# Технологии физического RFID доступа

идентификаторы

# IDETRIS 7X версия MOSAIC

Сменная панель клавиатуры

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

- Клавиатура (Mosaic)
- Конфигурирование
- Мощный микроконтроллер (В версии XR - Российский)
- Мобильный доступ
- Протокол OSDP v. 2.2.
- Wiegand


IP67 LOGO

**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)**

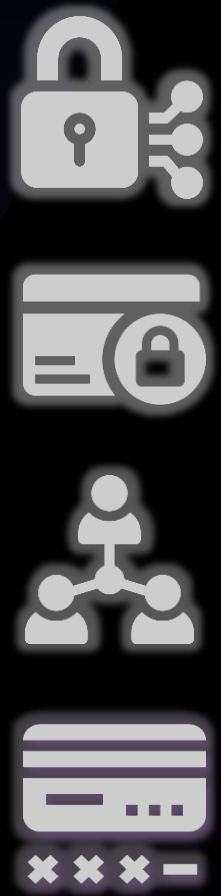
- SONY FELICA
- HID Prox
- INDALA
- Em Marin

# Уникальные возможности ADVENT IDETRIS в контексте безопасности и широкого спектра возможностей управления Идентификаторами:

- **Мультиформат:** Практически весь спектр известных в мире стандартов RFID-доступа  в одном считывателе, не только на программном, но и аппаратном уровне, что обеспечивает полный выбор возможностей использования технологии: Em Marin, Mifare, Mifare Plus, DESFire, Legic, HID prox, HID iClass, Indala, Sony Felica

- **Настройка инструментов Безопасности - Пользователем:** Возможность использования «кастомизированных» настроек считывания карт: порядок считывания, четный/нечетный паритет, различные типы карт – в одной системе, шифрование AES128/256, 3DES итд, доступ к «Памяти» (контенту) карт для загрузки ключей шифрования, а также функциональных приложений. Полный контроль алгоритмов безопасности и режимов работы системы. В итоге Пользователь защищен даже от утечек со стороны производства Считывателей карт.

- **Российский CPU управления в Версии «7XR»:** Серия считывателей ADVENT IDETRIS (в стадии завершенного НИОКР и регистрации): на базе Российских компонентов: Микроконтроллер и Чип памяти с тремя уровнями шифрования – AES128, Магма 128 и Кузнечик 256.



# Mifare Classic

## ИДЕНТИФИКАТОРЫ

# 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

**MIFARE**
Classic

● 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

**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

# 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

# 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)>**:**

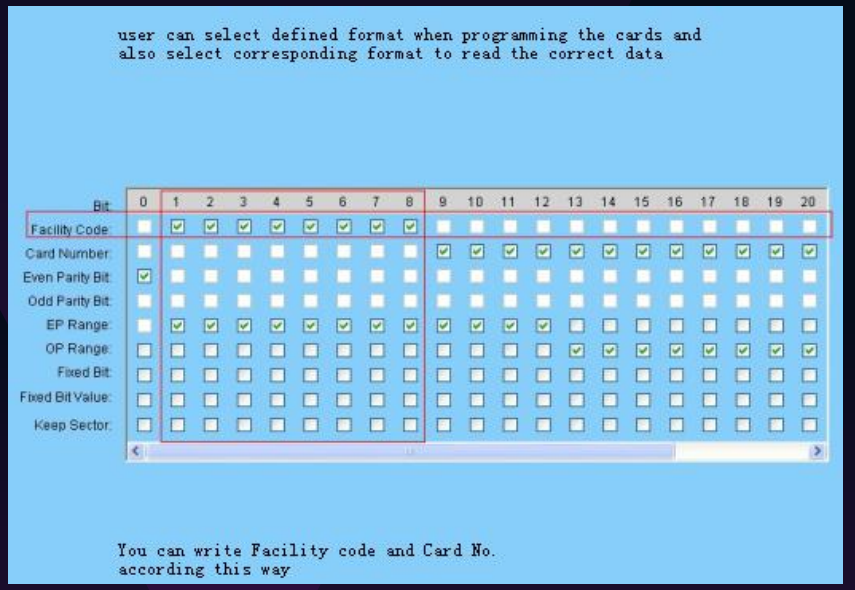
От:
D40 карта: 0 – 0f
D41 карта: 0 – 1f

- **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.

