНКАД»



Интерфейсы

- Контактный (ISO 7816, протоколы T0 и T1)
- Бесконтактный (ISO 14443, 13,56 MHz)

Объем памяти

- 364 кбайт ПЗУ
- 72 кбайт ЭСППЗУ

Безопасность и надежность

- Аппаратная и программная защита
- Стойкость к УФ и рентгеновскому излучению, электромагнитным полям

Основные элементы криптографии

Шифрование

- ГОСТ 28147-89
- DES и Triple DES
- AES-128 и AES-256

Электронная подпись

- ГОСТ Р 34.10-2001
- ECDSA-256
- RSA-1024 и RSA-2048

Хэширование

- ГОСТ Р 34.11-94
- SHA-1
- SHA-256

Аппаратные ускорители

- ГОСТ 28147-89
- DES (Triple DES) и AES
- модулярный сопроцессор с 1024-битными операндами

Возможные применения микроконтроллера

Транспортные карты

Микроконтроллер совместим с массовыми транспортными картами Mifare

Платежные карты

Микроконтроллер содержит сертифицированное платежное приложение MasterCard

Идентификационные карты

Микроконтроллер содержит сертифицированное идентификационное приложение УЭК

Средства электронной подписи

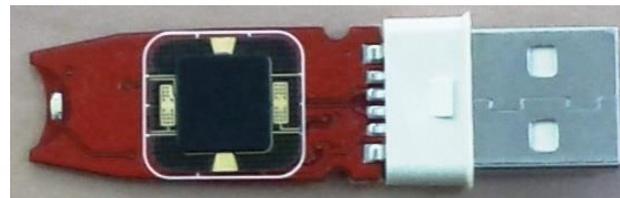
Микроконтроллер может быть использован для вычисления квалифицированной электронной подписи

Ключевые носители

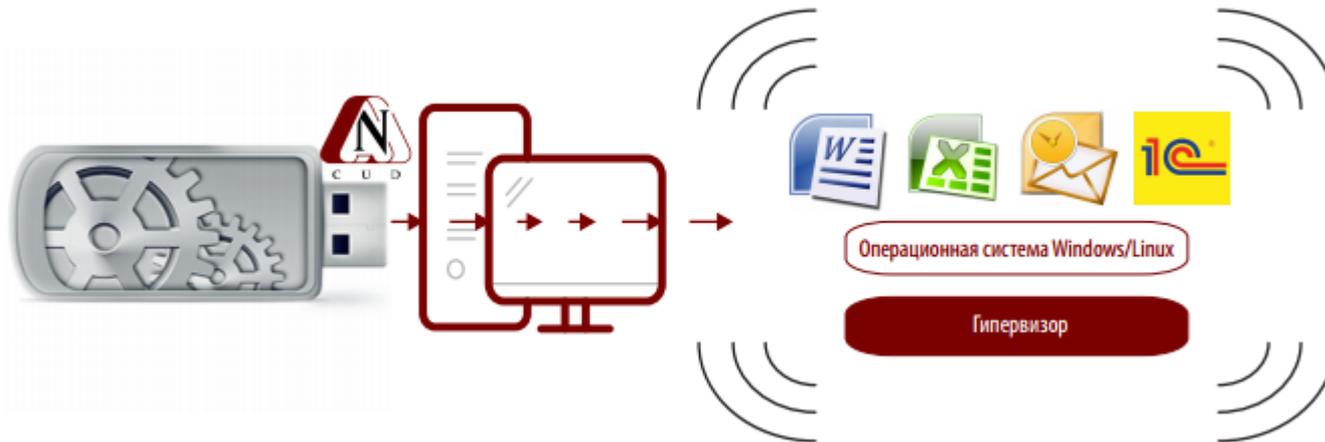
Поддерживаются строгая аутентификация и выполнение криптоопераций непосредственно в микроконтроллере

Прочие применения

Микроконтроллер поддерживает спецификацию Global Platform и содержит виртуальную машину Java Card



АНКАДЕР – мобильное защищенное рабочее место



АНКАДЕР обеспечивает:

- легкий и безопасный перенос рабочей среды и пользовательских данных с одного компьютера на другой;
- сохранение данных в безопасности от любого установленного на компьютерах программного обеспечения (включая вирусы и прочее зловредное ПО);
- обеспечение защищенной и привычной пользователю операционной среды на «чужом» компьютере.

Из чего состоит АНКАДЕР

Микроконтроллер

Генерация и хранение криптографических ключей и выполнение различных криптофункций

Micro SD-карта

Хранение гостевой ОС, а также пользовательских данных в зашифрованном виде

Корпус-считыватель

Для установки микроконтроллера и microSD-карты и взаимодействия с компьютером по интерфейсу USB

Программные компоненты:

- гипервизор, позволяющий запускать в виртуальной среде операционную систему Windows/Linux без ее предварительной модификации;
- гостевая виртуальная ОС, в которой непосредственно работает пользователь;
- пользовательские приложения и данные.

Совокупность средств защиты гипервизора и гостевой ОС формирует замкнутую программную среду для безопасной обработки пользовательской информации

Доверенные носители информации семейства «Озон»

Классическая структура

- Микроконтроллер для взаимодействия с USB и флэш-памятью и выполнения прочих операций
- Флэш-память 4 или 16 Гбайт (расширяемая до 64 Гбайт)

Собственное ПО микроконтроллера

- Модифицированный протокол USB
- Собственный протокол работы с флэш-памятью

Мощный процессор

Большие вычислительные возможности для выполнения дополнительных функций: протоколирования, теневого копирования, разграничения доступа к областям флэш-памяти и т. п.

