

RFIDIOts!!!

**RFID Hacking without a Soldering Iron
(... or a Patent Attorney :)**

Adam Laurie

adam@algroup.co.uk

<http://trifinite.org>

<http://rfidiot.org>

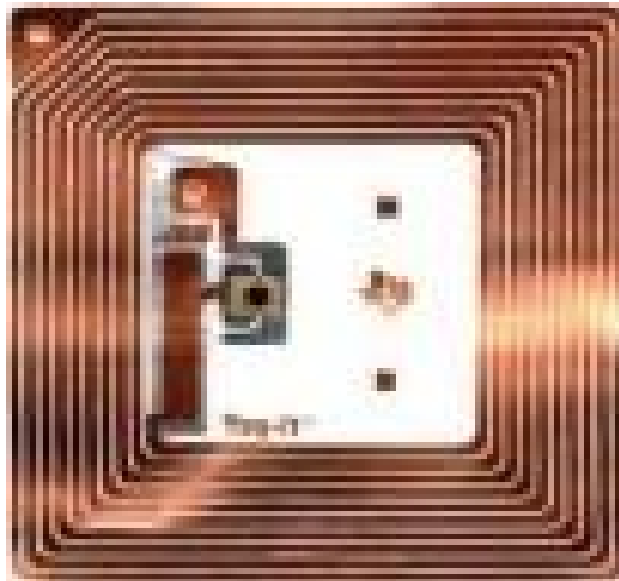
*CanSecWest
Vancouver, 2007*





What is RFID?

- Contactless Auto-ID technology
 - Radio Frequency or Magnetically Coupled chip
 - Chip is passive
 - Energy from reader activates the chip



What is it for?

- Simple ID only
 - Door Entry Systems
 - e.g. HID
- Smartcards
 - Payment Cards
 - e.g. Oyster
 - Biometrics
 - e.g. Passports



RFID – Moo am I?



- Animal ID
- Hotel Keys
- Car Immobilisers
- Ski Passes
- Goods Labels
- Luggage Handling
- Vending
- Human Implants

Selling the idea of Human Implants

DOCTOR FUN

16 Jan 2006



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

Human Implants



- Military
 - Access Control
- Mental Patients
 - Tracking
- Beach Bars
 - Digital Wallets

Unique ID?



- DIY Cloning Units
 - <http://cq.cx/vchdiy.pl>

Spot the original?



Unique ID?



Spot the original?



- DIY Cloning Units
 - <http://cq.cx/vchdiy.pl>
- Industry Defence:

Unique ID?



Spot the original?



- DIY Cloning Units
 - <http://cq.cx/vchdiy.pl>
- Industry Defence:

“Clones do not have the same form factor and are therefore not true clones”

Unique ID?



- Readers cannot 'see' so form factor irrelevant

Unique ID?