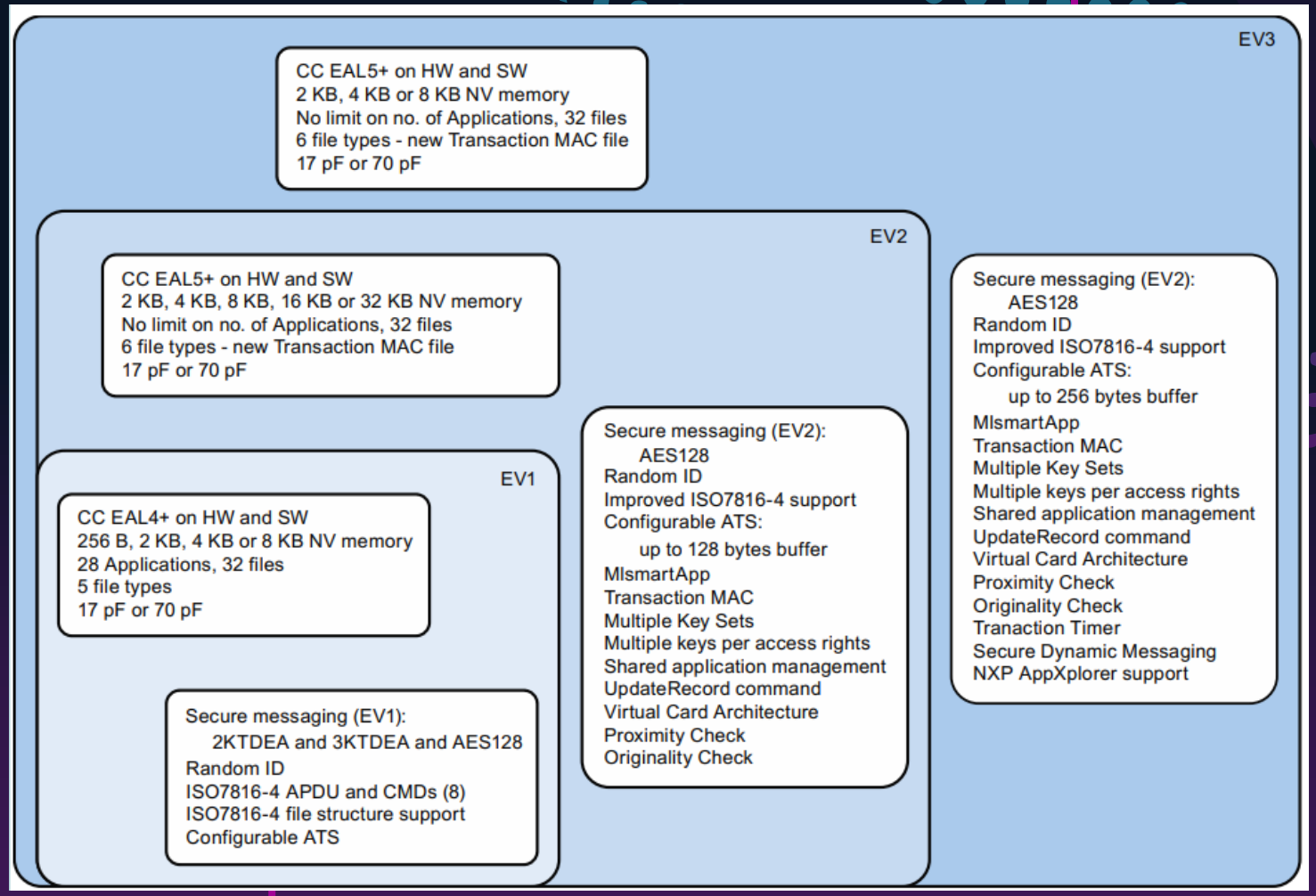
### Примечания:

- 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:



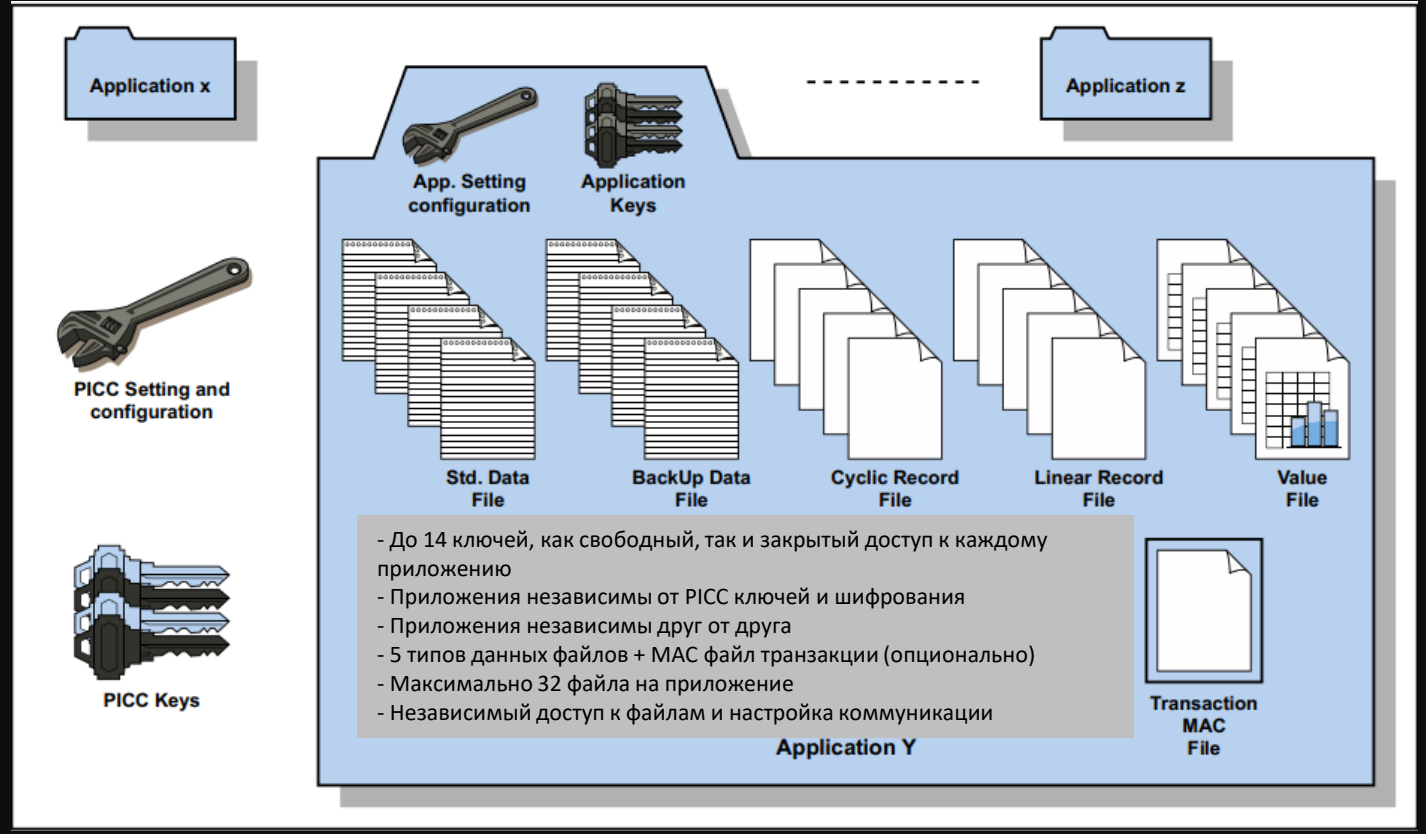
# Эволюция от DESFire EV1 => до DESFire EV3




