

MAGS TRIP EMAD NESS

VALID FROM

05/06

EXPIRES END

44/20

OF-3

MALFUNCTION, MAJ.

UNCON

ISSUER

0x09

ISSUE

DC-44-20

SORT CODE



who am i ?

- security professional by day
- white hat hacker by night, weekends & when traveling..
- DEFCON goon
- DC4420 P.O.C. (London)



why mag stripe ?

- old skool
- thoroughly insecure and yet still in use
- security by obscurity (again!)
- because it's there
- i have no life



SCORE 1689

LIVES 



FW



AV

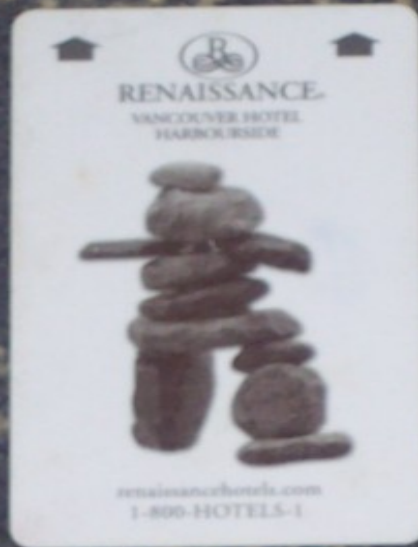


IDS

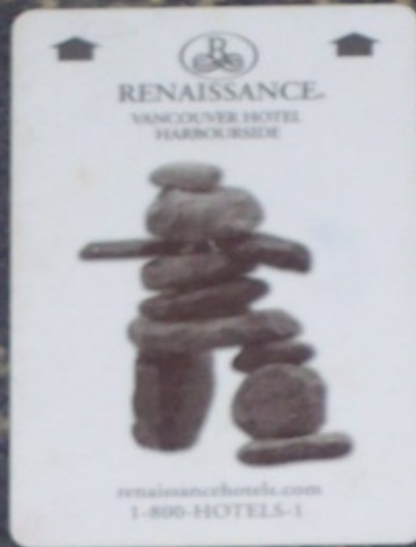


PEAKFLOW X

swipe cards



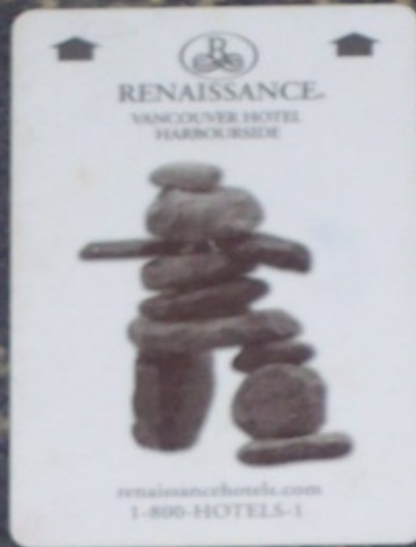
spot the room key...



spot the room key...



spot the ATM card...



spot the ATM card...



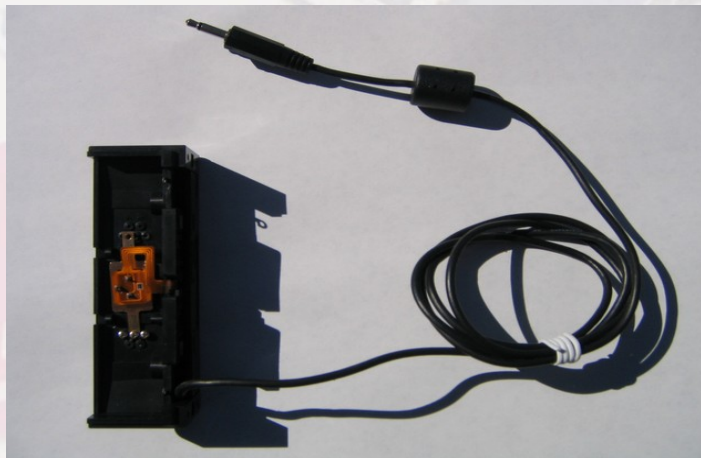
equipment - makstripe

- <http://www.makinterface.de>
- Parallel port
- Read / Write all 3 tracks
- Raw data
 - Does not care about checksums
 - Does not care about parity
- Windows support only :(
 - Doesn't work with VMWare :(:(

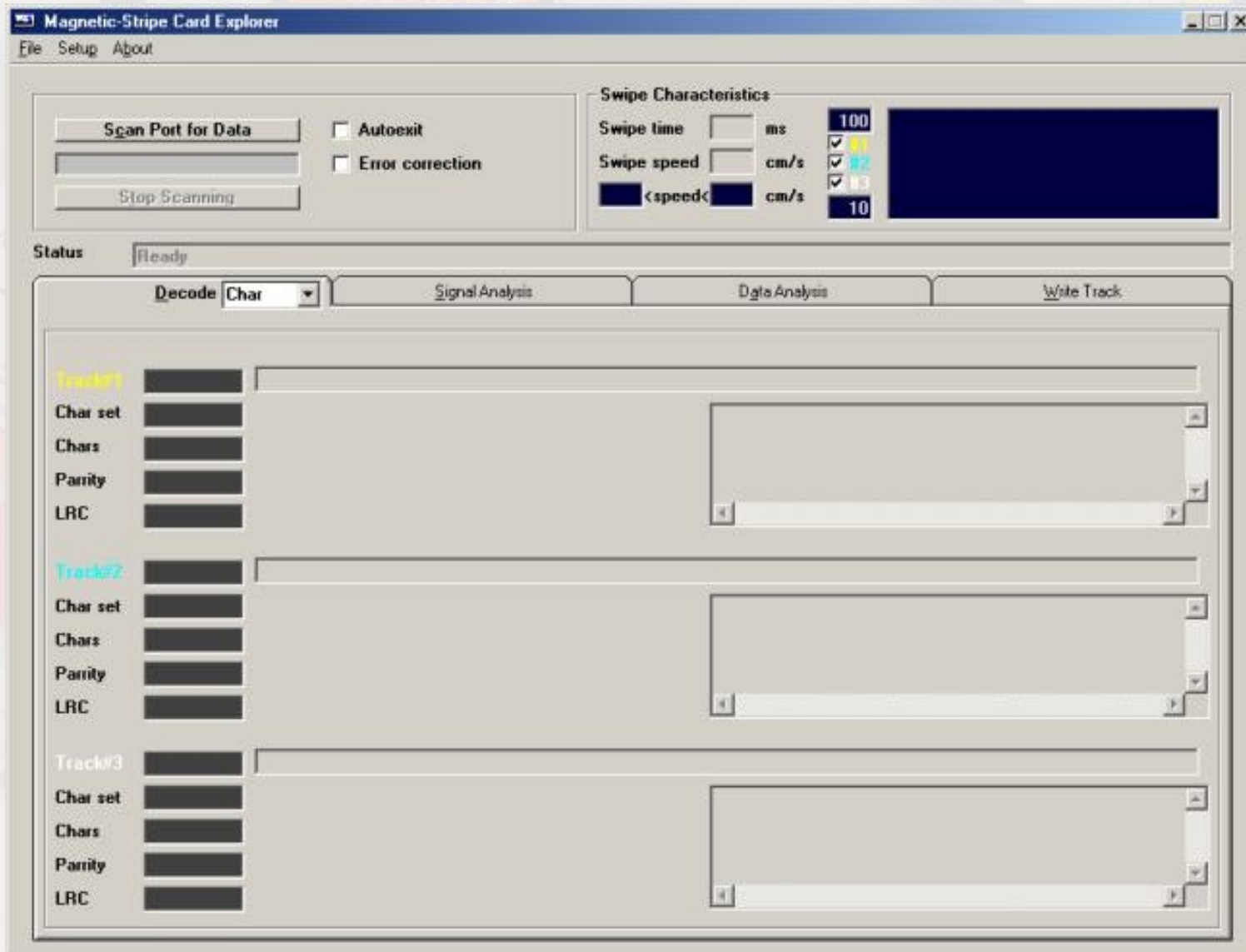


equipment

- <http://www.sephail.net/articles/magstripe>
- **Audio output**
 - Analyse WAV files offline
- **Read all 3 tracks plus non-standard**
- **Raw data**
 - Does not care about checksums
 - Does not care about parity
- **Read only**



