Security and Privacy Issues in RFID-Based Applications

Prof. Dr. Marc Langheinrich
Faculty of Informatics
Università della Svizzera italiana (USI)

Università della Svizzera italiana | Faculty of Informatics

Contents

- What is RFID?
- What is it good for?
- What does this have to do with security?

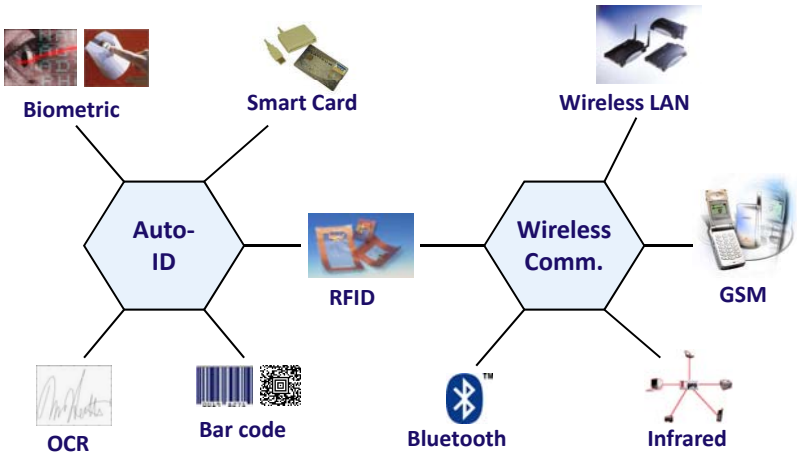
Università della Svizzera italiana | Faculty of Informatics

TECHNOLOGY

Università della Svizzera italiana | Faculty of Informatics

4

Classifying RFID Technology

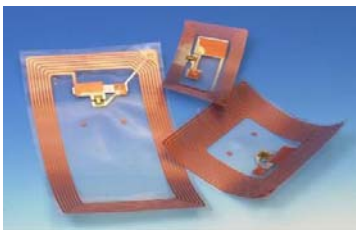


Università della Svizzera italiana | Faculty of Informatics

5

RFID

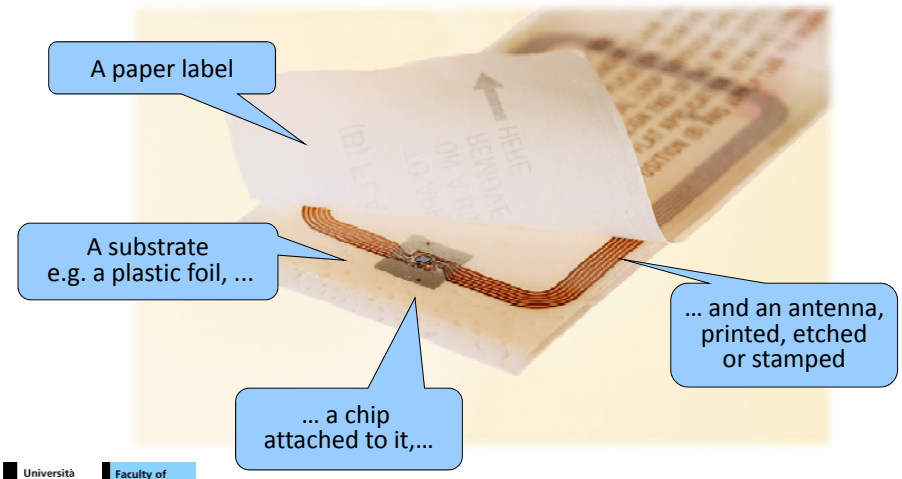
- Identify objects from distance
  - small IC with RF-transponder
- Wireless energy supply
  - up to ~ 5 m
  - magnetic field (induction) or electromagnetic field
- ROM or EEPROM (read/write)
  - ~ 100 Byte
- Cost > € 0.1
  - consumable and disposable



