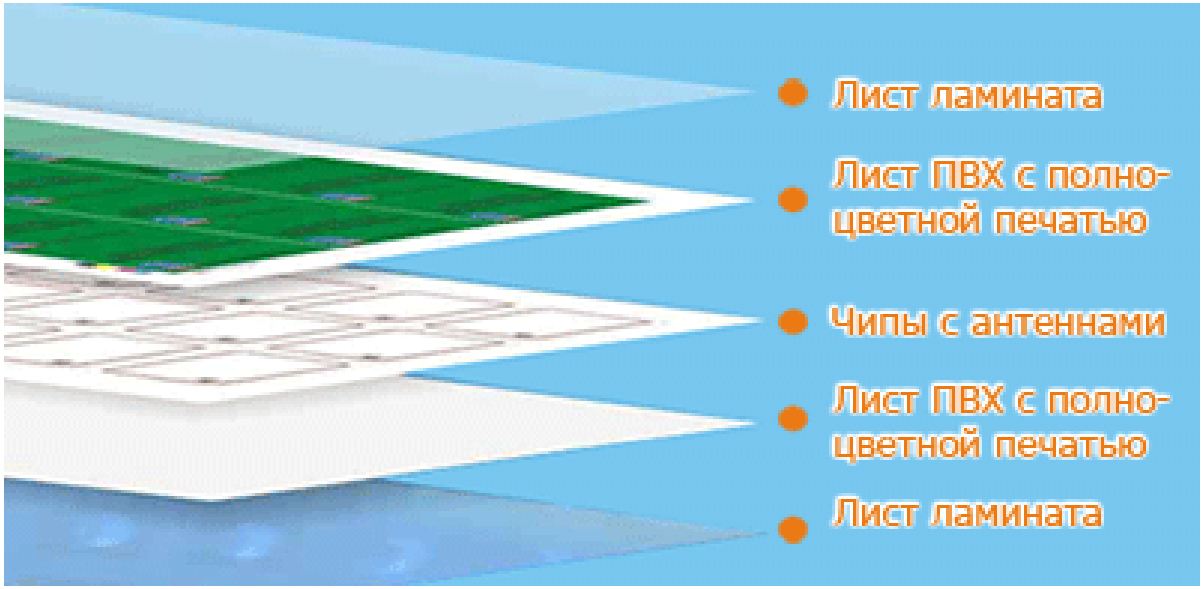
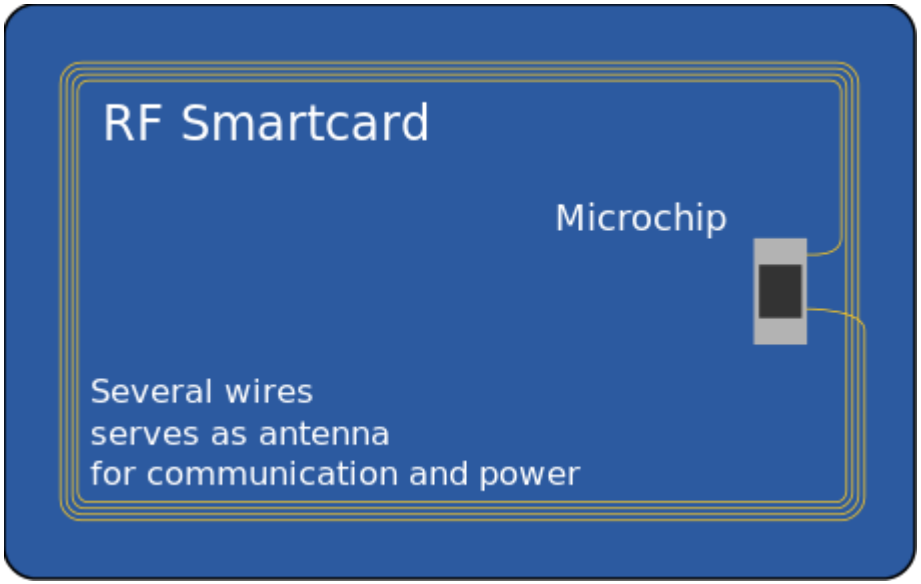
Основы RFID

С точки зрения информационной безопасности

Физическое устройство карты





Физическое устройство чипа

Размер чипа Mifare Ultralight = 0.6x0.6 мм.
100x, металлургический микроскоп BM-158J