equipment - makstripe



equipment - makstripe

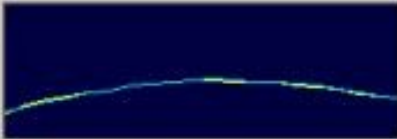
Magnetic-Stripe Card Explorer

File Setup About

Scan Port for Data Autoexit
 Error correction
Stop Scanning

Swipe Characteristics

Swipe time: 211 ms **100**
Swipe speed: 40 cm/s **27** <speed> **50** cm/s **10**



Status: Idle

Decode Char Signal Analysis Data Analysis Write Track

Track#01 **210 BPI** :xB4779 4^ ^02011 4000000000 300 00?5

Char set: **ALFA** B4779 4

Chars: **79** ✓

Parity: **Ok** 0201 11 0000 030 000

LRC: **Ok**

Start Sentinel: %
Data: B4779 4
Field Separator: ^
Data:

Track#02 **76 BPI** :47791 4-0201 11 0000?1

Char set: **BCD** 4779 14

Chars: **40** 020 11 0000

Parity: **Ok**

LRC: **Ok**

Start Sentinel: ;
Data: 4779 14
Field Separator: =
Data: 020 11 0000

Track#3

Char set

Chars

Parity

LRC



equipment - makstripe

Magnetic-Stripe Card Explorer

File Setup About

Scan Port for Data Autoexit
Stop Scanning Error correction

Swipe Characteristics

Swipe time: 211 ms 100
Swipe speed: 40 cm/s 10
27 <speed> 50 cm/s 10

Status: Ready

Decode Binary Signal Analysis Data Analysis Write Track

Track#1 210 BPI :B4779 4 ^02011 11 00000000 :30 000?S

Char set: ALFA
Chars: 79
Parity: Ok
LRC: Ok

Track#2 76 BPI :4779 4-02011 11 :30000: 1

Char set: BCD
Chars: 40
Parity: Ok
LRC: Ok

Track#3

Char set:
Chars:
Parity:
LRC:



analysis - makstripe

Decode Signal analysis Data analysis Write track

Get data from

- Track#01
- Track#02
- Track#03

Total number of bits: Examine: bits per Character Total parity errors:

First bit found at position: Start with bit position: Last valid LRC is at:

Last bit found at position:

```

0c000c000c00c000c000c0010c0c0c010110000c011c
0c101c1c0c1c1000c0011001c10110011c0c000c1c0000110
0c0001001c1c101c0c0110011c0c01100c000c100101100
1c0c1c1000c001001c1c0c1001101000c1c1100010c10c011c
1c0001100c1010c11110c100c1c1001c100c101100100110c
0c0011001c1c1c101c0c000c0c1001c10110011100000c10
1c0c01100c101000c100c000c0c100c1c0c00111c00c0100
111c1c1c0c0c1c00010c11000c1c1001101c00011c1000100
010c1c1010c0c0c0c1c0000c0c110011c1c001000101100
0c000110010c1c0c1c1000c0c1000c1c10110110011100111c
0c101c0c111c0c000c100100010c10010c11001c000101c1c
010c0c0c1c10c1c1c101c00110c1001100111c1c000c1c1110
0c000c000c00c000c000c00c
    
```

Char	Bits	from bit	to bit	parity	LRC
1	1010001	28	34	Ok	-
2	0010110	35	41	Ok	-
3	0001011	42	48	Ok	-
4	1001010	49	55	Ok	-
5	1100111	56	62	Ok	-
6	0000001	63	69	Ok	-
7	1001010	70	76	Ok	-
8	1100111	77	83	Ok	-
9	0000001	84	90	Ok	-
10	1000011	91	97	Ok	-
11	0000001	98	104	Ok	-
12	0010110	105	111	Ok	-
13	1111100	112	118	Ok	-
14	1111100	119	125	Ok	-
15	1111100	126	132	Ok	-
16	1111100	133	139	Ok	-
17	1111100	140	146	Ok	-

Examine: bits per Character Total parity errors:

Start with bit position: Last valid LRC is at:

Char	Bits	from bit	to bit	parity	LRC
32	00001	198	202	Ok	-
33	00001	203	207	Ok	-
34	00001	208	212	Ok	-
35	00001	213	217	Ok	-
36	00001	218	222	Ok	-
37	00001	223	227	Ok	-
38	00001	228	232	Ok	-
39	11111	233	237	Ok	-
40	01110	238	242	Ok	01110
41	00000	243	247	Invalid	-
42	00000	248	252	Invalid	-
43	11010	253	257	Ok	-
44	10101	258	262	Ok	-
45	10000	263	267	Ok	-
46	00001	268	272	Ok	-
47	10000	273	277	Ok	-
48	11001	278	282	Ok	-



write - makstripe

Magnetic-Stripe Card Explorer

File Setup About

Scan Port for Data Autoexit
 Error correction
Stop Scanning

Status Ready

Decode Signal Analysis Data Analysis **Write Track**

Source data Destination Reference Track Prepare to write Write data to Track

Track#1
 +
 Track#2
 +
 Track#3
 Custom

Track#1
 Track#2
 Track#3

Track#1
 Track#2
 Track#3

Erase #1 eBASE
Format Reference Track #2
Duration 4 seconds

0/1 adj.
BPI adj.
Write Track
 Swipe speed=Ref.

Custom data

Data

Auto properties Copy from Track Insert special chars Data properties

Copy Load Save

Track#1
 Track#2
 Track#3

Start Sentinel
Field Separator
End Sentinel
Insert LRC

Nr. of Chars Total nr. of Bits 252
Character set BCD Bits before data 84
BitsPerInch 75 Bits in data 0
 recalculate LRC Bits after data 168



standard track formats

- **track 1**
 - IATA - 210 BPI, 7 bit, 79 alphanumeric characters
- **track 2**
 - ABA - 75 BPI, 5 bit, 40 numeric characters
- **track 3**
 - THRIFT - 210 BPI, 5 bit, 107 numeric characters



track standards - IATA



Track 1: 210 BPI, 7 bit, 79
Alphanumeric characters



track standards - IATA

Data format

Airport

Flight No.

