Smart Identification

Friedemann Mattern

ETH Zürich

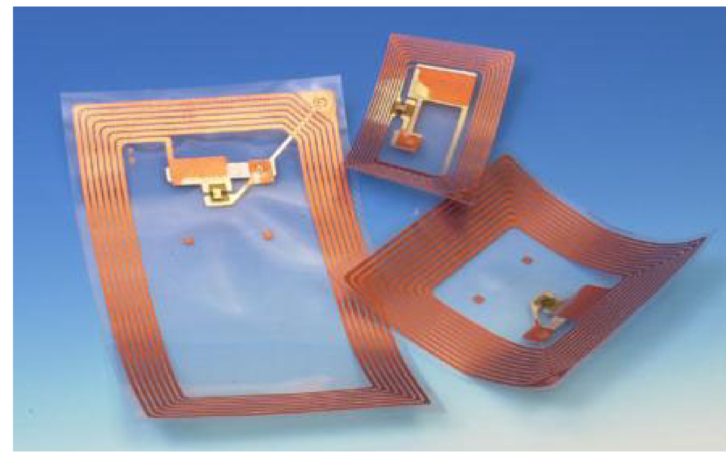
„Smart“ Identification

- Identify objects
  - typically: from distance
  - or: in a secure way
- Various techniques
  - RFID (Radio Frequency Identification)
  - barcodes
  - visual perception and recognition
  - ...
- Purpose
  - associate specific actions, attributes,... with the object
  - authenticate an object (or a person)
  - ...

- e.g., an instance-specific URL
- → virtual-physical integration

Radio Frequency Identification (RFID, „Smart Label“)

- Identify objects from distance
  - small IC with RF-transponder
- Wireless energy supply
  - ~ 1 m
  - (electro)magn. field (induction)
- ROM or EEPROM (read/write)
  - ~ 100 Byte
- Cost ~ € 0.1 ... € 1
  - consumable and disposable
- Smart labels: flexible tags
  - laminated with paper, adhesive



Advanced RFID Chips

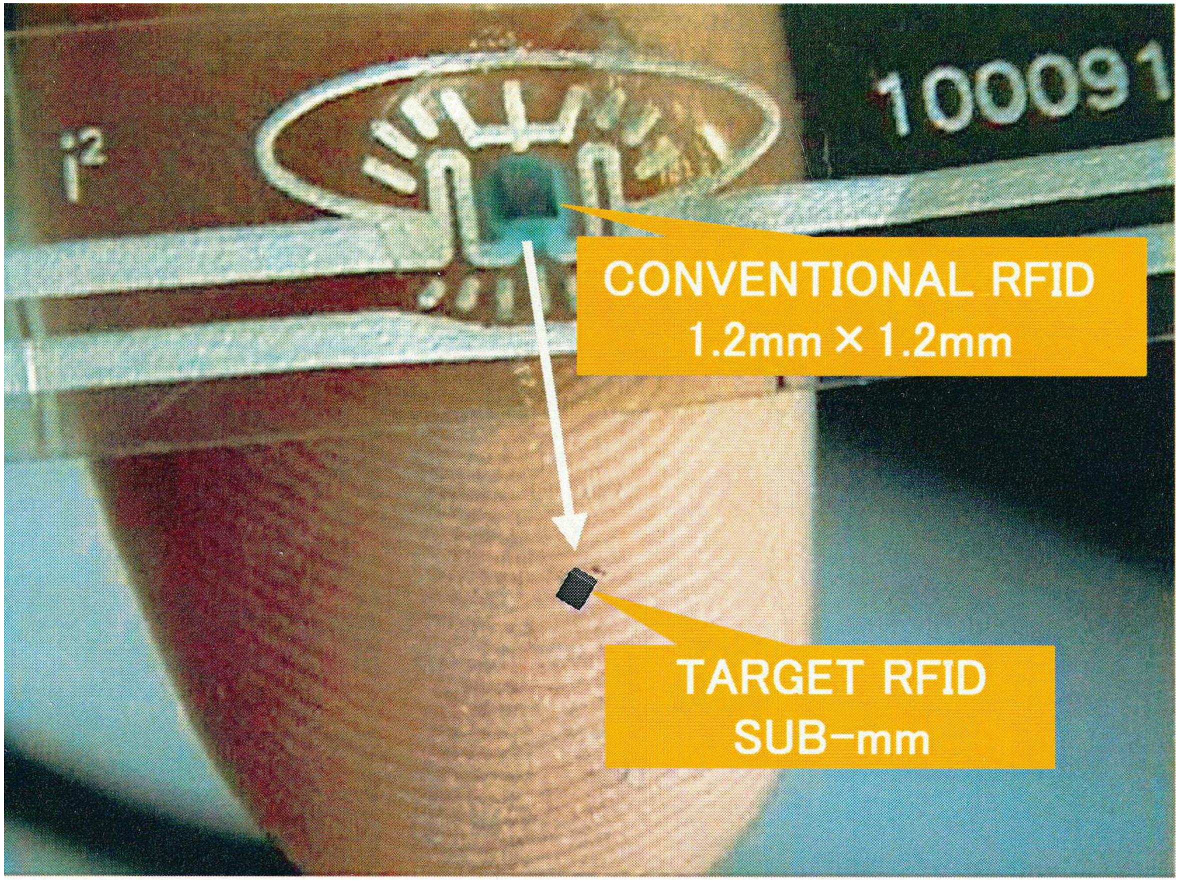
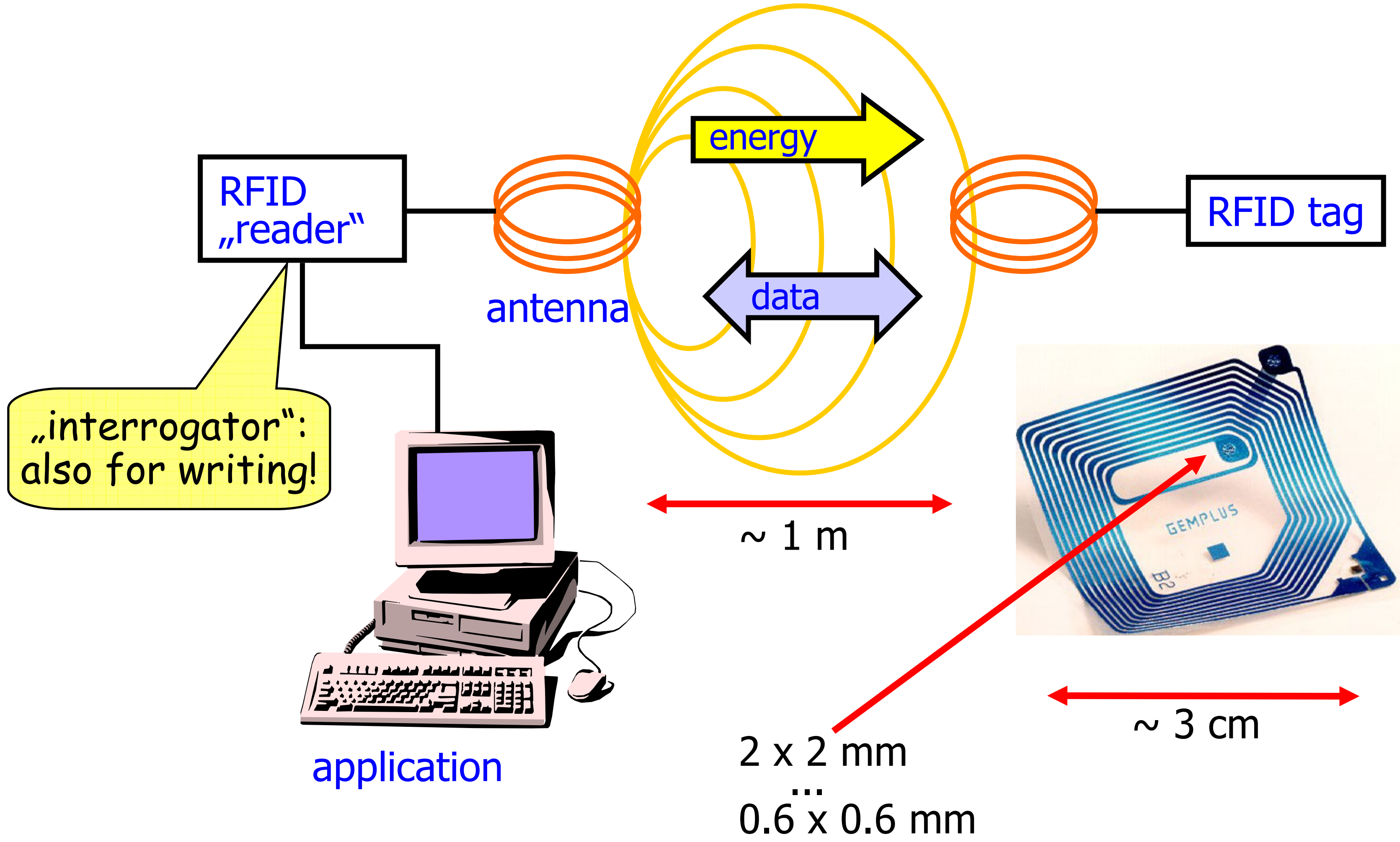


image source: Hitachi

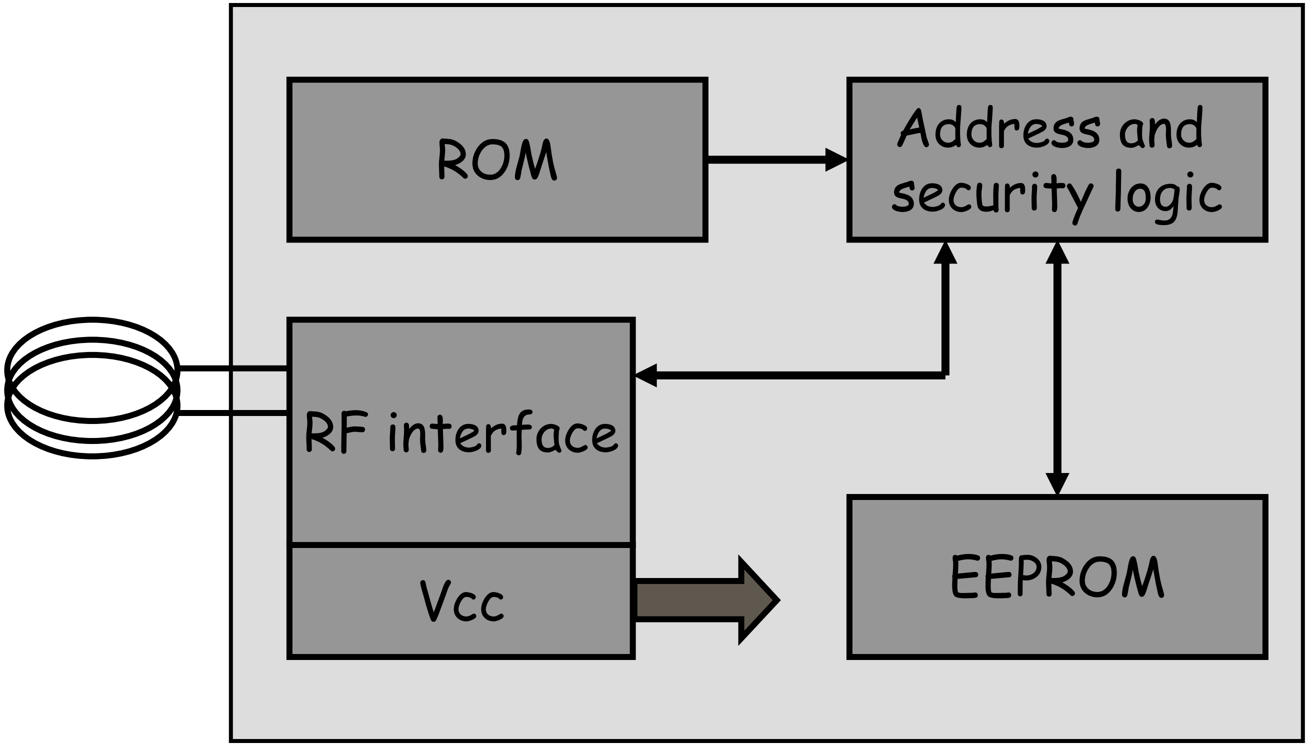
A Classical Application: EAS – Electronic Articel Surveillance