=



- Readers cannot 'see' so form factor irrelevant

Cloning Devices



Cloning Devices



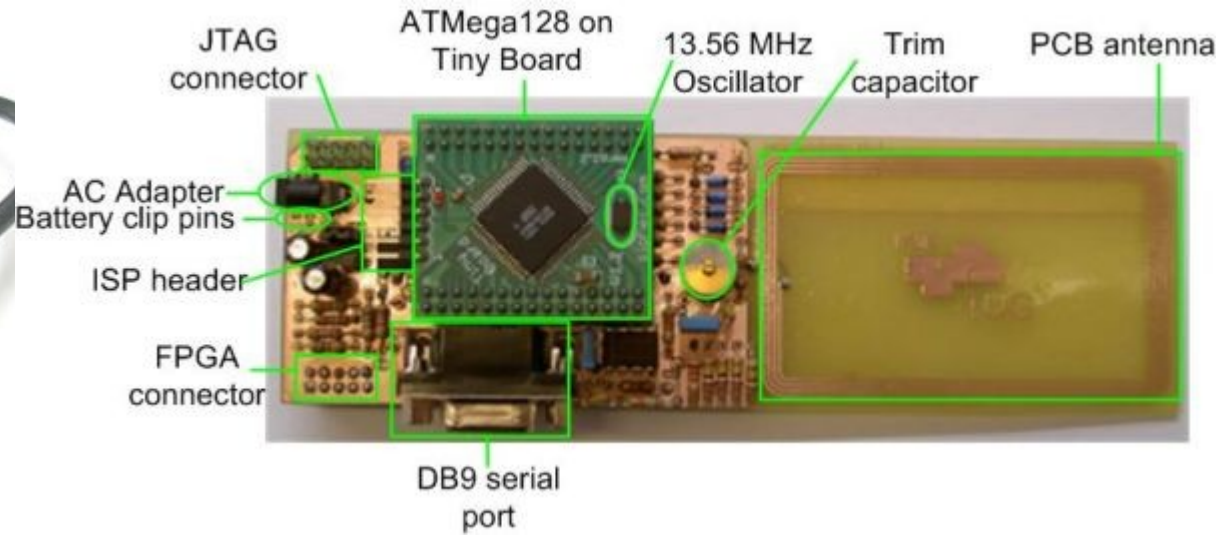
Cloning Devices



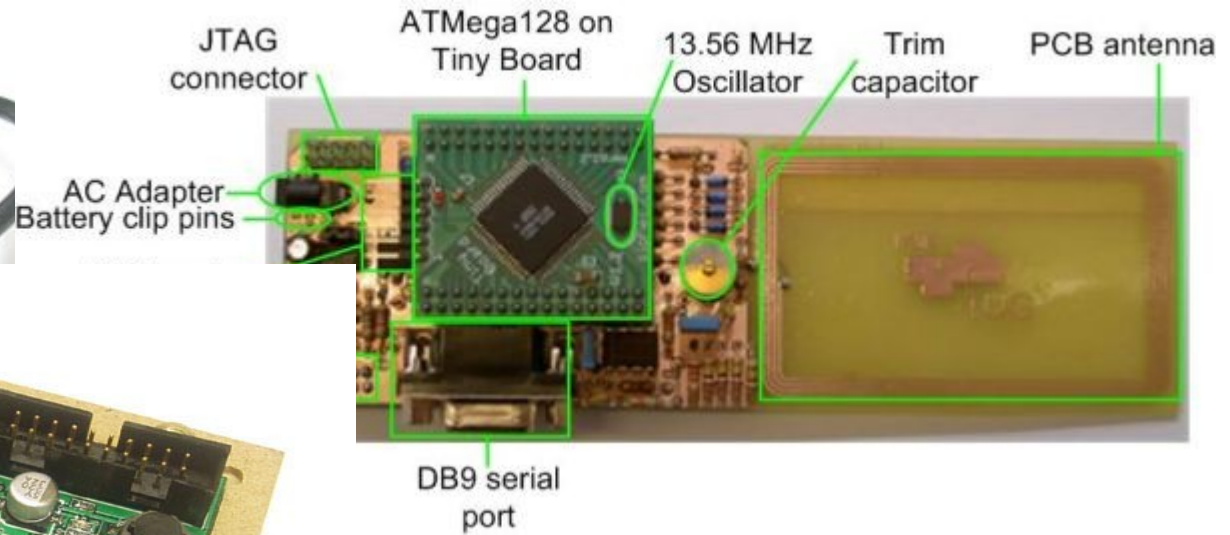
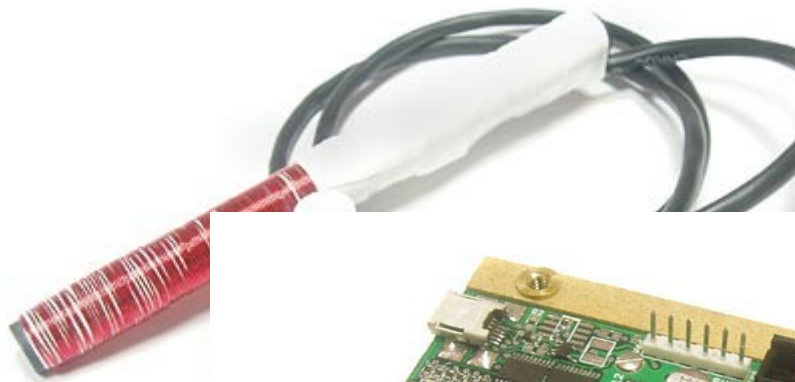
Cloning Devices