Day of year

Start

Format

From

To

Flight

Class

Day

Seat

Passenger

End

LRC



track standards - IATA

YVR

LHR

19K

LAURIE/ADAM MR

Start

Format

From

To

Flight

Class

Day

Seat

Passenger

End

LRC

%WYVRLHRBA 0084 W 034019K LAURIE/ADAM MR ?E



after

Magnetic Stripe Card Explorer

File Setup About

Scan Port for Data Autoexit
 Error correction
Stop Scanning

Swipe Characteristics

Swipe time 277 ms 100
Swipe speed 30 cm/s #1
24 <speed> 39 cm/s #2
 #3
10

Status: Ready to read - Card can be swiped

Decode Char Signal Analysis Data Analysis Write Track

Track#1 166 BPI %'OR 1=1;UPDATE FLT SET SEAT='1A' WHERE P='LAURIE/ADAM MR';?=
Char set ALFA 'OR 1=1;UPDATE FLT SET SEAT='1A' WHERE P='LAU Start Sentinel : %
Chars 69 Data : 'OR 1=1;UPDATE FLT SET SEAT='1A' WHERE
Parity Ok P='LAURIE/ADAM MR';
LRC Invalid = LRC :

Track#2
Char set
Chars
Parity
LRC

Track#3 135 BPI
Char set Unknown
Chars
Parity
LRC

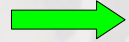


hotel door locks

- **passive**
 - all logic in the lock
- **active**
 - reader only
 - all logic on back-end
 - centralised alarms & reporting



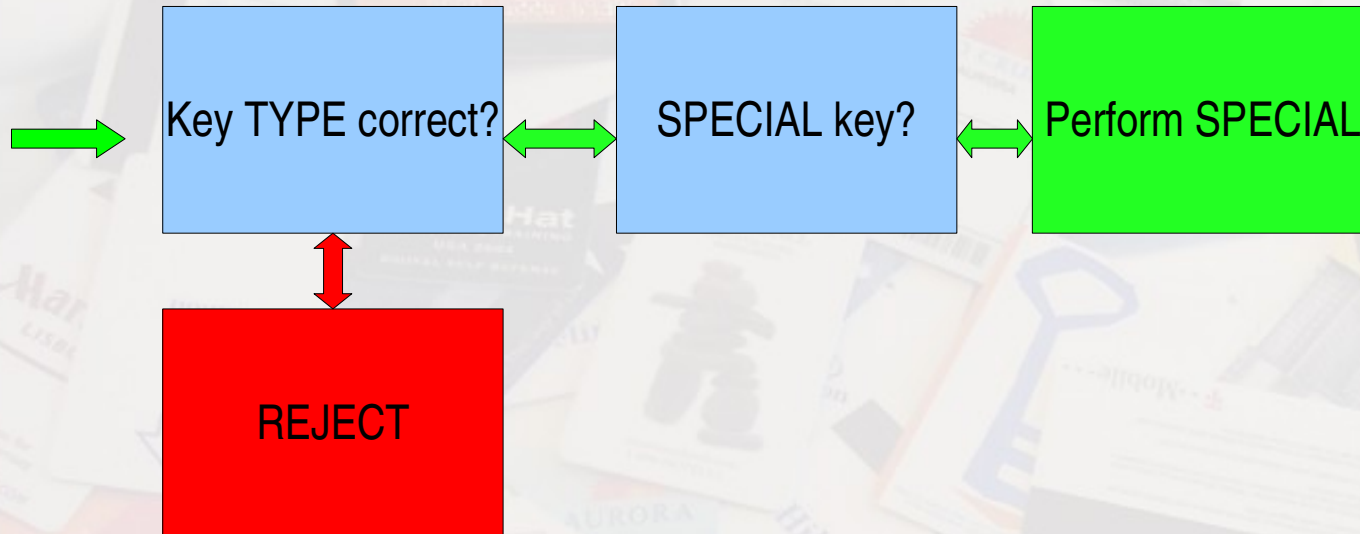
passive locks



Key TYPE correct?