image source: Peter H. Cole

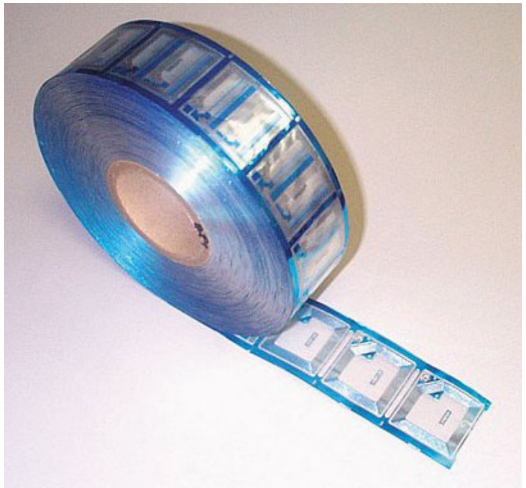
Components of an RFID System

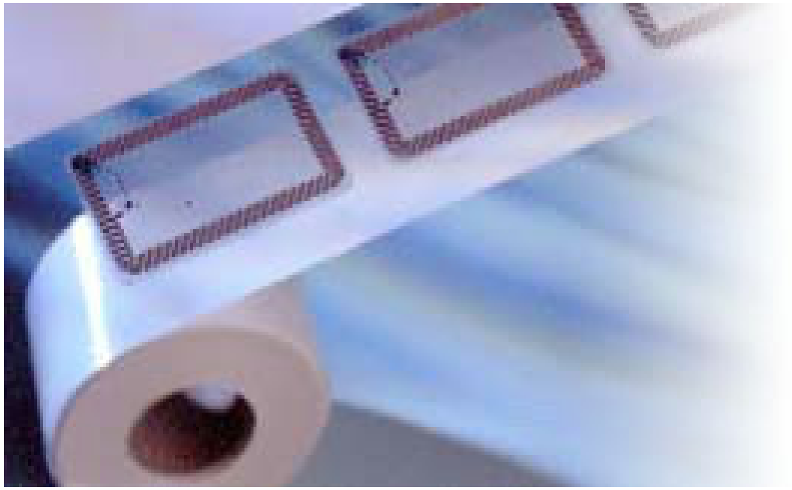


RFID Block Diagram



Smart Labels

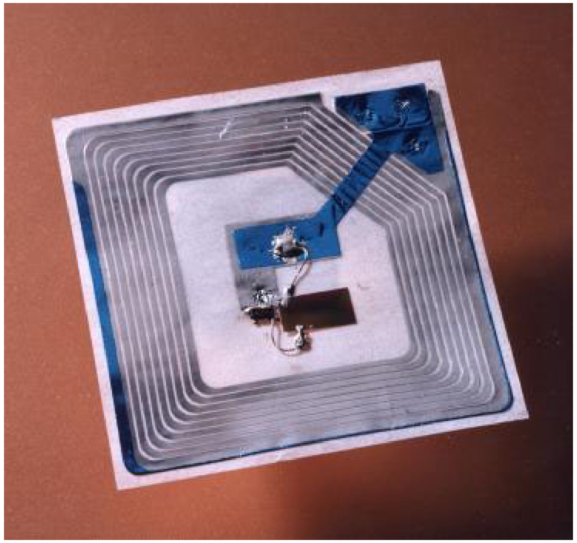




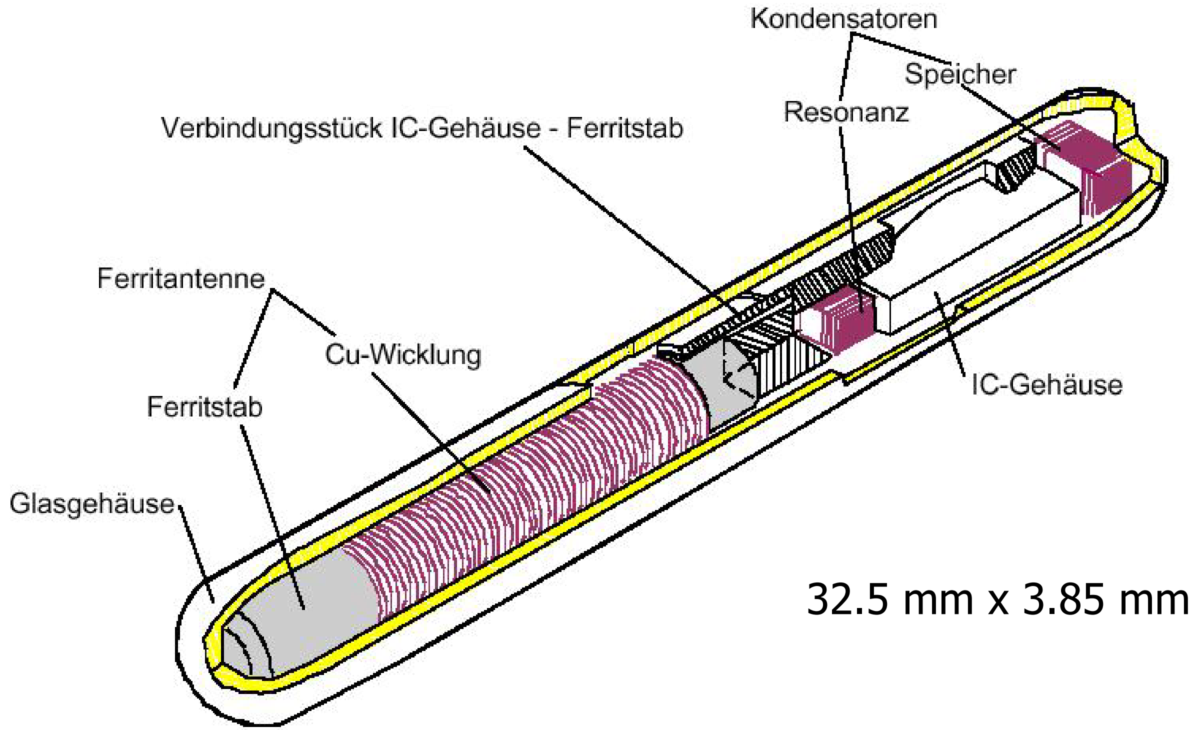
- Chip (without antenna): ~ 2 mm x 2 mm x 10 μm
  - fits into 80 μm thick paper!
- Antenna
  - copper or printed with conductive ink
  - or „coil on chip": micro galvanic antenna on CMOS wafer (for „close coupling systems")

Smart Labels

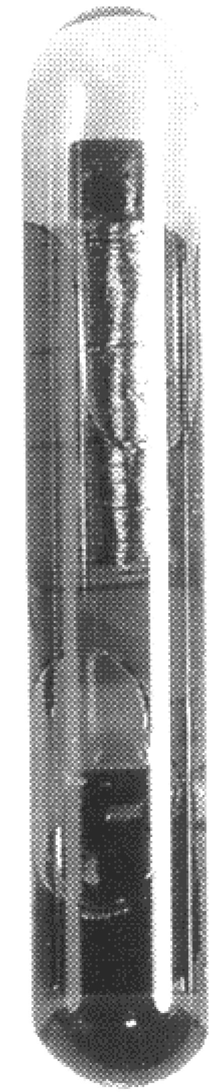
- Cheap 1 bit versions (without true IC) for EAS
- Advanced systems use anti-collision protocols



Glas Transponders

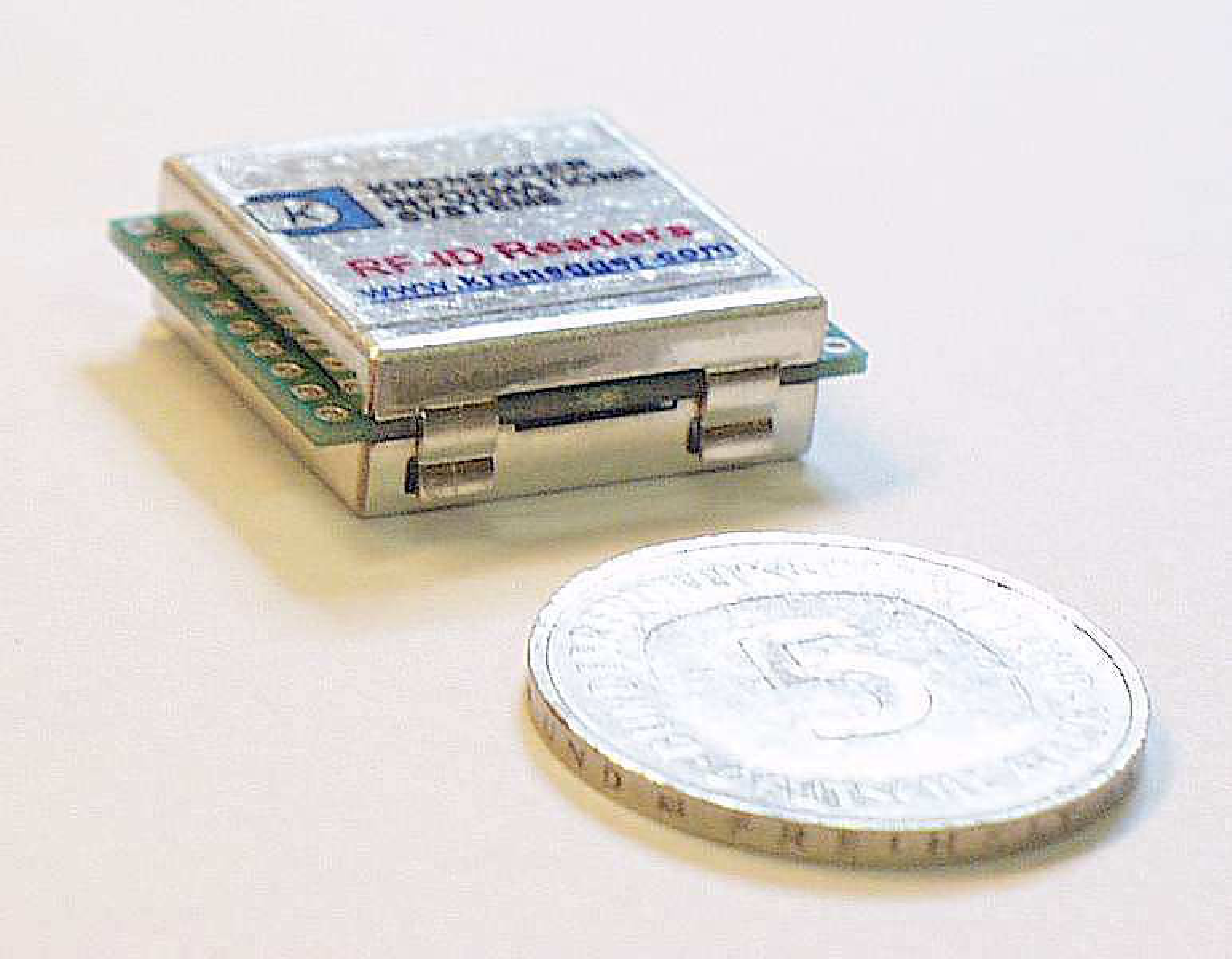


32.5 mm x 3.85 mm

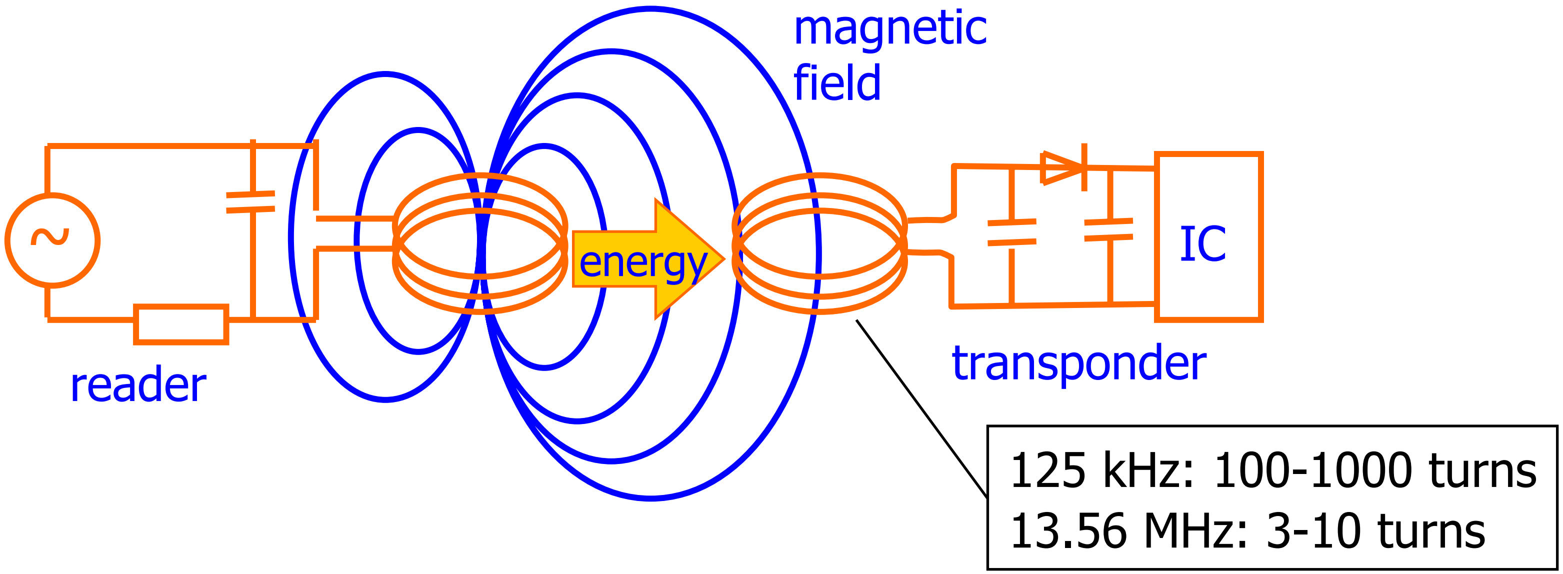


- To be implanted under the skin of animals
  - e.g., ear clips for pet dogs
  - or fed to a cow with the food and reside in its stomach

A Small RFID Reader

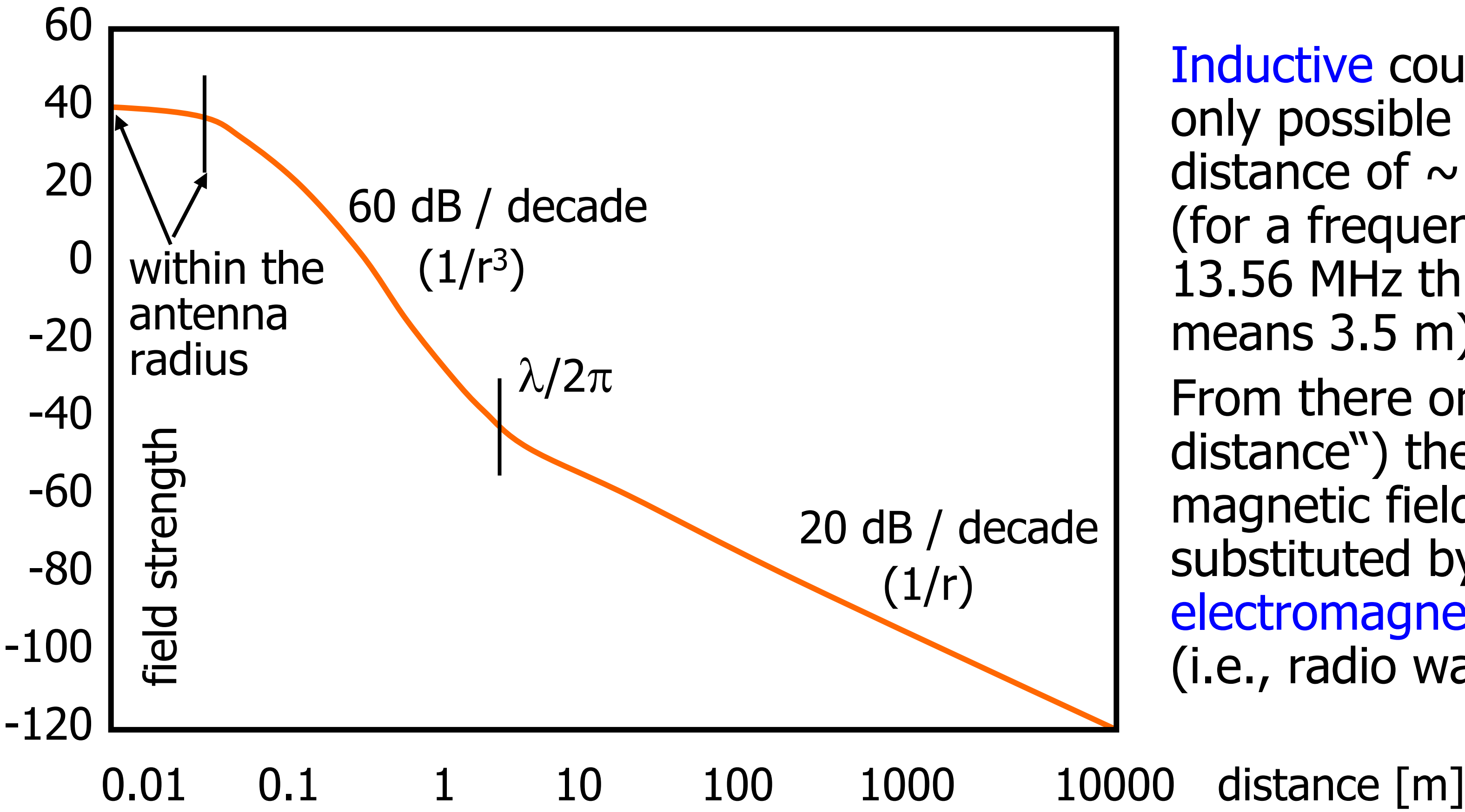


Energy Supply by Induction



- Inductive coupling (magnetic field)
  - similar to a transformer: magnetic field generated by the „reader" induces a voltage in the coil of the transponder
  - condensators for oscillating circuit can be made of 10 μm foils
  - typ. some 10 mW at 1 cm („close coupling"), 100 μW at 10 cm

