идентификаторы

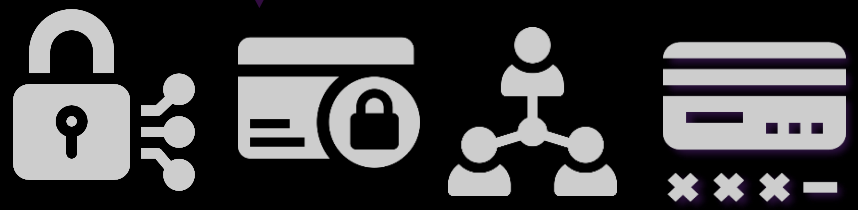
RFID

идентификаторы

Спектр технологических идентификаторов, интегрированных в IDETRIS:

Перечень «Идентификаторов» защищенного RFID-доступа:

- MIFARE Classic 1K (UID 4byte)
- MIFARE Classic 4K (UID 4byte)
- MIFARE Classic EV1 1K (UID 7byte)
- MIFARE Classic EV1 4K (UID 7byte)
- MIFARE Plus 2K
- MIFARE Plus 4K
- MIFARE Plus 2K EV1 / EV2
- MIFARE Plus 4K EV1 / EV2
- MIFARE DESFire 2K | 4K | 8K || EV1
- MIFARE DESFire 2K | 4K | 8K || EV2
- MIFARE DESFire 2K | 4K | 8K || EV3
- LEGIC ADVANT
- LEGIC PRIME
- HID PROX
- HID ICLASS
- SONY FELICA
- INDALA



IDETRIS 7X версия MOSAIC

Сменная панель клавиатуры

Спектр технологических идентификаторов, интегрированных в IDETRIS 7K Mosaic (пример):

- Клавиатура (Mosaic)
- Конфигурирование
- Мощный микроконтроллер (В версии R – Отечественный)
- Мобильный доступ
- Протокол OSDP v. 2.2.
- Wiegand

13,56MHz (UID / UID + CONTENT)

- MIFARE Classic 1K (UID 4byte)
- MIFARE Classic 4K (UID 4byte)
- MIFARE Classic EV1 1K (UID 7byte)
- MIFARE Classic EV1 4K (UID 7byte)
- MIFARE Plus 2K
- MIFARE Plus 4K
- MIFARE Plus 2K EV1 / EV2
- MIFARE Plus 4K EV1 / EV2
- MIFARE DESFire 2K | 4K | 8K || EV1
- MIFARE DESFire 2K | 4K | 8K || EV2
- MIFARE DESFire 2K | 4K | 8K || EV3
- LEGIC Advant
- LEGIC Prime
- HID IClass

125kHz (CSN – Card Serial Number)

- SONY FELICA
- HID Prox
- INDALA
- Em Marin

Глоссарий:

CRYPTO-1

Crypto-1 — проприетарный алгоритм шифрования, созданный NXP Semiconductors для использования в RFID-картах стандарта Mifare (Classic). Не является безопасным.
Crypto-1 является потоковым шифром, очень похожим на предшествующий Hitag2. Crypto-1 состоит из:
> одного 48-битного сдвигового регистра с обратной связью для хранения секретного состояния
> линейной функции
> двухуровневой нелинейной функции 20-в-1
> 16-битного регистра сдвига с линейной обратной связью, который используется при аутентификации. Некоторыми картами может использоваться как ГПСЧ.
Алгоритм может использоваться как регистр сдвига с нелинейной или линейной обратной связью в зависимости от входных параметров. Обычно шифры Crypto-1 и Hitag2 используют нелинейный режим только при инициализации и аутентификации, переключаясь на линейный режим с нелинейным выходным фильтром для шифрования передаваемых данных.

Транзакционный MAC-код

Функция транзакционного MAC-кода надежно проверяет подлинность транзакции. Например, в системах с несколькими поставщиками услуг, использующими один и тот же кошелек и клиринговую службу, функция транзакционного MAC подтверждает клиринговой палате подлинность транзакций между поставщиками услуг и клиентами. Ее также можно использовать для проверки транзакций в многочисленных офлайн-сценариях или в случаях, когда возможности онлайн-аутентификации в режиме реального времени недоступны для операторов системы.

CC – Common Criteria

Общие критерии оценки безопасности информационных технологий (далее — Common Criteria или **CC**) — это международный стандарт (ISO/IEC 15408) для сертификации компьютерной безопасности. В настоящее время он имеет версию 2022, редакция 1. Общие критерии — это структура, в которой пользователи компьютерных систем могут указывать свои функциональные требования и требования к обеспечению безопасности (**SFR** и **SAR** соответственно) в Целевом показателе безопасности (**ST**) и могут быть взяты из Профилей защиты (**PP**). В отличие от стандарта FIPS 140[4], Common Criteria не приводит списка требований по безопасности или списка особенностей, которые должен содержать продукт. Вместо этого он описывает инфраструктуру (framework), в которой потребители компьютерной системы могут описать требования, разработчики могут заявить о свойствах безопасности продуктов, а эксперты по безопасности определить, удовлетворяет ли продукт заявлениям.)

Стандарт ISO 14443

Все продукты «Семейства MIFARE» базируются на ISO 14443 Type A 13,56 МГц стандарте бесконтактных смарт-карт
> **ISO/IEC 14443** — стандарт, описывающий частотный диапазон, метод модуляции и протокол обмена данными посредством бесконтактных пассивных карт (RFID) ближнего радиуса действия на «магнитно-связанных индуктивностях». Стандарт можно отнести к первому поколению RFID-стандартов. Впоследствии вошёл в стандарт ISO/IEC 18000-3 и NFC-стандарты (ISO/IEC 18092 и ISO/IEC 21481). Российский аналог Стандарта - **(ГОСТ Р ИСО/МЭК 14443)**.
> Стандарт состоит из 4 частей, обозначенных цифрами 1 - 4. Например, ISO 14443-3:
- часть 1 определяет физические нормативы карт и условия нормальной работы;
- часть 2 определяет радиочастотные параметры и методы модуляции;
- часть 3 определяет протокол инициализации обмена (в основном это процедура антиколлизии — разделения нескольких карт в поле считывателя);
- часть 4 определяет протокол обмена данными.

> Стандарт содержит несколько разных протоколов обмена, обозначаемых буквами (A, B, и т. д.). Например ISO 14443A или ISO 14443A-4 (с указанием части). Первоначально стандарт содержал только протоколы A и B, однако добавлены несколько протоколов.
> Стандарт определяет использование свободного (нелицензируемого) диапазона частот 13,56 МГц с амплитудной модуляцией и девиацией 850 кГц. В России нормативным документом для использования этого частотного диапазона являются Приложения 4 и 9 к решению ГКРЧ от 7 мая 2007 года N07-20-03-001

Глоссарий:

● ISO 7816

ISO/IEC 7816 — стандарт относится к смарт-картам (в первую очередь контактным). Описывает форму карты, контактов, их расположение и назначение; протоколы обмена и некоторые аспекты работы с данными. Не смотря на то, что стандарт для «контактных» смарт-карт, для RFID (бесконтактных) идентификаторов он тоже применим, в частности для некоторых типов NFC-меток (карт), Mifare Plus и Desfire-интерфейсов.
> Стандарт можно назвать базовым для всех смарт-карт. Существует российская копия стандарта в виде ГОСТ Р ИСО/МЭК 7816.

● DES

DES (англ. *Data Encryption Standard*) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3). Размер блока для DES равен 64 битам. В основе алгоритма лежит сеть Фенистила с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Для DES рекомендовано несколько режимов:

> ECB (англ. ***e**lectronic **c**ode **b**ook*) — режим «электронной кодовой книги» (простая замена);
> CBC (англ. ***c**ipher **b**lock **c**haining*) — режим сцепления блоков;
> CFB (англ. ***c**ipher **f**eed **b**ack*) — режим обратной связи по шифротексту;
> OFB (англ. ***o**utput **f**eed **b**ack*) — режим обратной связи по выходу;
> Counter Mode (CM) — режим счётчика.

