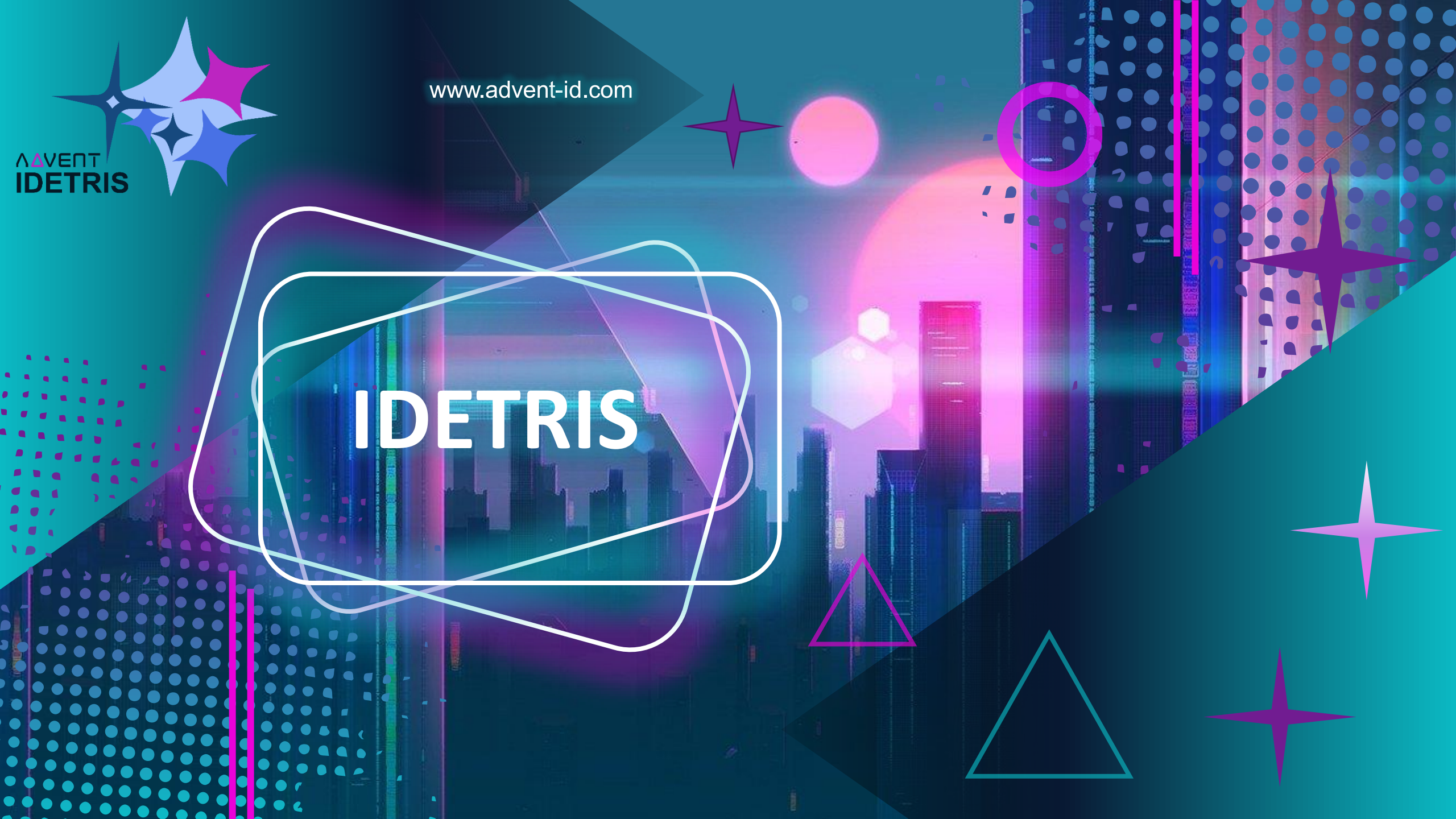

www.advent-id.com
ADVENT
IDETRIS
IDETRIS

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 станет самой большой 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®.

ADVENT IDETRIS

Например:

- Вы передали программному разработчику «Пароль» для разработки приложений? Что если, сотрудник покинет компанию, забрав с собой «Пароль»?
- А если «Пароль» был утерян или забыт?
- Чем больше Ваш инженер коммуницирует с сотрудниками, тем больше людей знают о Вашем пароле!
- Что, если Ваш сотрудник работает на Вашего Конкурента?
- Все Ваши системы и Бизнес в целом – защищены «Паролями»? Не так ли?
- Все Ваши системы и Бизнес в целом – защищены «Паролями»? Не так ли? Насколько Вы уверены в том, что злоумышленники не получат доступ к «Паролям» Вашей компании?
- Все Ваши системы и Бизнес в целом – защищены «Паролями»? Не так ли? Насколько Вы уверены в том, что злоумышленники не получат доступ к «Паролям» Вашей компании? Многие люди думают – «Чем длиннее пароль, тем выше защита». Однако Важным являются процедуры «управления» паролями.