Field Strength in the Near and Far Field

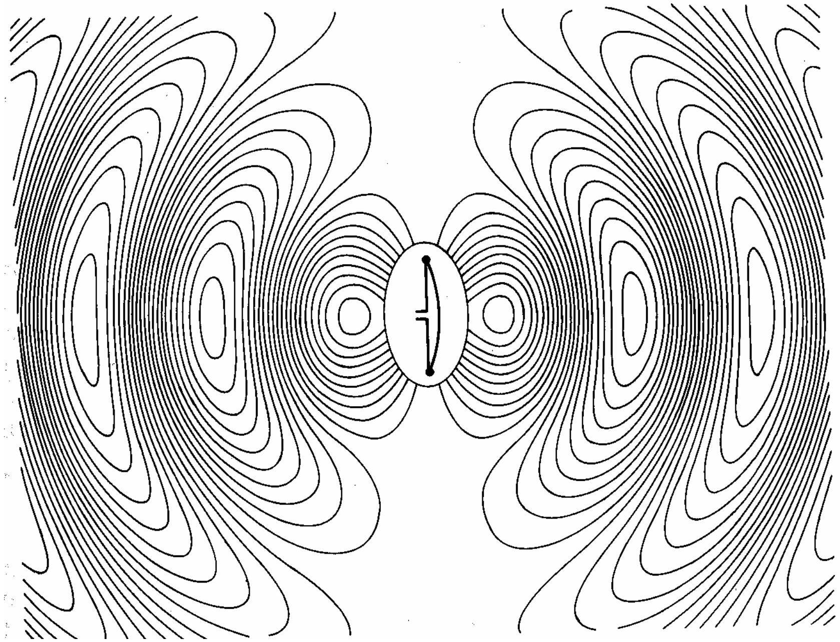


Inductive coupling is only possible up to a distance of ~ $\lambda/2\pi$ (for a frequency of 13.56 MHz this means 3.5 m).

From there on („far distance") the magnetic field is substituted by an electromagnetic field (i.e., radio waves).

Near and Far Field

- The near field is an energy storage field
  - strength: $O(1/r^3)$
- The far field is an energy propagating field
  - strength: $O(1/r)$
- Near field - far field boundary: $\lambda/2\pi$
  - same amplitudes at the boundary
  - examples
    - 100 kHz: 500 m
    - 10 MHz: 5 m
    - 1000 MHz: 50 mm
- The common 134.2 kHz and 13.56 MHz tags operate in the near field

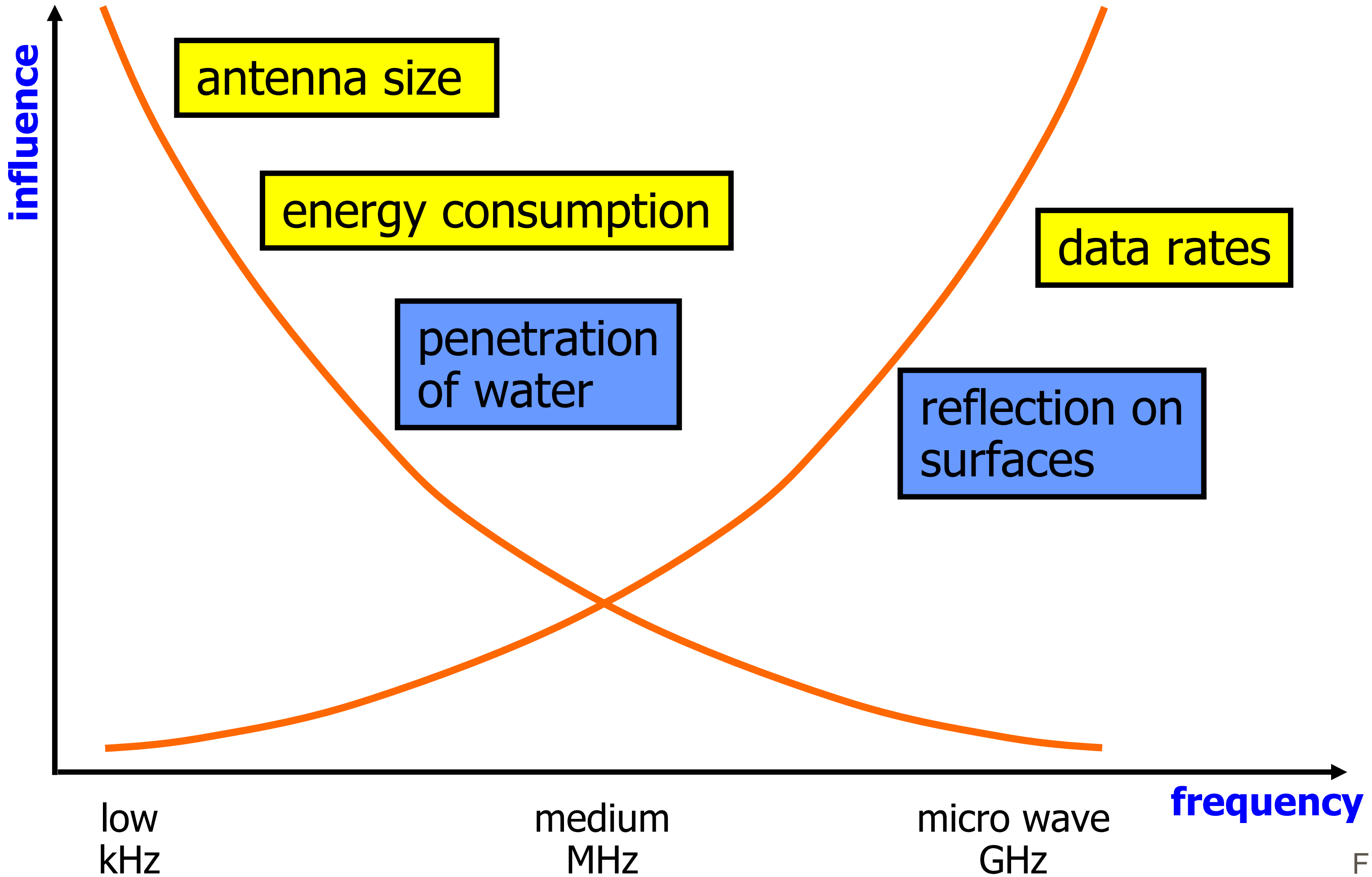


Field launched by an electric dipole

System Performance

- Low end systems
  - read only
  - small, cheap
  - tag repeatedly sends out its serial number
  - no collision detection
- Medium range
  - read-write memory (EEPROM, SRAM)
  - collision detection (typically 30 items / s)
- High end
  - e.g., contact less smartcards
  - complex functions (e.g., cryptography)

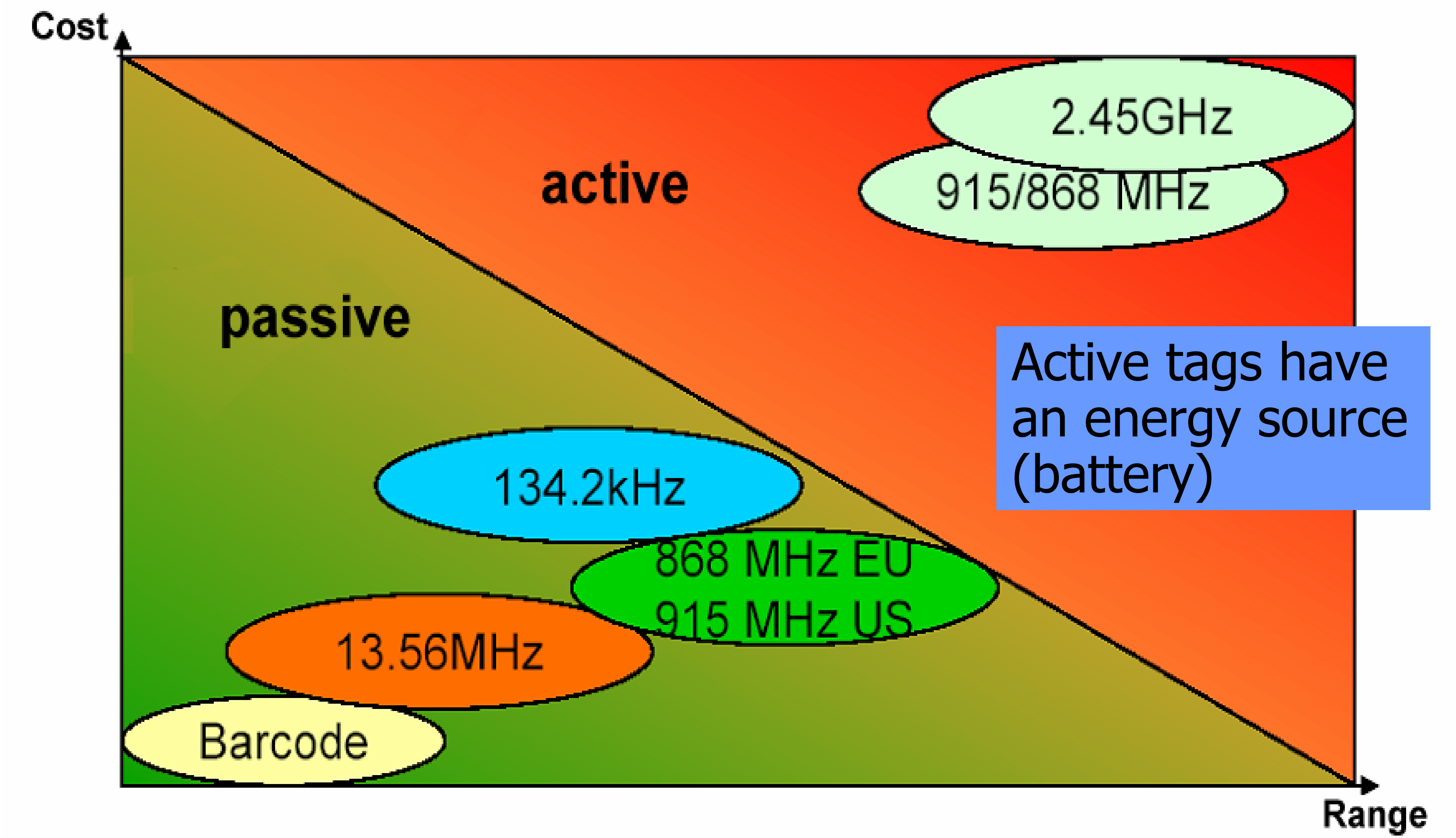
Influence of Frequencies



Frequencies

- Typical frequency domains (usually ISM - Industrial-Scientific-Medical - bands):
  - 100 - 135 kHz (LF)
  - 13.56 MHz (HF)
  - 868/915 MHz (UHF)
  - 2.45 GHz micro wave
  - different characteristics: sensitivity against metal parts (shielding, reflection), sensitivity to orientation of the antenna
  - national / international standards
  - frequencies are often used by many other services

RFID Types

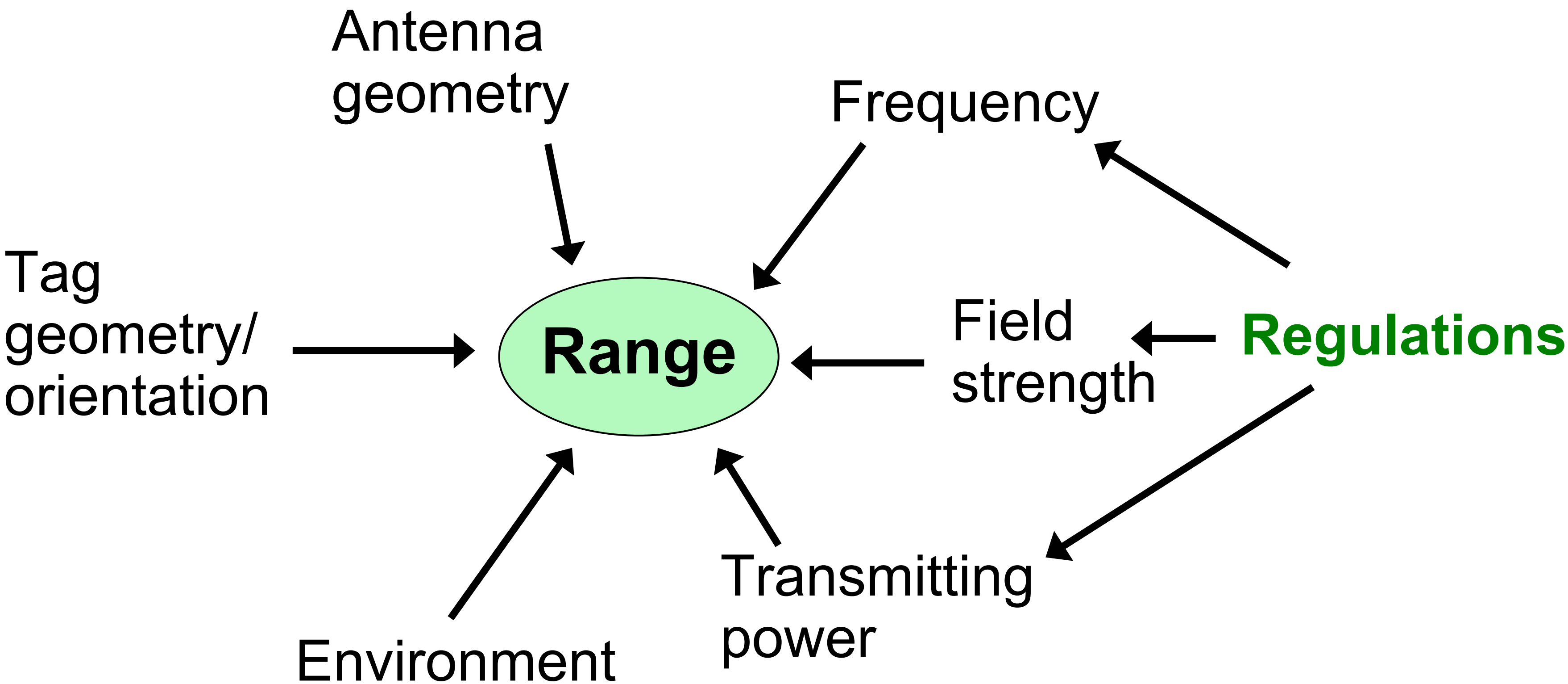


Active tags have an energy source (battery)