Это преобразование над векторами (блоками), представляющими собой левую и правую половины регистра сдвига. В алгоритме DES используются прямое преобразование сетью Фейстеля в шифровании (см. Рис.1) и обратное преобразование сетью Фейстеля в расшифровании (см. Рис.2).
Схема шифрования алгоритма DES указана на Рис.3.
Исходный текст — блок 64 бит. Процесс шифрования состоит из начальной перестановки, 16 циклов шифрования и конечной перестановки.

● 2DES / 3DES

> Чтобы увеличивать криптостойкость DES, появляются несколько вариантов: double DES (2DES), triple DES (3DES), DESX, G-DES.
Методы 2DES и 3DES основаны на DES, но увеличивают длину ключей (2DES — 112 бит, 3DES — 168 бит) и поэтому увеличивается криптостойкость.
> DES-EEE3: Шифруется три раза с 3 разными ключами.
> DES-EDE3: 3DES операции шифровка-расшифровка-шифровка с 3 разными ключами.
> DES-EEE2 и DES-EDE2: Как и предыдущие, за исключением того, что первая и третья операции используют одинаковый ключ.

Mifare Classic

ИДЕНТИФИКАТОРЫ

MIFARE

Базовые параметры MIFARE Classic:

● Стандарт: ISO 14443A-3

● Защищенность: Низкая

> SL1: 48 bit – ключ шифрования CRYPTO-1
(известны методы взлома)
> Уязвимый протокол для реле-атак

Версия Mifare Classic EV1 имеет дополнительные алгоритмы безопасности:

> Производителем запрограммирован 7-байтовый UID или 4-байтовый NUID-идентификатор для каждого устройства
> Поддержка случайных идентификаторов
> Взаимная трёхпроходная аутентификация (ISO/IEC DIS 9798-2)
> Индивидуальный набор из двух ключей на сектор для поддержки многозадачности с иерархией ключей
> Целостность данных 16-битного CRC, четность, битовое кодирование,подсчет битов

● До **100 000** циклов записи.
● Время получения идентификаторов: 3 мс.
● Время считывания **1 блока** (16 byte)
> 2,5 мс. (без аутентификации)
> 4,5 мс. (с аутентификацией)

● Полное считывание карты + контрольное чтение
> 8,5 мс. (без аутентификации)
> 10,5 мс. (с аутентификацией)

● Стандарт по выдаче данных < **100 мс.**
(включая идентификацию карты, чтение шести блоков (768 бит, 2 сектора аутентификации) и запись двумя блоками (256 бит) с дублированием).

> Рабочая частота 13,56 МГц
> Передача данных 106 кбит/с

MIFARE
Classic

1 сектор = 4 блока
- **1 блок (ключ)**
- **+**
- **3 блока (данные)**

> 1 блок = 16 byte
> 1 сектор = 164 byte
> 1 kb. карта = 16 секторов
> 4 kb. карта = 40 секторов

> Mifare Classic (1kB | 4kb) – UID 4 byte
> Mifare Classic EV1 (1kb | 4kb) - UID 7 byte

(с возможностью переключения на 4Kb.)
в версии EV1 - Собственные протоколы:

> Anticollision protocol - Интеллектуальная функция «антиколлизии» позволяет одновременно работать с несколькими картами. Алгоритм выбирает каждую карту индивидуально и гарантирует, что транзакция с выбранной картой будет выполнена корректно, без помех со стороны другой карты.
> Select protocol - С помощью этой команды считыватель выбирает одну отдельную карту для аутентификациии операций, связанных с памятью. Карта возвращает код Select AcKnowledge (SAK).
> Three Pass Auth Protocol (Протокол тройной аутентификации - После выбора карты считыватель определяет ячейку памяти для последующего доступа к ней и использует соответствующий ключ для тройной процедуры аутентификации. После успешной аутентификации все команды и ответы шифруются.
> После аутентификации можно выполнить любую из следующих операций:
> Чтение блока
> Запись блока
> Декремент: уменьшает содержимое блока и сохраняет результат во внутреннем буфере
> Инкремент: увеличивает содержимое блока и сохраняет результат во внутреннем буфере
> Восстановление: перемещает содержимое блока во внутренний буфер передачи
> Передача: записывает содержимое внутреннего буфера передачи в блок значений

Функционал ПО CSW и Считыватели IDETRIS

При работе с идентификатором MIFARE Classic:

● Настройка Формата Карты:

● ПО настроено по умолчанию на форматы карт 26-bit и 32-bit
● Кастомизированный формат:

> Длина Wiegand (1 – 64bit)
> Facility code (FC) (код объекта / помещения)
> Номер карты: конфигурирование номера карты
> Формат карты : 26 / 32bit > Имя формата | Особый формат карты
> Четный паритет (Even Parity)
> Четный диапазон (Even Range)
> Нечетный паритет (Odd Parity)
> Нечетный диапазон (Odd Range)
> Стартовый байт (Start byte) (0-20 | по умолч. - 8)
> Порядок (Order): Прямой / Обратный (Ascend / Descend)
> Проверка паритета (Check Parity) (дуальные проверки)
> Программируемый номер карты (PCN)
> Диапазон паритета (Parity Range)
> Фиксированный режим (Fixed)
> Фиксированный бит (Fixed Bit «1/0»)
> Фиксированное значение (Fixed Value)
> Завершение добавления (Complete Add)

● Программирование карты:

> USB – ключ доступа
> Facility Code (FC)
> Ключи безопасности A / B (HEX code)
> Код Сектора памяти (0 - 15)
> Номер Блока памяти (0 - 2)
> Ключ Конечного пользователя 1-65535
> @Инкрементный режим / Exl автоматический режим (USB-ключ)
> Пароль доступа
> Количество и порядок программирования карт
> Выбор файла формата карты (импорт, запись, чтение)

CSW SOFTWARE

MIFARE
Classic

● Карта конфигурирования считывателей IDETRIS:

> 14443A / 14443B UID / EV1
> Считывание UID / Контент / UID+Контент памяти карты
> Wiegand bits (WG0 / WG0+2 (Parity bits))
> Параметры 4 / 7 / 8 byte: нач. bit / нач. byte | контрольный bit
> Биты проверки (Checksum bits): 1 + Last position (напр. 12 bit + Odd parity)
> Настройка порядка вывода UID
> Прямой / Обратный порядок считывания данных (Ascend / Descend process)
> Facility code (открытый / закрытый FC)
> Имя карты | Номер карты

● Доп. «модальности» доступа считывателей IDETRIS:

> Пароль | PIN | PIN панель с технологией сменных значений MOSAIC
> Сканер рисунка вен ладони ABIOT (Advent Biotech)
> Сканер рисунка вен пальца HITACHI

CRYPTO-1:

● Криптоалгоритм Crypto-1 | Проблемы защищенности

● В картах Mifare Classic используется проприетарный лицензионный криптоалгоритм Crypto-1. Первоначально стойкость алгоритма была основана на его секретности. Однако низкая криптостойкость алгоритма и популярность технологии привела к тому, что на сегодняшний день алгоритм не является секретом и относительно легко взламывается.

Но в реальных системах далеко не вся безопасность построена на аппаратном шифровании карты. В качестве дополнительного фактора защиты могут использоваться, например, метки времени. Тем не менее, даже системы, безопасность которых не опирается целиком на алгоритм Crypto-1 (или даже не использует его совсем, как Mifare Ultralight), могут быть взломаны благодаря аппаратным особенностям карт.