Università della Svizzera italiana | Faculty of Informatics

F.Ma. 6

Smart Labels: Self-adhesive Flexible Tags Laminated with Paper



Università della Svizzera italiana | Faculty of Informatics

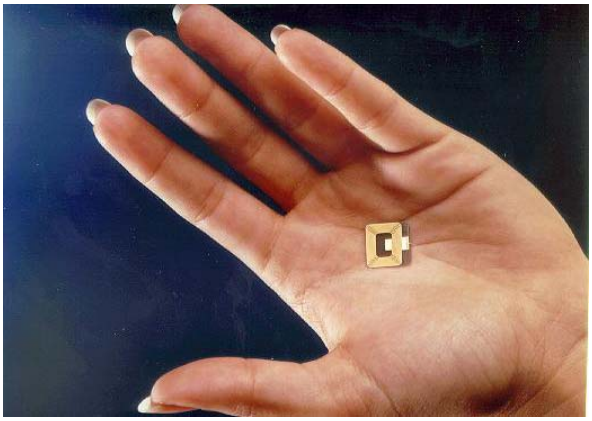
F.Ma. 7

A Paper Label with a "Hidden" RFID Tag

Università della Svizzera italiana | Faculty of Informatics

8

Small RFID Tags



Università della Svizzera italiana | Faculty of Informatics

F.Ma. 9

The μ-Chip

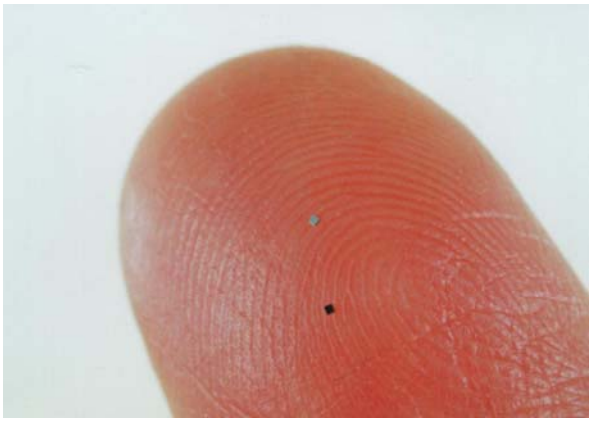
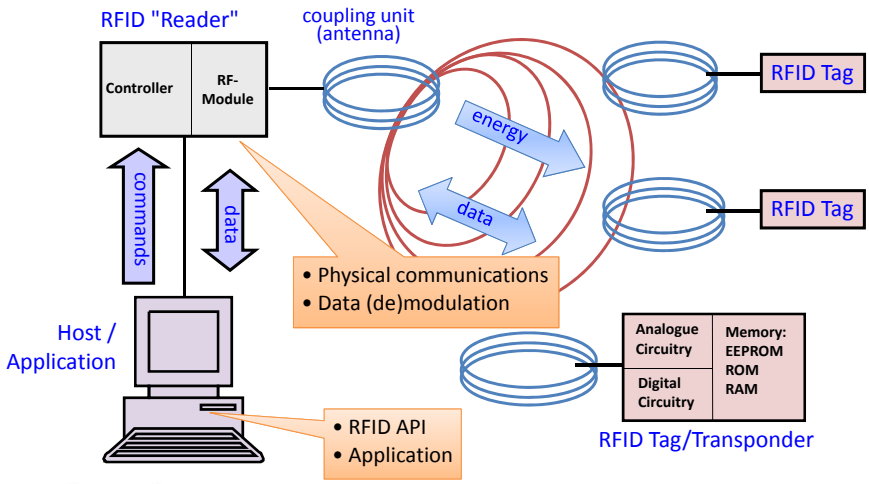