Система управления Паролями **(Password Management system):**

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

Далее- «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).

ΛΔVENT IDETRIS

Концепция «Master Token» от LEGIC:

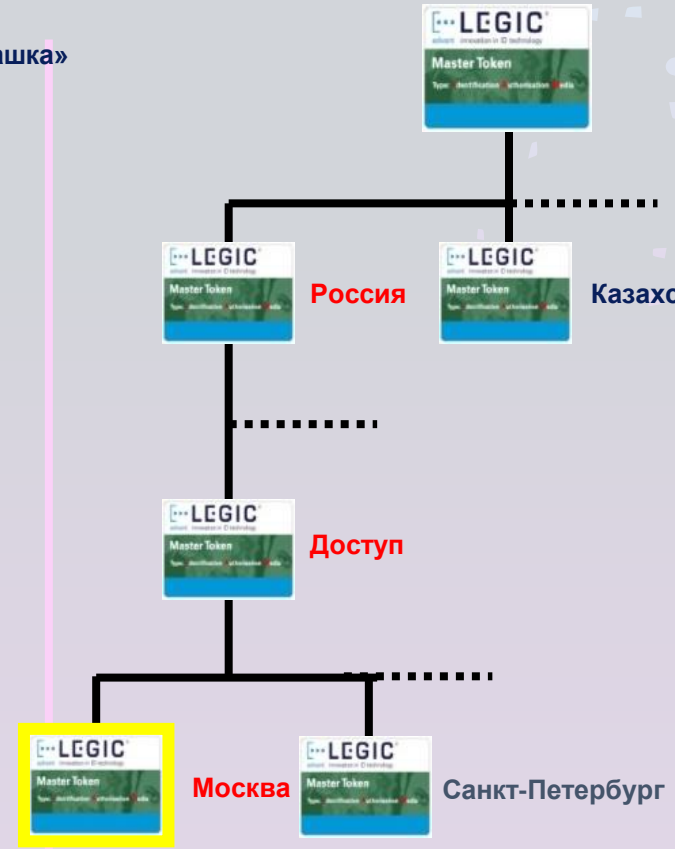
● Компания «Ромашка»

● Страна

● 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.
- Каждый «Токен» может быть:
  - **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».

AVENT IDETRIS

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.
- «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 дальнейшего контроля системы – позволит повысить безопасность.
- Это позволит добиться полноценного «владения» и «управления» системой, контролировать Бизнес, Комплексный доступ и процессы авторизации Сотрудников.

Технология **DesFIRE:**

- DesFire или Mifare DesFire – это технологии корпорации NXP!
- Технология построена на основе архитектуре CPU (ЦП) посредством интерфейса ISO14443.
- Ввиду того, что технология построена на CPU, безопасность COS измеряется «Общим критерием» (Common Criteria).

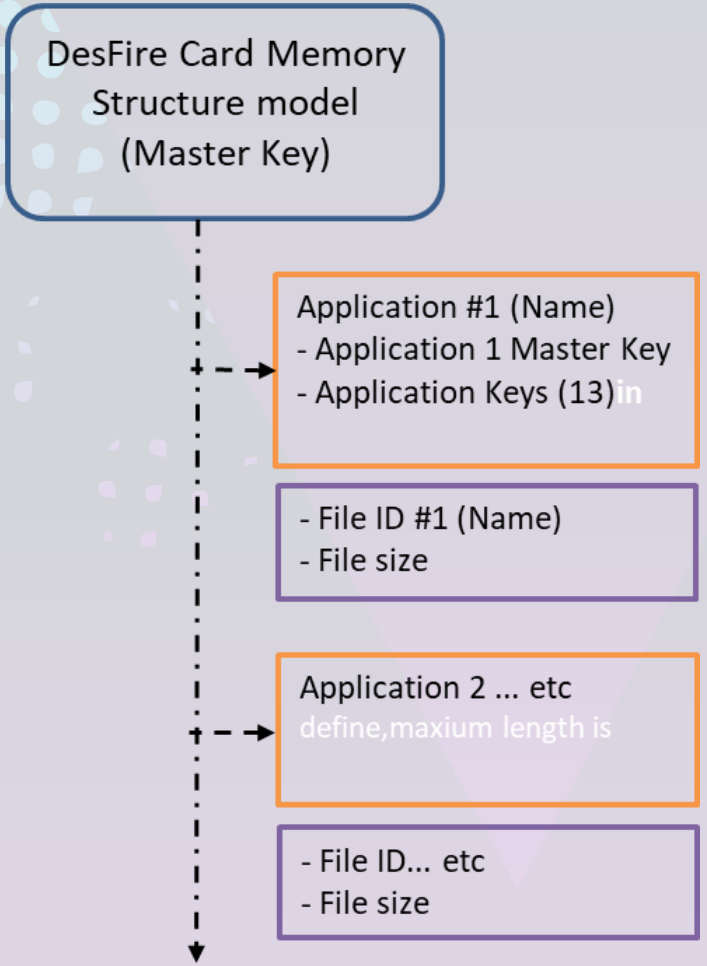
(Common Criteria for Information Technology Security Evaluation, Common Criteria, CC) — принятый в России международный стандарт по компьютерной безопасности. В отличие от стандарта FIPS 140[4], Common Criteria не приводит списка требований по безопасности или списка особенностей, которые должен содержать 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.)