● Все современные микросхемы считывателей Mifare фирмы NXP Semiconductors умеют работать с Crypto-1. Однако не все имеют возможность безопасного энергонезависимого хранения ключей. В микросхемы MFRC52x и NFC ключи **подгружаются перед каждой транзакцией по незащищённому интерфейсу**. Для сравнения, в остальных микросхемах ключ записывается однократно энергонезависимо и не может быть считан снаружи.

Известные случаи взлома Mifare Classic описаны в материалах:
> A Practical Attack on the MIFARE Classic
> Dismantling MIFARE Classic
> Wirelessly Pickpocketing a MIFARE Classic Card

● Так, если в 2008 году взлом Crypto-1 требовал около 200 секунд на стандартном ноутбуке, в 2009 году на то, чтобы узнать секретный ключ, требовалось уже около 40 мс[14]. Были разработаны варианты атаки, не требующие наличия валидного считывателя[15]. Это сделало возможным осуществление атаки со смартфона, без использования специализированного оборудования.

● Наиболее скомпрометированным стандартом карт Mifare является Mifare Classic. С 2008 года было предложено множество способов взлома этого типа карт. Большинство из них основано на уязвимости внутреннего ГПСЧ карты. Особенности его работы стали ясны после частичного реверс-инжиниринга чипа карты. Было выяснено, что генератор псевдослучайных чисел карты представляет собой 48-битный сдвиговый регистр с обратной связью. Это значит, что псевдослучайная последовательность однозначно определяется временем работы генератора. В процессе аутентификации карта посылает считывателю отклик (Nt), значение которого косвенно связано с состоянием генератора псевдослучайных чисел. Этот факт даёт возможность узнать два последовательно сгенерированных числа, чтобы, зная устройство генератора псевдослучайных чисел карты, определить следующее число последовательности. Таким образом, алгоритм атаки (называемой Nested attack) предполагает знание ключа к хотя бы одному из секторов карты, и выглядит следующим образом:

● Аутентификация и считывание сектора карты с помощью известного ключа. Сохранение ответа карты (Nt).
Повторная аутентификация с тем же ключом. Сохранение значения ответа карты.
Вычисление состояния ГПСЧ по двум последовательным значениям Nt.
Перебор ключей к остальным секторам, используя знание состояния ГПСЧ
Но, даже не используя уязвимостей генератора псевдослучайных чисел, можно осуществить перебор ключей на ПЛИС за время порядка 10 часов на ключ.

● Энтузиастами был разработан набор открытого ПО NFC-tools для работы с бесконтактными картами. В пакете NFC-tools существует отдельная библиотека Libfreefare, предназначенная для работы с картами стандартов Mifare, а также утилита, реализующая вышеописанную атаку на Mifare Classic: MFOC

Mifare Plus

ИДЕНТИФИКАТОРЫ

MIFARE

Базовые параметры MIFARE Plus:

● Стандарт: ISO 14443A-3 | ISO 7816-4

● Защищенность: СРЕДНЯЯ

> Включает SL1: 48 bit – ключ шифрования CRYPTO-1 (SL3)
> Уровни безопасности (Security Levels): SL1, SL2, SL3
> В соответствии с ISO/IEC 14443-31 **Random ID** режим
> SL3 использует **AES128** bit | Оболочка: **ISO 7816-4**

> Mifare Plus EV1 позволяет использовать стандарт **AES** для шифрования данных, даже для приложений, работающих под управлением **Crypto1**
> **AES-128** криптография для аутентификации и безопасного режима отправки сообщений (опционально для SL1, обязательно для SL3)
> Возможно повышение стандарта безопасности до SL3 как всей карты, так и отдельных секторов памяти.
> Последовательная запись Ключей персонализации (SL0)
> NFC API – совместимый протокол ISO 7816-4 APDU передачи данных с макс. размером буфера 256 byte
> MIFARE Application Directory (MAD) – упрощает спектр возможных приложений для карт MIFARE Plus и делает интеграцию более удобной

> **Mifare Plus EV1** – соответствует ISO: лимит дистанции и таймер
приема-передачи во время аутентификации, что затрудняет перехват
> «**end-2-end**» защищенный канал | Защита от атак **«man in the middle»**
> «**over-the-air**»-обновления с защитой (SL1SL3 mix mode) (в частности для защиты «backend connections» в секторах SL1
> Передача **MAC** команды по значениям и блокам данных
> Карты могут генерировать дополнительный код аутентификации поверх транзакции, который может быть верифицирован посредством сервиса, независимого от ключей считывателя
> Common Criteria Certification: EAL5+ стандарт
> Проверка оригинальности ECC подписи

MIFARE
Plus

● Структура Памяти:

EEPROM память 2 kB => 32 сектора = 4 блока
+

EEPROM память 4 kB
- **32 сектора = 4 блока**
- **8 секторов = 16 блоков**

> **1 блок** = **16** byte
> **1 сектор** = **164** byte
> **4 kb. карта** = **40** секторов

> Mifare Plus (2kb | 4kb) - UID 4 byte
> Mifare Plus EV1 (2kb | 4kb) - UID 7 byte
> Mifare Plus EV2 (2kb | 4kb) - UID 7 byte
(EV2 - улучшены скорость и качество передачи данных)

> 2 kB, 4 kB EEPROM
> 7-byte UID, 4-byte NUID
> Первый блок данных (блок 0) первого сектора (сектор 0) содержит данные производителя PICC
> Коммуникационная скорость: 848 kbps
> Относительно легко настраиваемые условия доступа
> «Мультисекторная» аутентификация
> «Мультиблоковая» запись и считывание
> Режим генерации Виртуальной карты VCC (Virtual card concept) по стандарту метода выборки ISO/IEC 7816-4
> Сектора с 0D по 31D содержат по 3 блока каждый, а сектора с 32D по 39D содержат 15 блоков для хранения данных. Блоки данных можно настроить с помощью битов доступа как:

>> блоки чтения/записи для хранения бинарных данных
>> блоки значений

> Блоки значений — это специальные счётчики, где сохранённым значением можно управлять с помощью специальных команд, таких как «Increment», «Decrement» и «Transfer».Эти блоки значений имеют фиксированный формат данных, что позволяет обнаруживать и исправлять ошибки, выполняя управление резервным копированием.

> MIFARE Plus EV1 SL3 предоставляет ещё две команды, которые можно использовать для оптимизации производительности при использовании блоков значений. Это:

>> «Increment Transfer»
>> «Decrement Transfer»

Функционал ПО CSW и Считыватели IDETRIS

При работе с идентификатором MIFARE Plus:

● Настройка Формата Карты:

● ПО настроено по умолчанию на форматы карт 26-bit и 32-bit
● Кастомизированный формат:

> Длина Wiegand (1 – 64bit)
> Facility code (FC) (код объекта / помещения)
> Номер карты: конфигурирование номера карты
> Формат карты : 26 / 32bit > Имя формата | Особый формат карты
> Четный паритет (Even Parity)
> Четный диапазон (Even Range)
> Нечетный паритет (Odd Parity)
> Нечетный диапазон (Odd Range)
> Стартовый байт (Start byte) (0-20 | по умолч. - 8)
> Порядок (Order): Прямой / Обратный (Ascend / Descend)
> Проверка паритета (Check Parity) (дуальные проверки)
> Программируемый номер карты (PCN)
> Диапазон паритета (Parity Range)
> Фиксированный режим (Fixed)
> Фиксированный бит (Fixed Bit «1/0»)
> Фиксированное значение (Fixed Value)
> Завершение добавления (Complete Add)

● Программирование карты:

> USB – ключ доступа
> Facility Code (FC)
> Код Сектора памяти (0 - 15)
> Номер Блока памяти (0 - 2)
> Ключ Конечного пользователя 1-65535
> @Инкрементный режим / Exl автоматический режим (USB-ключ)
> Пароль доступа
> Количество и порядок программирования карт
> Выбор файла формата карты (импорт, запись, чтение)
> ID файла

CSW SOFTWARE

MIFARE
Plus

● Карта конфигурирования считывателей IDETRIS :