image source: Hitachi

Università della Svizzera italiana | Faculty of Informatics

10

RFID Operating Principle



Università della Svizzera italiana | Faculty of Informatics

11

A Classical Application: EAS – Electronic Articel Surveillance

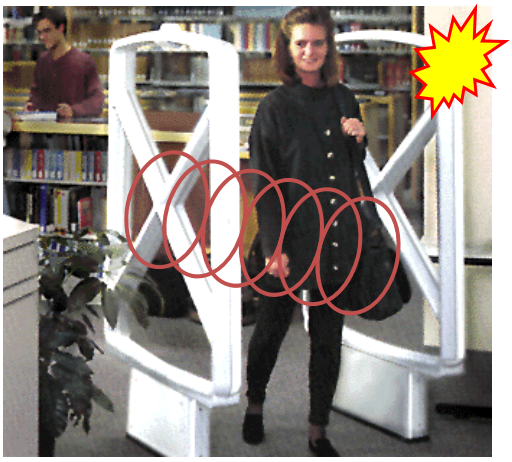


image source: Peter H. Cole

Università della Svizzera italiana | Faculty of Informatics

F.Ma. 13

A Classical Application: EAS – Electronic Articel Surveillance

Università della Svizzera italiana | Faculty of Informatics

Source: Peter

F.Ma. 14

RFID Tag Form Factors I

Smart Labels

Contactless RFID Cards

Hitachi Coil-on-Chip

Università della Svizzera italiana | Faculty of Informatics

15

APPLICATIONS

Università della Svizzera italiana | Faculty of Informatics

17

Ski Ticketing

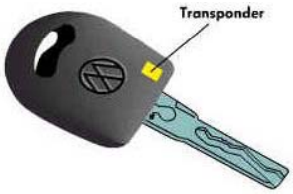
Swatch Snowpass

Postcard „Ticket“

Università della Svizzera italiana | Faculty of Informatics

F.Ma.

Car Immobilizer (Anti-Theft Device)



- RFID tag integrated into key
- Reader in ignition powers RFID tag and checks validity of key
- If electronic key is not valid, engine electronics is blocked

Università della Svizzera italiana | Faculty of Informatics

F.Ma.

Automatic Wireless Toll Collection

- Active RFID transponder mounted in the vehicle
  - reader at toll plaza
  - central database
  - video enforcement
- Benefits:
  - drive through at ~ 40 km/h
  - throughput 1200 cars/hour

- Uses Dedicated Short Range Communications (DSRC)
  - RFID-communication protocol for automotive applications
  - 5.8 GHz (EU/Japan) / 5.9 GHz (US)

Università della Svizzera italiana | Faculty of Informatics

F.Ma. /M.L.

Contactless „Smart“ RFID Cards for Public Transport Systems

- Example: prepaid „Suica“ train pass in Japan (2001) for JR trains

Università della Svizzera italiana | Faculty of Informatics

F.Ma./M.La.
23

JR Suica Payment Model

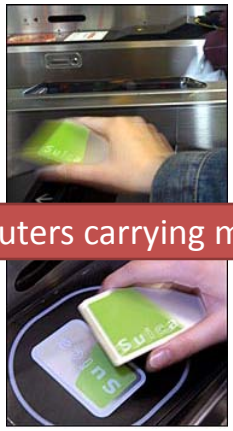
- Cards are loaded with pre-paid amount
  - options for topping off if not enough money left
- Charges stored on card
  - can be inspected with USB reader at home

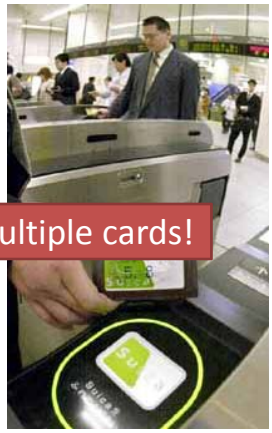
Università della Svizzera italiana

M.La. 24

Contactless „Smart“ RFID Cards for Public Transport Systems

- Example: prepaid „Suica“ train pass in Japan (2001) for JR trains





Problem: Commuters carrying multiple cards!

Università della Svizzera italiana

F.Ma./M.La.
25

Animal Identification & Tracking

- RFID tags attached to or injected into animals
- Readers at feeding or milking stations

Università della Svizzera italiana | Faculty of Informatics

F.Ma. 27

Dog Tagging (Switzerland)

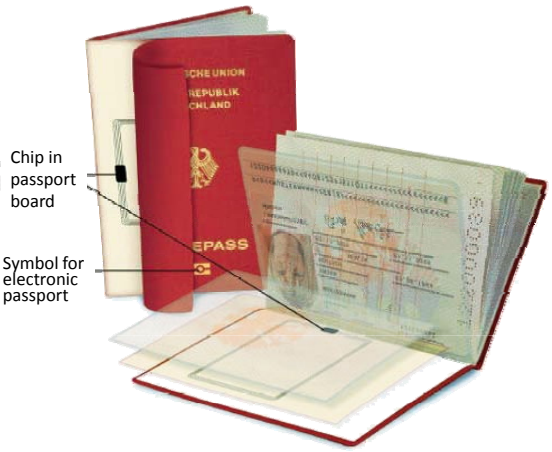
- Legal requirement as of January 1, 2007
  - „Bis zum 31. Dezember 2006 müssen alle Hunde in der Schweiz eindeutig und fälschungssicher markiert und bei ANIS registriert sein. Damit sollen Abklärungen nach Beissunfällen, in Seuchenfällen sowie bei entlaufenen, verwahrlosten oder ausgesetzten Hunden erleichtert werden."