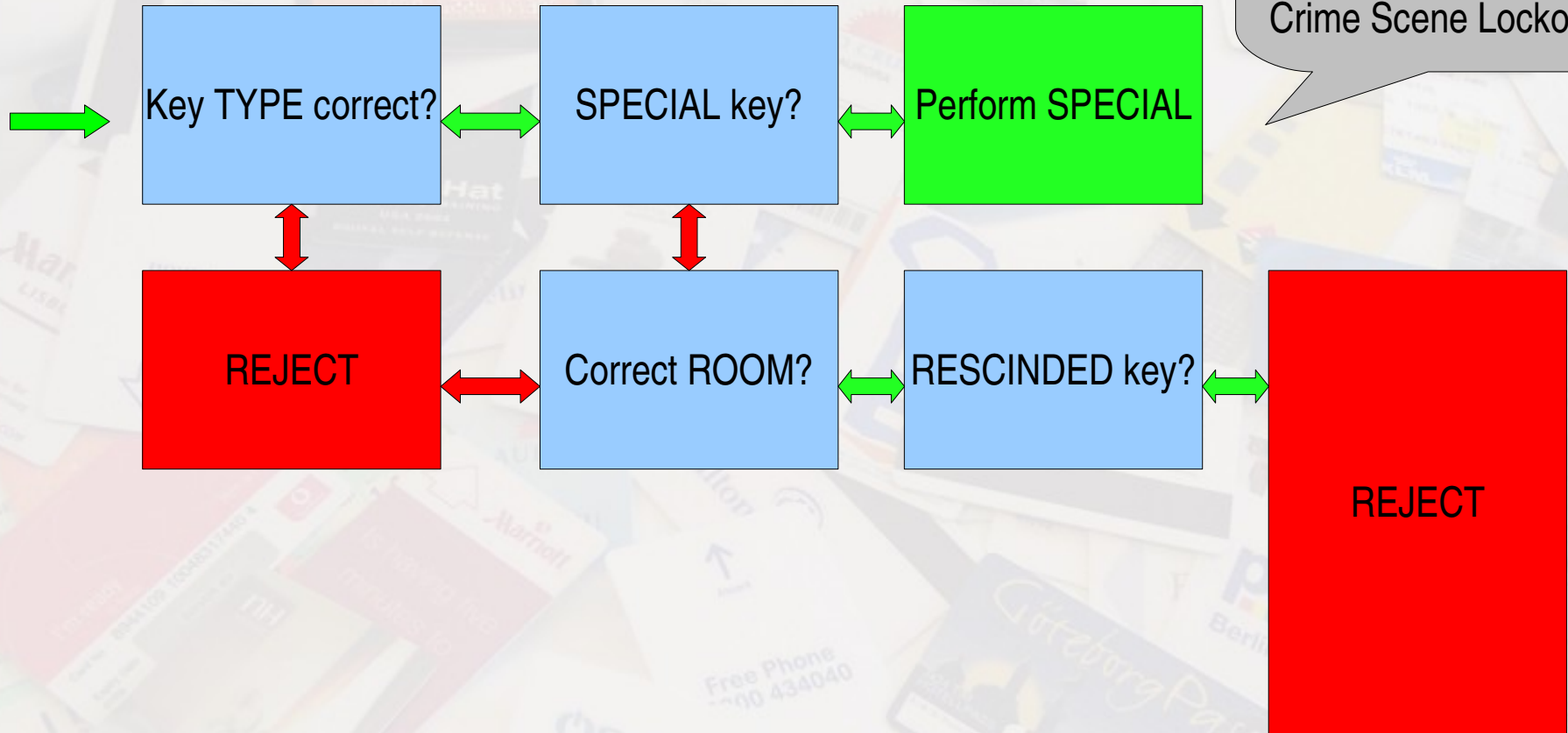
passive locks



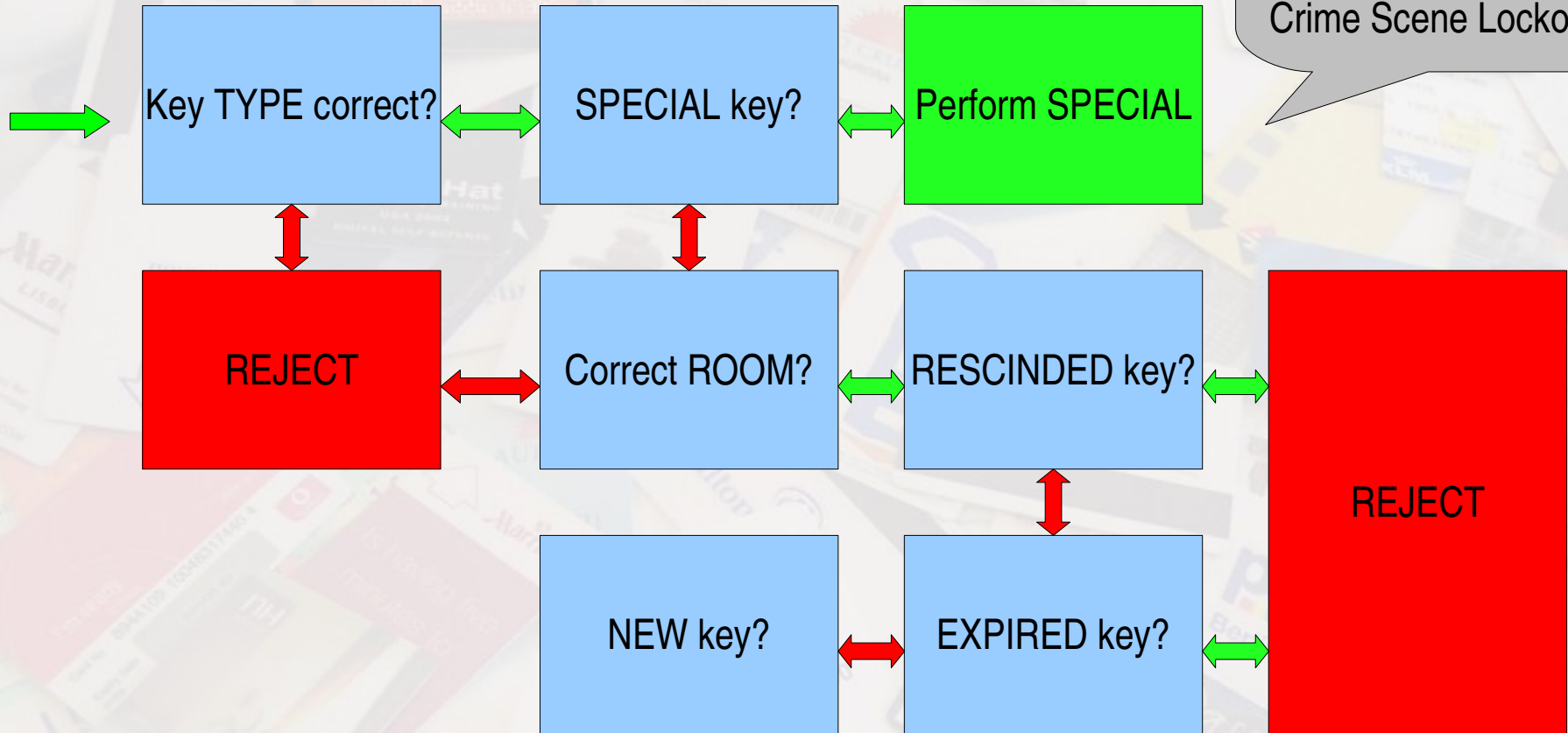
- Housekeeping Open
- One-Time Open
- Guest Lockout
- Crime Scene Lockout



passive locks



passive locks

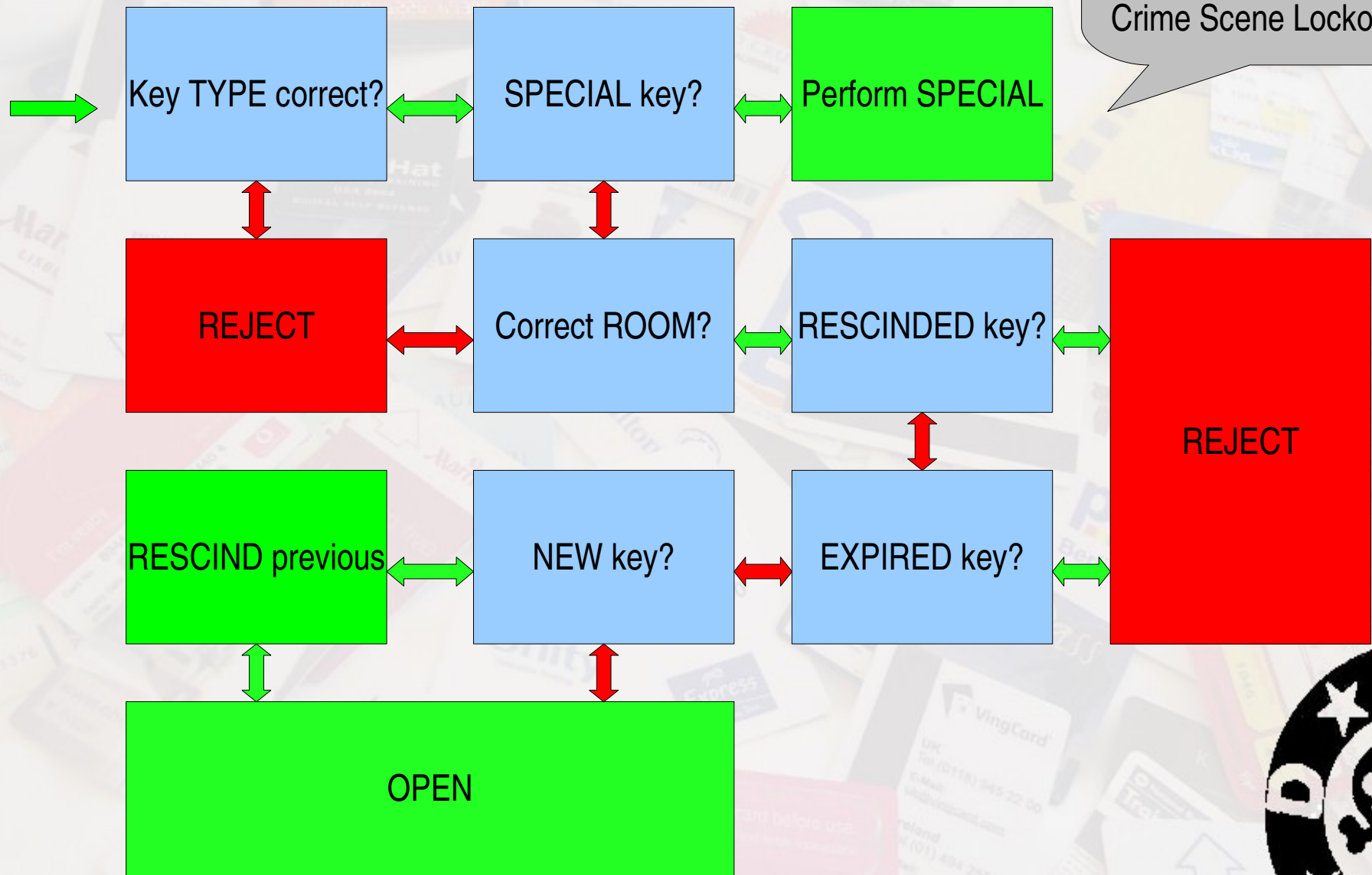


Housekeeping Open
One-Time Open
Guest Lockout
Crime Scene Lockout



passive locks

- Housekeeping Open
- One-Time Open
- Guest Lockout
- Crime Scene Lockout



keycard – multiple keys

- ;51011535280101766301250001200000000000?8
- ;51011535280201766301250001200000000000?;

Start	Property?	Room No.	Key No.	Magic Number?	Expire	Key Type?	End	LRC
;	510115	3528	01	01766	30125	0001200..	?	8
;	510115	3528	02	01766	30125	0001200..	?	;



keycard – new key!