Characteristics of Passive RFIDs

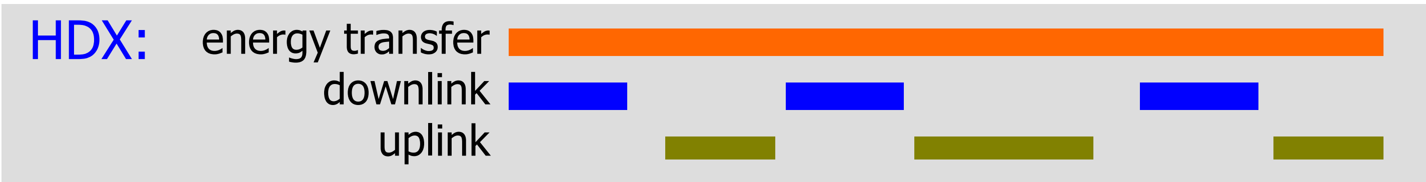
	LF 134,2 kHz	HF 13,56 MHz	UHV 868 MHz (EU) 915 MHz (US)	MW 2,45 GHz
Type of coupling	Near-field (inductive)		Far-field (EM wave)	
Price	Higher	Low	Low	Low
Theoretical read-range	– 355 m	– 3.5 m	Power dependent $\sim \sqrt[4]{Power}$	Power dependent $\sim \sqrt[4]{Power}$
Typical read-range	– 1.5 m	– 1.0 m	– 0.6 m (EU: 0.5W max) – 3 m (US: 4W max)	– 0.5 m (EU: 0.5W max) – 2.0 m (US: 4W max)
Availability	~ 1990	ISO standard since Sep 01	2002: first products in US	2002: first products in US
Environmental influences	▪ Shielding ▪ Conductive materials (e.g. metal)		▪ Shielding ▪ Absorption dependent on material ▪ Reflection ▪ Refraction ▪ Penetration into liquids	
Influences of closely located tags	Antenna detuning of closely located tags		Distortion of radio patterns due to antenna coupling	

Constraints on Read Range

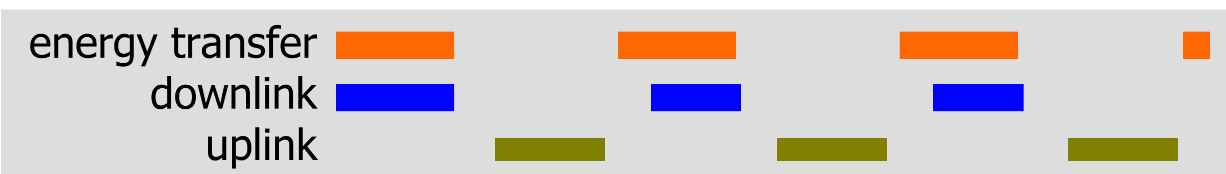


Communication Principles

- Typically half-duplex (HDX)

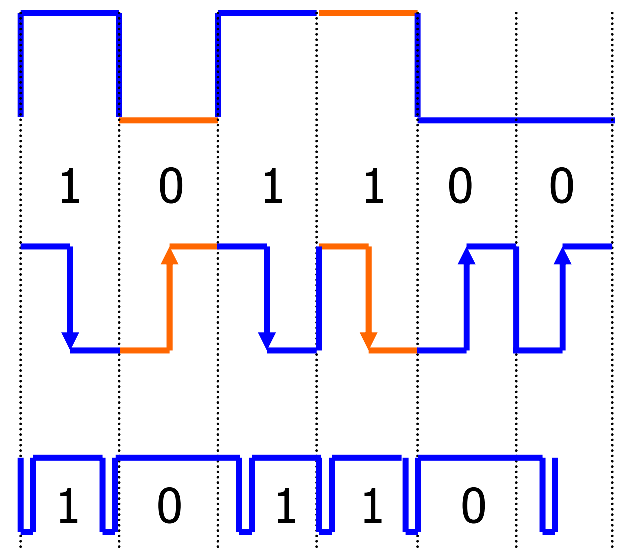


- Field of the reader is turned off periodically
  - to allow transponders to send in-between
  - requires condensator on transponders to store energy



Typical Encoding Schemes

- NRZ
  - 1 = „high“, 0 = „low“
- Manchester coding
- Pulse pause coding (PPC)
  - 1 = short pause to next pulse
  - 0 = long pause
  - with inductively coupled systems: continuous energy flow if pulse<<t_{bit}

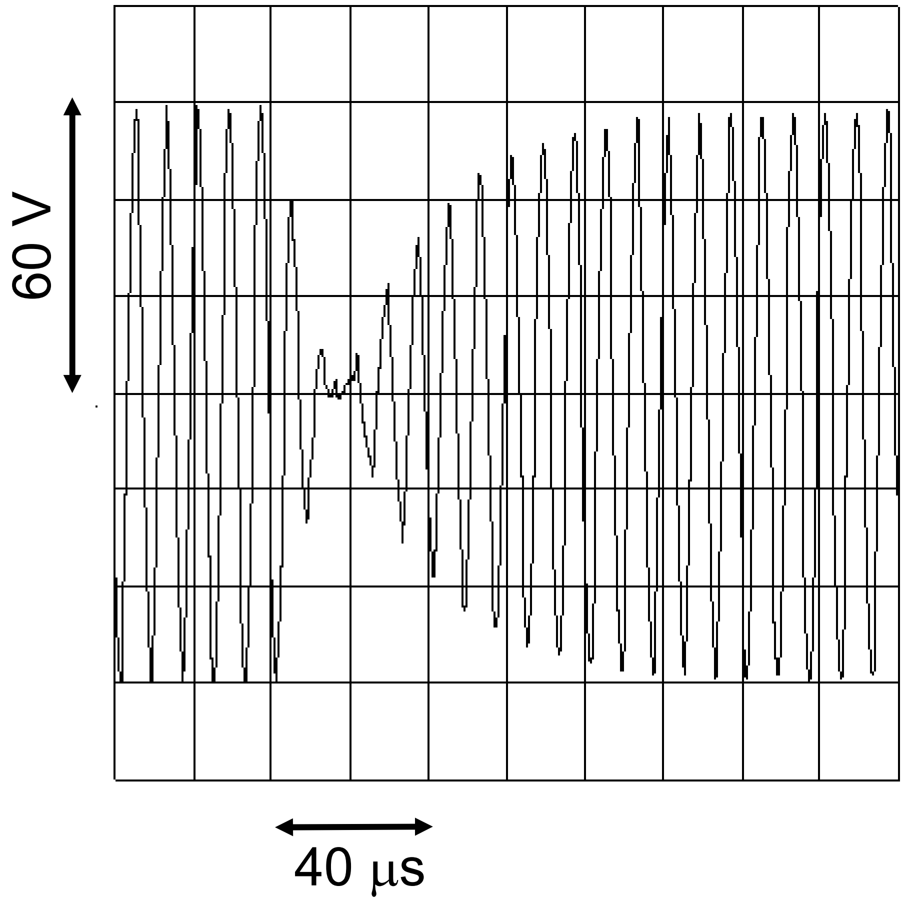


Data Transfer Reader → Transponder

- Typically ASK (Amplitude Shift Keying) of the reader`s field
  - switching off the field for short periods (transponder then gets its energy from its resonant circuit)
- Typ. several kbit/s, up to ~100 kbit/s
  - but: setup time

Switching on / off the Antenna of the „Reader“

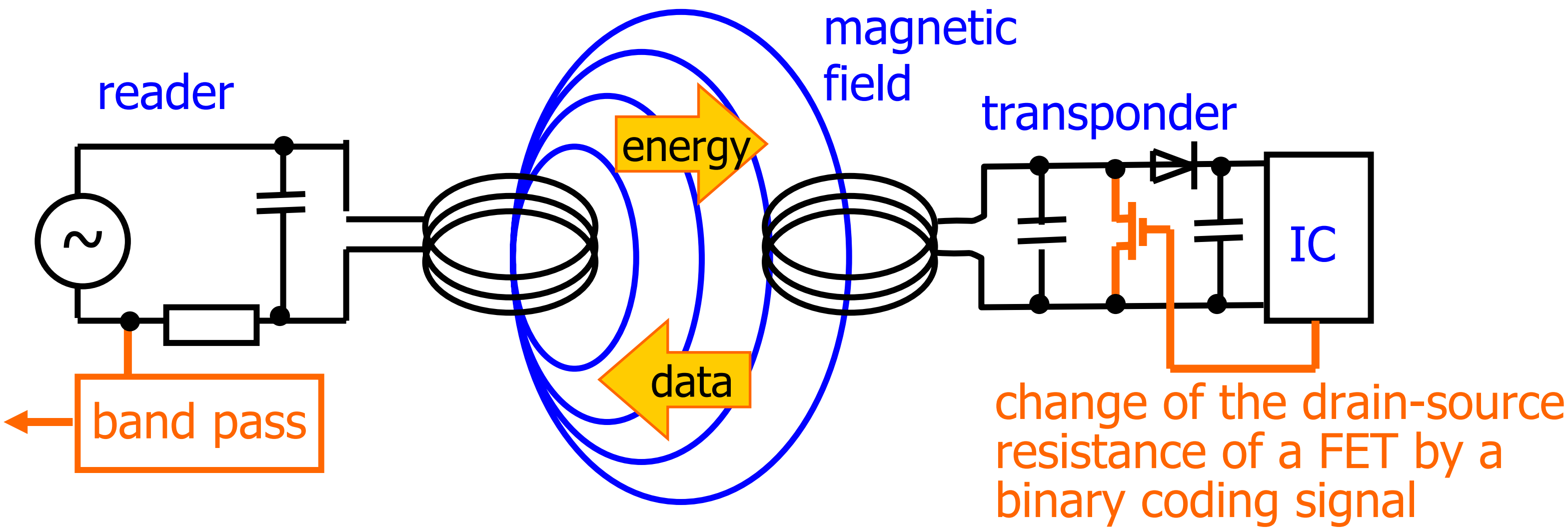
- Typical field gap for sending data to the transponder with „on / off keying“ of the magnetic field



Data Transfer Transponder → Reader

- Several principles:
  - capacitive coupling, ~ 10 pF (electrical field, some mm)
  - load modulation (near distance, magnetic field)
  - backscatter (long range, electromagnetic field)
- Data rate: typ. several kbit/s, up to ~100 kbit/s
  - but: time for anti-collision!

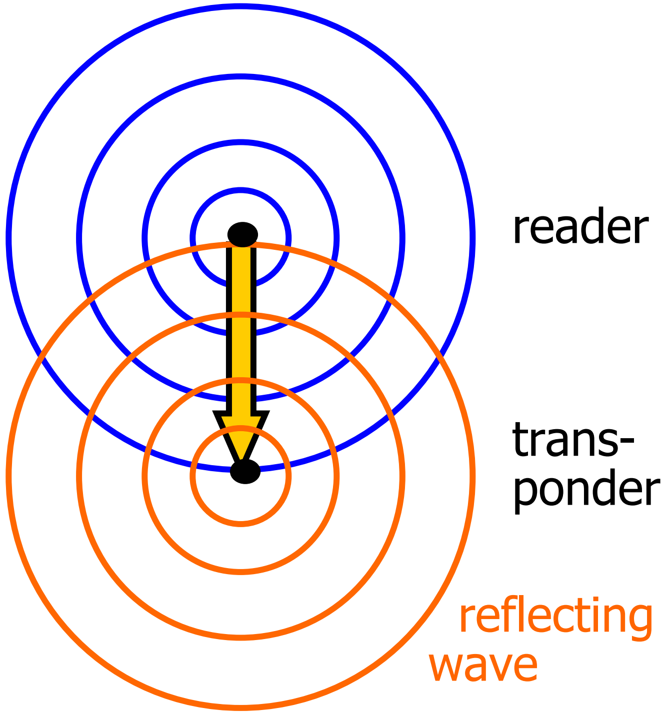
Load Modulation



- Transponder absorbes some energy of the magn. field
- Turning on and off a resistor in the oscillating circuit of the transponder yields a small voltage change at the antenna of the reader
  - typically only ~ 10 mV for a reader antenna with 100 V (i.e., 80 dB signal-“noise“ ratio)

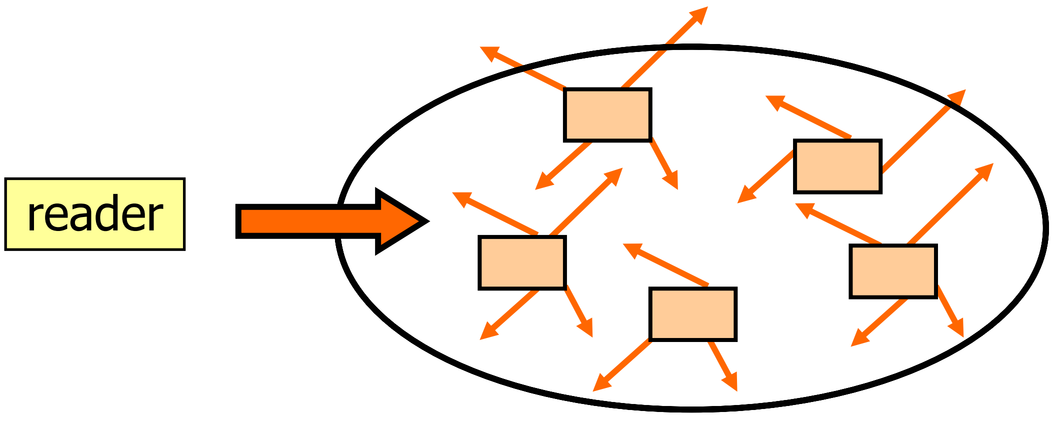
Backscatter Modulation

- Electromagnetic coupling
  - for „long range“ systems
  - but usually no energy transfer with electromagnetic waves
- Reflection of the HF signal
  - > ~2 GHz (microwave)
  - radar principle
- Change of the reflection properties by switching on and off a resistor parallel to the transponder antenna



The Collision Problem

- Reader broadcasts energy and its signals to many transponders



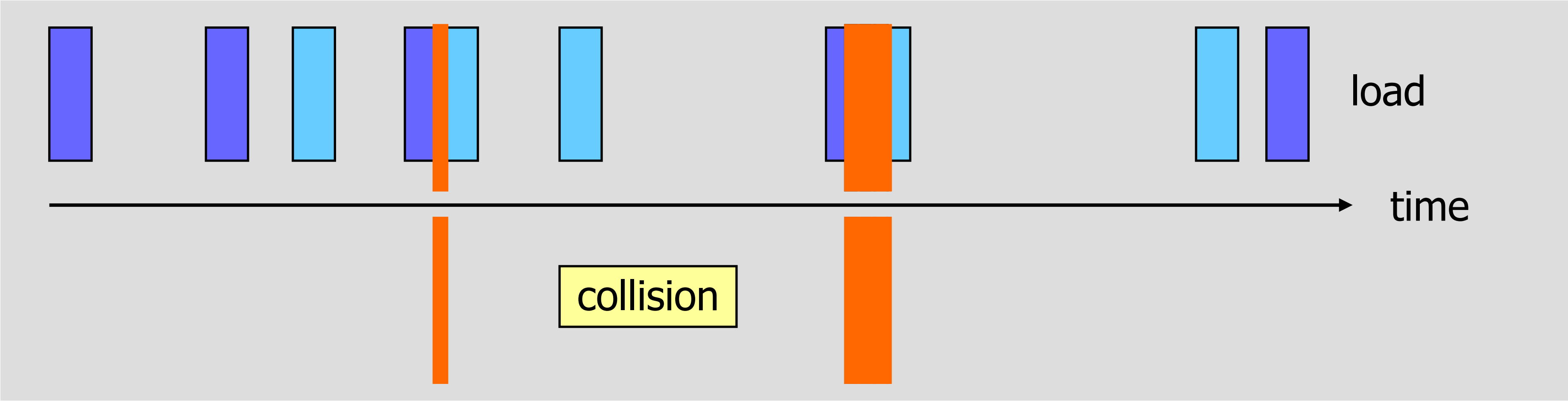
- All transponders may react simultaneously
  - they will interfere if there is only a single channel
  - why can‘t we use the Ethernet principle (CSMA/CD)?