> Имя конфигурирования Mifare Plus
> 14443A / 14443B UID / EV1 / EV2 / SL1 / SL2 / SL3 (AES)

> Настройка порядка вывода UID
> Прямой / Обратный порядок считывания данных (Ascend / Descend process)
> Facility code (открытый / закрытый FC)
> Имя карты | Номер карты

> Считывание UID / Контент / UID+Контент памяти карты / +File 2
> Считывание File 1 / File 2
> Тип Ключа: Key A / Key B
> Стартовый байт (Start Byte)
> Стартовые биты (Start Bits)
> WG биты (Wiegand bits): WG0 / WG0+2 (Parity bits))
> Параметры 4 / 7 / 8 byte: нач. bit / нач. byte | контрольный bit
> Биты проверки (Checksum bits): 1 + Last position (напр. 12 bit + Odd parity)
> Сектор No (Sector No.): Выбор номера сектора
> Блок No. (Block No.): Выбор номера блока
> Длина блока (Block length): Длина блока в байтах
> Ключ Mifare Plus: Выбор при считывании SL2 / SL3
> Уровень безопасности (Sec. level): SL1, SL2, SL3 (AES)
> Защищенные Коммуникационные режимы:
<Ciphertext-Шифр>
<Plaintext-Простой текст>
• Ciphertext + MACedCmd + UnMACedResp
• Ciphertext + MACedCmd + MACedResp
• Plaintext + MACedCmd + UnMACedResp
• Plaintext + MACedCmd + MACedResp
• Ciphertext + UnMACedCmd + UnMACedResp
• Ciphertext + UnMACedCmd + MACedResp
• Plaintext + UnMACedCmd + UnMACedResp
• Plaintext + UnMACedCmd + MACedResp

● Дополнительные Модальности доступа IDETRIS:

> Пароль | PIN | PIN панель с технологией сменных значений MOSAIC
> Сканер рисунка вен ладони ABIOT (Advent Biotech)
> Сканер рисунка вен пальца HITACHI

DESFire

ИДЕНТИФИКАТОРЫ

MIFARE DESFire

Базовые параметры DESFire:

● Стандарт: ISO 14443A-3
● Защищенность: ВЫСОКАЯ

> Полностью соответствует стандарту 3 и 4 блоков ISO 14443A с mask-ROM OS
> Предварительное программирование с DESFire (а также Mifare) OS
> Криптозащищенная (DES, 2DES, 3DES, AES) файловая система и специальная структура директорий с гибко настраиваемыми условиями доступа
> Имеет две версии: 1) только 3DES с 4kb и 2) AES шифрование (память 2, 4, 8kb). Быстрая передача данных 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbit/s. Конфигурируемы FSCI для поддержки до 256 байт frame.
> В основе 8051 MCU процессор 3DES/AES криптографическим акселератором

● Технология построена на основе архитектуре CPU (ЦП) посредством интерфейса ISO14443.
● Ввиду того, что технология построена на CPU, безопасность COS измеряется «Общим критерием» (Common Criteria).
● Главное отличие EV2 от EV1:
> Большая дальность считывания.
> Поддержка неограниченного набора приложений (ограничение лишь – размер физической памяти).
> Поддержка неограниченного числа файлов (ограничение – размер физической памяти).
● Ввиду того, что технология DESFire базируется на CPU, структура памяти отличается от Mifare Classic, Sony Felica, HID iClass, HID Legic – «крипто-технологий» в области выпуска карт.
● Пожалуйста, примите к сведению, что «крипто-технологии» выпуска карт не имеют каких-либо параметров оценки безопасности.

DESFire

1 карта = 28 приложений
- 1 приложение <= 14 ключей
- 1 приложение <= 16 файлов данных

> MIFARE DESFire EV1 (2kb | 4kb | 8kb)
> Реверсивно адаптирован (распознает Mifare)
> Режим «динамического» (случайного) ID
> Шифрование AES128 bit
> Сертифицирован Common Criteria EAL4+

> MIFARE DESFire EV2 (2kb | 4kb | 8kb)
> Включает все параметры и совместимость EV1
> MI smart App позволяет использовать массив памяти для дополнительных приложений третьих сторон без необходимости передачи секретных ключей
> Передача MAC кода для аутентификации передачи данных (транзакций) третьими сторонами
> VCA (Virtual Card Auth) Аутентификация виртуальной карты для защиты данных
> Proximity check против релейных атак
> Сертифицирован Common Criteria EAL5+

> MIFARE DESFire EV3 (2kb | 4kb | 8kb)
> Включает все параметры и совместимость EV1+EV2
> Совместимость с ISO/IEC 14443 A 1-4 и ISO/IEC 7816-4
> Сертифицирован Common Criteria EAL5+
> SUN Auth и защита данных (стандарт считывания NDEF)
> Возможность выбора открытых режимов протоколов шифрования **DES / 2K3DES / 3K3DES / AES**
> Гибкая файловая структура: может хранить столько приложений, сколько позволяет память
> Подтверждение транзакции (передачи данных) посредством MAC кода, генерированного картой
> Защита от атак **«man in the middle»**

(Карта DESFire EV3C обладает всеми функциями DESFire EV3, а также может эмулировать карту MIFARE Classic 1K. Некоторые файлы DESFire можно сверять с данными MIFARE Classic 1K, что открывает возможность постепенного отказа от Mifare Classic и перехода на DESFire)

Функционал ПО CSW и Считыватели IDETRIS

При работе с идентификатором DESFire:

● Настройка Формата Карты:

● ПО настроено по умолчанию на форматы карт 26-bit и 32-bit
● Кастомизированный формат:
> Длина Wiegand (1 – 64bit)
> Facility code (FC) (код объекта / помещения)
> Номер карты: конфигурирование номера карты
> Формат карты : 26 / 32bit > Имя формата | Особый формат карты
> Четный паритет (Even Parity)
> Четный диапазон (Even Range)
> Нечетный паритет (Odd Parity)
> Нечетный диапазон (Odd Range)
> Стартовый байт (Start byte) (0-20 | по умолч. - 8)
> Порядок (Order): Прямой / Обратный (Ascend / Descend)
> Проверка паритета (Check Parity) (дуальные проверки)
> Программируемый номер карты (PCN)
> Диапазон паритета (Parity Range)
> Фиксированный режим (Fixed)
> Фиксированный бит (Fixed Bit «1/0»)
> Фиксированное значение (Fixed Value)
> Завершение добавления (Complete Add)

● Программирование карты:

> Имя Конфигурирования: English / Русский
> USB – ключ доступа
> Мастер-ключ (Application Master Key): Инициализация операций
> ID Приложения (Application ID): Имя приложения (диапазон 0 >>)
> Режим Аутентификации (Authentication Mode): Метод верификации при чтении карт: DES, 3DES, 3K 3DES, AES
> Ключ: Установка рабочих ключей при диапазоне значений 0-14
>> 0 – Мастер ключ
>> 1-13 Рабочие ключи (16 байт каждый)
> Код Конечного пользователя 1-65535
> @Инкрементный режим / Exl автоматический режим (USB-ключ)
> Параметр файла | Размер файла (по умолчанию 100)
> ID файла: 0-1
> Чтение No ключа
> Запись No ключа (0-13)

CSW SOFTWARE

DESFire

● Карта конфигурирования считывателей IDETRIS :