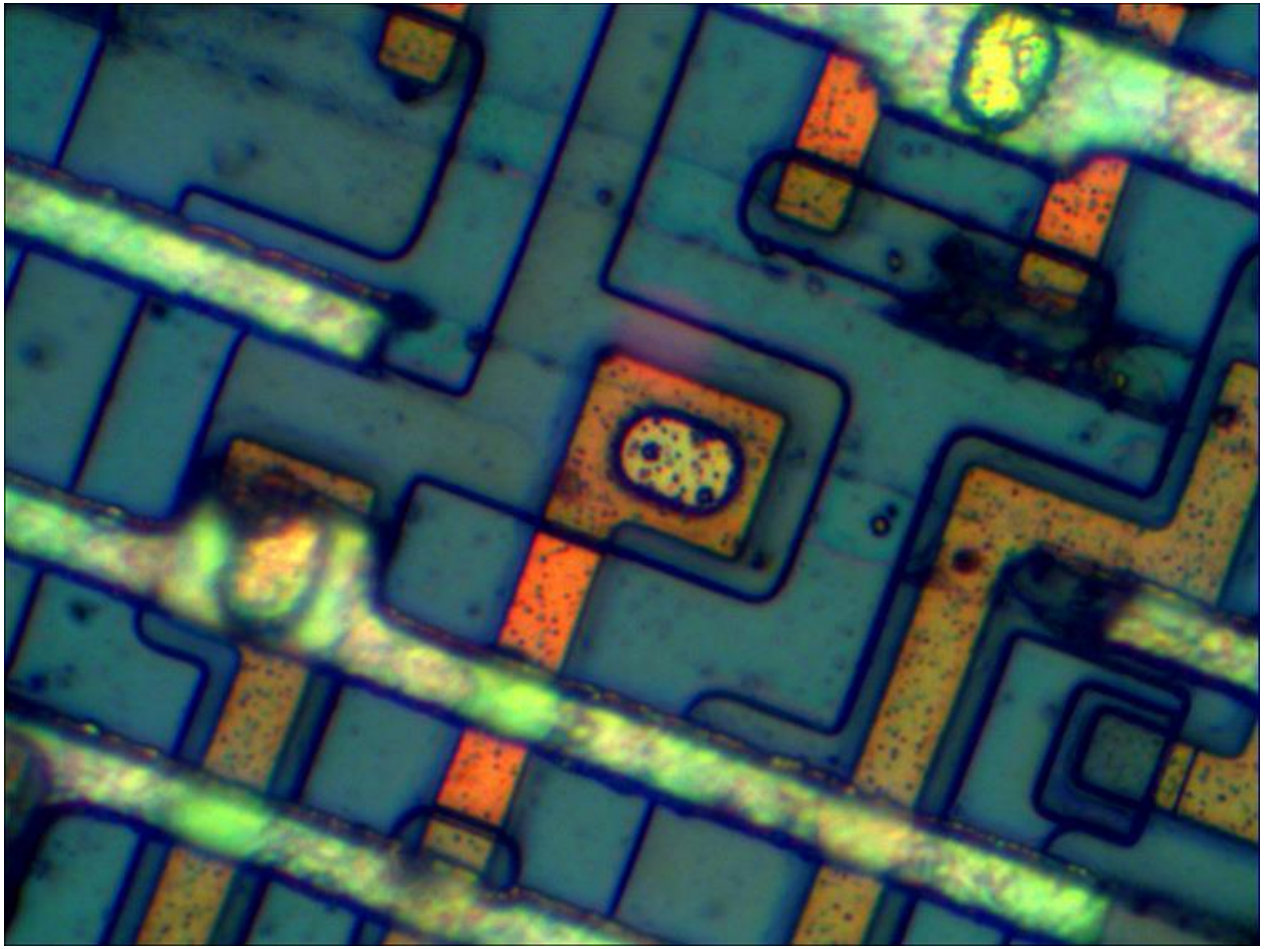


Фото:
Михаил Сваричевский

Физическое устройство чипа

10x, металлургический микроскоп BM-158J

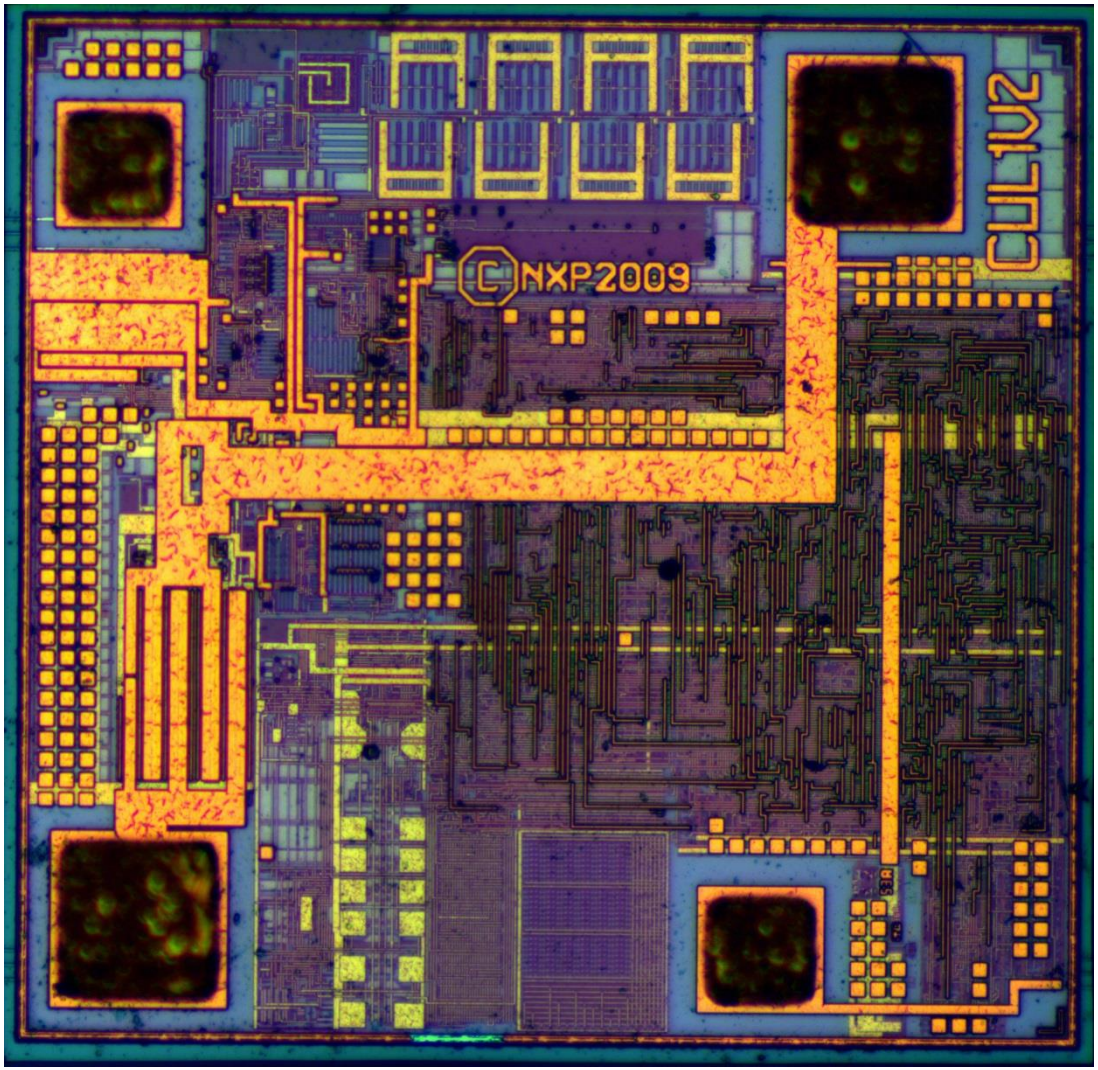


Фото:
Михаил Сваричевский

Области применения RFID

- Инвентаризация
- Контроль доступа
- Удостоверение личности
- Платежные операции
- Передача данных
- …

RFID = ISO18000

- 125–135 kHz (LF)
- **13.56 MHz (HF)** ⟸ NFC
- 433 MHz
- 860–960 MHz (UHF)
- 2.45 GHz

125Khz
EM-Marin и HID®

125Khz
EM-Marin и HID®

Чипы mifare

- Mifare Ultralight (U1x)
- Mifare Ultralight C (V2x)

Устройство памяти Mifare Ultralight

Mifare Ultralight	Mifare Ultralight C
16 стр./4 байт	36 стр./4 байт

Mifare Ultralight	Mifare Ultralight C
16 стр./4 байт	36 стр./4 байт
Нет аутентификации	Triple-DES

Чипы mifare

- Mifare Standard 1k and 4k (S50 and S70)

Устройство памяти Mifare Classic

Mifare Classic 1k	Mifare Classic 4k
16 сект./64 байт	32 сект./64 байт, 8 сект./256 байт

Память читается/записывается блоками по 16 байт

Нулевой блок содержит UID и защищен от перезаписи
Длина UID – 4 (старые чипы) или 7 байт

Последний блок каждого сектора = трейлер сектора

Устройство памяти Mifare Classic

Для чтения/записи блока необходимо пройти аутентификацию в соответствующем секторе.

Проприетарный криптоалгоритм Crypto-1

Трейлер сектора содержит 2 ключа по 6 байт и биты доступа

Ключ А	Биты доступа	Ключ Б
6 байт	3 + 1 байта	6 байт

Транспортные ключи = ключи по умолчанию, заводские:
ff ff ff ff ff ff
a0 a1 a2 a3 a4 a5
a1 a2 a3 a4 a5 a6