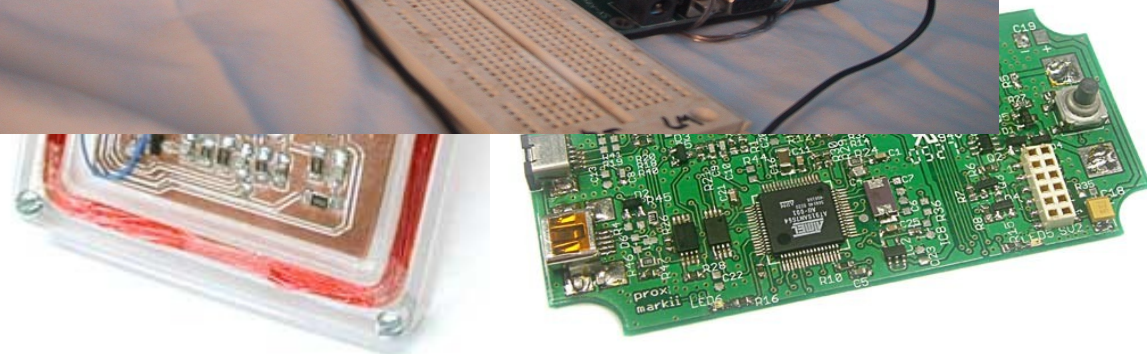
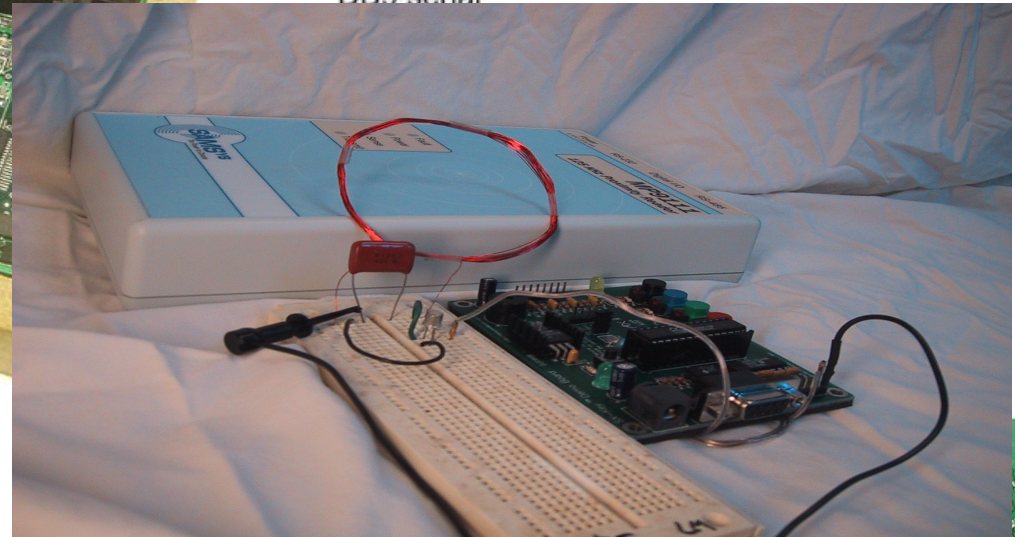
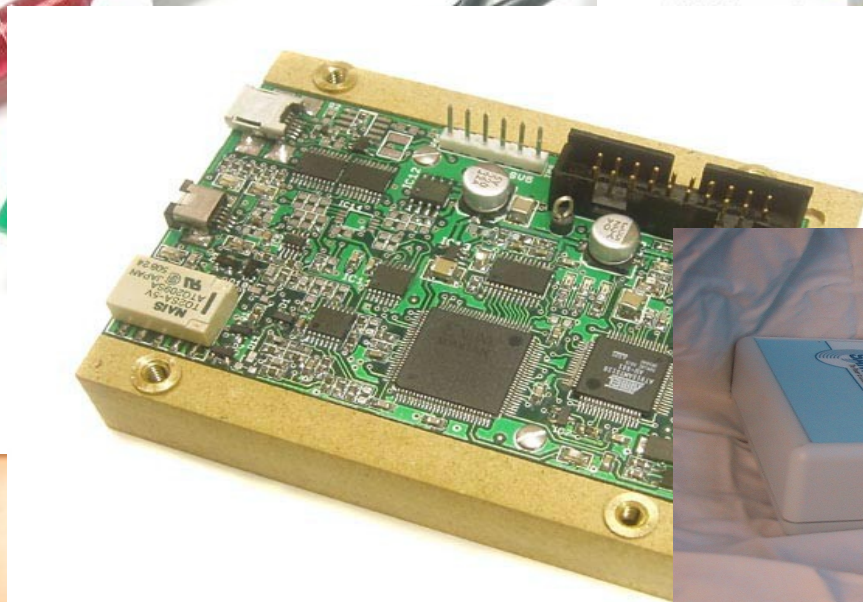