Anti-Collision Schemes: Requirements and Properties

- A transponder should only have exclusive access to the shared channel for the short period where it transmits its few bytes
- Transponders usually don‘t hear the signals from other transponders, they can only listen to the reader‘s signal
- Reader should always detect collisions
- Access control and collision detection / avoidance should be fast and reliable
- Most anti-collision schemes are either patented or undisclosed

The ALOHA Principle

- Stochastic TDMA (Time Domain Multiple Access)
- Transponders repeatedly send out their data
  - with long quiet periods in-between



- If collisions happen only occasionally, the data of each transponder should eventually get through

Performance of ALOHA

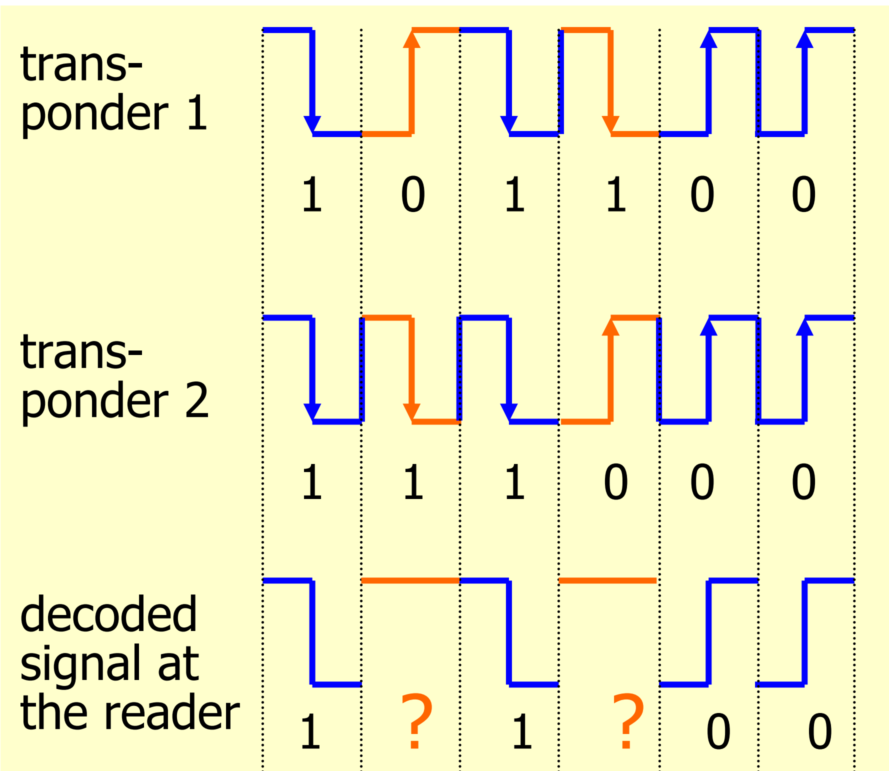
- Probability p that a single packet is transmitted without collision depends on the load: **$p = e^{-2G}$**
- Performance of a sample system [Finkenzeller]:

Number of transponders	average	99%	99.9%
2 transponders	150 ms	350 ms	500 ms
4 transponders	300 ms	750 ms	1000 ms
6 transponders	500 ms	1200 ms	1600 ms
8 transponders	800 ms	1800 ms	2700 ms

- 100% ?

A Tree-based Collision Avoidance Algorithm - The Coding Scheme

- With Manchester encoding it is possible to locate the bits where two different digital signals differ:



- Illegal signal („high" or carrier signal during the whole bit period)
- Requires bit synchronization (e.g. slotted ALOHA)
- Note that this is not possible with NRZ coding

A Tree-based Collision Avoidance Algorithm - The Basic Idea

- Reader broadcasts a „sync“ command to all transponders and requests their serial number
- Reader determines leftmost bit b that yields a collision (if any…)
- Reader broadcasts „mute“ with „position b=0“
- Only transponders with b=1 move to the next round, all others remain mute from now on

collision

no collision

- Reader requests data from unique transponder x
- Reader sends halt command to x
  - so that it does not compete again until next sync

A Tree-based Collision Avoidance Algorithm

- Once a transponder has been served, one moves up one level and changes the value of b
- Straightforward tree traversal! (Details omitted)
- Sync command should reset the state of all transponders

Algorithm is deterministic
(may, in contrast to ALOHA, reach 100% - at least in theory)

Challenges for RFID Systems

- Many practical application demand
  - large population of tags
  - dynamic tag population
  - random orientation of tagged objects
  - very high speed reading

- Examples
  - courier & postal
  - laundries
  - warehousing
  - retail

An Example System: Philips I-Code Tags

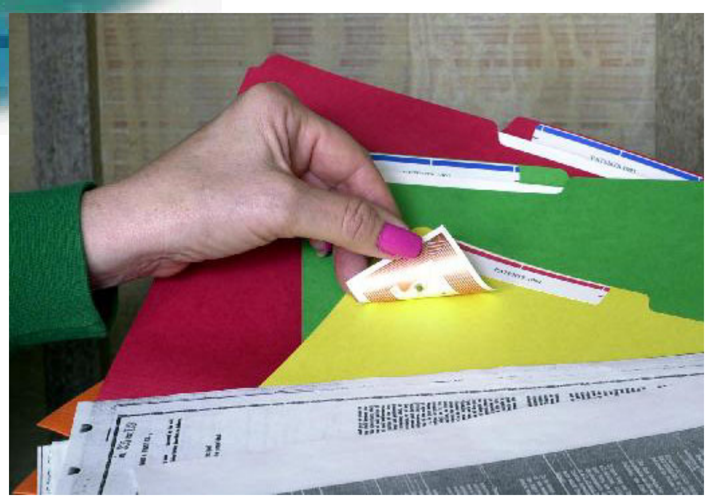
- 384 bit user memory; 64 bit serial number
- 10 years data retention time
- r/w up to 1.2 m, EAS detection up to 1.5 m
- 13.56 MHz
- Typically 30 tags / s (anti-collision)
- Labels with different antenna sizes:
  - 20x20 mm, 49x49 mm, 48x78 mm,…
- Prices (2000) per label:
  - 100 million, 20x20 mm, inlet only: $ 0.33
  - 10 000, 48x78 mm with color printing: $ 1.55

Classical Application Domains

- Inventory control
  - shops or mini bar in hotel rooms
- EAS (electronic article surveillance)
  - anti-theft functionality
- Libraries, video rental

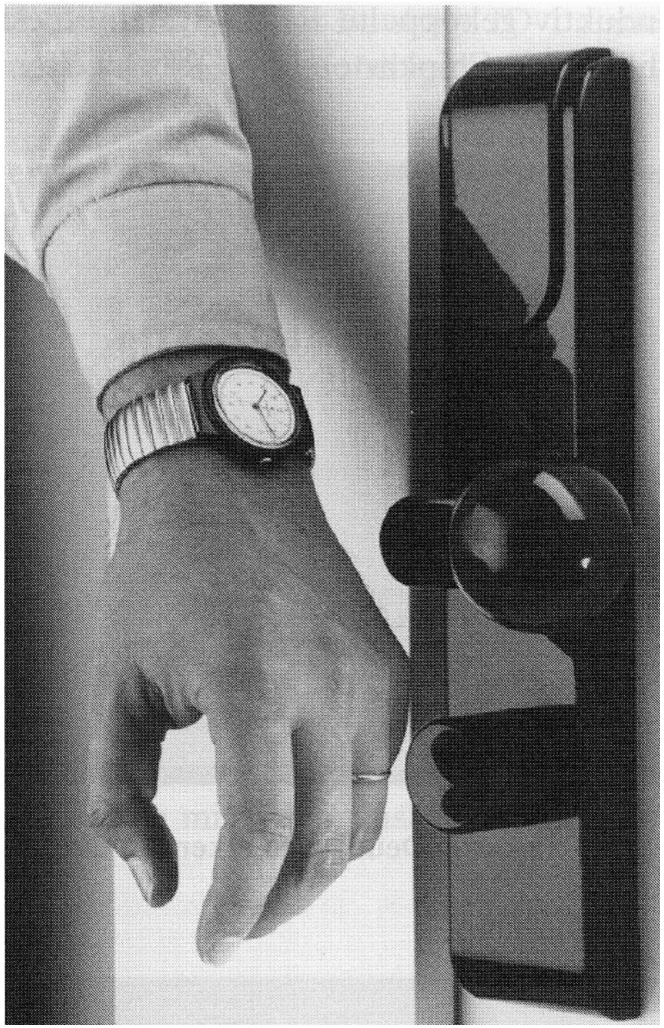
Application Domains for RFIDs

- Transport of mail and parcels
- „Radio signature" of documents
- Tracking of goods
- Ear clips for animals
- Access token (e.g., ski pass)



Electronic Baggage Labels

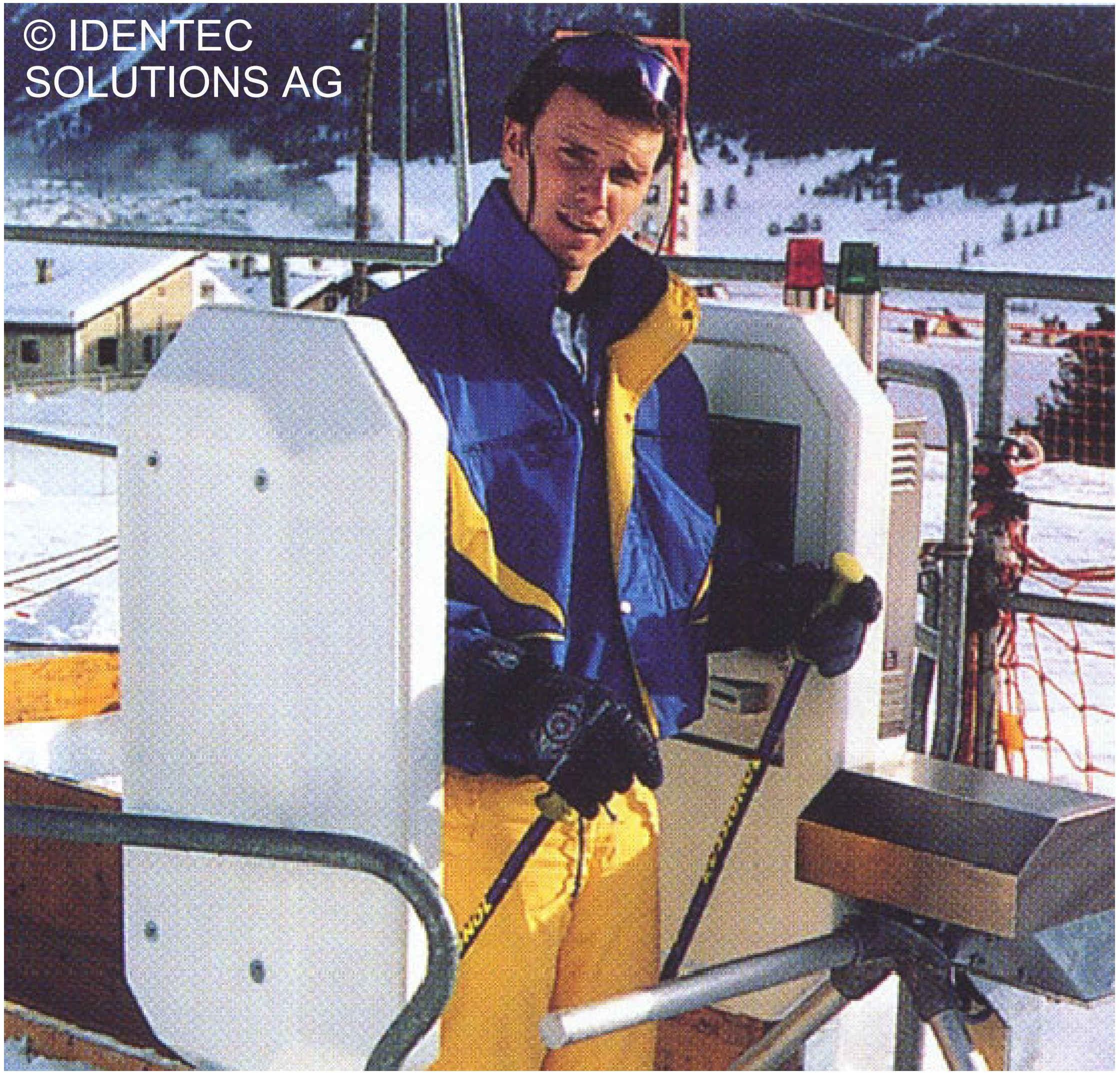
Contactless Access Control



Watch and car key with integrated RFID for contactless access control (e.g., lock a computer when operator leaves it)