Устройство памяти Mifare Classic

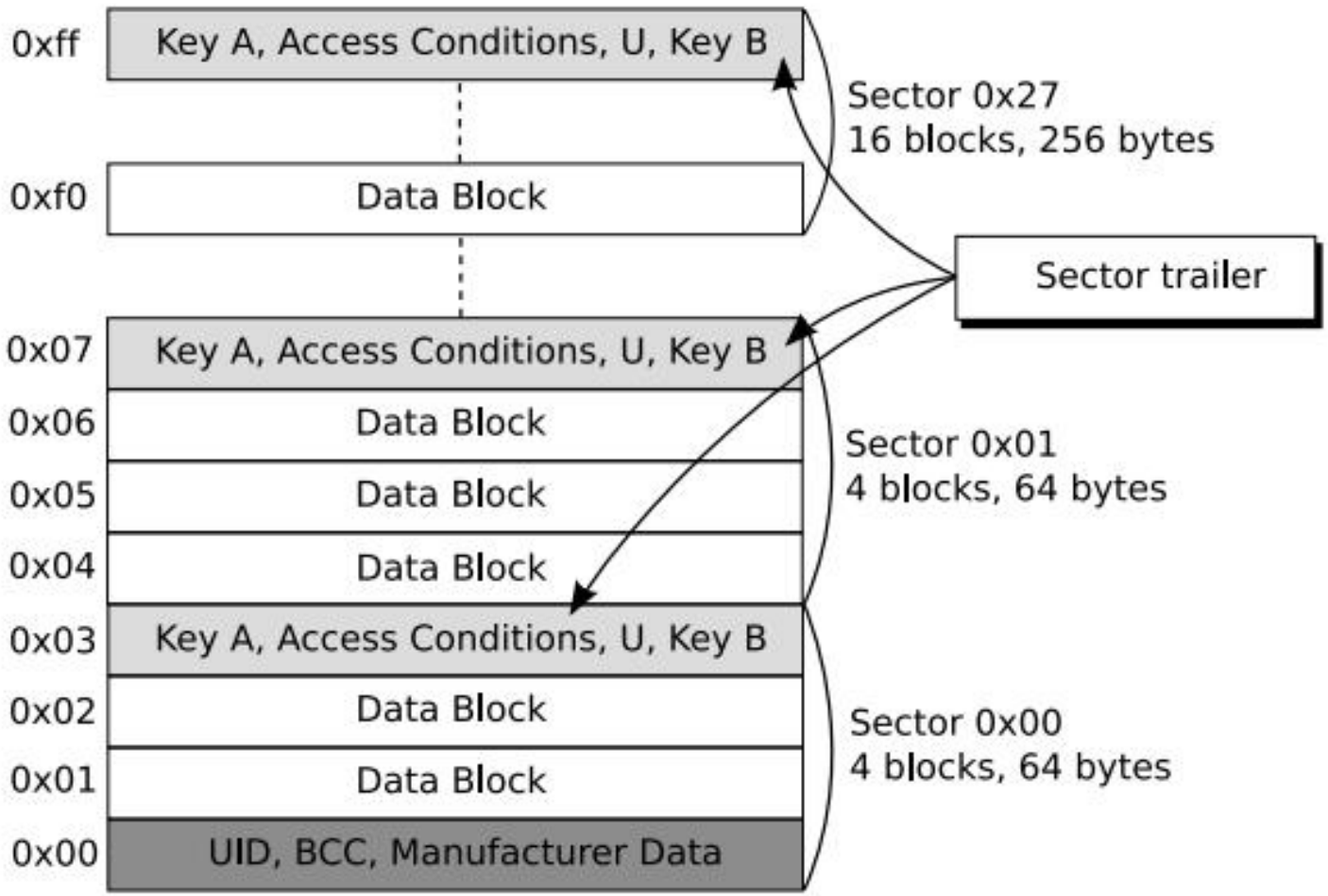


Fig. 1: MIFARE Classic 4k Memory

Скорость передачи данных

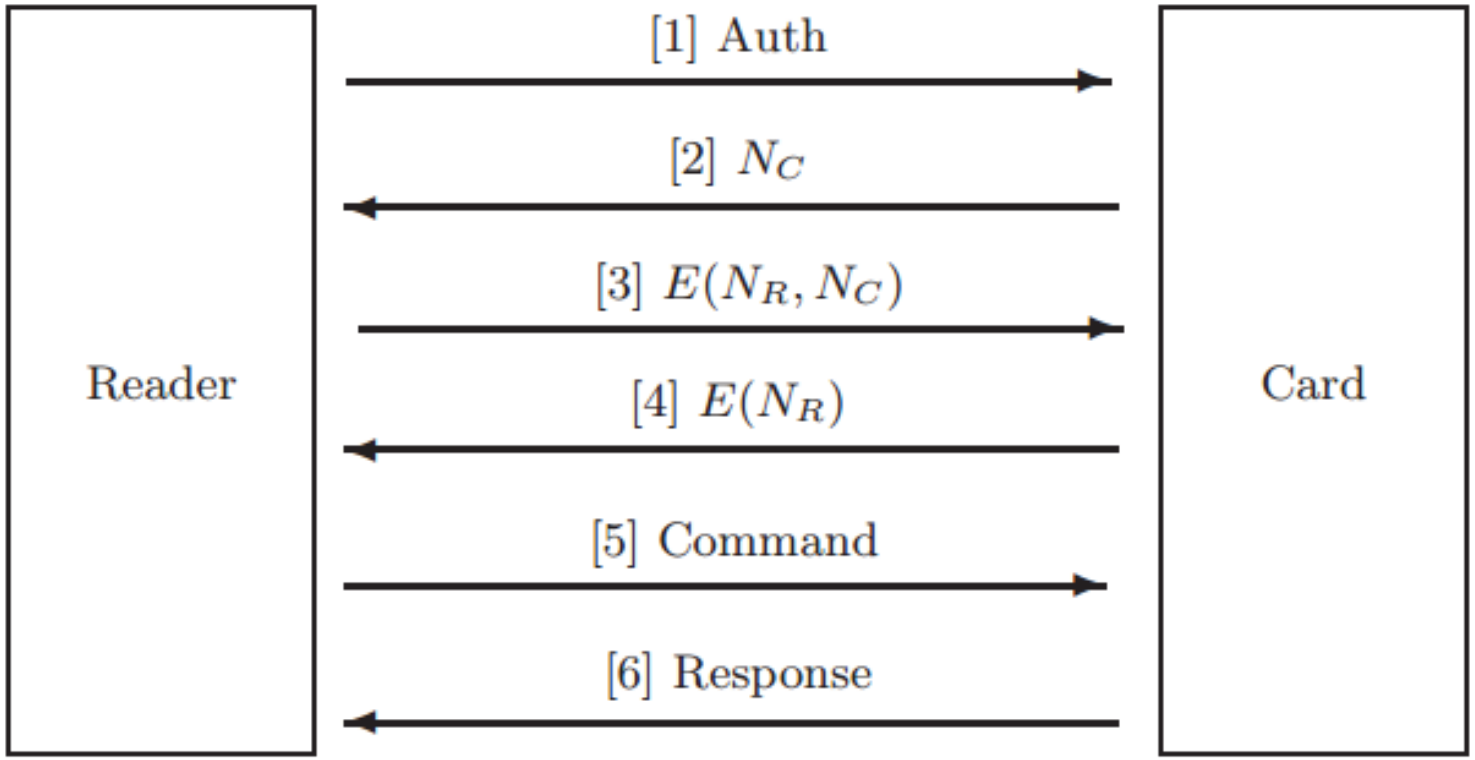
>= 106 kbit/s

- >=1 мс – идентификация карт в зоне и выбор карты для работы
- >= 2 мс – аутентификация в сектор
- >= 2,5 мс – чтение блока
- >= 6мс – запись блока

Команды Mifare Classic

- Аутентификация в сектор
- Чтение/запись блока
- Инкремент/декремент блока-значения
- Push/Pop блока-значения

Аутентификация Mifare Classic



Аутентификация Mifare Classic

ETU	SEQ	who	bytes	
0	01	PCD	26	Anticollision
64	02	TAG	04 00	
12097	03	PCD	93 20	
64	04	TAG	2a 69 8d 43 8d	
16305	05	PCD	93 70 2a 69 8d 43 8d 52 55	
64	06	TAG	08 b6 dd	
16504	07	PCD	60 04 d1 3d	Authentication
112	08	TAG	3b ae 03 2d	
6952	09	PCD	c4! 94 a1 d2 6e! 96 86! 42	
64	10	TAG	84 66! 05! 9e!	
396196	11	PCD	a0 61! d3! e3	Increment & Transfer
208	12	TAG	0d	
8442	13	PCD	26 42 ea 1d f1! 68!	
5120	14	PCD	8d! ca cd ea	
2816	15	TAG	06!	
1349238	16	PCD	2a 2b 17 97	Read
72	17	TAG	49! 09! 3b! 4e! 9e! 5e b0 06 d0!	
			07! 1a! 4a! b4! 5c b0! 4f c8! a4!	