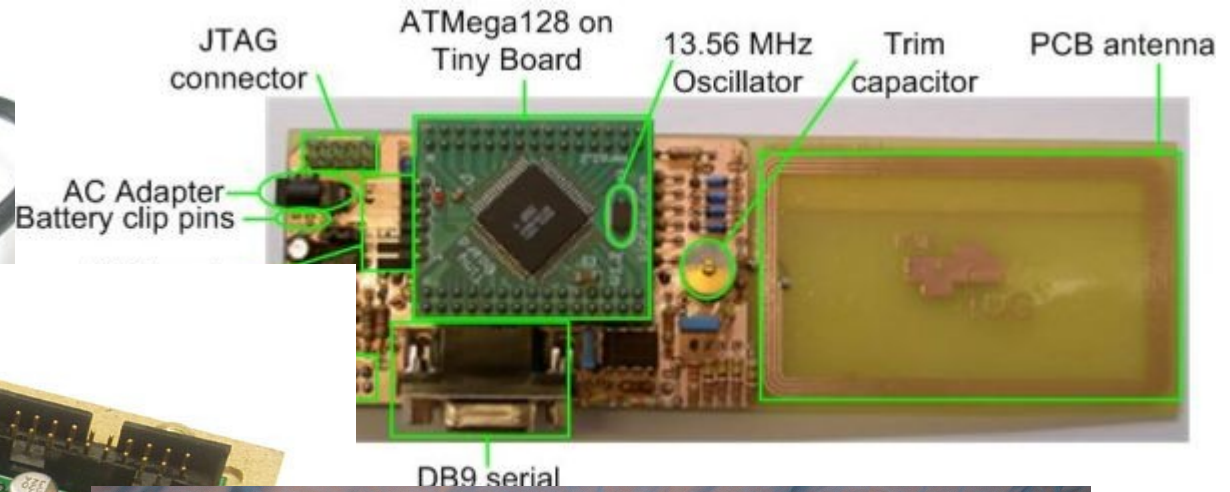
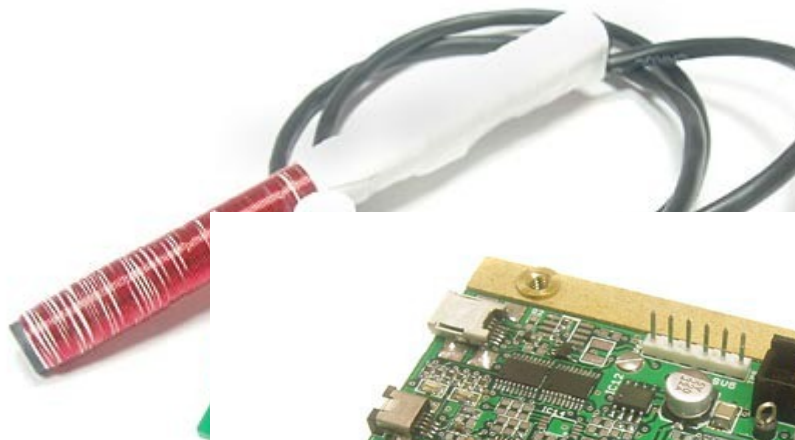
Cloning Devices