Leisure Park Entry System

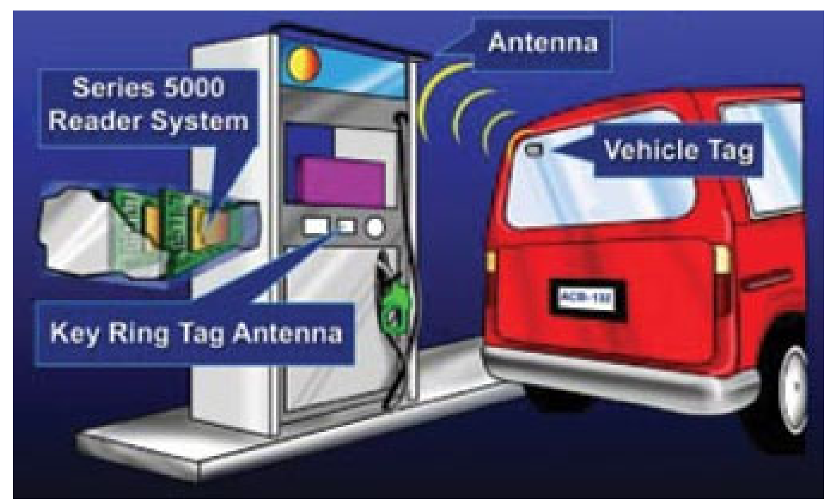
Ski Ticket



RFID tags in wrist belts

Wireless Payment

- ExxonMobils RFID-based „Speedpass“ payment system
  - small, portable transponder
  - reader at point of sale
  - centralized customer database
- Fast and convenient way to pay
  - authorization and transaction in less than one second
  - amount payable is debited from credit card



Waste Collection

image source: Peter H. Cole

RFIDs in Logistics

RFIDs in Logistics

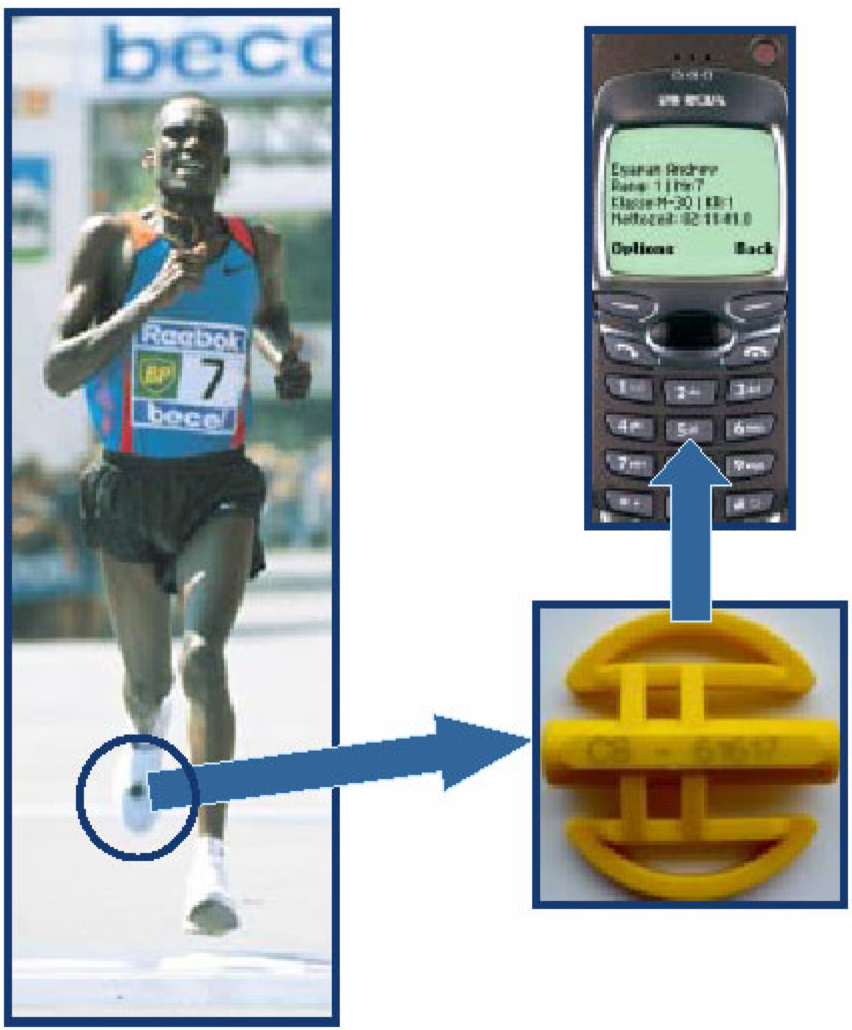
- Product tracking
- Realtime inventory
- Fast check in and check out process
  - unload of an entire truckload takes 30 min (instead of 150 minutes)
- Optimization of shelf life time

Food supply chain management at Sainsbury

RFIDs in Logistics

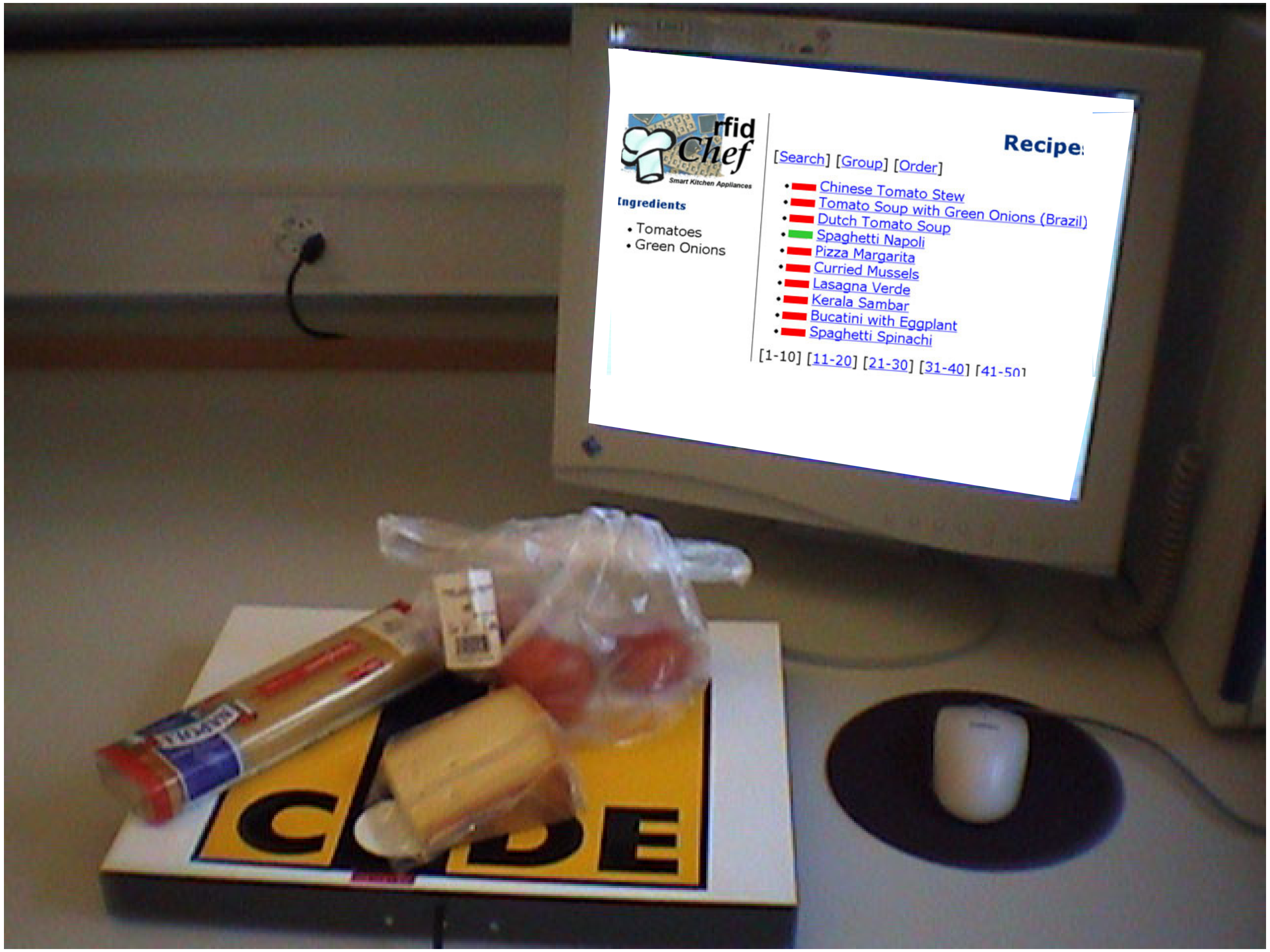
Identification of Vehicles with RFIDs

Real-Time Measurements



Supermarket: Automatic Checkout

A Context Sensitive Cookbook



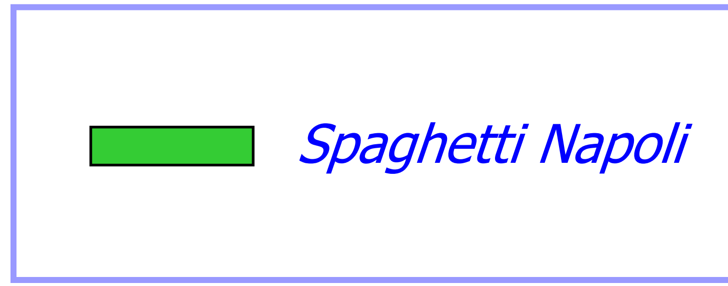
A Context Sensitive Cookbook

- Place grocery items on the kitchen counter

- Nearby display shows dishes that can be prepared with available ingredients

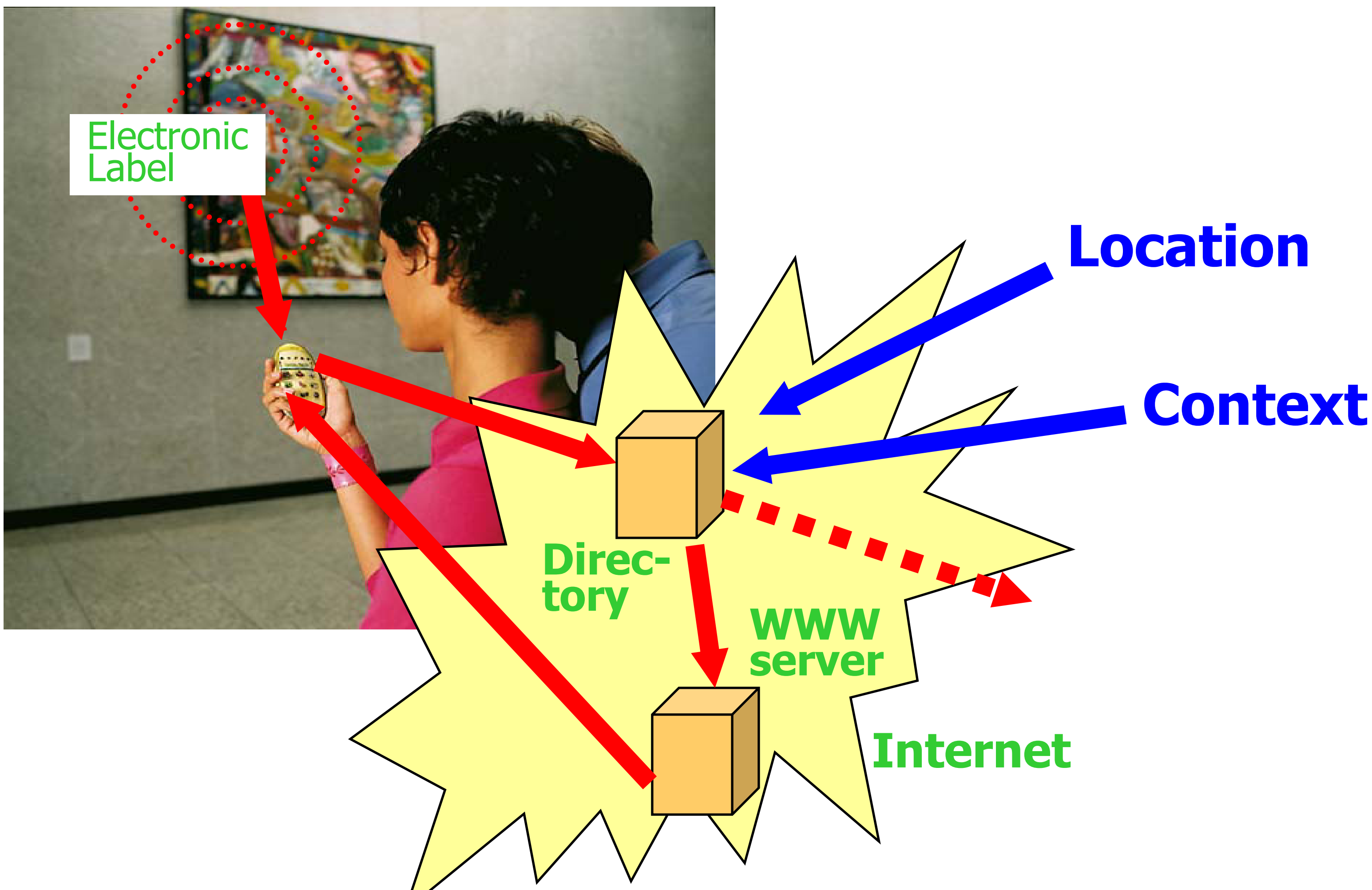
Context Awareness

- Properties of the ingredients
  - check whether there is enough of an ingredient
  - prefer ingredients with earlier best-before data



- Properties of the kitchen
  - check whether required tools and spices are available
- Preferences and abilities of the cook
  - prefers Asian dishes
  - expert in vegetarian dishes

The Power of Smart Labels: Copy by Reference



www.usatoday.com
USA TODAY
Money
SECTION B

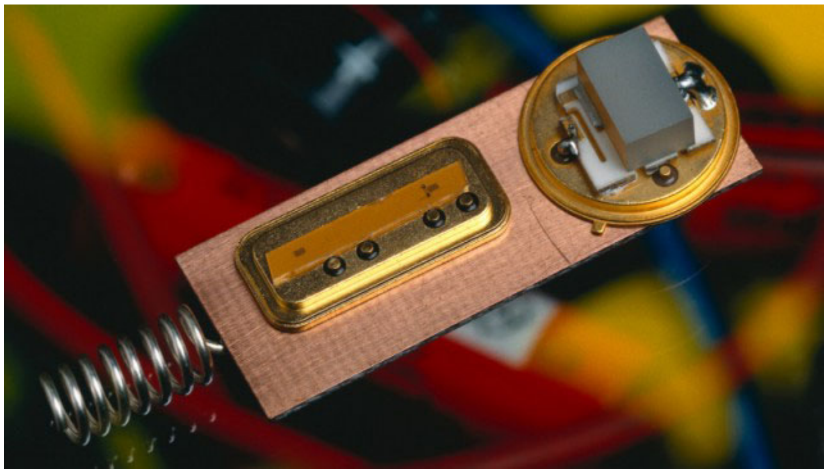
Friday, April 12, 2002

New chips could make everyday items 'talk'