> Имя конфигурирования DESFire
> 14443A / 14443B UID / EV1 / EV2 / EV3 / DES, 2DES, 3DES, 3K 3DES, AES
> Параметры считывания карт Desfire (File1 + File2)
> Настройка порядка вывода UID
> Прямой / Обратный порядок считывания данных (Ascend / Descend process)
> Facility code (открытый / закрытый FC)
> Имя карты | Номер карты
> Считывание UID / Контент / UID+Контент памяти карты / +File 2
> Считывание File 1 / File 2
> Стартовый байт (Start Byte)
> Стартовые биты (Start Bits)
> File 2: Биты Четного паритета
> WG биты (Wiegand bits): WG0 / WG0+2 (Parity bits))
> Параметры 4 / 7 / 8 byte: нач. bit / нач. byte | контрольный bit
> Биты проверки (Checksum bits): Первая и последняя позиция (бит проверки – 24)
> Номер ключа: Ключ используется для считывания файла
> Режим Аутентификации (Authentication Mode): DES, 3DES, 3K 3DES, AES
> Защищенные Коммуникационные режимы:
<Ciphertext-Шифр>
<Plaintext-Простой текст>
• Ciphertext + MACedCmd + UnMACedResp
• Ciphertext + MACedCmd + MACedResp
• Plaintext + MACedCmd + UnMACedResp
• Plaintext + MACedCmd + MACedResp
• Ciphertext + UnMACedCmd + UnMACedResp
• Ciphertext + UnMACedCmd + MACedResp
• Plaintext + UnMACedCmd + UnMACedResp
• Plaintext + UnMACedCmd + MACedResp

> ID Приложения (Application ID): Приложение для считывания
> ID Файла (File ID): ID файла для считывания
> Стартовый байт файла считывания (Start Byte of Read File)
> Длина файла считывания (Length of Read File)

● Дополнительные Модальности доступа IDETRIS:

> Пароль | PIN | PIN панель с технологией сменных значений MOSAIC
> Сканер рисунка вен ладони ABIOT (Advent Biotech)
> Сканер рисунка вен пальца HITACHI

Важные Особенности

работы с идентификатором DESFire:

Параметры карты DesFire (Card setting):

- **Мастер-ключ** <Card Master Key>**:** Мастер–ключ, который Покупатель использует для выпуска карт, максимально – 16 byte.
- **Формат карт** <Card Format>**:** Введение детальных данных характеристик использования и записи карты. **Пример: рис 1:**

Параметры рабочей архитектуры системы DesFire (Application setting):

- **Функциональный Мастер-ключ** <Application Master Key>: Функциональным Мастер-ключ карты пользователя, устанавливается до 16 byte.
- **Количество функциональных ключей** <Key quantity of Application>: Настройка количества «функциональных ключей»: от 1 до 14.
- **Метод Верификации** <Verification Method>: Аутентификация при считывании карты.
- **Функциональное имя (шестнадцатеричное)** <Application Name> (hex): Настройка «Функционального имени». От 0 до ffffff.

Настройки файловой системы (File Setting):

- **Имя рабочего файла (шестнадцатеричное)** <Application File Name (Hex)>**:**

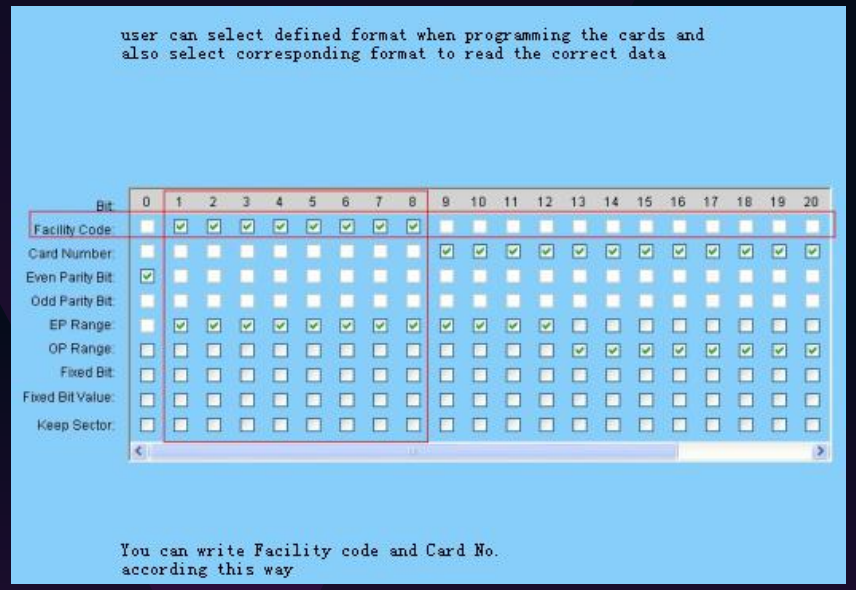
От:
D40 карта: 0 – 0f
D41 карта: 0 – 1f

- **Размер рабочего файла (в байтах)** <Application File Size (Byte)>**:** От: 0 – 111.
- **Ключ для считывания карты** <Key used for Reading cards>: ключ для считывания карт, обычно - 1 значение.
- **Ключ для кодирования карт** <Key used for Writing cards>: ключ для записи карт, обычно - 1 значение.
- **Считывание и запись ключа номера карты:** определение номера ключа, который позволит читать и записывать данные карт: 1-12.
- **Считывание номера ключа карты** <Reading of card key number>: определение номера ключа, который считать карту: От 1 – 12.
- **Запись номера ключа карты** <Writing of card key number>**:** определение номера ключа, который считать карту: От 1 – 12.
- **Считывание и запись ключа номера карты <Reading and writing card key>:** Ключ считывания и записи карты. Настройки позволяют настроить ключ – 16 byte.
- **Считывание ключа карты <Reading card key>:** Ключ считывания и записи карты. Настройки позволяют настроить ключ – 16 byte.
- **Запись ключа карты <Writing card key>:** Ключ записи карты. Настройки позволяют настроить ключ – 16 byte.
- **Редактирование R/W (считывание/запись) ключа доступа <Modify R/W ключа доступа>:** Ключ доступа считывания/записи карты. Настройки позволяют настроить ключ – 16 byte.

Примечания:

- Каждая карта DesFire требует «Мастер ключ карты» для записи данных.
- В память каждой карты Вы можете установить 28 приложений максимум.
- В каждом приложении Вы можете установить до 14 разных ключей.
- В каждом приложении Вы можете создать до 16 файлов разного размера.