- Article 16.3. SR 916.401 (Tierseuchenverordnung)
  - registration of: name, gender, birth date, race, parentage, color, breeder, owner, veterinarian, date
- Registration in national ANIS database
  - www.anis.ch

Università della Svizzera italiana | Faculty of Informatics

M.La.
28

E-Tickets and E-Passports



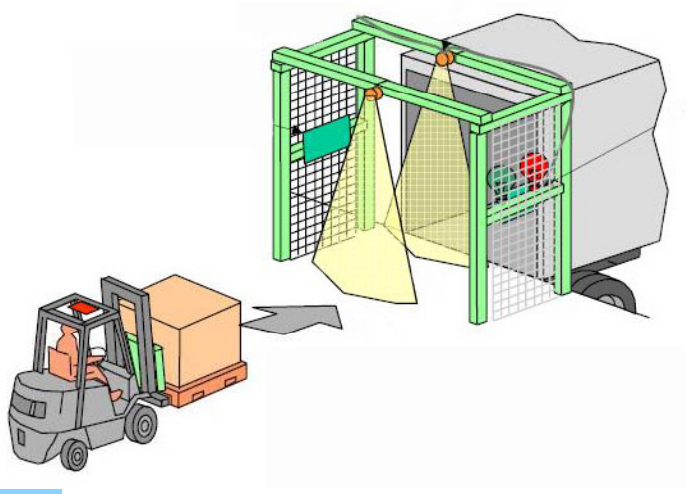
- Secure identification
- Speed-up access control
- Anti-counterfeiting

Università della Svizzera italiana
Faculty of Informatics
29

Improving Logistics with RFID

Università della Svizzera italiana
Faculty of Informatics
30

Improving Logistics with RFID



Università della Svizzera italiana
Faculty of Informatics
31

Minimizing Out-Of-Stock Situations

- Out-of-stock in the grocery industry runs at 5-10% which leads to lost sales of 3-4% for retailers