Эмуляция и перехват

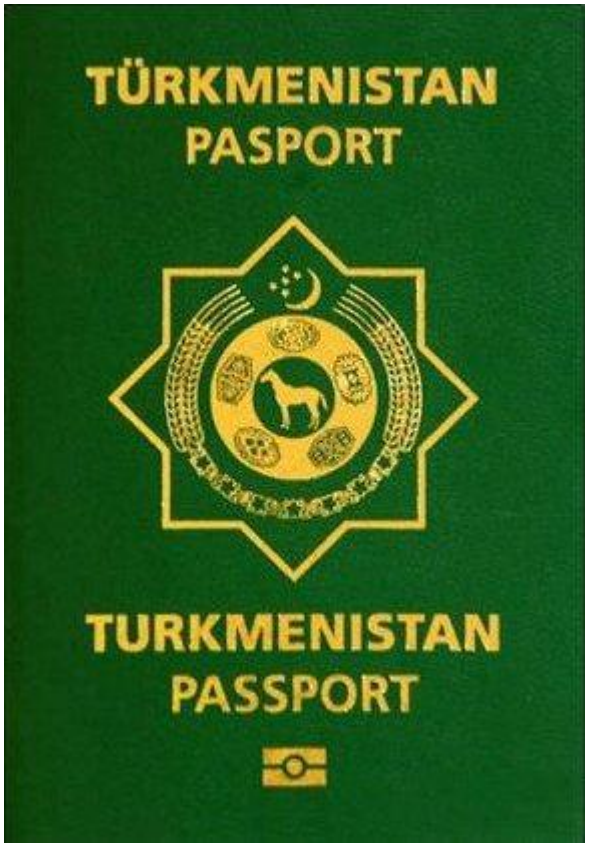
http://www.proxmark3.com/

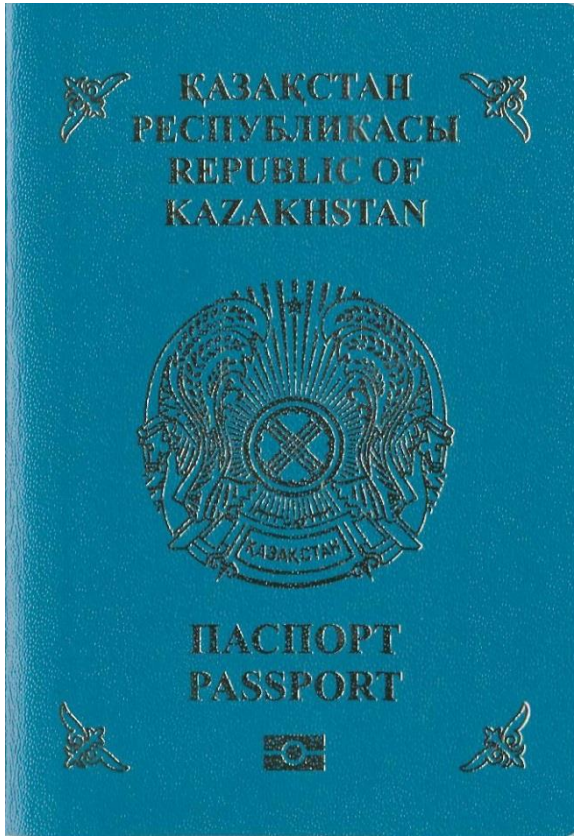
Чипы mifare

- **Mifare Plus**

- **Mifare DESFire EV1**

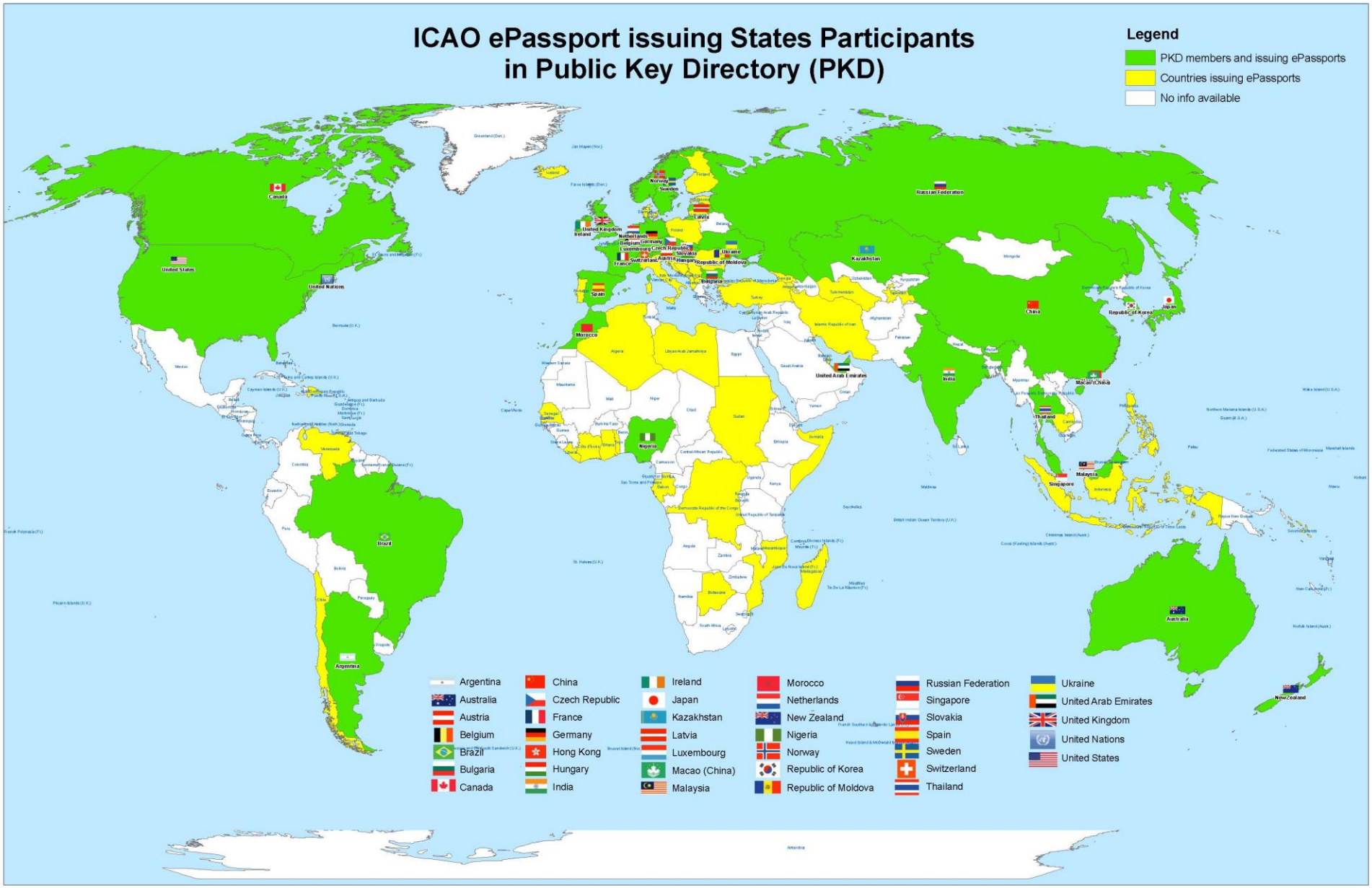
Чипы в паспортах





Поддержка ISO 14443

Страны, использующие паспорта с чипом в 2012 г.



Чипы в паспортах:
Что внутри?

EEPROM >= 32Kb

Хранит паспортные данные и фотографию лица

Опционально фотографии сетчатки
и отпечатков пальцев

(Фотографии ~ 15kb в формате JPEG/JPEG2000)

Чипы в паспортах: первичные функции

Проблема:
UID позволяет следить за носителем

Решение:
Случайный UID на каждую активацию

Чипы в паспортах: первичные функции

Проблема: Подмена данных на чипе

Решение:
Passive Authentication: на чипе хранится перечень хешей всех файлов и цифровая подпись этих хешей (подписывается гос. органом страны выдачи). Список публичных ключей стран хранится в **ICAO Public Key Directory (PKD)**

Чипы в паспортах: опциональные функции

Basic Access Control – симметричное шифрование.

Ключ генерируется из даты рождения, номера документа и даты истечения срока действия

K = 3DES*(SHA1*(MRZ_DATA))

MRZ

Чипы в паспортах: опциональные функции

Active Authentication:

На чипе хранится ключевая пара RSA.

Приватный ключ недоступен для чтения извне.

Терминал отправляет challenge и проверяет его с помощью публичного ключа чипа.

Чипы в паспортах:
Что внутри?

EEPROM >= 32Kb

Хранит паспортные данные и фотографию лица

Опционально фотографии сетчатки
и отпечатков пальцев

(Фотографии ~ 15kb в формате JPEG/JPEG2000)

Чипы в паспортах: опциональные функции

Extended Access Control:

Аутентификация чипа**:**

Терминал с цифровой клавиатурой и дисплеем

Дополнительный слой шифрования над BAC

Аутентификация считывателя:

Сертификат для терминала, действующий короткий промежуток времени