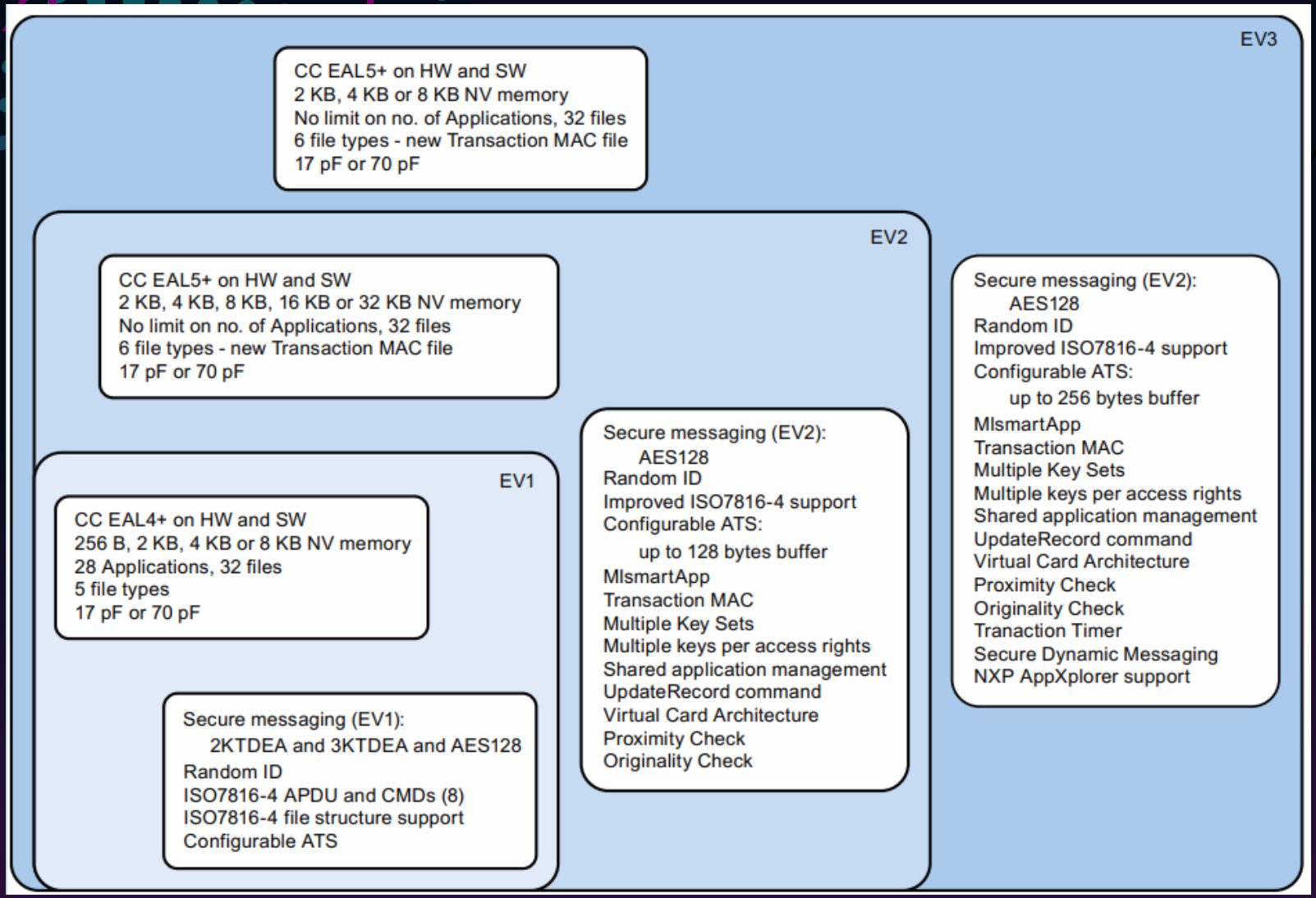
рис 1:



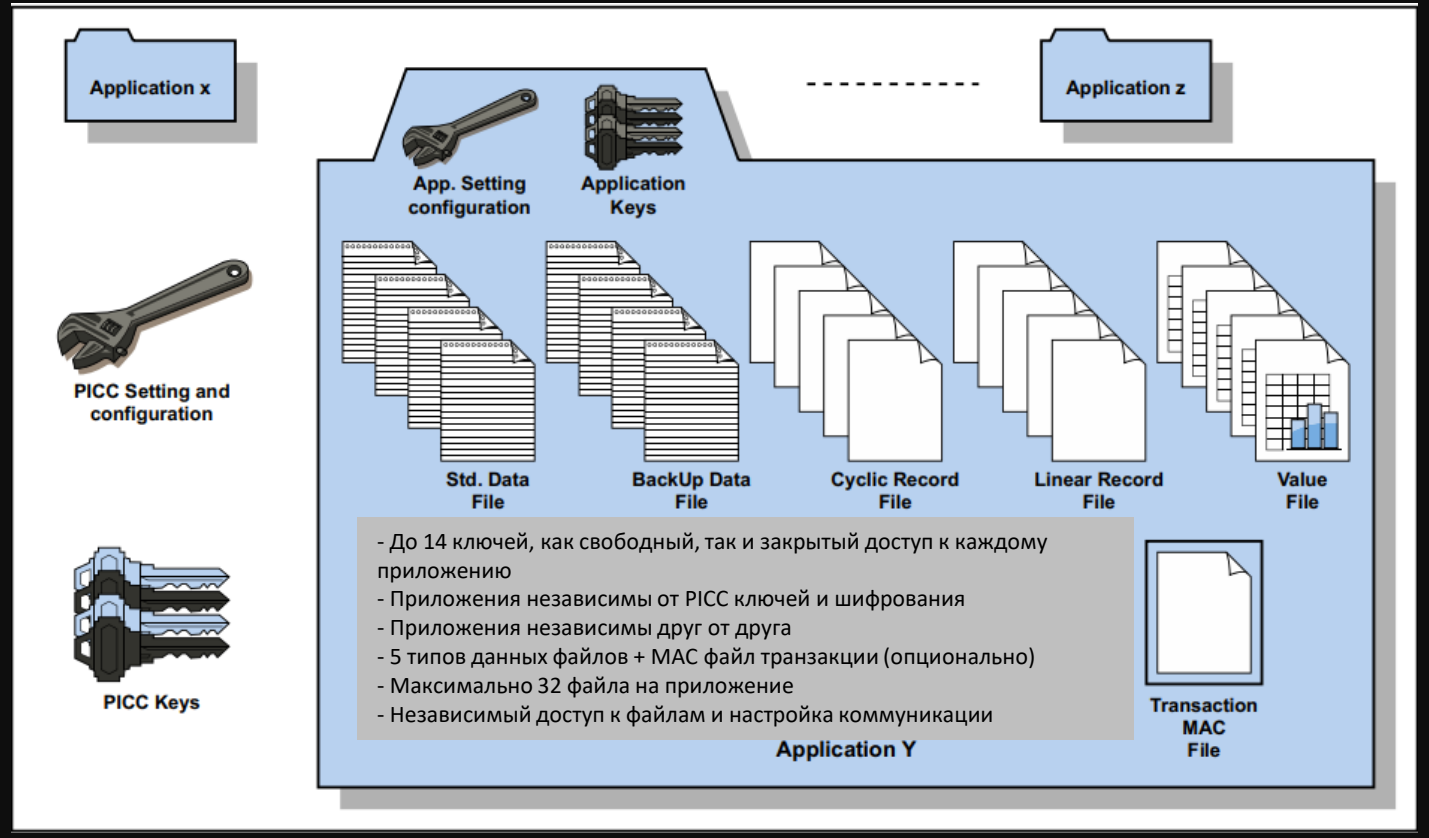
Эволюция от DESFire EV1 => до DESFire EV3

- MIFARE DESFire со временем развивался, улучшая свои характеристики безопасности для защиты от текущих и будущих угроз безопасности, а также добавляя новые функции для лучшего соответствия новым требованиям пользователей.

- MIFARE DESFire EV3 — это четвертое поколение продуктов семейства MIFARE DESFire, пришедшее на смену MIFARE DESFire EV2. Он функционально обратно совместим со всеми предыдущими поколениями MIFARE DESFire, а именно MIFARE DESFire EV2, MIFAREDESFire EV1 и MIFARE DESFire D40 (MF3ICD40).



Структура памяти DESFire EV3:



- Гибкая файловая система: пользователь может свободно определять структуру приложений на PICC
- Количество приложений ограничено объемом памяти, поддерживаемым одной PICC
- До 32 файлов в каждом приложении (6 типов файлов)
- Размер файла определяется при создании (не для файла MAC транзакции)
- Повторное использование памяти в приложениях DAM (форматирование приложений)
- Доступ к файлам из любых двух приложений за одну транзакцию

Типы Файлов в приложении :

- Стандартные файлы данных
- Резервные файлы данных
- Файлы значений с резервным копированием
- Файлы линейных записей с резервным копированием
- Файлы циклических записей с резервным копированием
- Файл MAC транзакций