- 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

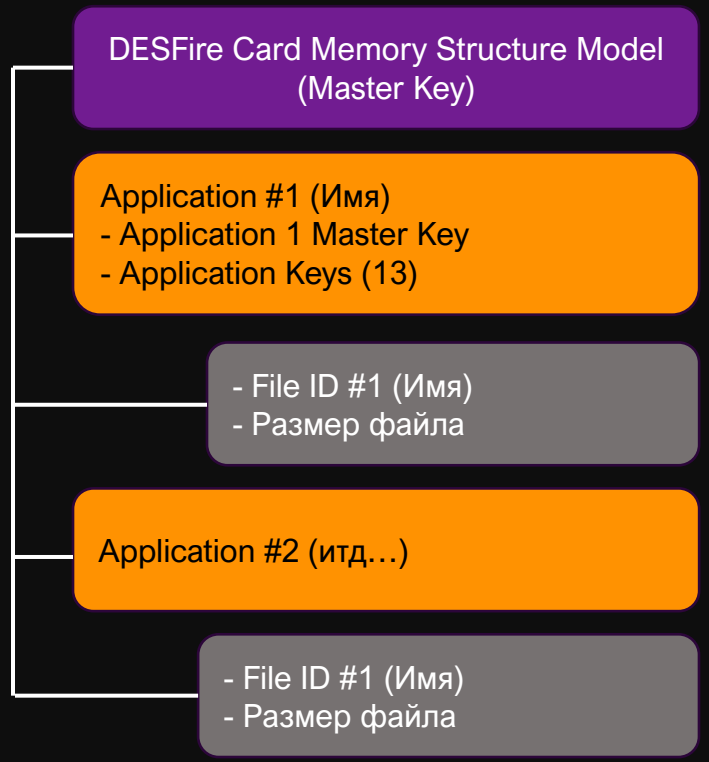
- Организация памяти MIFARE DESFire EV3 гибкая и может динамически структурироваться в соответствии с требованиями любого приложения.
- Структура приложения и файлов показана на рисунке. Каждая папка приложения представляет собой контейнер файлов данных, которые можно использовать в определенном реальном 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.

HID iClass

# ИДЕНТИФИКАТОРЫ

# Базовые параметры HID iClass:

## ● Стандарт: ISO 15693 | 14443B

● Полностью соответствует стандартам ISO 15693 | ISO 14443B
> собственный алгоритм шифрования для обеспечения целостности данных и взаимной аутентификации между картой и считывателем.
> 64-битный диверсифицированный ключ шифрования, полученный из 56-битного главного ключа и серийного номера карты. Этот алгоритм диверсификации ключей встроен во все считыватели iClass.
● Уязвимость: Карты iClass используют один ключ шифрования и этот ключ хранится в энергонезависимой памяти
каждого считывателя (● IDETRIS поможет кастомизировать этот алгоритм под заказчика, формируя проприетарный дополнительный ключ шифрования и усилить технологию другими инструментами)
● Зафиксированы случаи реконструирования алгоритма шифрования и протокола аутентификации iClass злоумышленниками и неподтвержденный случай взлома посредством Flipper Zero устройства

● Технология сочетает два важнейших фактора безопасности:

Радиосигналы между картой и считывателем – шифруются

Аутентификация через шифрование + Быстрая обработка и передача данных = **< 100ms +e-purse**

● Шифрование самого «коннекта» защищает от утечки данных и создания дубликатов карт доступа, также возможно дополнительное шифрование самого коннекта посредством открытых протоколов DES и 3DES

● Частота: 13,56MHz | Дальность считывания – до 7 см.
● Интерфейс: в соответствии с ISO 15693 / 14443B зап/счит.: 106kbps.
● Скорость: <100ms.
● Baud Rate: 14443B2: 212kbps. | 15693: 26kbps.
● Среда использования: -40 до +70C | 100 000 циклов | 10 лет – карта

# iClass

● Типы Карт (Основное):

> Part Num 2000 | 2K bit (256 Byte)
> Part Num 2001 | 2K byte + 2 App areas
> Part Num 2002 | 16 bit (2K byte) + 16 Apps areas
> Part Num 2003 | 32k bit (4K byte) + 15K/2+16K/1
> Part Num 2004 | 32k bit (4K byte) 16k/16+16k/1

## ● Сферы применения:

● ACS *Access control systems
● Network Log-On
● Машинная идентификация (оборудование)
● Платежные сервисы и совместимость с NFC
● Хранение биометрических оцифрованных паттернов

## ● Структура и «Логика безопасности»:

● Множество разнесенных файлов безопасным образом активируют множество приложений что помогало реализовать широкий спектр проектов на основе защищенных приложений
● Память: EEPROM | запись/считывание
● Память Multi-App:
> 2K bit (256 byte) = 2 apps массив*
> 16K bit (2K byte) = 2 или 16 apps массив*
> 32K bit (4K byte) = 16K bits в 2 или 16 apps + 16K bits user конфигурируемая память

● Каждое из приложений защищено 64-битными «диверсифицированными» ключами безопасности записи / считывания данных, что создает «многосложность» используемых приложений и является удобным алгоритмом для параллельных задач
● Реверсивно адаптирован (новые серии iClass распознают предыдущие)
● Возможность выбора дополнительных открытых режимов протоколов шифрования **DES / 2K3DES / 3K3DES / AES,** включая шифрование самого сеанса радио-коннекта iClass шифрование + DES и 3DES
● 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+
● Защита от атак **«man in the middle»**

● Считыватели IDETRIS с идентификатором iCLASS позволяют использовать Legic единовременно с iCLASS

**Массив – имеется ввиду зона памяти, а не программные arrays, tuples итп.*

# Функционал ПО CSW и Считыватели IDETRIS

**При работе с идентификатором HID iCLASS:**

## ● 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**

**iClass**

! Дополнительные параметры – могут быть добавлены!

## ● Карта конфигурирования считывателей IDETRIS :

> Имя конфигурирования DESFire
> 14443B UID / DES, 2DES, 3DES, 3K 3DES, AES
> Параметры считывания карт Шифрованный / Без шифра
> 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
> 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): 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>

> ID Приложения (Application ID): Приложение для считывания

**● 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

# Базовые параметры HID iClass: Память

**● Структура памяти iClass:**

> Стандартные карты iClass выпускаются в двух версиях: 2KS и 16KS, то есть 256 и 4096 байтами памяти.

> Память разделена на блоки по восемь байт.