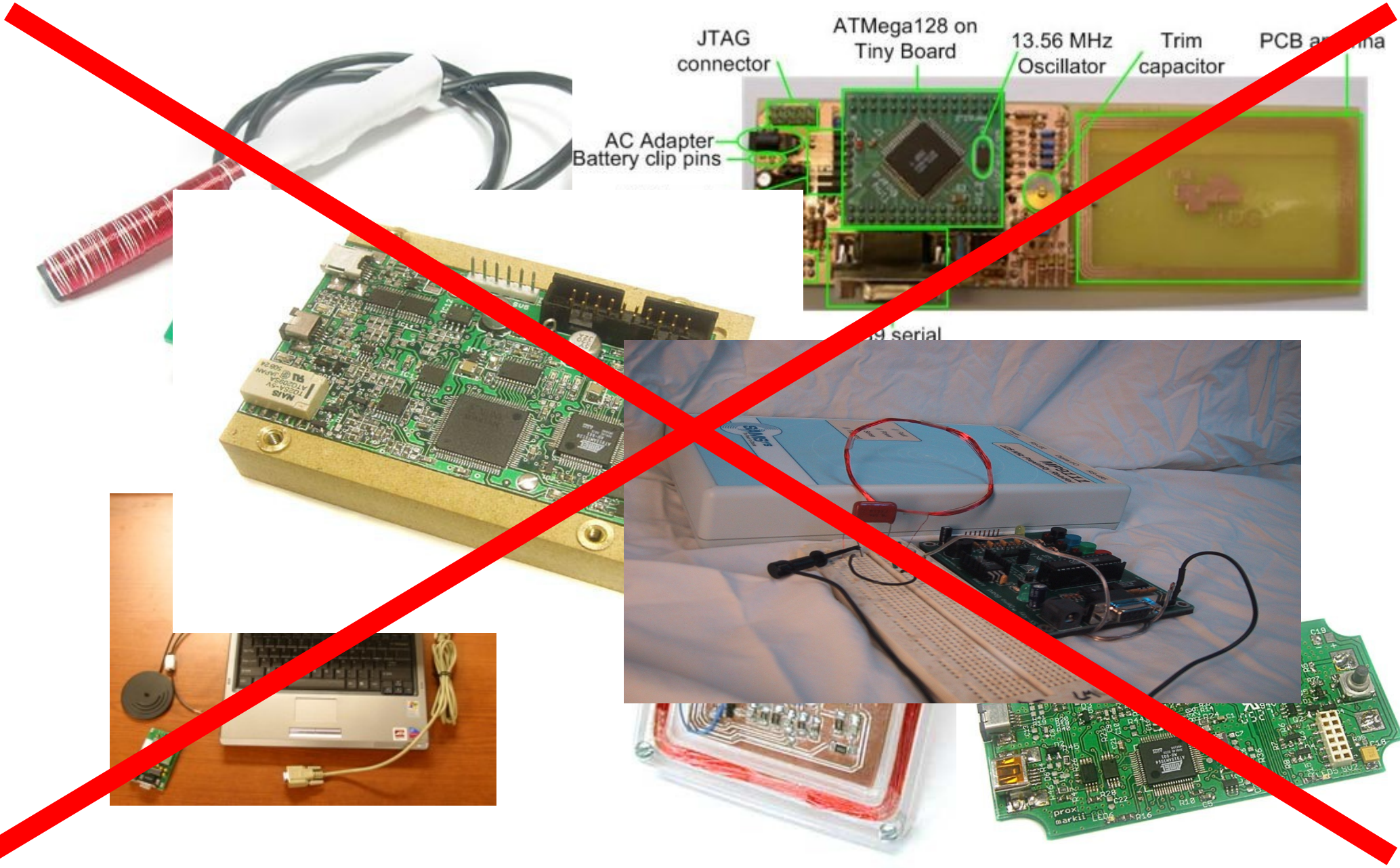
Cloning Devices



Cloning Devices



Cloning Devices



The Challenge

- Create a 'true' clone
 - Same ID
 - Same Form Factor

Understanding the ID

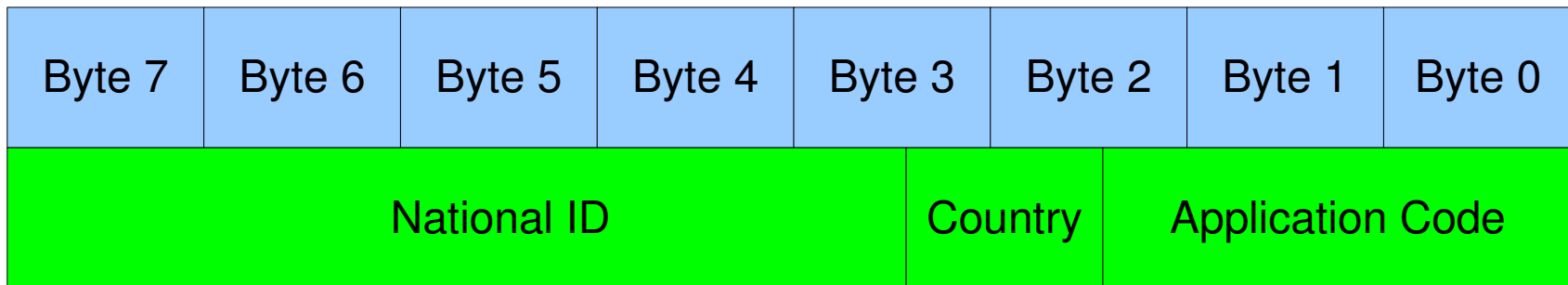
- Industry standard example
 - Animal Tagging
 - ISO-11784/5 FDX-B
 - Application flag (Animal/Non-Animal)
 - 3 Digit Country or Manufacturer code
 - National ID

Sending the ID

- Reader and TAG will communicate with
 - Specific frequency
 - 125/134.2 kHz
 - (13.56 MHz)
 - Specific data bitrate
 - RF/2 - RF/128
 - Specific encoding (modulation) scheme
 - FSK, Manchester, BiPhase, PSK, NRZ
 - Specific bit patterns
 - Header / Data / CRC

Decoding the ID

- 8 Byte raw ID from 'dumb' reader



- Reverse MSB/LSB
- Reverse each Nibble
- Right shift (x2)
- Convert to Decimal

Decoding the ID

- 8 Byte raw ID

70	91	53	12	EA	6F	00	01
----	----	----	----	----	----	----	----

– Reverse MSB/LSB

10	00	F6	AE	21	35	19	07
----	----	----	----	----	----	----	----

– Reverse each Nibble

80	00	F6	57	48	CA	89	0E
----	----	----	----	----	----	----	----

Decoding the ID

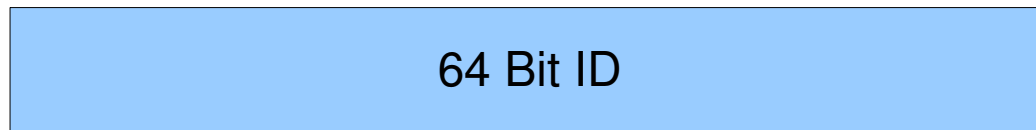
- 8 Byte raw ID

80	00	F6	57	48	CA	89	0E