Lose your glasses? A computer could tell you they're under the couch

By Bob Laird, USA TODA

Standalone Radio Sensors



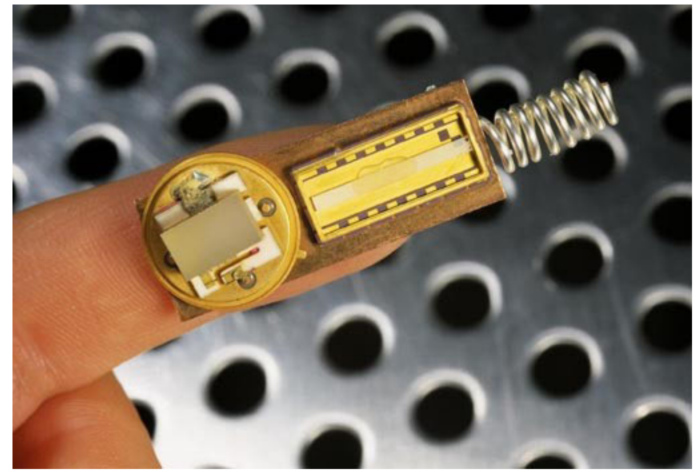


image source: Siemens

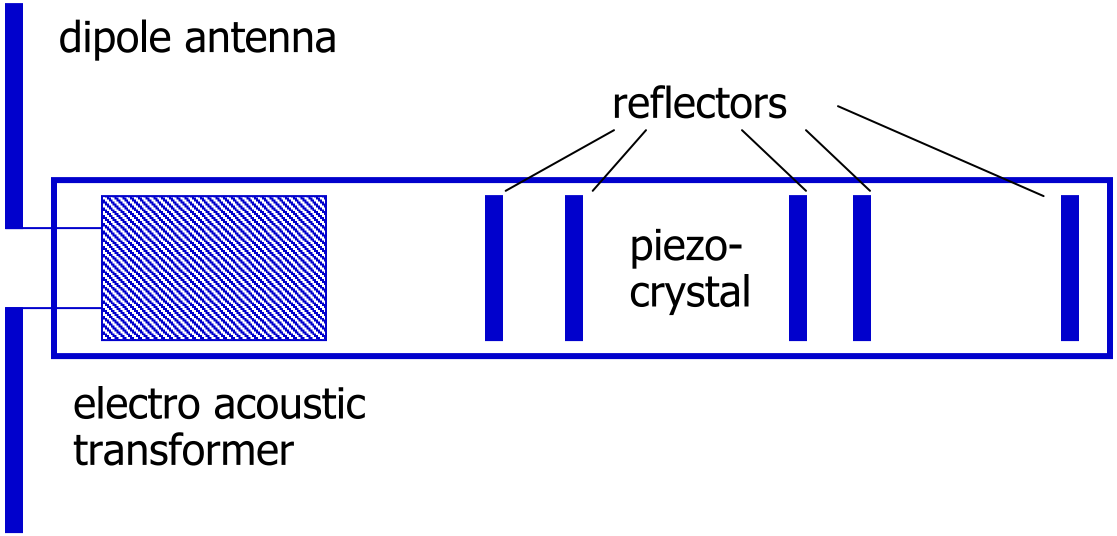
- No external power supply
  - energy from the actuation process
  - piezoelectric and pyroelectric materials transform changes in pressure or temperature into energy
- RF signal is transmitted by an antenna (up to 20 m)

Radio Sensors - Applications

- Wireless light switch
- Remote control
- Temperature surveillance
- Fire detectors
- Inventory control
- …

Piezoelectric Transponders

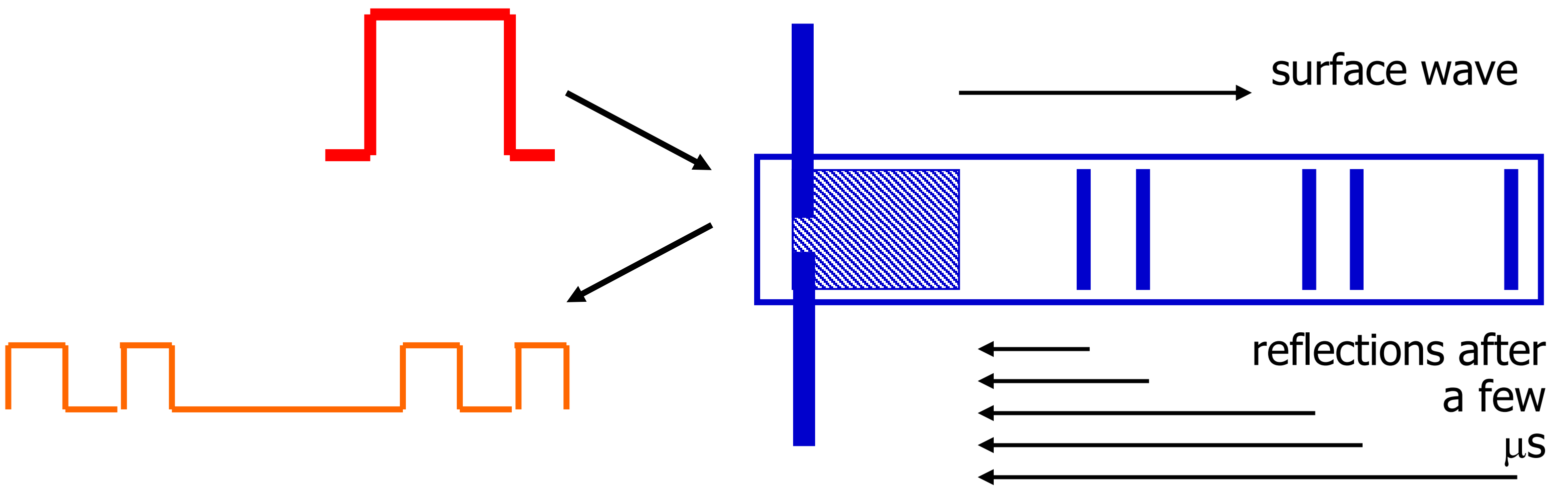
- Transformer:
  electrical signal $\leftrightarrow$ acoustic surface wave
  - in both directions
- Surface wave:
  propagates on the surface of a body
  - on piezo crystals:
    ~ 3500 m/s



- Reflectors consist of 0.1 μm thinn aluminium stripes

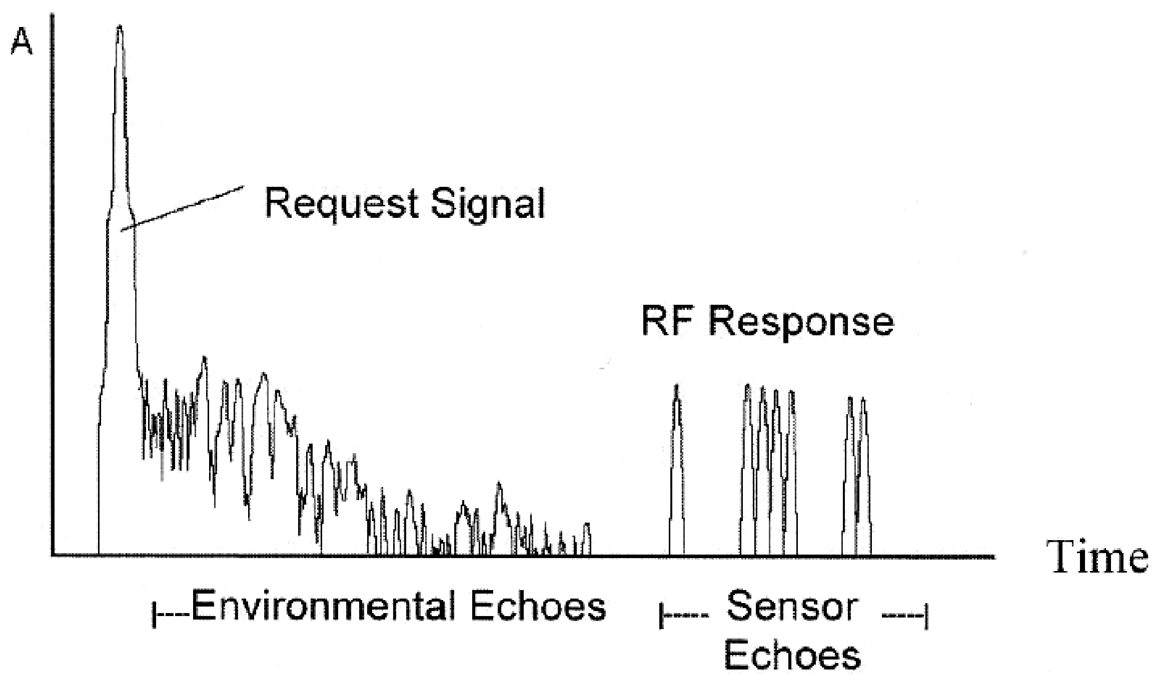
Piezoelectric Transponders

- External energy pulse
- Transformed into a surface wave
- Each reflector sends parts of the wave back to the transformer
- Transformed into RF pulses and sent out



Piezoelectric Transponders

- Surface wave is much slower than RF wave
  - RF noise (e.g., reflections by the environment) vanishes after 1 μs
  - RF response takes more than 2 μs

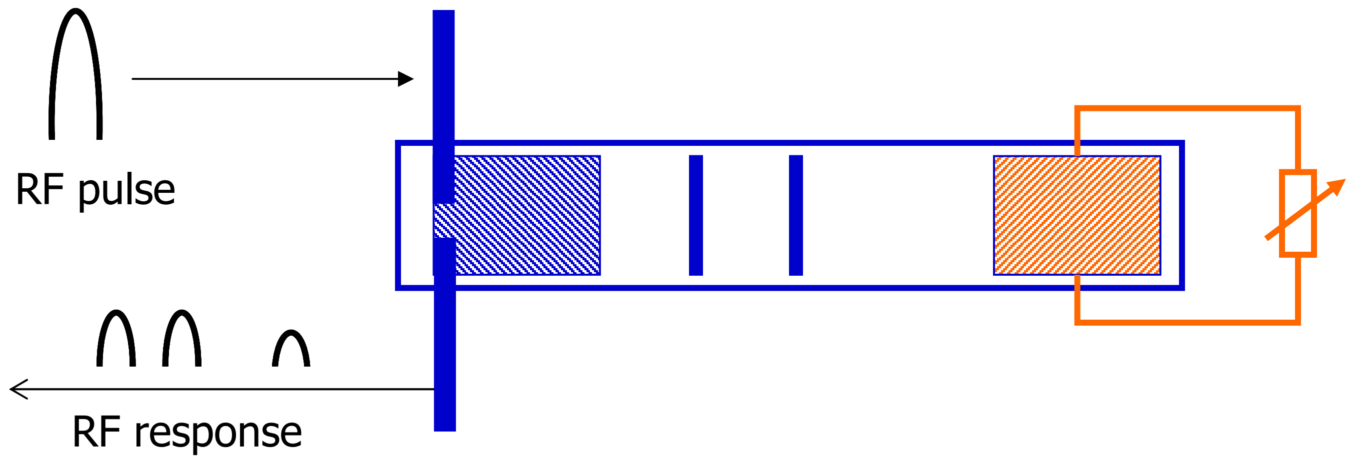


Remote Identifications

- Characteristic pulse sequence by specific alignment of the reflectors
  - e.g., binary digits → up to 32 bits
  - → identification of remote objects

- Use as a temperature sensor:
  - $LiNbO_3$ has a temperature coefficient of 94 ppm/^{o}C
  - measurement of the time difference of the signals (independent of the distance of the sensor!)

Remote Sensors



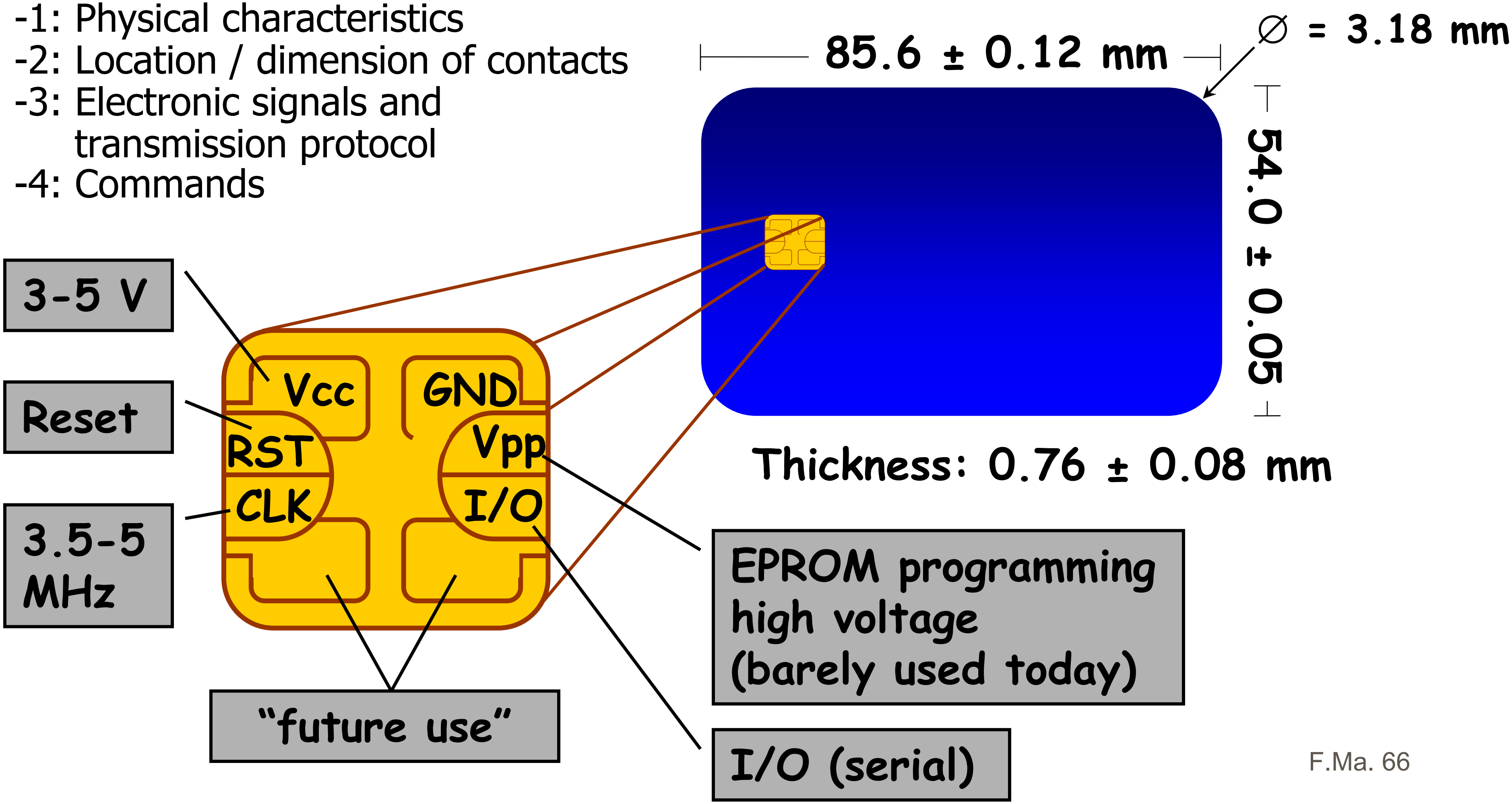
- Second transformer at the end changes the impedance
- Can be controlled by a resistor that depends on some sensor value
  - e.g., photo resistor, NTC/PTC resistor, hall sensor