> Блоки памяти 0, 1, 2 и 5 общедоступны, содержат идентификатор серийного номера карты. Они содержат идентификатор серийного номера карты, биты конфигурации, данные запроса карты и информацию об эмитенте. Блок 3 и 4 содержат два диверсифицированных криптографических ключа, которые полученны из двух разных главных ключей HID. Эти мастер - ключи в документации называются дебетовым ключом, кредитный ключ.

> На карте хранятся только разнообразные ключи. Остальные блоки разделены на две области так называемых приложений. Размер этих приложений определяется блоком конфигурации.

> Первое приложение карты iClass представляет собой HID приложение, хранящее идентификатор, ПИН-код, пароль и другую информацию контроля доступа.

> Доступ для чтения и записи для приложения HID требуется действительная взаимная аутентификация с использованием запатентованного алгоритма, который подтверждает процесс.

> Второе приложение определяется пользователем и защищено ключем. По умолчанию kc-ключ (но не kd) хранится в том же двоичном файле, который содержит секретный ключ для безопасного режима Omnikey.

# iClass

**● Блоки памяти**

> Первые 6 блоков содержат специальные данные. Блок 0 содержит серийный номер карты (CSN), используемый в процедуре предотвращения коллизий. Блок 1 имеет конфигурацию карты информация, содержащая параметры безопасности, лимит приложений для защищенной страницы, и доступ для чтения/записи.

> Значение, хранящееся в блоке 2, предназначено для электронного кошелька. Увеличение и уменьшение этого значения должно быть подтверждено с помощью Kc (CreditKey) и Kd (Дебетовый ключ) соответственно.

> Блоки 3 и 4 содержат секретные ключи, которые являются производными значениями из главного ключа и CSN для создания уникального ключа.

Эти ключи используются для аутентификации со считывателем, чтобы разрешить выполнение команд чтения и записи. Блоки данных с 6 по 18, область применения 1, защищены Kd, а остальные, область применения 2, защищены Kc.

**● Протоколы связи с использованием INCrypt32**

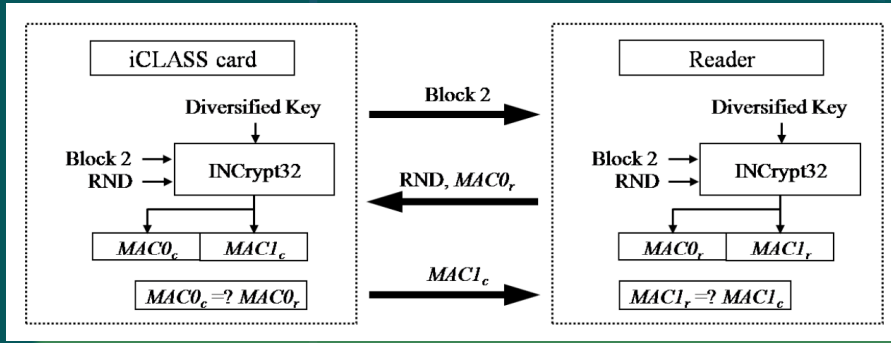
> iCLASS использует только фирменный симметричный криптографический алгоритм INCrypt32 при выполнении команд аутентификации и записи.

| 2K Memory | | 16K/2 Memory | | 16K 16 Memory | | |
|---|---|---|---|---|---|---|
| Block | Data | Block | Data | Page | Block | Data |
| 0 | Card serial number | 0 | Card serial number | 0 | 0 | Card serial number |
| 1 | Configuration data | 1 | Configuration data | | 1 | Configuration data |
| 2 | Stored value area | 2 | Stored value area | | 2 | Stored value area |
| 3 | Key 1 ($K_d$) | 3 | Key 1 ($K_d$) | | 3 | Key 1 ($K_d$) |
| 4 | Key 2 ($K_c$) | 4 | Key 2 ($K_c$) | | 4 | Key 2 ($K_c$) |
| 5 | Application issuer data | 5 | Application issuer data | | 5 | Application issuer data |
| 6–18 | Application area 1 | 6–18 | Application area 1 | | 6–18 | Application area 1 |
| 19–31 | Application area 2 | 19–255 | Application area 2 | | 19–31 | Application area 2 |
| | | | | | Page 1–7 | |

# Базовые параметры HID iClass: Операции

## ПРОТОКОЛ АУТЕНТИФИКАЦИИ

- Протокол аутентификации. Чтобы получить право доступа к карте iCLASS, карта и считыватель должны выполнить протокол аутентификации. Этот протокол основан на INCrypt32 с 8-байтовым ключом Kd или Kc.
- Перед выполнением протокола аутентификации считыватель формирует диверсифицированный ключ (Kd или Kc) для карты из мастер-ключа и серийного номера карты.
- Карта отправляет сохраненное значение блока 2. Затем считыватель отправляет 4-байтовое случайное число (RND) со своей 4-байтовой подписью (MAC0r), которая является половиной 8-байтового MAC-кода. ● На этом этапе карта может вычислить 8-байтовый MAC-код таким же образом. Если MAC0r верен, карта ответит на другую 4-байтовую подпись (MAC1c), которая позволяет считывателю аутентифицировать карту.
- Следовательно, протокол аутентификации должен выполнять INCrypt32 с 12-байтовыми входными и 8-байтовыми выходными данными.

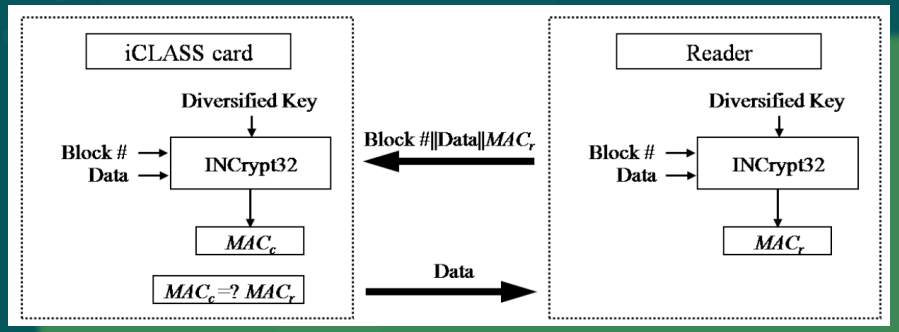



**iClass**

## ПРОТОКОЛ РЕГИСТРАЦИИ

- Протокол записи. Если протокол аутентификации пройден успешно, читатель может считывать блоки данных без дополнительной процедуры аутентификации. Однако, чтобы записать 8-байтовые данные в блок данных, читателю необходимо выполнять INCrypt32 каждый раз.