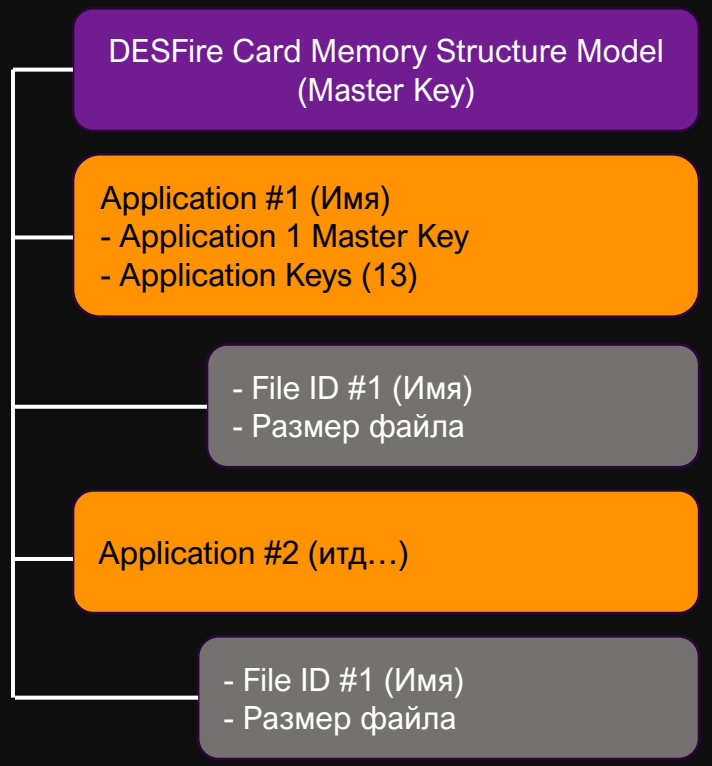
- Организация памяти MIFARE DESFire EV3 гибкая и может динамически структурироваться в соответствии с требованиями любого приложения.
- Структура приложения и файлов показана на рисунке. Каждая папка приложения представляет собой контейнер файлов данных, которые можно использовать в определенном реальном приложении.
- Доступно 5 типов файлов для хранения данных и 1 тип файла для хранения MAC-адресов транзакций.
- В папке приложения находится набор ключей и настроек конфигурации, предназначенных для приложения. Владелец приложения может свободно организовывать структуру файлов и настройки безопасности внутри своего приложения. Смежное приложение не будет иметь доступа к его файлам, пока не получит необходимые права доступа.
- MIFARE DESFire EV3 также поддерживает файловую структуру ISO/IEC 7816-4 и APDU.На уровне PICC существует другой набор ключей и настроек безопасности для владельца PICC. Владелец PICC будет иметь право создавать или удалять любое приложение, но у него не будет доступа к файлам приложения, если он не знает также и ключи приложения.

Помимо поддержки файловой структуры приложения, MIFARE DESFire EV3 предлагает множество дополнительных функций, таких как:

- Делегированное управление приложениями (MIsmartApp) для предоставления прав на создание и управление сторонними приложениями.
- Поддержка нескольких наборов ключей в приложении с механизмом смены ключей и поддержкой миграции ключей.
- Общие файлы между двумя приложениями, поддерживающие одну транзакцию через два приложения одновременно.
- Несколько ключей для каждого права доступа к файлам.
- MAC-код транзакции на уровне приложения, который сопоставляет транзакционные данные с секретным ключом на карте и служит подтверждением транзакции для внутренней системы.
- Безопасный динамический обмен сообщениями (SDM), который отображается в виде текста в сообщении NDEF.
- Архитектура виртуальной карты, обеспечивающая механизм защиты конфиденциальности при выборе карты.
- Проверка близости для предотвращения атак через ретранслятор.
- Проверка оригинальности для подтверждения подлинности продукта MIFARE DESFire EV3

Форма задаваемых параметров программирования DESFire:

Для настройки технологии от Заказчика требуются следующие данные:	
Card Setting (Настройка карт)	
Card Master Key (Мастер-ключ карты)	Мастер-ключ — для форматирования карты даже без других ключей. Длина 16 байт.
Card Format (Формат карты)	Выбор формата данных карты
Application Setting (Настройка приложения)	
Application Master Key (Мастер ключ приложения)	Мастер ключ приложения — для защиты всего приложения без учета остальных ключей. Длина 16 байт.
Application ID name (ID имя приложения)	3 байта, 6 значений от 0 до F
Application Key#1 >>>> #13 (#Ключ приложения)	Установка, как минимум, 1 ключа (из 13 возможных)
File Setting (Настройка файловой структуры)	
File ID Name (ID имя файла)	1 байт, 2 значения от 0 до F
File Size (Размер файла)	Определяется Заказчиком
Read Card Key # (Ключ # чтения карты)	Выбор от #1 до #13 «Ключей» приложения
Write Card Key # (Ключ # записи карты)	Выбор от #1 до #13 «Ключей» приложения
Read / Write Card Key # (Ключ # записи / чтения карты)	Выбор от #1 до #13 «Ключей» приложения
Modify Key # (Ключ # Корректировки)	Выбор от #1 до #13 «Ключей» приложения
Encryption (Шифрование)	AES (AES128) или DES (3DES)



- Энергонезависимая память организована с использованием гибкой файловой системы.
- Эта файловая система позволяет использовать несколько различных приложений на одном устройстве MIFARE DESFire EV3.
- Каждое приложение может иметь несколько файлов. Каждое приложение представлено 3-байтовым идентификатором приложения (AID) и необязательным именем ISO DF.
- Поддерживаются 6 различных типов файлов данных и 1 тип файла транзакций MAC.

Безопасность DESFire EV3:

- Сертификация Common Criteria: EAL5+ (аппаратное и программное обеспечение)
- Уникальный 7-байтовый серийный номер для каждого устройства
- Дополнительный случайный идентификатор (RANDOM) для повышения безопасности и конфиденциальности
- Взаимная трёхпроходная аутентификация
- Взаимная аутентификация согласно ISO/IEC 7816-4• Гибкое управление ключами: 1 главный ключ-карта и до 14 ключей на приложение
- Назначение нескольких ключей для каждого права доступа к файлу (до 8)
- Несколько наборов ключей на приложение с механизмом быстрой смены ключей (до 16 наборов)
- Аппаратный DES с использованием 56/112/168-битных ключей с указанием версии ключа• Аппаратный AES с использованием 128-битных ключей с указанием версии ключа
- Аутентичность данных благодаря 8-байтовому CMAC• Совместимый режим с MF3ICD40: 4-байтовый MAC, CRC 16

Шифрование данных на радиочастотном канале

- Аутентификация на уровне приложений
- Аппаратные датчики исключений
- Самозащищённая файловая система
- MAC-адрес транзакции, подписанный секретным ключом для каждого приложения• Архитектура виртуальной карты для расширенного выбора карты/приложения на устройствах с несколькими виртуальными картами с защитой конфиденциальности
- Проверка близости для защиты от атак через ретранслятор
- Проверка оригинальности для подтверждения подлинности

- 7-байтовый UID фиксирован и запрограммирован в каждое устройство во время производства. Он не может быть изменен и обеспечивает уникальность каждого устройства. UID может использоваться для получения диверсифицированных ключей для каждого билета.
- Диверсифицированные ключи MIFARE DESFire EV3 способствуют созданию эффективного механизма защиты от клонирования и повышают безопасность исходного ключа.
- Перед передачей данных между MIFARE DESFire EV3 и PCD может быть выполнена взаимная трехпроходная аутентификация в зависимости от конфигурации с использованием 56-битногоDES (одинарный DES, DES), 112-битного DES (тройной DES, 3DES), 168-битного DES (тройной DES с тремя ключами 3K3DES) или AES.
- Во время аутентификации устанавливается уровень безопасности всех последующих команд во время сеанса.