Чипы в паспортах: Известные атаки

Атаки на случайно генерируемый UID

Определение страны-эмиттера:

2008 “Fingerprinting Passports”
Henning Richter, Wojciech Mostowski, Erik Poll

Определение конкретного документа:

2010 "A Traceability Attack Against e-Passports”
Tom Chothia and Vitaliy Smirnov"

2010 "Defects in e-passports allow real-time tracking”
Dan Goodin

Чипы в паспортах: Известные атаки

Basic Access Control

Чтение данных на паспортах без BAC:

2007 "Belgian Biometric Passport does not get a pass"
Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater

Сокращение числа возможных ключей BAC:

2005 “Attacks on Digital Passports”
Marc Witteman

Чипы в паспортах: Известные атаки

Passive Authentication

Клонирование паспорта без PA:

2006 “Hackers Clone E-Passports”
Lukas Grunwald

Использование самоподписанного списка хешей:

2008 "‘Fakeproof’ E-Passport is Cloned in Minutes"
Jeroen van Beek

Чипы в паспортах: Известные атаки

Active Authentication

Получение приватного ключа по побочному каналу:

2005 “Attacks on Digital Passports”
Marc Witteman

Отключение проверки AA (downgrade):

2009 ePassports reloaded
Jeroen van Beek

Чипы в паспортах: Известные атаки

Extended Access Control

Отказ в обслуживании:

2007 “Security by Politics - цwhy it will never work”
Luks Grunwald

Golden Reader Tool

Picture

Facial Image

< >

Personal Data

Name	Surname
ELVIS AARON	PRESLEY
Date of Birth (dd.mm.yy)	Nationality
08.01.35	United States
Sex	Valid until (dd.mm.yy)
Male	16.08.77
Document Number	Document Type
TH4P3LV1S	P
Issuer	Optional Data
United States	

Printed MRZ

```
P<USAPRESLEY<<ELVIS<AARON<<<<<<<<<<<<<<<<<<<<
TH4P3LV1S1USA3501081M7708165<<<<<<<<<<<<<<04
```

Operation

- Autodetect
- Read
- Read BAC / EAC
- Read from Disk
- Write to Disk
- Reset Display
- About...
- Options
- Configuration
- Close