- Параметры безопасности для EV1: EAL4+
- Параметры безопасности для EV2: EAL5+
- 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, Legic – «крипто-технологий» в области выпуска карт.
- Пожалуйста, примите к сведению, что «крипто-технологии» выпуска карт не имеют каких-либо параметров оценки безопасности.

Структура Памяти **DesFIRE:**

DesFire Card Programming Form		
Card Setting	**Fill in by customer**	**Description**
*Card Master Key		Master Key - to format the card even without other Keys. 16 bytes long. *See defination below.*
*Card Format		Please choose: Card data format
Application Setting	**Fill in by customer**	**Description**
*Application Master Key (Key #0)		Application Master Key - to rest the whole Application without knowing the rest of the Keys. 16 bytes long.
*Application ID/Name		3 bytes - 6 characters from 0 to F
Application Key #1		*Setup **at least** one Key
Application Key #2		
Application Key #3		
Application Key #4		
Application Key #5		
Application Key #6		
Application Key #7		
Application Key #8		
Application Key #9		
Application Key #10		
Application Key #11		
Application Key #12		
Application Key #13		
File Setting	**Fill in by customer**	**Description**
*File ID/Name	??	1 byte - 2 characters from 0 to F
File size	? Bytes	Determine by customer
*Read Card Key #	Which Key?	Choose from Application Keys #1 to #13
*Write Card Key #	Which Key?	Choose from Application Keys #1 to #13
*Read/Write Card Key#	Which Key?	Choose from Application Keys #1 to #13
*Modify Key #	Which Key?	Choose from Application Keys #1 to #13
Encryption	AES128	Choose AES or 3DES

Note:
- Field marked with "*" has to fill in.
- 16 bytes means 32 characters. Each character could be from 0 to F, which means you can choose from 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F. (Hexadecimal)
- Every Desfire card require a Master Key
- Every card supports 28 applications for EV1 and unlimited for EV2
- Every Application can set max of 14 different Application Keys
- Every Application,you can creat up to 16 Files with different size
- For Access Control, only one Application, one File is good enough



Конфигурирование Считывателя **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 использоания карт за рамками системы и может быть использована только для настройки разрешенных считывателей.
- Существует две 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.

Базовые понятия создания архитектуры:

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.

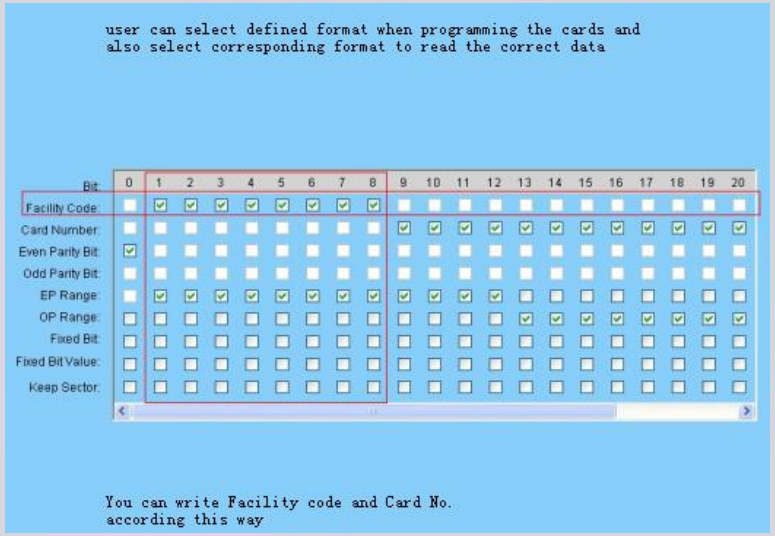
Настройки файловой системы (File Setting):

- **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.

рис 1:



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.

IDETRIS

ΛDVENT
IDETRIS

www.advent-id.com