Кроме того, настройки связи файла/приложения определяют следующие параметры безопасной связи между MIFARE DESFire EV3и PCD:

- Обычная передача данных (возможна только в режиме обратной совместимости с MF3ICD40и защищенном обмене сообщениями EV2)
- Обычная передача данных с криптографической контрольной суммой (MAC): Аутентификация в режиме обратной совместимости с MF3ICD40: 4 байта MAC; Все остальные аутентификации основаны на DES/3DES/AES: 8 байтов CMAC
- Зашифрованная передача данных (защищенная CRC перед шифрованием): Аутентификация в режиме обратной совместимости с MF3ICD40: 16-битный CRC вычисляется для потокаи прикрепляется.
- Результирующий поток шифруется с использованием выбранного криптографического метода. Все остальные методы аутентификации основаны на DES/3DES/AES: 32-битный CRC-код вычисляется для потока и прикрепляется к нему. Результирующий поток шифруется с использованием выбранного криптографического метода.
- Криптографическая контрольная сумма (CMAC) также будет прикрепляться при использовании безопасного обмена сообщениями EV2.
- Дополнительную информацию о концепции безопасности продукта можно найти в [1]. Имейте в виду, что не все уровни безопасности рекомендуются.
- Для новых проектов рекомендуется безопасный обмен сообщениями EV2.

Конфигурирование Считывателя IDETRIS DESFire:

- Карта «Конфигурирования» используется для перенастройки Считывателя карт.
- Технология предполагает выпуск «Ключ Клиента» (Customer Key) и выпуск «Кода Клиента» для каждого Прямого клиента.
- Ввиду причин Безопасности, карта Конфигурирования должна совпадать с Ключом Клиента, который заблаговременно записан в считыватель.
- Поскольку карта конфигурирования считывателя может изменять параметры на месте, Система использования DESFire не предполагает возможность использования карт за рамками системы и может быть использована только для настройки разрешенных считывателей.
- Существует три области конфигурирования Считывателей:

> Функции считывателей
> Что конкретно должно быть считано из памяти карты
> Алгоритм передачи информации на Контроллер

- Пожалуйста, примите к сведению, что, не смотря на гибкий эффективный характер системы, она, все же, не является неуязвимой.

ИДЕНТИФИКАТОРЫ

LEGIC

LEGIC

Главное о LEGIC

- Одна из уникальных особенностей технологии RFID - LEGIC® - это использование «Паролей» для защиты данных и данные «Паролей» хранятся и защищены в памяти карт доступа. Тем не менее, если случится утечка пароля, это может стать серьезной уязвимостью технологии LEGIC.
- Если произошла утечка пароля, не важно, насколько безопасна технология, Данные больше не являются защищенными должным образом.
- Соответственно, защита «Паролей» является Важным фактором Безопасности доступа при использовании технологии LEGIC®.

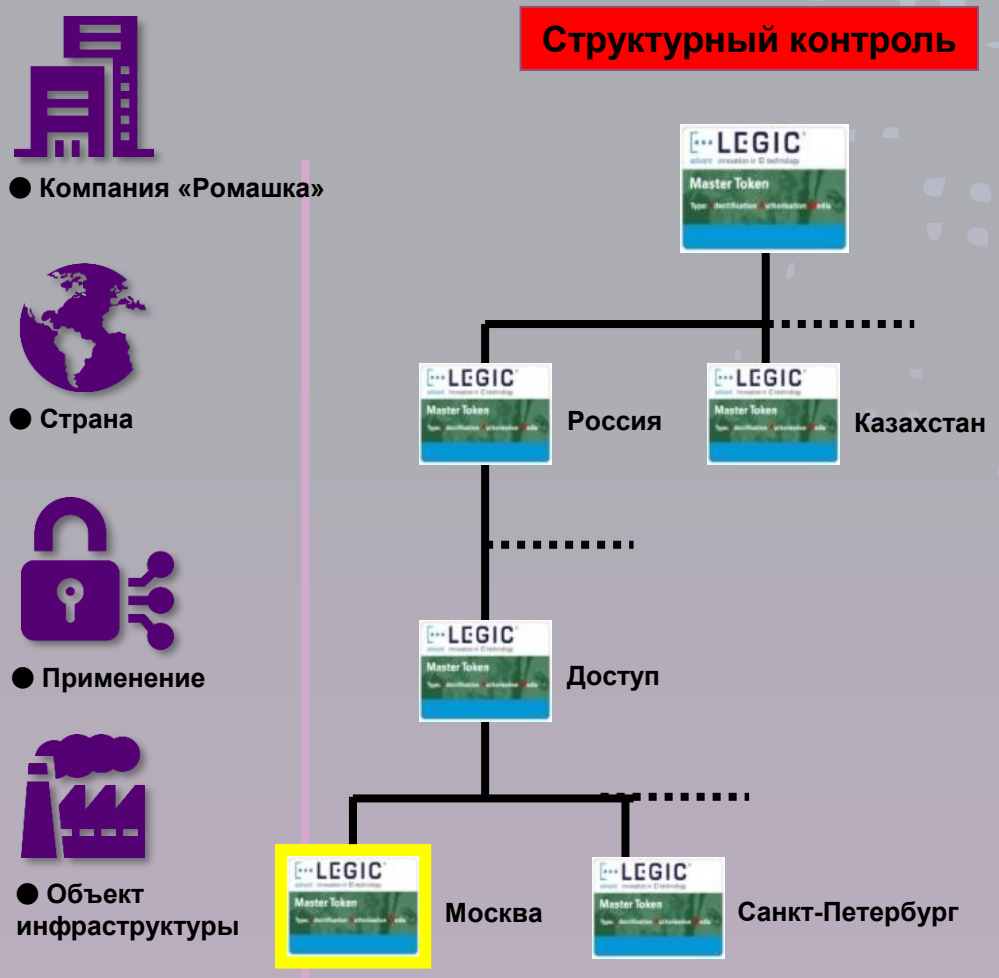
Система управления Паролями (Password Management system):

LEGIC

- Технология генерирования «Мастер-ключей» (Master Tokens) от LEGIC: «Мастер Токены»

- Каждый Клиент получает УНИКАЛЬНЫЙ Мастер-ключ (Master Token) (карта, привязанная к уникальному Коду) от LEGIC, что гарантирует уникальность каждого «Токена» среди всех пользователей в Мире).

Концепция «Master Token» от LEGIC:



- Каждый «Мастер-Токен» может сгенерировать 256 токенов на более низком уровне управления.
- Один «Мастер-Токен» может сгенерировать 12 уровней токенов.
- Типы «Токенов»:

> GAM (General Authorization Token) (Токен Главной Авторизации)

- Может сгенерировать Токен нового уровня (либо IAM или SAM)

> IAM (Initialization Authorization Token) (Токен Авторизации Инициализации)

- Может или не может сгенерировать следующий уровень IAM, что зависит от Конфигурации.
- Используется только для процесса «Инициализации карт».
- Может контролировать количество карт, которые могут быть «инициализированы».

> SAM (Security Authorization Token) (Токен Авторизации режима Безопасности)

- Может или не может сгенерировать следующий уровень IAM, это зависит от конфигурации.
- Используется для авторизации считывателя для считывателя карт, если он имеет функцию «Блокировки Считывания карт».

Преимущества концепции «Master Token» от LEGIC

- Не требуется «Пароль»! Просто используйте «Токен» (Карту).
- Полный контроль Ваших рабочих систем – даже если Вы не являетесь техническим специалистом!
- Вы можете передать «Токен» (карту) физически или забрать его назад.
- Считыватель и Авторотационный «Токен» (Карта) разделены, что позволяет лучшим образом контролировать процессы корпоративного управления и доступа.
- «Токен» может быть сгенерирован. Инженер или сотрудник не может «Скопировать» данные «Токена», что повышает защиту систему и безопасность доступа или авторизации.
- Если «Токен» утерян – требуется немедленная реакция и в данном случае необходим продуманный протокол в рамках системы «Управления рисками».
- Система выпуска «Токенов» может быть адаптирована под структуру корпоративного управления или систему управления государственных служб.
- Выпуск единственного «Токена» для контроля системы – позволит повысить безопасность.
- Позволяет добиться полноценного «владения» и «управления» системой, контролировать Бизнес, Комплексный доступ и процессы авторизации Сотрудников.

IDETRIS

ADVENT IDETRIS

www.advent-id.com