Smartcards

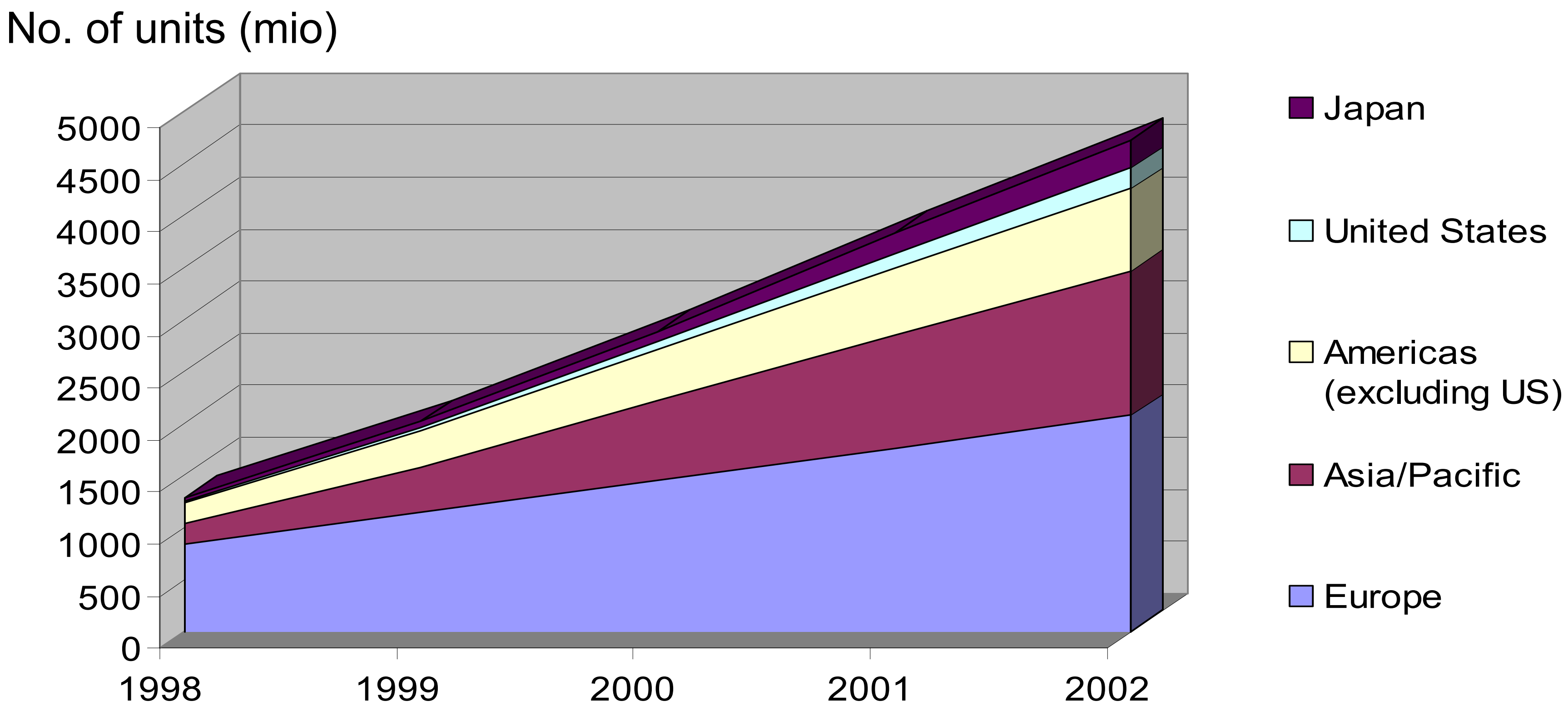

C@PPUCCINO
Giesecke & Devrient
The Java chameleon for all markets
GemXpresso
Bull
Odyssey
Java Card
Who wouldn't be attracted to a Smart Card that supports Java?
Schlumberger
Cyberflex, the card for Java
Microsoft Windows Smart Card Toolkit
Microsoft Windows Powered

ISO 7816 Standard

ISO 7816
-1: Physical characteristics
-2: Location / dimension of contacts
-3: Electronic signals and
transmission protocol
-4: Commands



Smartcard Market Forecast
Regional



Source: Dataquest (August 1998)

Why Smartcards?

- Main use today:
  - portable and secure container for secret data (keys...)
  - secure execution environment for cryptographic algo- rithms (e.g., processing keys that never leave the card)

- Interesting technology for the future:
  - general "trusted computing base"
  - portable computer
  - enabler for ubicomp applications (contactless…)

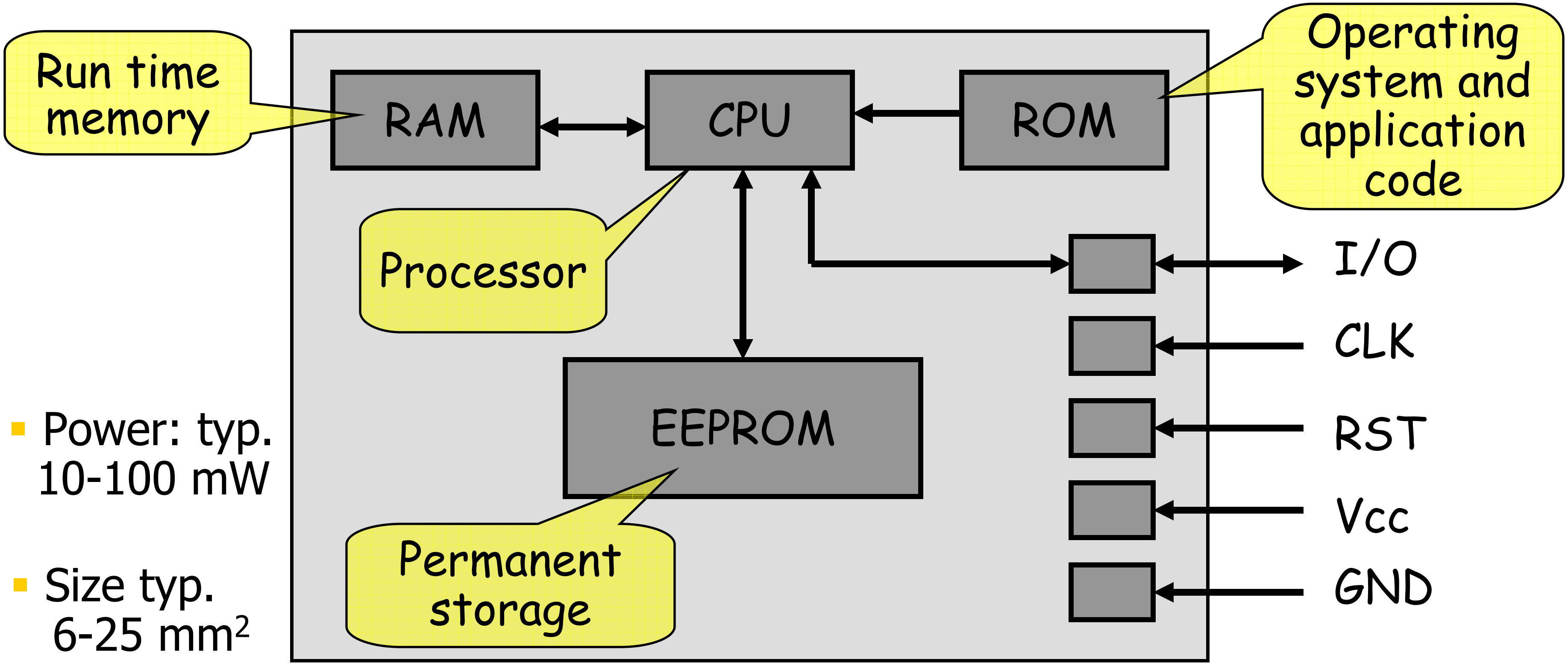
Application Areas

- Financial
  - credit cards, electronic purses, e-banking,...
- Telecommunication
  - phone cards, subscriber-identification in mobile networks,...
- Healthcare
- ID
- Security device
  - digital signature, e-mail encryption,…
- Access control
  - e.g., alternative or in addition to passwords
- Loyalty cards
- Pay TV
- Electronic ticketing (e.g., mass transit)

Processor Cards

- True "smartcards"
  - internal microprocessor (typically: 8 bit processor, but up to 32 bit possible)
  - card can perform calculations internally, thus secret data does not need to leave the card (security!)
  - true random generator difficult (digital signatures!)
  - memory typ. 2-72 kB EEPROM, 24-256 kB ROM, 256-8192 byte RAM
  - 2 - 20 €
- Trend: application platform ("virtual machine") inside the card
  - e.g. JavaCard

Processor Cards



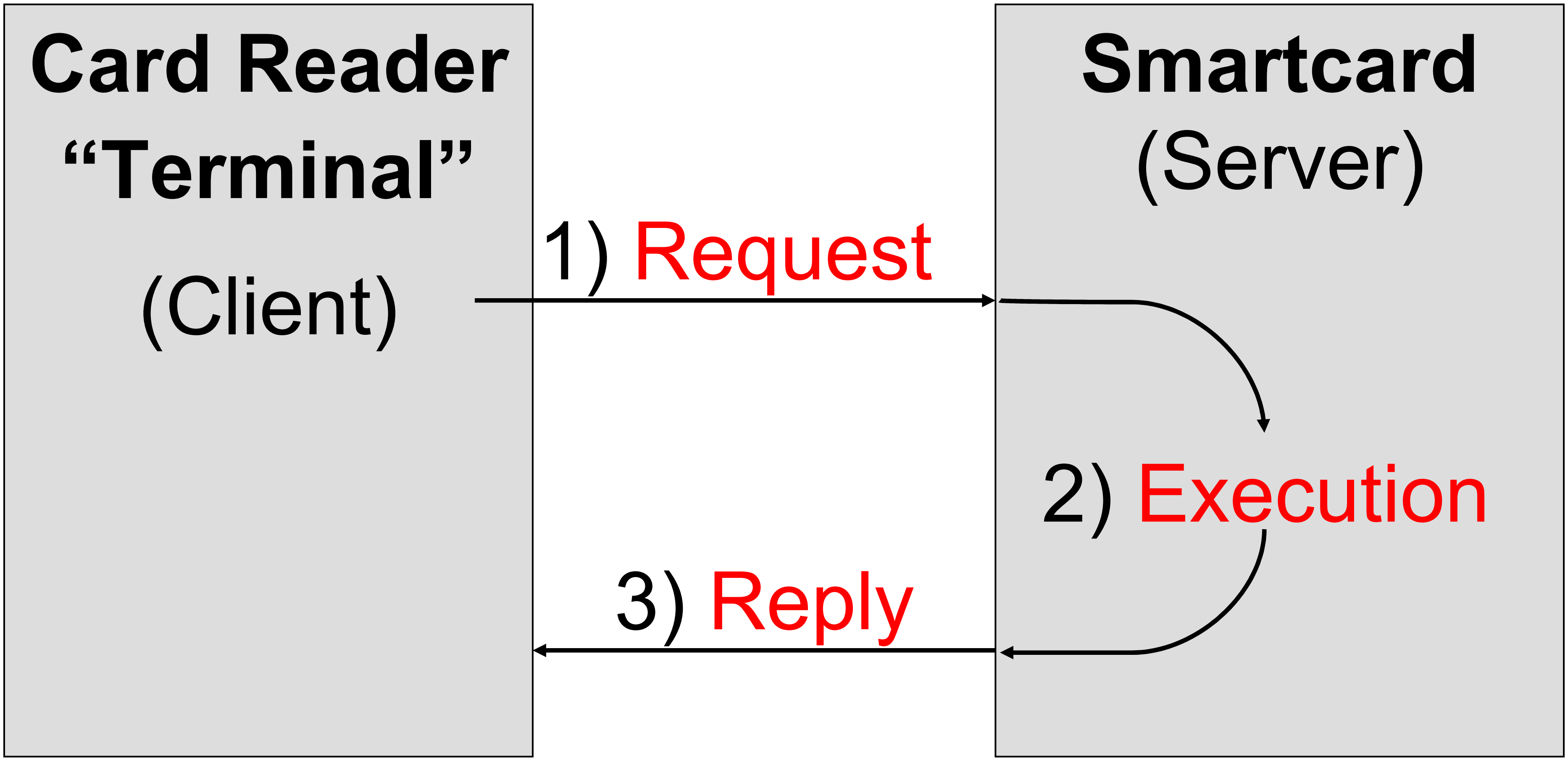
- Power: typ. 10-100 mW
- Size typ. 6-25 mm²

- Optional: random noise generation, security sensors and logic, crypto co-processor (e.g., for DES or modular exponentiations), MMU (necessary for multi application smartcards)

Contactless Smartcards ISO 14443

- External energy source, similar to RFIDs
  - note: usual batteries do not fit in 0.76 mm
- Frequency: 13.56 Mhz
- Data rate: 9600 bit/s (for ATR)
  - higher rates (up to 848 kbit/s) may be “negotiated”
- Combination of analog and digital technologies makes them more expensive than contact-based smartcards
- Better security and privacy compared to simple RFIDs
  - on-board cryptographic protocols (such as authentication)

Smartcard Communication



Smartcard Operating Systems

- Typically 3-30 kB
  - smartcards don't have much memory!
- „Simple": no user interface, no external devices, no interrupts, no multiprogramming…
- Highly dependent on the hardware
- Security of prime importance
- Basically „command interpreters"
- API to internal functions
  - only recent OS
  - downloadable program code gets access to file system, cryptographic functions, I/O via the API

Most important OS:
- JavaCard
- MULTOS
- „Smart Card for Windows"

Smart Identification

Friedemann Mattern

ETH Zürich