Access Control

- BAC
- Chip Authentication
- EAC
- Terminal Authentication
- Active Authentication

Chip Data

UID	ATR/ATS	ISO-14443
n/a	3b8a80014a434f503431563232317f	n/a

Reading time: 7.86 Seconds

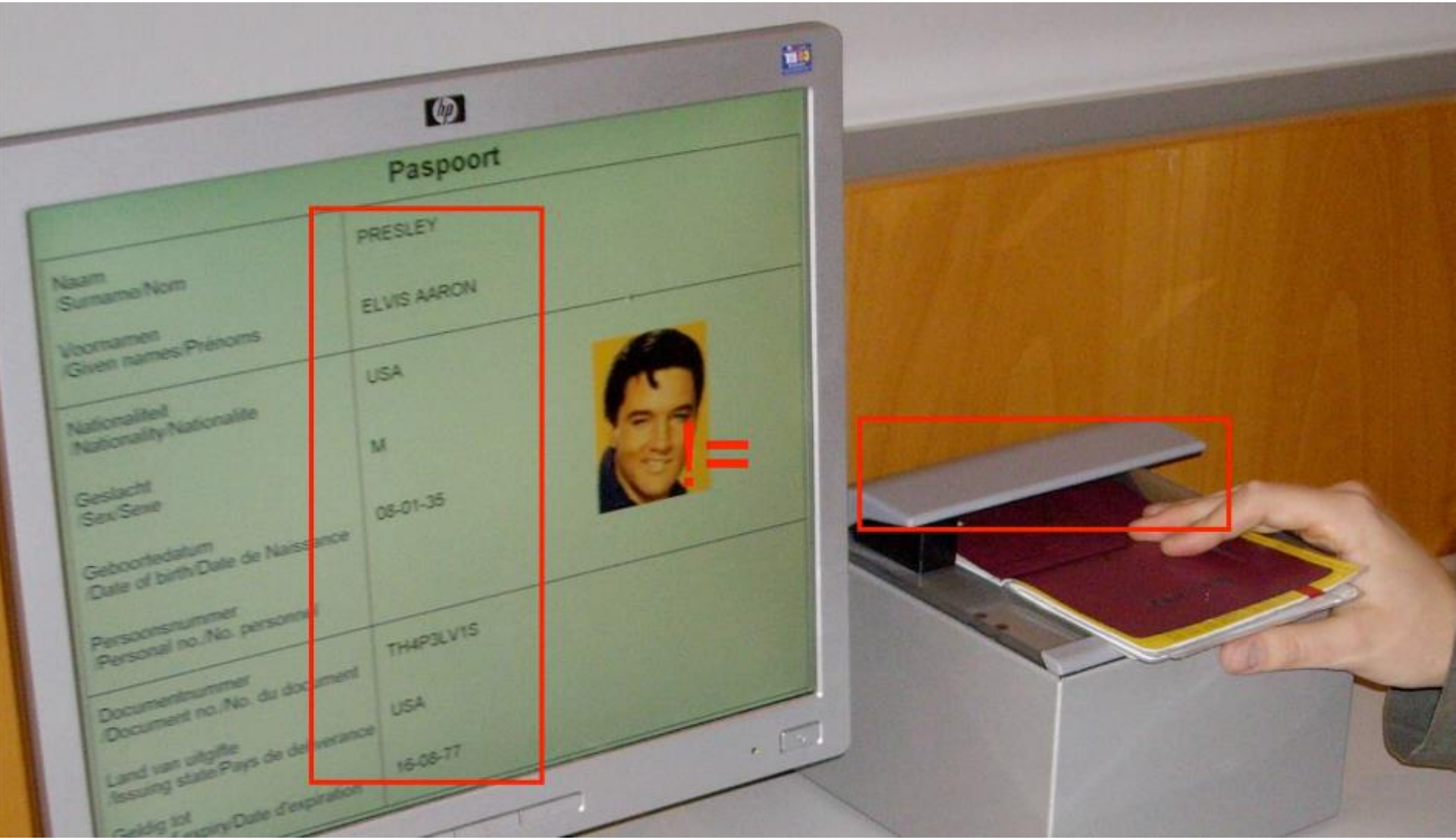
Passive Authentication

DG1 ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ DG16

- Signature EF.SOD
- Algorithm RSA / SHA256
- Certificate-Chain
- Revocation

Logging

```
7.75    : Size EF_DG2: 14302 Bytes.
7.75    : DG2 read successfully.
7.75    : Hash Datagroup 2 OK.
7.75    : CBEFF Format Type 0008
7.78    : Facial Image Type 0000
7.81    : Image data type: JPEG
7.86    : The overall size is 19633
7.88    : The average reading speed was 19.99 kpbs.
```


Paspoort
PRESLEY
ELVIS AARON
USA
M
08-01-35
THAPSLV1S
USA
16-08-77
!=

Спасибо

peter.r.volkov@ya.ru