- После выбора и аутентификации карты считыватель может записать адресованный блок памяти. Считыватель отправляет 8-байтовые данные с 1-байтовым адресом блока и 4-байтовой подписью (MACr). На этом этапе карта может вычислить 4-байтовую подпись MACc таким же образом. Если MACr верный, карта записывает
8-байтовые данные в адресованную память и отвечает, что данные должны быть сохранены. Следовательно, протокол записи должен выполнять INCrypt32 с 9-байтовыми входными и 4-байтовыми выходными данными.



# ИДЕНТИФИКАТОРЫ

LEGIC

LEGIC

# Базовые параметры LEGIC:

● **Защищенность: ВЫСОКАЯ (Advant) / Средняя (Prime)**

**Главные инструменты безопасности:** Legic Advant и Legic Prime

● Legic Prime: 13,56MHz LEGIC RF Standard (собственный стандарт)
● Legic Prime – безопасность Legic Prime строится на «проприетарной» логике безопасности, но имеет большую технологическую уязвимость по сравнению с Legic Advant.

● Legic Advant: ISO15693 (считывание/запись 64 битный SN), ISO14443A (считывание/запись) 32 битный (считывание/запись), CC EAL4+, MTSC Token structure
● Основные принципы безопасности LEGIC:
> Legic Prime: Проприетарный алгоритм
> Legic Advant: Криптографический алгоритм обмена данными: 3DES при передаче данных и AES128(AES256) + Grain128 (MM) + ALG55 (64bit) + 2K3DES + 3K3DES
> Принцип «Взаимной Аутентификации» Считывателя и карты
> До 127 приложений данных на одной карте (Plug and Play)
> Возможность Организациям записывать собственные приложения безопасности, защищенные паролями
> Принцип Мастер-Токенов (контроль Ключей безопасности)
● **MTSC:** Права Авторизации и правила безопасности хранятся на физических Мастер-Токенах. Это позволяет Организациям полностью контролировать алгоритмы безопасности и спектр прав доступа Пользователей:
> Безопасность процесса выпуска карт
> Контроль проектов, департаментов и точек доступа
> Управление безопасностью Приложений
● Каждое приложение памяти хранится и обрабатывается отдельно

## 1 карта = 12 / 59 / 32 / до 127 приложений

**Dynamic (memory segmenting) (в зависимости от типа карт и стандартов)**

● Legic Advant: Объем памяти: UID 4/7 byte | 4096 byte (стандарт)
● Legic Prime: Объем памяти: UID 4/7 byte | 224 / 944 / 1002 byte (стандарт) (в зависимости от типа)
● Legic Advant: Дальность: max 8cm. | 424kbit/sec.
● Legic Prime: Дальность: max 10cm. | 424kbit/sec.

Существуют гибридные карты: Advant + Prime | Advant + Mifare

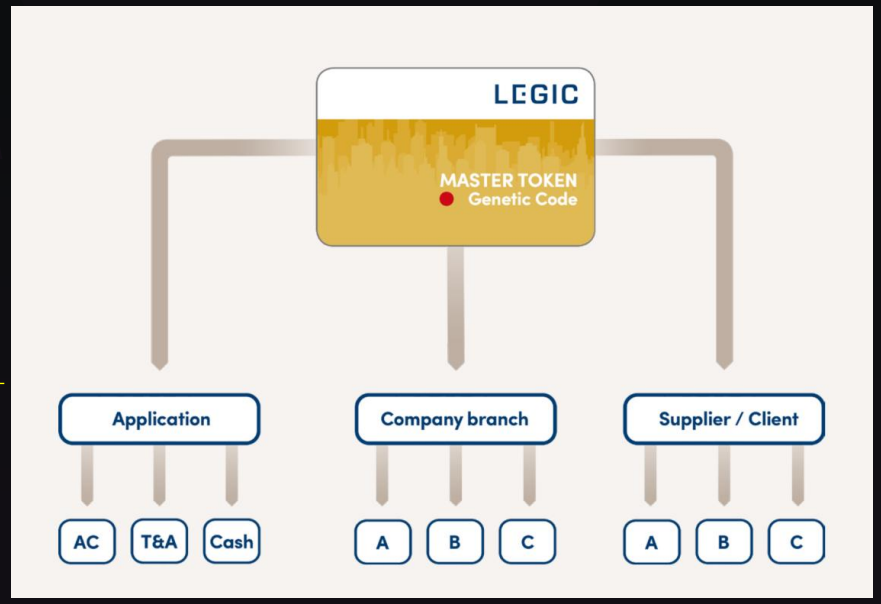
## > LEGIC Advant:

Типы Карт (2025) :
● **Advant [4096 byte] ATC4096-MP (ISO 14443A | CC EAL4+) |** 3DES шифрование передачи | шифрование данных: AES128 / 256 bit / 3DES / DES / Legic encryption
● **Advant [4096 byte] + Mifare [3520 byte] ATC4096-MP313 (ISO 14443A | | CC EAL5+) |** 3DES / AES128 шифрование передачи | шифрование данных: AES128 / 256 bit / 3DES / DES / Legic encryption
● **Advant [2984 byte] + Prime [1002 byte] CTC4096-MM410 (ISO 14443A+ISO15693 MM) |** AES128 / Grain128 шифрование передачи | шифрование данных: AES128 / 256 bit / 3DES / DES / Legic encryption

## > LEGIC Prime:

Типы Карт (2025) :
● **Prime [224 byte] ATC256-MV410 (ISO 15693 | CC EAL4+) |** Grain128A шифрование передачи | шифрование данных AES128/256 / 3DES / Legic
● **Prime [944 byte] ATC1024-MV110 (ISO 15693 | | CC EAL5+) |**
ALG55 шифрование передачи | шифрование данных: 3DES / DES / Legic
● **Prime [234 / 1002 byte] MIM256-MN / MIM1024-MN (legacy) |** Legic шифрование передачи | шифрование данных: Legic