Application ID 8000		Country F65	National ID 748CA890E				

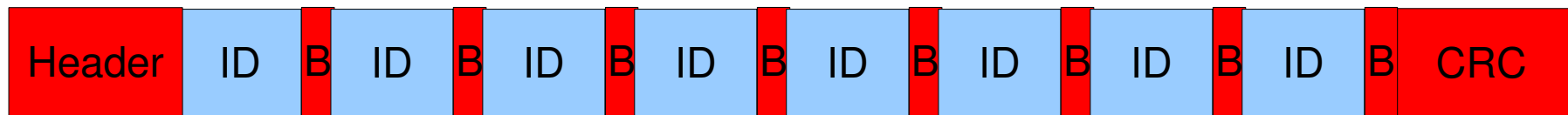
- Country F65 rightshifted: 3D9 == '985' decimal
 - icar.org: 'Destron Fearing / Digital Angel Corporation'
- National ID 748CA890E == '31286003982'

Encoding the ID

- Reverse the decoding process



- Add Header / CRC to raw binary ID



- Fixed bits embedded in ID prevent header being duplicated in datastream
- Now we have 128 bits of raw bit-level ID
 - How do we deliver it?

Multi-Format Transponders

- Why make 10 transponder types when you can make 1?
 - Lower manufacturing costs
 - Lower stocking/distribution costs
 - Convenience

Multi-Format Transponders

- Independently configurable parameters
 - Q5
 - Configuration for Bit Rate, Modulation etc.
 - 224 Bits user programmable memory
 - Dump <n> data blocks on wakeup
- Multiple 'personalities'
 - Hitag2
 - Configuration for 'Public Modes'
 - 256 Bit user programmable memory
 - Dump <n> data blocks on wakeup as per Mode setting

Sending the ID

- Take a redundant Door Entry tag
 - Re-Set configuration as appropriate
 - Bit Rate
 - Modulation
 - Inversion
 - Number of blocks to dump on 'wakeup'
 - Program data blocks with raw ID