- ;51011535280101766301250001200000000000?8
- ;51011535280201766301250001200000000000?;
- ;51011535280301766301250001200000000000?:

Start	Property?	Room No.	Key No.	Magic Number?	Expire	Key Type?	End	LRC
;	510115	3528	01	01766	30125	0001200..	?	8
;	510115	3528	02	01766	30125	0001200..	?	;
;	510115	3528	03	01766	30125	0001200..	?	:



keycard – rescinding

- ;51011506110107004311250001200000000000?6
- ;51011506110107032311250001200000000000?3

Start	Property?	Room No.	Key No.	Magic Number?	Expire	Key Type?	End	LRC
;	510115	0611	01	07004	31125	0001200..	?	6
;	510115	0611	01	07032	31125	0001200..	?	3



RESCINDING keys

New magic number

12345



Lock stores
last 100 keys

85123

56787

23677

...



active locks

- **all locks connected to central computer**
 - one wire
- **checking done against live database**
- **key swipe as messaging system**
 - room clean, out of service etc.
- **security**
 - access attempts
 - raise alarm!
 - audit trail
- **much more expensive**
 - harder to retrofit



non-standard stripes



non-standard equipment



magnasee

- **magnetic field visualisation**
- **head alignment**
 - audio
 - 1/2" Tape
 - lead-in
- **Carbon Tetrachloride!**
 - (carbon chloride, methane tetrachloride, perchloromethane, tetrachloroethane, or benziform)
 - + iron filings
 - banned as a carcinogen!! =:0



magnasee



magnasee

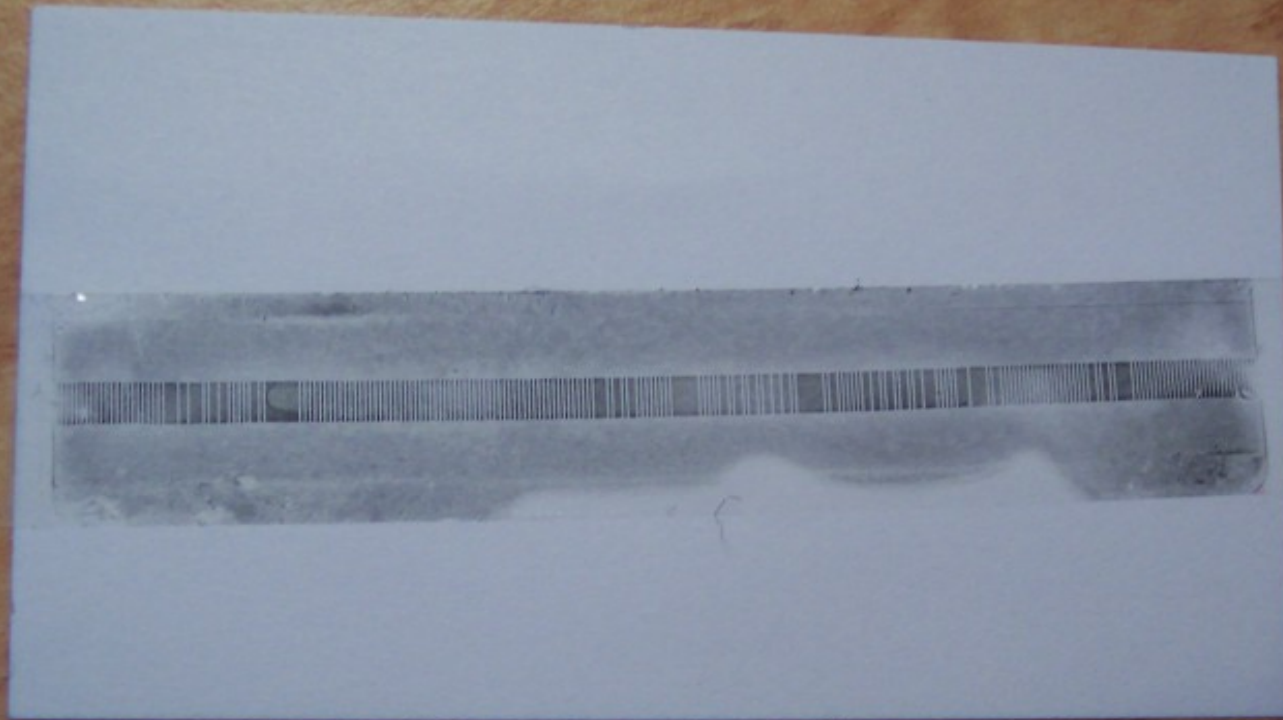


Companies' trains is subject to the

magnasee



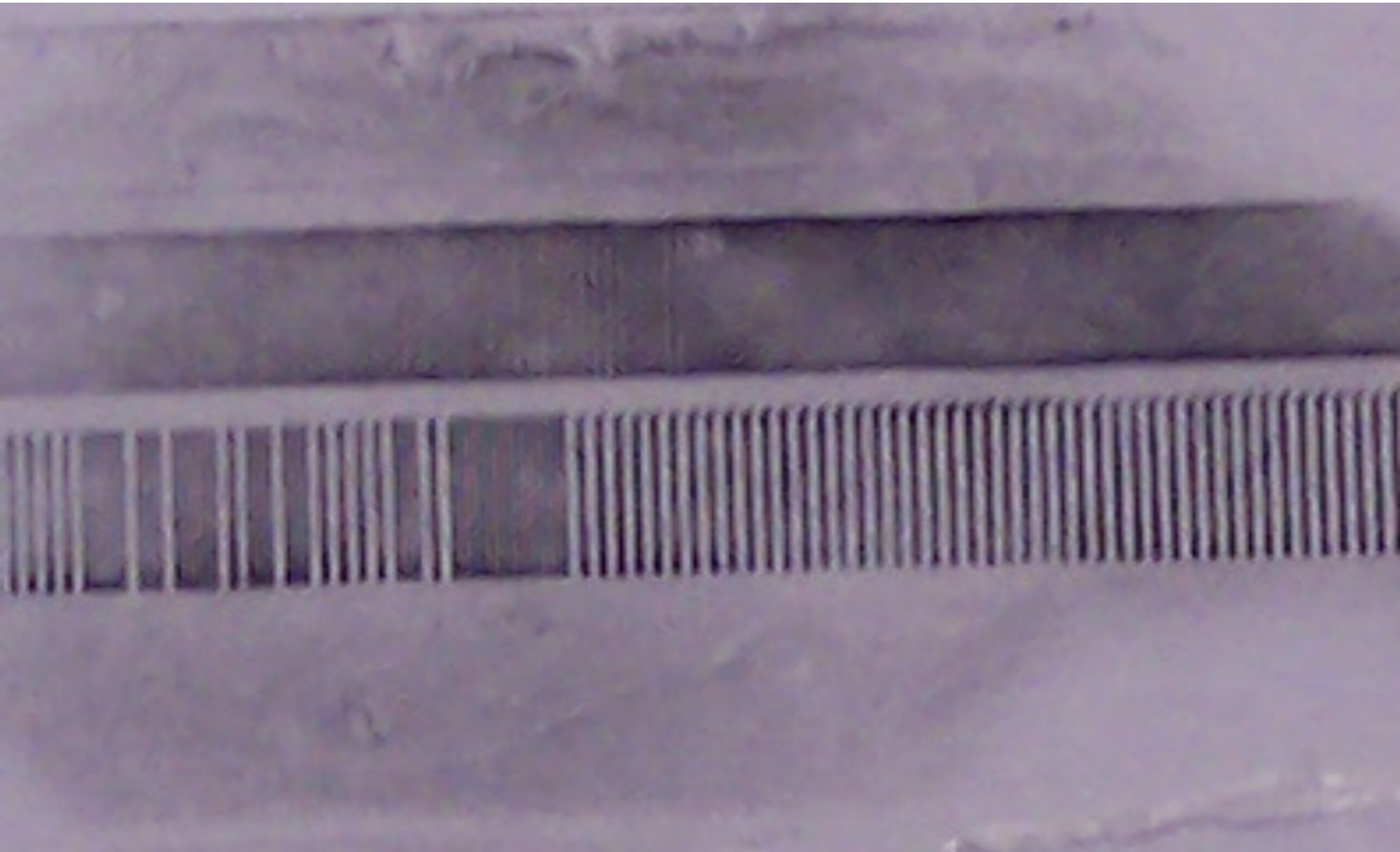
magnasee





magnasee

magnasee

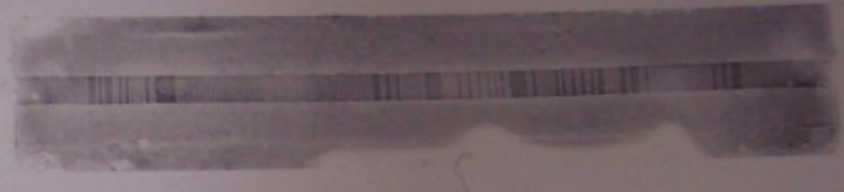


size matters!