**LEGIC**



# Функционал ПО CSW и Считыватели IDETRIS

**При работе с идентификатором LEGIC:**

## ● Настройка Формата Карты:

● ПО настроено по умолчанию на форматы карт
● Контент LEGIC Кастомизированный формат:
> Длина Wiegand (1 – 233 bit)
> 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:

В открытой версии CSW эта функция пока отсутствует для LEGIC

(Внимание! Мы можем добавить дополнительные функции LEGIC в программную платформу CSW IDETRIS)

+ Пароль
+ Display
+ Status
+ Programmed Card Number

**CSW SOFTWARE**

**LEGIC**

## ● Карта конфигурирования считывателей IDETRIS :

**(Внимание! Мы можем добавить дополнительные функции LEGIC в программную платформу CSW IDETRIS)**

> Имя конфигурирования LEGIC
> Legic Advant/Prime
> Flash Reader / Mini USB Reader / Стандартные считыватели
> Выбор Контроллера: 2XLEDs, OSDP, Single LED
> Режим Конфигурирования: через 5 сек. / 30 мин.
> Считывание: UID / Content
> Код Токена (Token Code)
> Длина Токена (Token Length)
> Номер Сегмента (Segment Number) 1-255
> Wiegand Bits: 1-255
> Стартовый байт (Start Byte)
> Стартовые биты (Start Bits)
> Контрольный бит (E-checkbit): 1-255

## ● 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

# Главное о LEGIC

- Одна из уникальных особенностей технологии RFID - LEGIC® - это использование «Крипто-Токенов» с «Паролями» 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®.

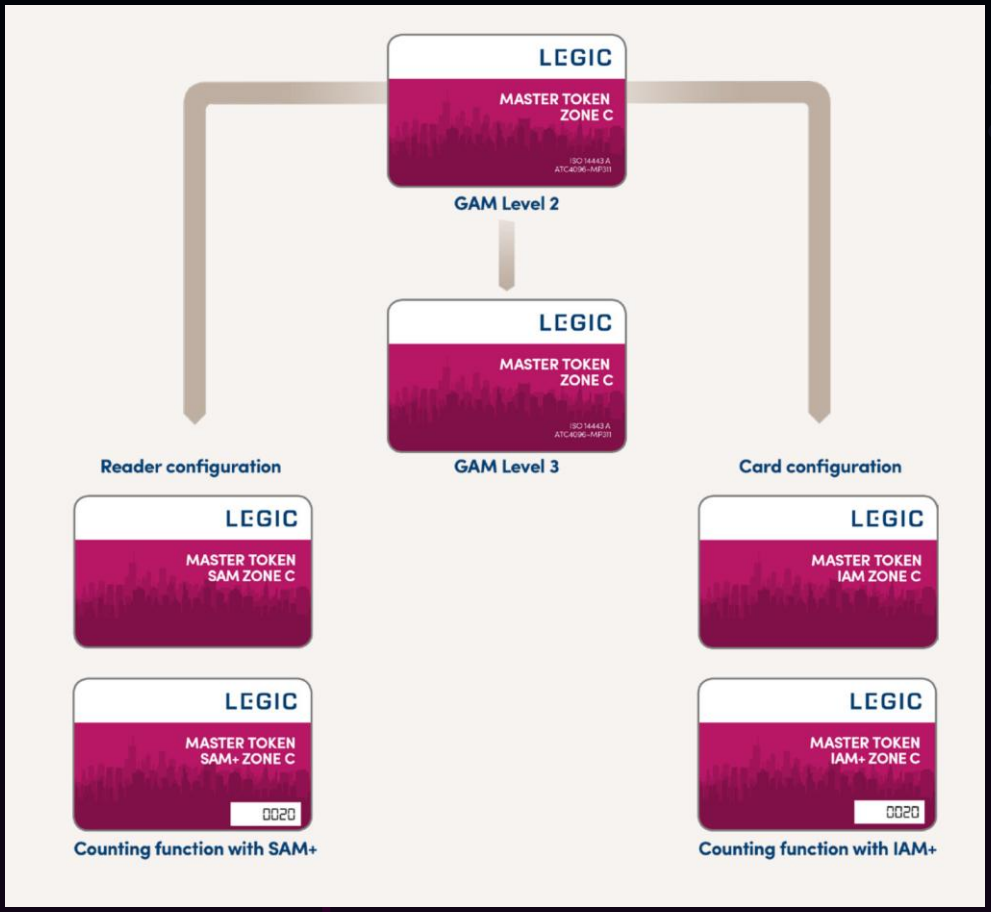
LEGIC

# 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.

# MTSC LEGIC

- Преимущества Master-Token System-Control (MTSC
- Простое и безопасное назначение прав дочерним компаниям, партнерами поставщикам
- Свободное комбинирование и администрирование приложений
- Приложения можно добавлять или удалять в любое время на месте
- Стандартизированные приложения обеспечивают взаимодействие и независимость от поставщиков
- Простая и интуитивно понятная реализация иерархий авторизации без использования данных в виде обычного текста
- Несколько независимо управляемых приложений на одной карте