Università della Svizzera italiana
Faculty of Informatics
32

After-Sales Services with RFID

Università della Svizzera italiana | Faculty of Informatics

33

After-Sales Services with RFID

Università della Svizzera italiana | Faculty of Informatics

34

After-Sales Services with RFID

Receiptless Returns

Università della Svizzera italiana | Faculty of Informatics

35

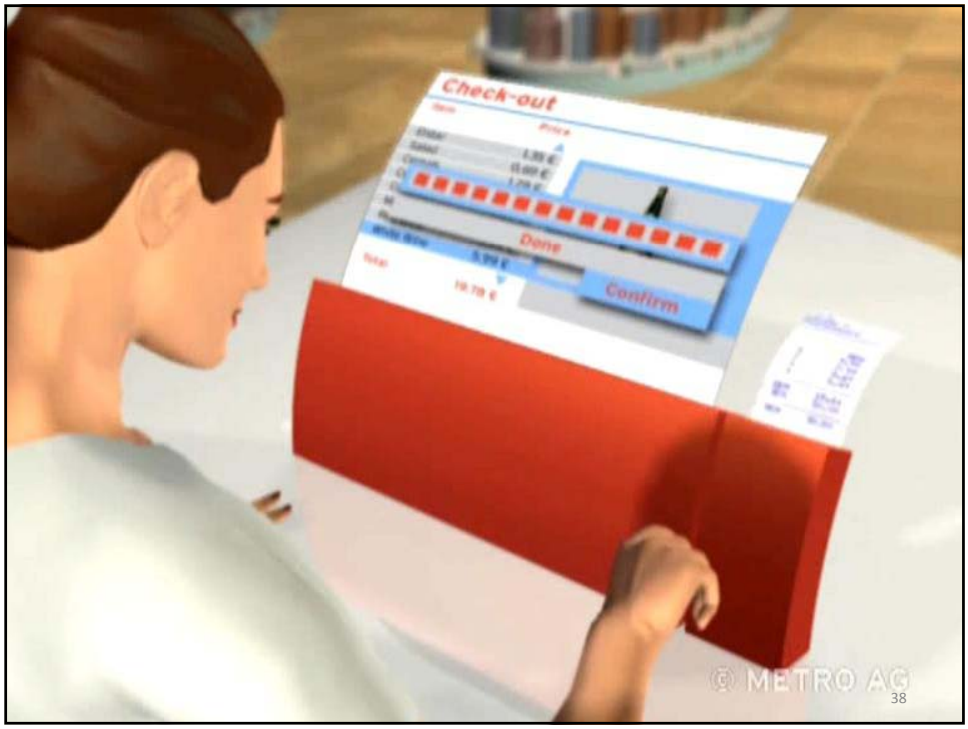
After-Sales Services with RFID

Fast Checkout

Università della Svizzera italiana | Faculty of Informatics

36


© METRO AG


Check-out
Done
Confirm
© METRO AG
38

SECURITY AND PRIVACY

Università della Svizzera italiana | Faculty of Informatics

39

RFID: just a wireless license plate

(Ari Juels, RSA Labs)

- Tags reply when entering field
  - Tags usually „promiscuous“ (reply to *any* reader)
- Reader is pretty much „blind“
  - If tag does not reply, reader cannot detect it
- Identity is „just a number“
  - Numbers easy to copy, how to tell if it‘s „real“?
- Readout process invisible to human
  - 10-100m range, depending on technology, system

Università della Svizzera italiana | Faculty of Informatics

40

Security and Privacy

- Security goals
  - Ligitimate readers can detect & identify
  - Illegitimate tags cannot falsify identity

- Privacy goals
  - Illegitimate readers cannot detect (track)
  - Illegitimate readers cannot identify

Università della Svizzera italiana | Faculty of Informatics

41

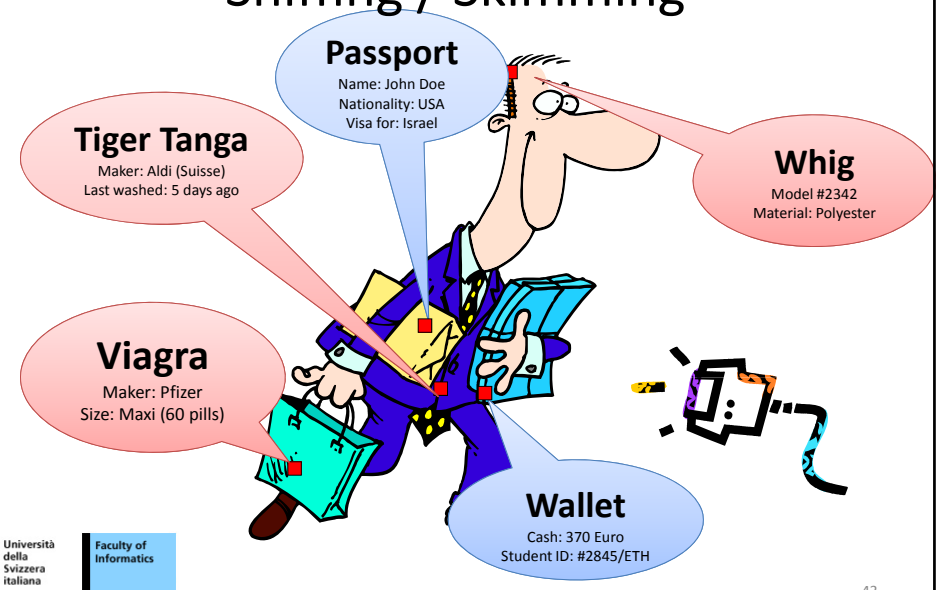
RFID Application Areas & Threats

- Alerting => Denial of Service
  - Paid/Not paid
- Identification => Sniffing
  - „Barcodes on steroids“ (more data, faster to process)
- Monitoring => Tracking
  - Automation makes continuous tracking feasible (i.e., much easier!)
- Authentication => Forgery
  - E-Passport, Car Immobilizer, Credit Cards, …

Università della Svizzera italiana | Faculty of Informatics

42

Sniffing / Skimming



Original "RFID-Man" Artwork (c) 2006 Ari Juels, RSA Laboratories

Università della Svizzera italiana | Faculty of Informatics

43

Solutions?