British Rail



K-west



Chip and PIN

Chip and **PIN** is coming.
Do you know
your pin number?

Travel on Train Companies' trains is subject to the National Rail Conditions of Carriage and to the conditions of carriage of other operators on whose services this ticket is valid. This ticket is not transferable. Unless otherwise stated, it may be used on any Train Company's trains by any Permitted Route, and if marked "+", on London Underground trains between Train Company stations via any recognised route appropriate to the through journey being made but it is not available for joining or alighting at an intermediate LRT Underground station.

Names of the Train Companies, copies of the National Rail Conditions of Carriage and details of Permitted Routes are available at Ticket Offices.

RSP No. 9599

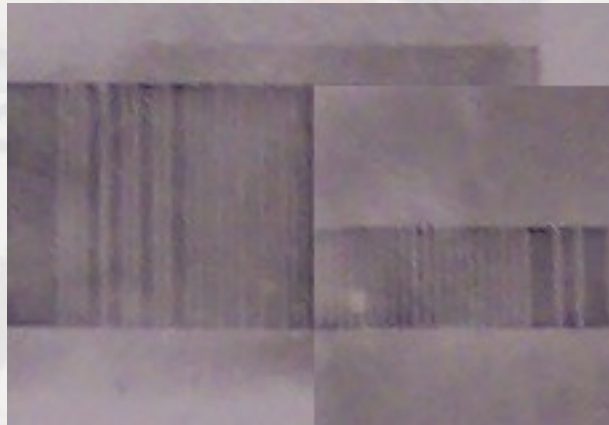
5 BB 1305 9 8 7 6

THIS EDGE IN SLOT



K WEST
RICHMOND WAY
LONDON W14 0AX
TEL +44 (0)20 7674 1000
FAX +44 (0)20 7674 1050
www.k-west.co.uk

size matters!



**British Rail track is 2.5 times the width
of ISO standard**



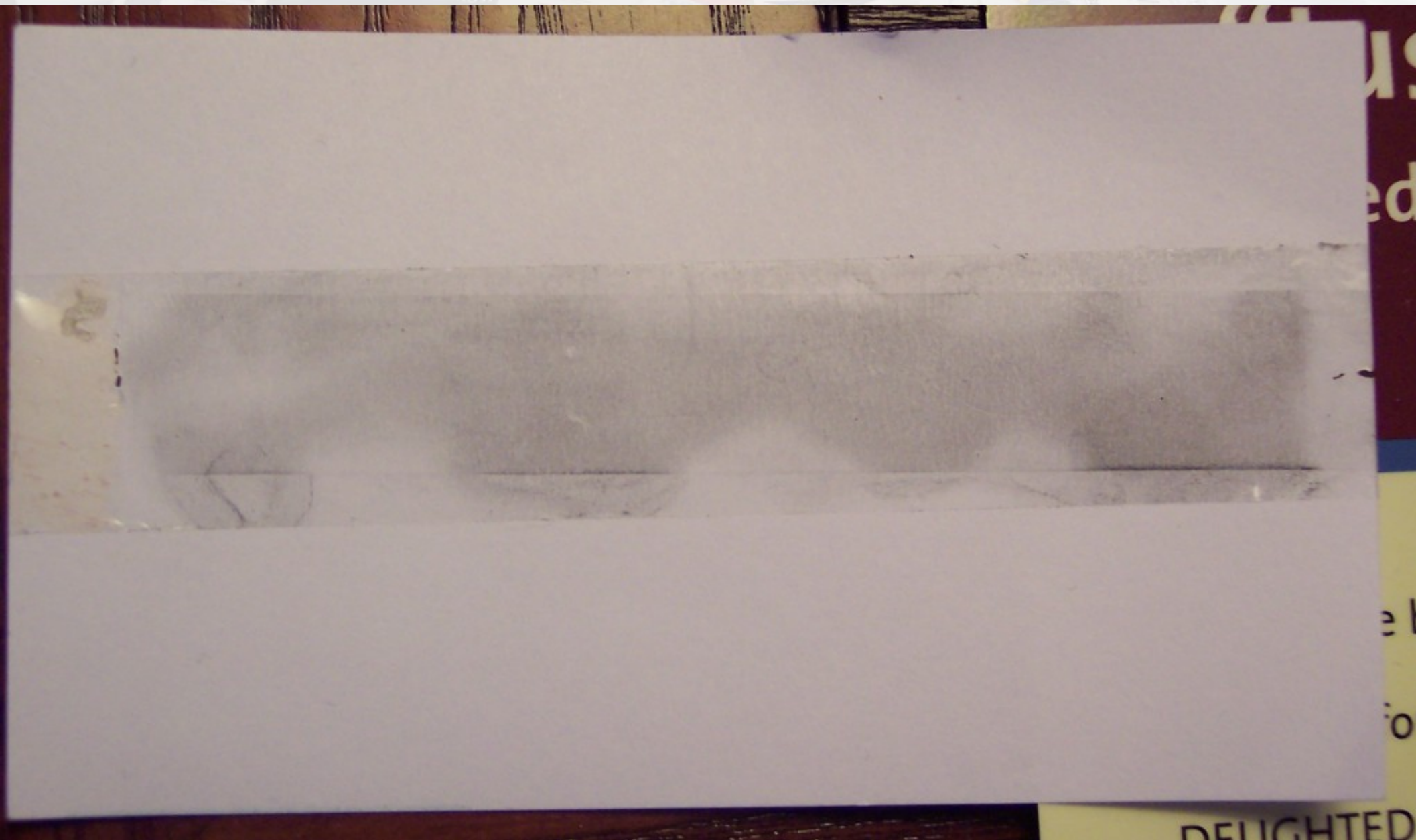
size matters!