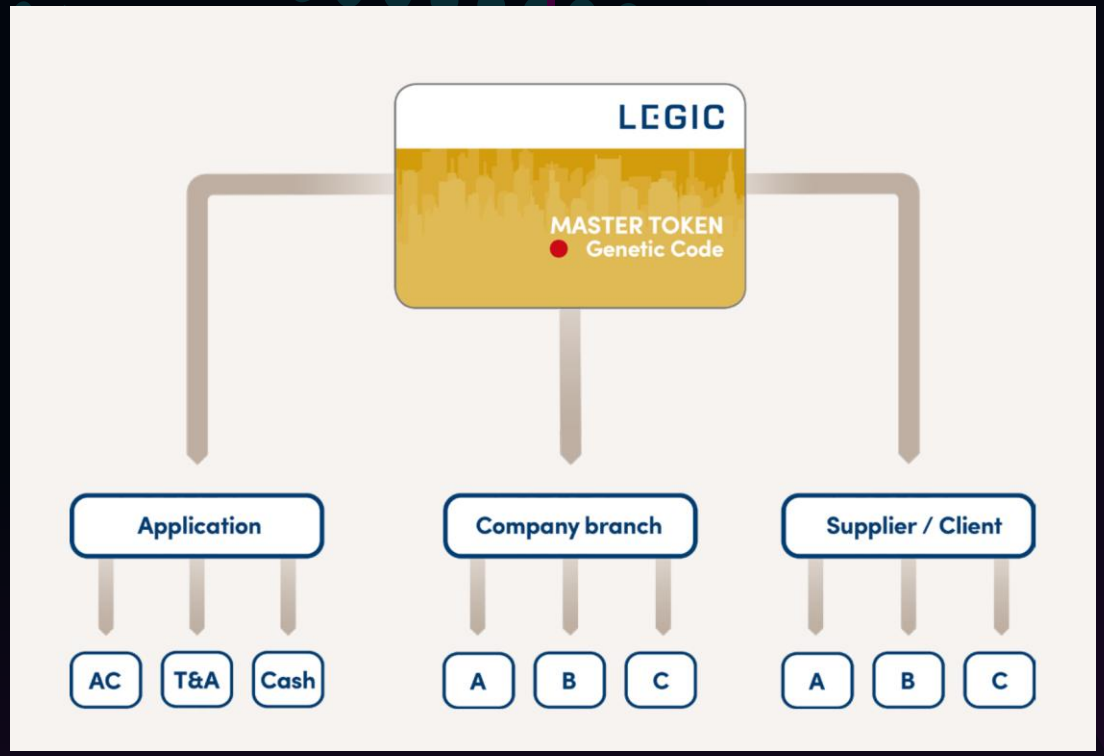




| | | |
|---|---|---|
| GAM | General Authorization Medium | Авторизация выпуска новых Sub-Master-Tokens (Саб-Мастер-Ключей) |
| SAM | System Authorization Medium | Авторизация Трансфера функции Записи/Считывания считывателей с аппаратным управлением LEGIC (Авторизация Режима Безопасности и управления Считывателями) |
| SAM+ | System Authorization Medium plus | Ограниченное число «Инициализаций» считывателей (со счетчиком) (Авторизация Режима Безопасности и управления Считывателями)) |
| IAM | Identification Authorization Medium | Авторизация для «Инициализации» и удаления сегментов данных Смарт-карт LEGIC Advant и Prime (Инициализация режимов) |
| IAM+ | Identification Authorization Medium plus | Лимит числа сегментов «Инициализации» (с функцией счетчика) (Инициализация режимов) |
| XAM | Extended Authorization Medium | Авторизация для «Инициализации» и удаления сегментов карт LEGIC Advant и Prime (перманентное хранение в EEPROM) |

> Master-Token GAM, Zone A
> Master-Token GAM, Zone B,
incl. 50 Blanks (AFS4096-JP11)
> Master-Token GAM, Zone C,
incl. 50 Blanks (ATC4096-MP311)

LEGIC

# Главное о LEGIC: Мастер-токены




- Мастер-токен можно использовать для генерации на, так называемых, «заготовках» различных sub-мастер-токенов с разными кодами. Они могут быть назначены различным приложениям, филиалам компании, поставщикам или даже клиентам.
- Если считыватель инициализирован мастер-токеном более высокой иерархии, он получает доступ ко всем приложениям соответствующих sub-мастер-токенов.

LEGIC

# Главное о LEGIC: Мастер-токены и «Зоны»

| | Zone A | Zone B | Zone C |
|---|---|---|---|
| Master-Token |  |  |  |
| Smartcards | Older transponders<br>▪ ATC1024-MV110<br>▪ MIM1024<br>▪ MIM256 | Newer transponders<br>▪ ATC256-MV410<br>▪ ATC1024-MV010<br>▪ ATC4096-MP311<br>▪ ATC4096-MP312<br>▪ CTC4096-MP410/MM410<br>▪ AFS4096-JP1x | |
| Zone origin | No | Yes | |

- Зоны мастер-токена Безопасность бесконтактной смарт-карты в основном зависит от используемой технологии. Уникальная концепция зоны мастер-токена учитывает технологию носителяи мастер-токена.
- Концепция зоны гарантирует, что мастер-токен всегда соответствует стандарту безопасности технологии, используемой транспондером, и, следовательно, обеспечивает безопасную долгосрочную работу системы. При необходимости, технология может быть выборочно деактивирована.
- Технологическая генерация мастер-токена наследуется при генерации сегментов LEGIC наATC256-MV410, ATC1024-MV010,ATC4096-MP311, CTC4096-MP410 /MM410 и AFS4096-JP1x. Это позволяет считывателям специально исключать отдельные сегменты в зависимости от технологии их происхождения.

LEGIC

# СУТЬ MTSC LEGIC

● Страна

● Компания «Ромашка»

● Применение

● Объект инфраструктуры

**Структурный контроль**



● 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».

# Возможные уязвимости LEGIC (факторы особого внимания)


● **Безопасность:** настолько же сильна, насколько и самое слабое звено. Мы все ежедневно сталкиваемся с современной технологией контроля доступа на основе смарт-карт – большинство из нас используют её при входе в офисы или здания предприятий, используя бейдж в качестве удостоверения личности.
Основа безопасности – гарантия того, что никто не сможет получить доступ к ключу шифрования (также называемому «паролем, PIN-кодом и т. д.»), хранящемуся в защищённой памяти дверного замка. Для шифрования AES это просто 128-, 192- или 256-битное число. Современная полупроводниковая технология в форме «элемента безопасности» (см. Глоссарий) ограничивает физический или технический доступ к этому ключу шифрования так как он хранится в электронных дверных замках, даже самому опытному хакеру. Однако одна уязвимость всё ещё существует.

● **Как устанавливаются ключи шифрования?** Когда речь идёт об управлении доступом в здания, помещения и складские помещения, наиболее уязвимой точкой атаки является не сама система контроля доступа сама по себе, используемое шифрование и не физические носители, такие как бейджи сотрудников, а то, как криптографические ключи, встроенные в считыватели карт, попадают туда. Нарушение на этом самом фундаментальном уровне безопасности доступа может сделать уязвимой всю систему контроля доступа.