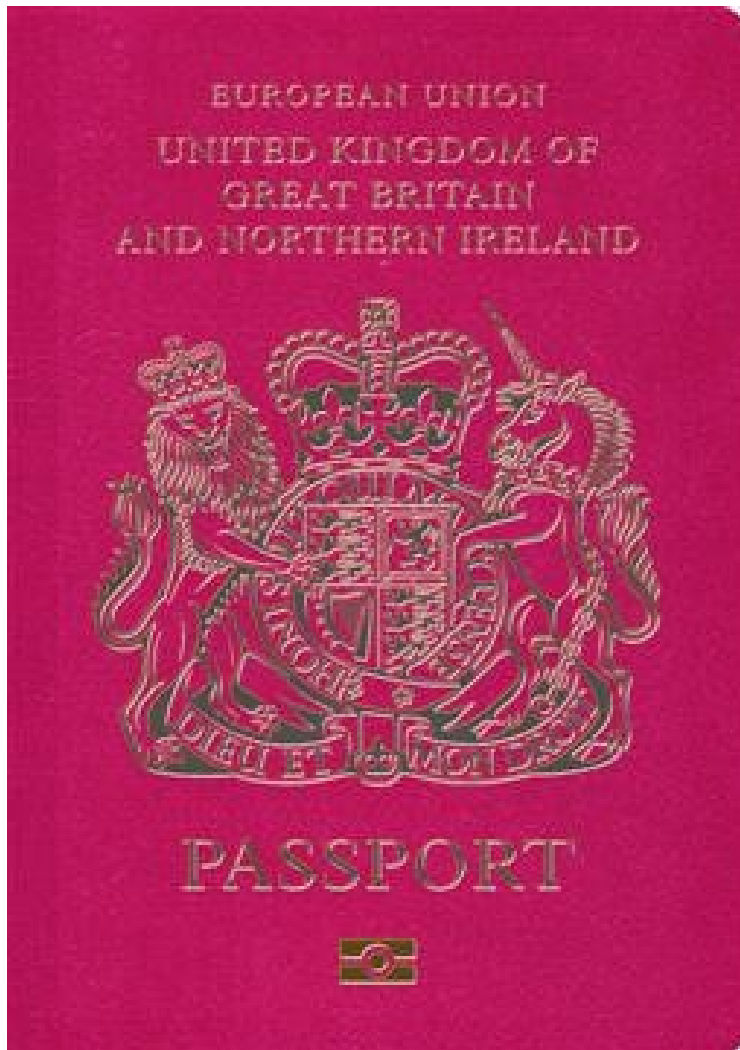
Demonstration

- Clone Trovan 'Unique' TAG
 - Access Control System
- Clone ISO 11784 'Animal' TAG (FDX-B)
 - Cow Implant
 - VeriChip paperweight

RFID implanted chip threats

- Track individuals
- Target individuals
- Impersonate individuals
 - Gain access to restricted areas
 - Provide alibi for accomplice!
- 'Smart' Bombs
 - Device only goes off if target of sufficient rank is in range.

Encryption is your friend



- RFID Enabled 'Biometric' passports
- 48 Items of Data
 - Fingerprint
 - Facial Image
 - Birth Certificate
 - Home Address
 - Phone Numbers
 - Profession

Keys to your kingdom



- Pseudo random UID
 - Cannot determine presence of specific passport without logging in
- Strong Authentication
 - Basic Access Control
 - 3DES
- Content Encryption
 - Extended Access Control

ePassport threats

- Key data may be obtained through other channels
- Passport profiling
 - Determine country of origin without logging in
 - Implementation errors:
 - Australian passport ID does not start with '08' on select
 - Australian passport does not require Basic Auth on 'File Select', only on 'File Read'.
- Target specific passport holders
 - Bomb that detonates for Australians only...

RFIDIOT

- Open Source Python library
- Hardware independent
 - ACG
 - Frosch
 - OpenPCD coming soon
- Low cost reader/writers now available

<http://rfidiot.org>

ACG reaction to RFIDIOt

“Unfortunately your companies activities seem to be counter to ACG's interests so we will not be able to support you any further.”

Email - 3rd January, 2007

Questions?

<http://rfidiot.org>

adam@algroup.co.uk