But BPI is the same...



data matters!



data analysis

- **dmsb**

- decode standard track formats & character sets
- Joseph Battaglia
 - <http://www.sephail.net/articles/magstripe/>

- **binchop**

- aid to look for patterns and parity
- Major Malfunction
 - <http://www.alcrypto.co.uk>



demonstration



making sense of the data

- character sets

- <http://www.magtek.com/documentation/public/998750b5-4.pdf>

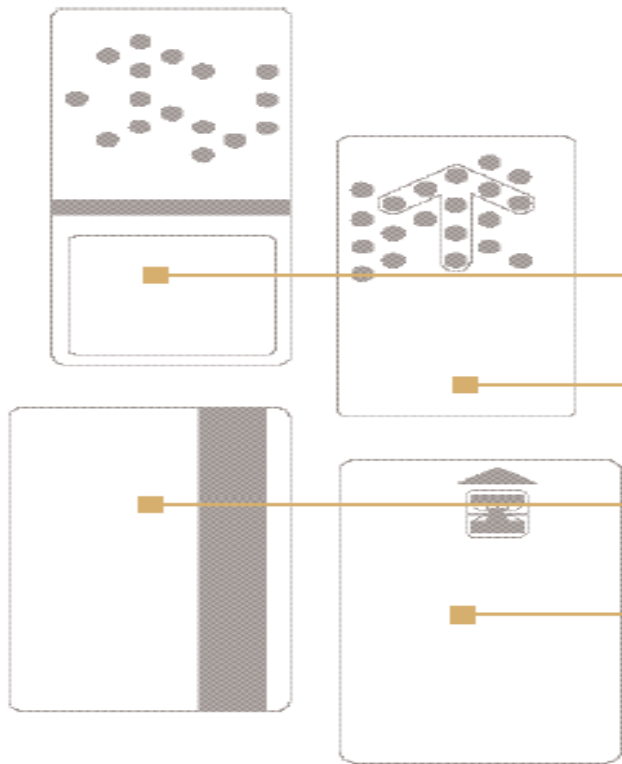


attack combining

mmirda + magstripe = drinks are on me!



evolution



Key cards for mechanical, optical, magnetic stripe and smart card operated locks.

Punched-hole cards

1. **Mechanical cards:** For all VingCard mechanical locking systems: 1040, 1050 and 1060 – VingCard Original.
2. **Optical cards:** For all VingCard optical electronic locking systems: 1070, 1080, 1090 and 1090e.
3. **Magnetic stripe cards:** For all VingCard magnetic stripe locking systems: 3000 and 2100 – Vision, 2100 Plus and DAVINCI.
4. **Smart cards and combination smart/magnetic stripe cards:** For all VingCard smart card locking systems – DAVINCI



Step 1



Step 2



Step 3



Step 4



next generation

- RFID
- biometric



RFID I/O tools: RFIDIOT

- <http://rfidiot.org>
 - python library
 - ISO 14443A/B
 - **MIFARE Standard, MIFARE 4k**, MIFARE Pro, MIFARE Ultralight, **MIFARE DESFIRE**, MIFARE SmartMX, SLE 55Rxx, SLE 66CL160S, SLE 66CLX320P, SR17b, SR1X4K, ISO14443A Tags, ISO14443B Tags, Jewel Tag (IRT0302B11 KSW DIY Eng. Sample), Sharp B, ASK GTML2ISO, TOSMART P0b4
 - support for ACG Dual ISO reader
 - <http://www.acg.de>
 - no drivers required – serial device