● **Недостатки заводского программирования.** Один из способов гарантировать безопасную установку криптографических ключей в считыватели — сделать это на этапе производства — «заводское программирование» каждого замка перед тем, как он покинет производственную линию. Это гарантирует, что ключи шифрования будут безопасно встроены в замок перед доставкой клиентам. Однако существуют три основные проблемы:

1) Скомпрометированный контроль безопасности: Предварительное программирование электронных замков у внешнего поставщика немедленно подвергает риску систему безопасности. Сколько сторонних поставщиков, ИТ-специалистов и логистических специалистов имели доступ к ключам шифрования во время производства и доставки до установки замка? Ответ:— вы не знаете. Процессы безопасности у внешних поставщиков определены, контролируются и проверяются внутри их собственных четырёх стен, и эти процессы не на 100% прозрачны для конечных потребителей. По этой причине следует избегать заводского программирования ключей шифрования ,за исключением отдельных ограниченных случаев, и конечный пользователь должен иметь возможность (пере)настроить свою инфраструктуру доступас ключами шифрования, которыми он владеет и управляет самостоятельно.

2) Логистика: Производители электронных дверных замков и считывателей ежегодно выпускают миллионы устройств для тысяч клиентов. Пока замки поставляются в виде «заготовок», которые конечный потребитель может настроить на конечном этапе, логистика может быть простой – один продукт подходит всем. Как только создаются замки с заводским программированием, то, что когда-то было единым продуктом, подходящим для многих клиентов, становится продуктом, разработанным под конкретного клиента, со всеми сопутствующими проблемами хранения и логистики, связанными с управлением тысячами различных вариантов. Это значительно увеличивает стоимость устройства, создавая риски перепроизводства или недопроизводства, а также ошибок.

# Возможные уязвимости LEGIC (факторы особого внимания)


3) Смена владельца Компании регулярно закрываются, переезжают и меняют владельца. Чтобы предотвратить доступ предыдущих владельцев к инфраструктуре, которую они освободили, каждый считыватель должен быть перепрограммирован новым владельцем. Системы контроля доступа могут быть скомпрометированы еще до завершения установки.

4) Риски перепрошивки считывателей Физическое программирование на месте Если дверные замки установлены в «пустом» состоянии (без установленного ключа), их невозможно программировать по сети из-за отсутствия шифрования – шифрование возможно только после установки ключа шифрования (дешифрования). При этом возможность удаленной «перепрошивки» устройства создает дополнительные риски как и человек, устанавливающий ключ на месте, также является фактором риска, если незашифрованный ключ виден – его можно легко скопировать, запомнить или сфотографировать сам код. При инициализации большинства систем контроля доступа сотрудникам службы безопасности поручено физически установить ключи шифрования на каждый дверной замок с помощью специального устройства. Чтобы предотвратить утечку ключа во время инициализации замка, уникальное решение LEGIC «Master-Token System-Control» и управления авторизацией(MTSC) было разработано для предоставления компаниям и учреждениям абсолютной независимости и контроля над безопасностью доступа своей организации, включая карты и считыватели.

Секрет, которым делятся, больше не секрет Главная функция безопасности MTSC заключается в преднамеренном упущении секретов, которыми обмениваются сотрудники, ответственные за установку и безопасность, таких как ключи шифрования или пароли. Вместо этого авторизации предоставляются с использованием физических токенов, нечитаемых человеком, в виде не копируемых бесконтактных смарт-карт. Компании, использующие видимую систему безопасности с паролями, обычно не знают, насколько легко их поднять. Видимые пароли могут быть раскрыты в любой момент, совершенно незамеченными. MTSC не использует пароли, что обеспечивает лучший контроль безопасности в приложениях с бесконтактными смарт-картами. MTSC основана на уникальном коде доступа, встроенном в бесконтактные смарт-карты. Код в этой технологии гарантирует, что все необходимые учетные данные уникальны. Код передается через бесконтактную RFID-метку во время инициализации карты и на считыватели во время настройки системы. Использование физического токена также позволяет администраторам безопасно управлять своим набором бейджей и легко добавлять или отзывать приложения по мере необходимости (например, контроль доступа, учёт рабочего времени, безопасная печать, электронные платежи в торговых точках и столовых и т. д. – до 127 приложений можно разместить на одной карте). Кроме того, владение собственным физическим токеном предоставляет сотрудникам службы безопасности полную автономию в выборе доверенных поставщиков, если они захотят это сделать.

Обеспечение безопасности посредством организационной структуры и процессов. Благодаря скрытию ключей шифрования от посторонних глаз, общая безопасность системы обеспечивается физической защитой мастер-токена, находящегося на смарт-карте, подобно хранению золота в сейфе. Соблюдение простых и базовых мер обеспечивает безопасность инициализации считывателя карт и изготовления карты благодаря соответствующему уровню безопасности и уполномоченному персоналу. Мастер-токены можно извлечь только с использованием документированного рабочего процесса с соответствующими уровнями одобрения и, помимо прочих методов, согласно принципу «четырех глаз».

Возможность проверяемых процессов Благодаря тому, что ключ шифрования заперт в токене и не может быть прочитан человеком или передан по цифровым сетям, становится легко реализовать базовые и проверяемые организационные меры для обеспечения высокого уровня безопасности мастер-токена. Защита аналогична той, которая обеспечивается для физических объектов, таких как наличные деньги или драгоценные металлы. Тот же процесс для человекочитаемой информации или информации, передаваемой по сети, гораздо сложнее и сопряжен с гораздо большим количеством рисков безопасности. Таким образом, MTSC позволяет легко внедрить проверяемые процессы

# Наши контакты

www.advent-systems.com – General website | HUB

www.advent-id.com – Security, ACS, RFID, Identification

Главный офис: Москва, Киевское ш., домовладение 3, стр. 1
Бизнес ТехноПарк — G10
4 этаж офис XCIII (офис 93)

+7499-213-00-58
info@sprx.ru

Sk Resident

ADVENT SYSTEMS

YouTube

ADVENT IDETRIS