Università della Svizzera italiana | Faculty of Informatics

44

Example

Università della Svizzera italiana
Faculty of Informatics

45


Information on Smart Chip
Deactivate Smart Chip?
Do you want to deactivate the information on the Smart Chip?
Yes
© METRO AG


METRO Group
Future Store Initiative
Entwerter für RFID-Chips
RFID-Etiketten unlesbar machen?
Dafür nutze ich den De-Activator!
» Ich habe Produkte mit einem RFID-Etikett gekauft. Wenn ich die darauf gespeicherten Daten unlesbar machen will, gehe ich einfach zum RFID-De-Activator: Produkt draufstellen, Informationen überschreiben lassen – so schnell geht das! «
Università della Svizzera italiana
Faculty of Informatics
48

Killing

- Kill-Command
  - Part of EPCGlobal/AutoID standard
  - Software lock that renders tags silent

Metro RFID De-Activator

Università della Svizzera italiana | Faculty of Informatics

49

50

Killing

Metro RFID De-Activator

- Kill-Command
  - Part of EPCGlobal/AutoID standard
  - Software lock that renders tags silent
- Prevents future use!
  - Receiptless returns? Smart fridge?
- Requires encryption to prevent DoS
  - „Killing“ all tagged items in a store

Università della Svizzera italiana | Faculty of Informatics

51

Encryption

- „The Siren Song of Encryption“ (Juels, 2007)
- Powerful stuff
  - „Secured“ tags could talk only to „authorized“ readers
  - would only disclose the „right“ information to the „right“ recipients
- Lots of proposals, very active field of research
  - G. Avoine‘s Web Page: http://lasecwww.epfl.ch/~gavoine/rfid/
- The Solution?!

Università della Svizzera italiana | Faculty of Informatics

52

Problem: Which Password?

Università della Svizzera italiana | Faculty of Informatics

53

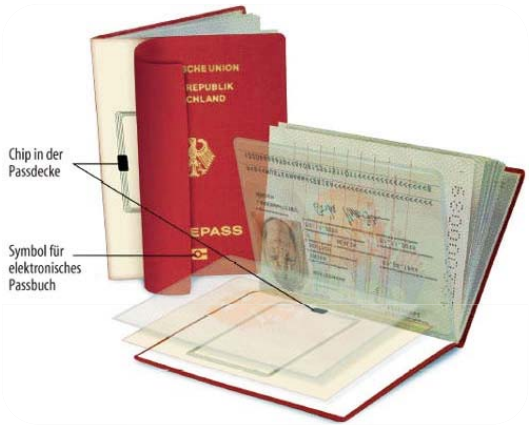
Problem: Which Password?

- Reader must know password
  - Unless only one password (which is bad), reader needs to know which tag it is ☹
  - => Reader must „try“ hundreds of passwords!
- How does the reader know about the password?
  - Needs to be fed into reader system
  - From where? When?
- Works well in controlled environm. (e.g., car key)
  - How to do this at checkout for a can of soda?

Università della Svizzera italiana | Faculty of Informatics

54

Example 2



Università della Svizzera italiana
Faculty of Informatics

55

RFID in Passports

Standard for "Contactless Proximity Cards", read distance up to 10cm

- ICAO Guidelines 9303
  - Requires RFID-tags in passports (ISO 14443A/B)
  - Early adopter DE (since 11/05; CH: 9/06, US: 10/06)
- Contents (Personal Data)
  - Required: name, birth date, sex, nationality, facial image
  - Optional: fingerprint (EU:2008), …
- Security
  - Data digitally signed ("Passive Auth.", required)
  - Readout requires key ("Access-Control", optional)
  - Copy protection ("Active Authentication", optional)

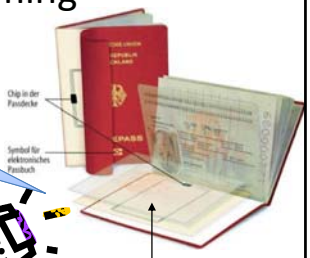
Università della Svizzera italiana
Faculty of Informatics

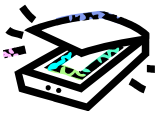
56

Basic Access Control

- Preventing eavesdropping, skimming
  - for MRZ-data, facial image

Challenge-Response Mechanism
Proves that reader knows key.
Derives session key for encrypted communication.