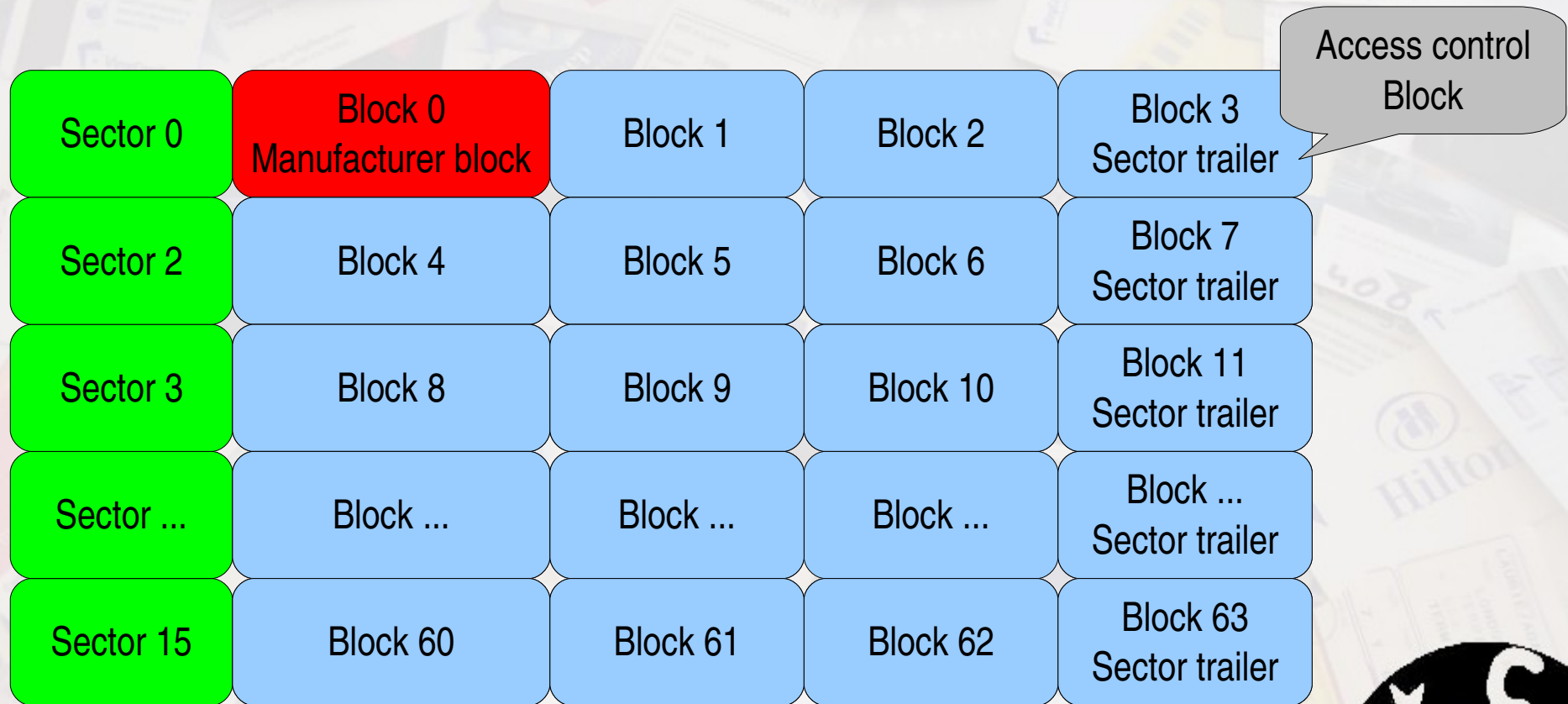


MIFARE tags

- Block layout
- Access controls
- Demonstration



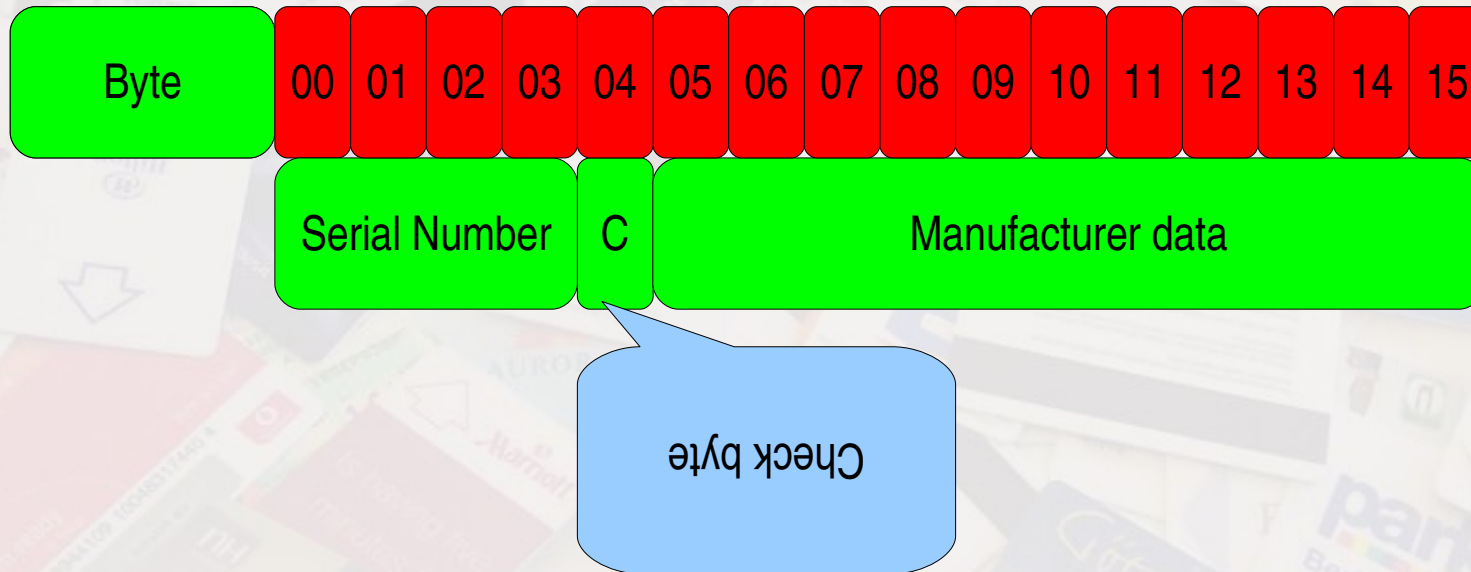
MIFARE 1K – block layout



**16 sectors, 4 blocks per sector,
16 bytes per block = 1024 bytes**



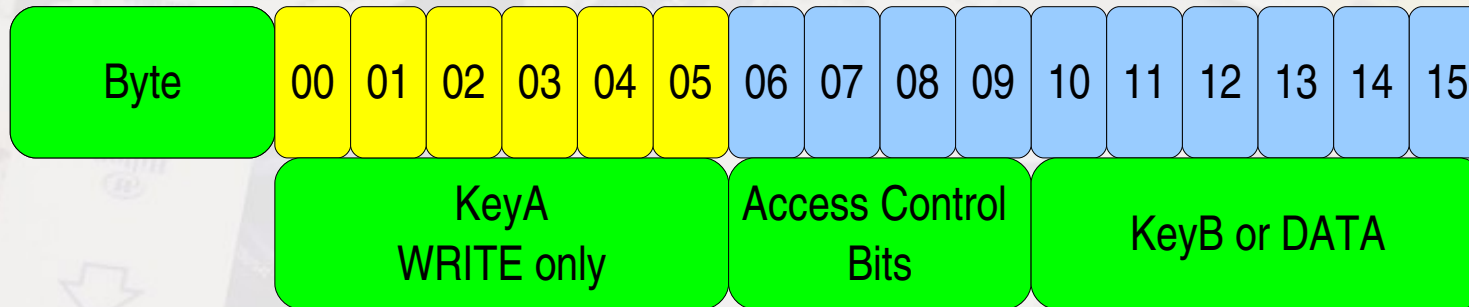
manufacturer block layout



Whole block is read only



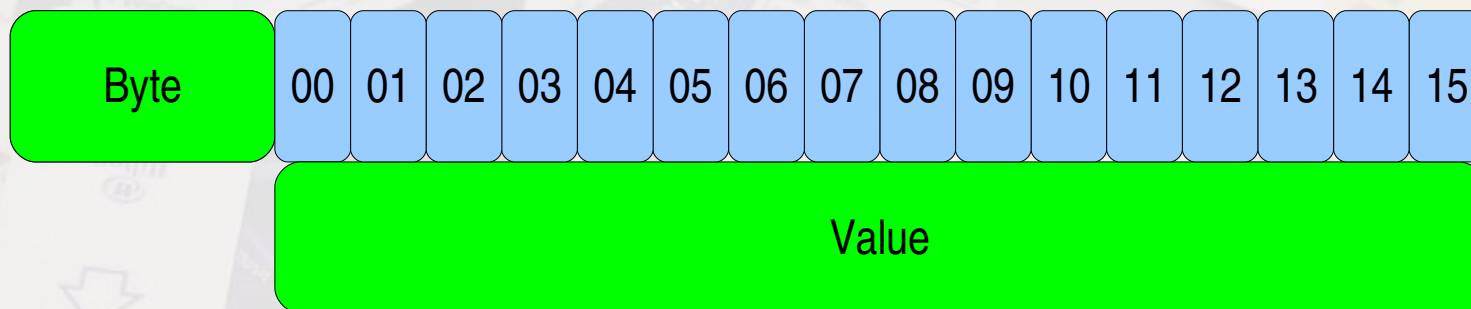
access control block layout



- **KeyA can never be read**
- **KeyB may be read and/or written**
 - depending on ACB
- **ACB for various combinations**
 - who may read/write keys
 - who may increment/decrement/restore value blocks



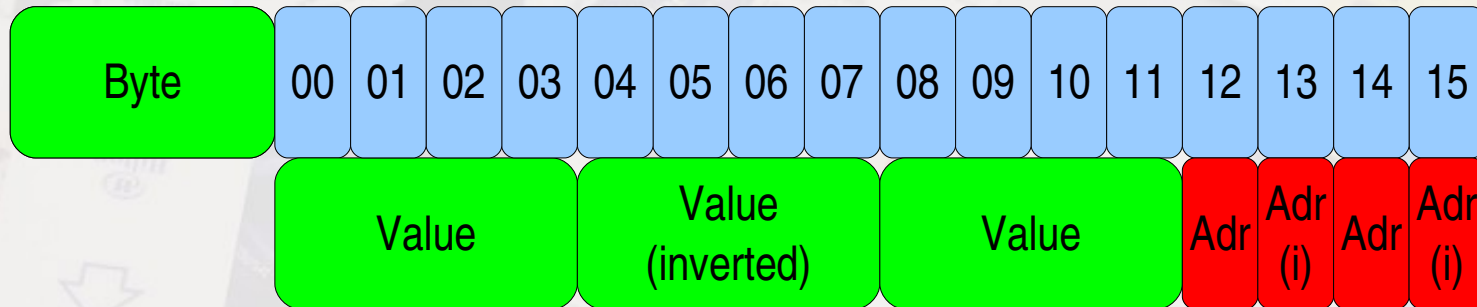
data block



- **16 bytes free storage**



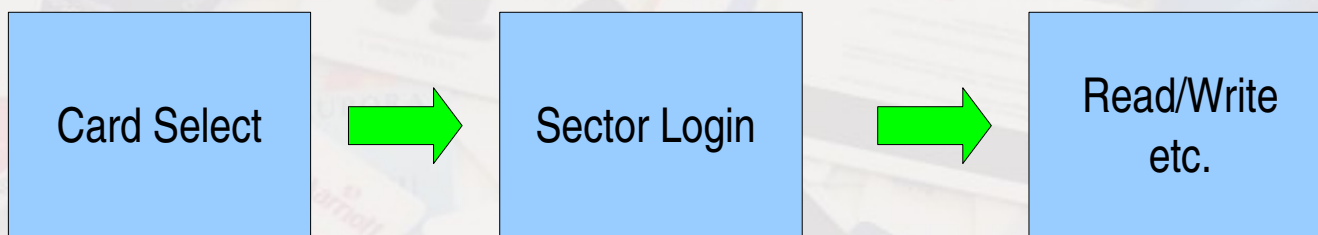
value block



- **Value stored 3 times**
 - Twice non-inverted, once inverted
- **Address byte stored 4 times**
 - Twice non-inverted, twice inverted
 - Audit trails
 - Backup
 - Read only (by value commands)



tag operations



demonstration



Questions?



oh dear...



majormal@pirate-radio.org
<http://www.alcrypto.co.uk>