Защищенный корпус

- Металлический корпус с улучшенными специальными свойствами
- Противоударность и пылезащищенность
- Существует вариант в обычном пластиковом корпусе

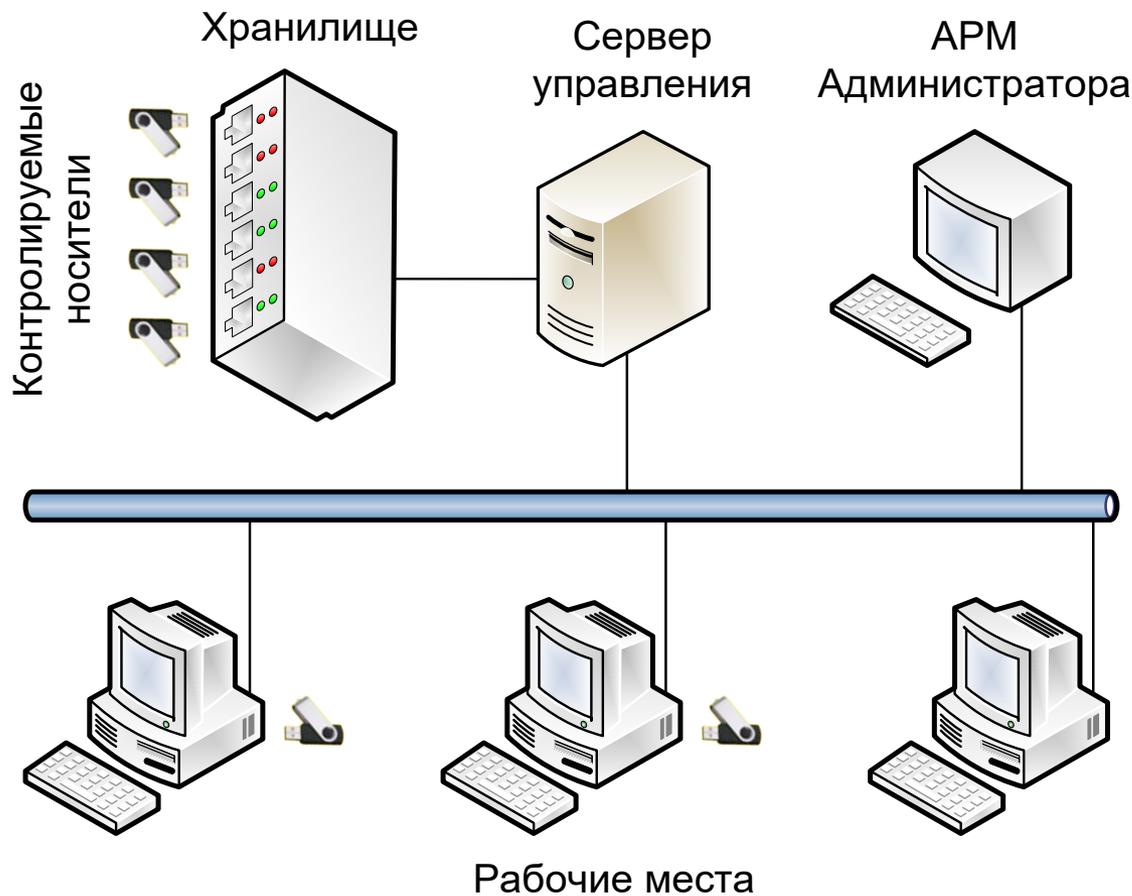
Оригинальный разъем

- USB-разъем в форм-факторе HDMI
- Наличие переходника для подключения к обычному порту USB

Вариант с клавиатурой на корпусе

- Наличие аккумулятора для взаимодействия с носителем, не подключенным к компьютеру
- Парольная аутентификация на чтение, запись и полный доступ к флэш-памяти

Система мониторинга доверенных носителей



- Мониторинг местонахождения контролируемых доверенных носителей в режиме реального времени.
- Информирование администратора о возникновении нестандартных ситуаций и тревожных событий.

Фрагмент интерфейса АРМ Администратора

Утилита администрирования

Управление пользователями | Тревожные события

Список тревожных событий

Номер тревожного события	Серийный номер носителя	Источник тревоги	Дата и время	Дополнительная информация
6	000713000002	Система мониторин...	04.09.2014 14:48:41	Превышено время транспо...
7	000713000002	172.16.200.205	04.09.2014 14:48:56	Носитель установлен на РМ
8	000713000002	Система мониторин...	04.09.2014 14:50:57	Потеря связи между сервер...
9	000713000002	172.16.200.205	04.09.2014 14:51:32	Носитель установлен на РМ
10	000713000001	172.16.200.229	04.09.2014 15:00:26	Изменение состояния носи...
11	000713000002	172.16.200.229	04.09.2014 15:01:51	Изменение состояния носи...
12	000713000002	172.16.200.229	04.09.2014 15:02:16	Носитель установлен в хра...
13	000713000002	172.16.200.229	04.09.2014 15:16:50	Изменение состояния носи...
14	000713000001	Система мониторин...	04.09.2014 15:19:34	Превышено время транспо...
15	000713000001	172.16.200.229	04.09.2014 15:32:20	Носитель установлен в хра...

Погасить

Настройки

Проигрывать звук при возникновении нового события

C:\Windows\Media\tada.wav ... Проиграть



ANCUD
· ANGSTREM CUSTOM DESIGN ·

www.ancud.ru

Спасибо за внимание!