Read MRZ → Compute key → Read RFID

The Machine-Readable-Zone (MRZ):
Name, Sex, Passport Number, Birthday, Expiration, Checksum

```
P<D<<LANGHEINRICH<<MARC<<<<<<<<<<<<<<<<<<<<
123456789?D<<710123?M070101?<<<<<<<<<<<<<<?
```

Original Slide: Dennis Kügler

Università della Svizzera italiana
Faculty of Informatics

57

Preventing Forgery

Digital Signature

Università della Svizzera italiana
Informatics

58

Extended Access Control

- For fingerprints
  - Chip authentication + terminal authentication
- Chip Authentication
  - Unique private key in tag crypto-chip (Not readable!)
  - Prevents 1:1 copies on forged passports
- Terminal Authentication
  - Public key of authorized readers in Crypto-Chip
  - Limits access to authorized terminals (countries)
  - Requires complex certificates update schedule

Università della Svizzera italiana | Faculty of Informatics

60

Original Slide: Dennis Kügler

WIRED
BETA

SUBSCRIBE | SECTIONS » | BLOGS » | READ MAGAZINE | « WIRED MOBIL

SCIENCE : DISCOVERIES RSS

Hackers Clone E-Passports

Kim Zetter 08.03.06 | 2:00 AM

Two RFID researchers created a video showing how an RFID reader attached to an improvised explosive device could theoretically identify a U.S. citizen walking past the reader and set off a bomb. They haven't yet tested the theory on a real U.S. passport since the documents have yet to be distributed. The still here shows an attack using a prototype passport with RFID chip placed in the pocket of the victim. As the chip passes the reader, the reader detonates an explosive device placed in the trash can. View Slideshow

LAS VEGAS -- A German computer security consultant has shown that he can clone the electronic passports that the United States and other countries are beginning to distribute this year.

The controversial e-passports contain radio frequency ID, or RFID, chips that the U.S. State Department and others say will help thwart document forgery. But Lukas Grunwald, a security consultant with DN-Systems in Germany and an RFID expert, says the data in the chips is easy to copy.

"The whole passport design is totally brain damaged," Grunwald says. "From my point of view all of these RFID passports are a huge waste of money. They're not increasing security at all."

Università della Svizzera italiana | Faculty of Informatics

61

ePass Problems

- Tag-Detuning with eVisa
  - Use of multiple RFID-tags problematic
- Key for Basic Access-Control
  - Once read, allows access forever
  - MRZ (key!) known to hotels, travel agencies, …
  - Smart bombs?

Università della Svizzera italiana | Faculty of Informatics

62

Università della Svizzera italiana | Faculty of Informatics

63

TIMESONLINE

NEWS | COMMENT | BUSINESS | MONEY | SPORT | LIFE & STYLE | TRAVEL | DRIVING

UK NEWS | WORLD NEWS | POLITICS | ENVIRONMENT | WEATHER | TECH & WEB | VIDEO | PHOTO

Where am I? › Home › News › UK News › Crime News

From The Times

August 6, 2008

‘Fakeproof’ e-passport is cloned in minutes

Steve Boggan

New microchipped passports designed to be foolproof against identity theft can be cloned and manipulated in minutes and accepted as genuine by the computer software

TIMES RECOMMENDS

- Russia's new elite grabs a bit of London
- Rumpole creator John Mortimer dies at 85
- Strife at union erupts into all-out war

„ ...cloned and **manipulated**... “

Università della Svizzera italiana | Faculty of Informatics

64

Broken?

Università della Svizzera italiana | Faculty of Informatics

65

Broken!

Mustermann
Christian
0000000000000

Proof of Genuine Passport

Università della Svizzera italiana | Faculty of Informatics

66

The Take Home Message

- RFID becoming increasingly popular
  - Ski passes, car keys, ePass, groceries?
  - Huge potential in logistics, counterfeiting
- Significant implications for privacy, security
  - Unwanted identification and tracking
- Simple technology, challenging solutions
  - Small size, low cost often lead to low security
  - Huge number of tags (password management?)

Università della Svizzera italiana | Faculty of Informatics

67